Alpha High Level Description

Alpha is a Windows Domain Controller (DC) and Domain Name System (DNS) Server. Because Alpha was the first DC in the aia.class domain, it is also (by default) the Windows global catalog server as well as the operations and schema master. At the very highest level, this means Alpha is central to identifying windows universal group membership during logons and when altering certain aspects of the active directory (AD) schema and infrastructure. Alpha will perform other functions in this course:

- Alpha's DNS server is configured with an active directory integrated zone which simply means all DNS IP address to domain name pairing information will be stored in AD.

Following are descriptions of Alpha's specific hands-on tasks that students must complete:

Task 1. Windows Host System Hardening
Students will be minimizing non-essential services and unnecessary network configurations. As a domain controller, Alpha doesn't require any of these components and students will follow security best practices by minimizing them.

Task 2. Configuring Time Synchronization
Network Time Protocol (NTP) is used to synchronize the host computer's time to a local time server, in this deployment it is the Internet firewall (Quebec).

Alpha will synchronize to Quebec every ten minutes; the Linux hosts will synchronize with Quebec every ten minutes; and the Window domain hosts will synchronize with Alpha every forty-five minutes until three good synchronizations occur, then once every eight hours. With all the hosts' time across the network synchronized, the cross examination of multiple hosts' logs, or the logs at the syslog Server, become more meaningful and easier to examine.

Task 3. Applying Windows Domain Security (Policy)
Students will edit a Windows Security Configuration template file to create logon banners and apply the security template to the domain.

Task 4. Applying Windows Domain Security (Organizational Units)
Students will add 2 new containers (OUs) to the Active Directory and will move the appropriate domain computers into these containers. This allows granular application of group policy settings to specific domain computers.

Task 5. Applying Windows Domain Security (Servers)
Students will edit a Windows Security Configuration template file to minimize system services and rename the local administrator account.

Task 6. Applying Windows Domain Security (Workstations)
Students will edit a Windows Security Configuration template file to minimize system services and rename the local administrator account.

Task 7. Applying Windows Domain Security (Domain Controllers)
Students will edit a Windows Security Configuration template file to minimize system services and facilitate secure functionality of Microsoft Exchange Server.

Task 8. Configuring OSSEC Agent
Students will install and configure the OSSEC Agent, which will then send information about security events to the syslog/OSSEC server (Foxtrot).

Task 9. Windows Security Configuration Wizard
The Windows SCW wizard will take students through a series of questions which will help them harden the server as per industry best practices. Unnecessary services will be disabled, auditing functions are enabled, the windows firewall is configured, and if necessary, IIS will be hardened.

Windows Server Baseline Hardening Steps

1 Harden Network Interfaces

1.1 Remove Unnecessary Protocols

By default, Microsoft Windows network interfaces are enabled with unnecessary protocols and services. These should be unbound from the interface (if not uninstalled completely). If your server is intended to provide these services, obviously you would NOT disable it.

1. If you have not already done so, log on to the machine using:

   Username: **`AIACLASS\Administrator`** Password: **`tartans@1`**

2. Open the 'Start' menu and right-click on 'Network' and select 'Properties' to open the 'Network and Sharing Center'.
3. Click on 'Local Area Connection 2' and then click 'Properties'.
4. Clear the box next to 'Internet Protocol Version 6 (TCP/IPv6)'. Then click 'OK'.

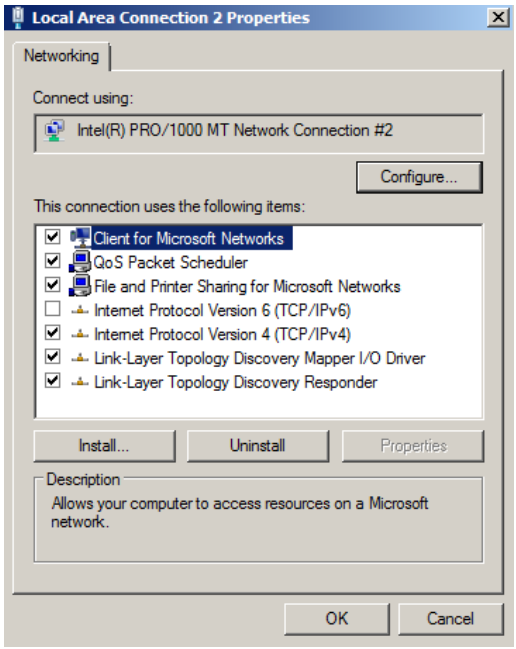


Figure 1: Remove IPv6

2 Harden TCP/IP Properties

2.1 Disable NetBIOS name resolution

As part of our defense-in-depth strategy, it is import to minimize even those parts of the environment that are normally not utilized. Since our network will be entirely native mode Windows 2000 or higher, NetBIOS name resolution would not normally be utilized, however we will eliminate the possibility of it being used altogether (NetBIOS name resolution is chatty and can divulge network information).

1. If the Properties window for your Local Area Connection is not still open, open it by following steps 1 and 2 from the section above.
2. From within the ‘Properties’ of your ‘Local Area Connection’, select the ‘Internet Protocol Version 4 (TCP/IPv4)’ item (leave it checked), and click on the ‘Properties’ button, then click the ‘Advanced’ button.
3. Next click on the ‘WINS’ tab at the top of the window.

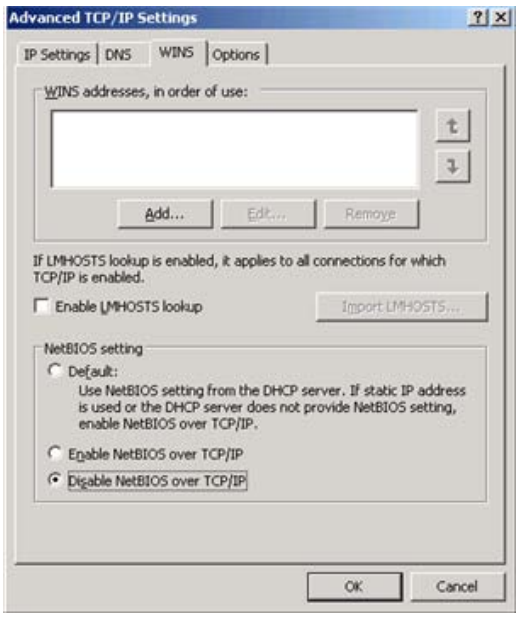


Figure 2: Minimize NetBIOS services

4. Uncheck ‘Enable LMHOSTS lookup’.
5. Select the radio button ‘Disable NetBIOS over TCP/IP’.
6. Click ‘OK’ to accept these settings.
7. Click ‘OK’ to confirm all ‘TCP/IP Properties’ changes.
8. Click ‘OK’ to confirm all ‘Local Area Connection Properties’ changes.
9. Close the ‘Local Area Connection 2 Properties’ and ‘Status’ windows.
10. Close the ‘Network and Sharing Center’ to return to the Desktop.

3 Install ClamWin for Anti-Virus Protection

3.1 Installation

1. Open the Course CD by clicking ‘Start’ -> ‘Computer’, right click ‘CD Drive (D:) AISTS’ and select ‘Open’.
2. Navigate to ‘Tools\Windows\ClamWin’ and double-click the ‘clamwin-0.96.1-setup’ icon.
3. Click ‘Next’.

Figure 3: Install ClamWin Antivirus

4. Accept the license agreement and click ‘Next’.
5. Accept the default option to install for ‘Anyone who uses this computer (all users)’ and click ‘Next’.
6. Select the default installation path and click ‘Next’.
7. At the ‘Select Components’ prompt, accept the default option of ‘Typical Installation’ and click ‘Next’.
8. Click ‘Next’ to create the default start menu folder.
9. Uncheck ‘Download Virus Database Files’ and click ‘Next’.

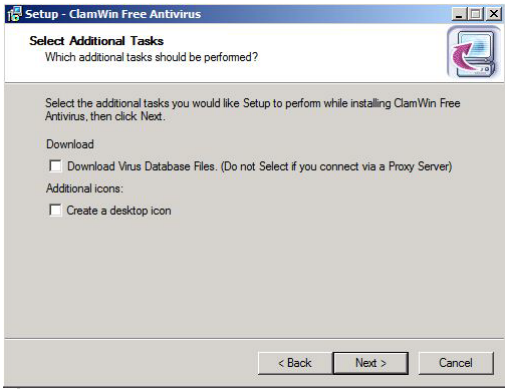


Figure 4: ClamWin Setup

10. Click ‘Install’ to install the program.
11. Click ‘Finish’ to complete the installation.
12. Close Windows Explorer.

3.2 Configuration

1. Click the upward facing arrow in the taskbar and then double-click on the ClamWin icon.

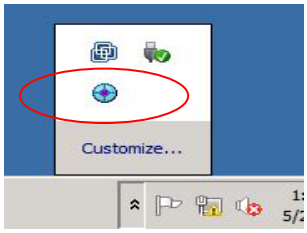


Figure 5: ClamWin Icon

2. Choose ‘No’ if asked to update the virus database.
3. Select ‘Tools’ from the menu, and click on ‘Preferences’.

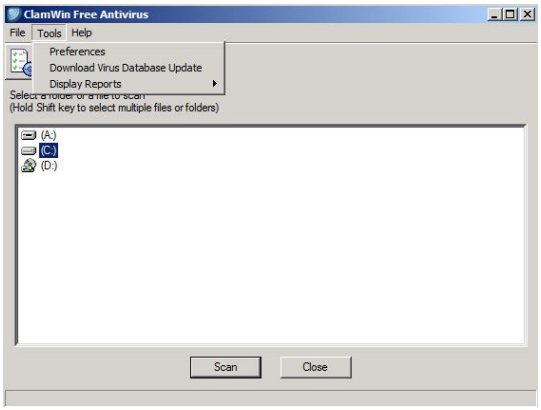


Figure 6: ClamWin Configuration

4. Click on the ‘Internet Updates’ tab. Leave the updates to be done daily, but change the time to 2:30:00 AM.

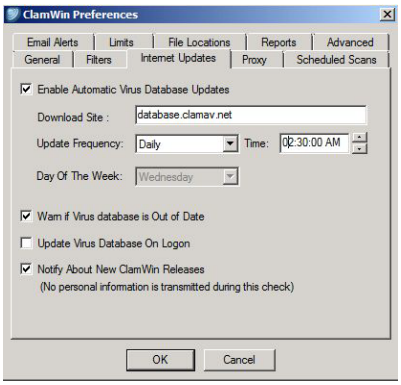


Figure 7: ClamWin Internet Updates

5. Click on the ‘Scheduled Scans’ tab. Click ‘Add’. Choose the scanning frequency to be done Daily at 3:30:00 AM. Enter `C:\` as the folder to scan. Enter a description, such as `Nightly Virus Scan`. Click ‘OK’.

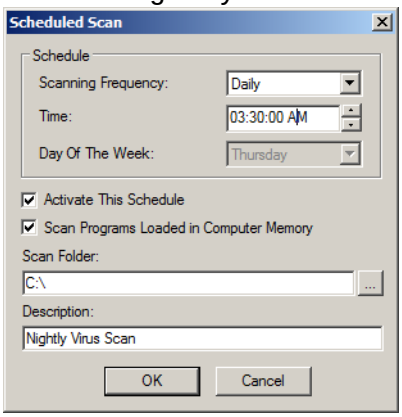


Figure 8: ClamWin Scheduled Scan

6. Click on the 'Email Alerts' tab. Check the box labeled 'Send Email On Virus Detection'. Enter in the following information:
   Mail Server – `10.0.2.3`
   From – `clamwin@Alpha`
   To – `eventwatch@aia.class`

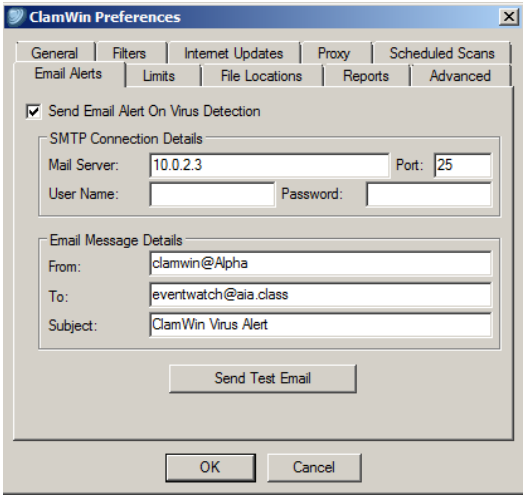


Figure 9: ClamWin Email Alerts

7. Click on the 'Proxy' tab. Enter in the IP address of the Squid Proxy server, Quebec, which is `10.0.2.1`. Ensure that the port is 3128.

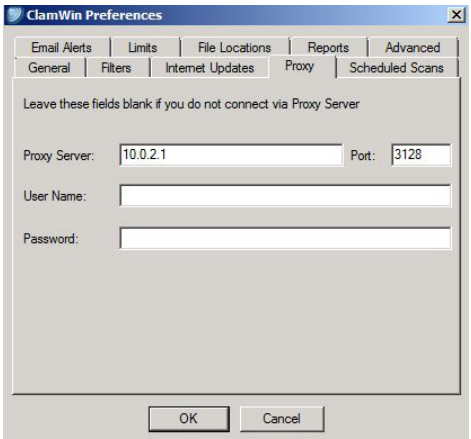


Figure 10: ClamWin Proxy Settings

8. Click 'OK' to accept all changes.
9. Choose 'No' if asked to update the virus database.
10. Click 'Close' to close the ClamWin window.

This page left intentionally blank for pagination purposes

Network Time Protocol (NTP) Client Setup

1 Windows Server 2008 Time Synchronization using Local Policy

An alternative to using the Date and Time control panel Internet Time tab is to configure time synchronization settings within the registry. Using the Local Policy snap-in for the Microsoft Management Console (MMC) these settings can easily be changed.

1. ‘Start’ -> ‘Run’ -> `MMC` and click ‘OK’.
2. Click ‘File’ -> ‘Add/Remove Snap-In’.
3. Select ‘Group Policy Object Editor’ from Available snap-ins, click ‘Add’ and then ‘Finish’ on the ‘Welcome to the Group Policy Wizard’ screen.
4. Click ‘OK’ to close the ‘Add Snap-In’ dialog.
5. Navigate the hierarchy to the following folder: ‘Local Computer Policy\Computer Configuration\Administrative Templates\System\Windows Time Service\Time Providers’.

Here you can enable and configure the NTP client along with configuring the computer as a NTP time server.

6. Double click the ‘Enable Windows NTP Client’.
7. Select ‘Enabled’, and click ‘OK’.
8. Double click ‘Configure Windows NTP Client’ and select the ‘Enabled’ option.
9. Set the ‘NTP Server’ to 10.0.2.1,0x1 (Quebec). This will set Alpha to synchronize time with the firewall. The 0x1 parameter after the IP address directs the computer synchronize with the NTP server as per the value set with ‘SpecialPollInterval’.
10. Change the ‘Type’ to ‘NTP’. The default setting of ‘NT5DS’ is for computers participating in a windows domain. Non-domain computers should use ‘NTP’ or the ‘AllSync’ option which will try to synchronize using all available methods.

11. Change the ‘SpecialPollInterval’ to ‘600’, which is every 10 minutes.

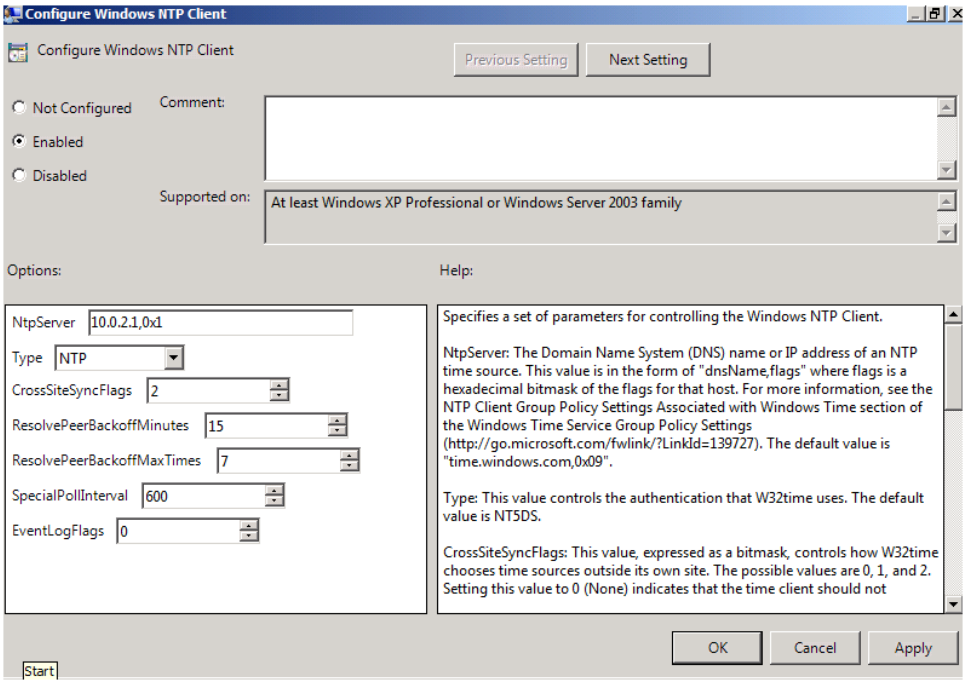


Figure 1: NTP Client Settings

12. Click ‘OK’, to save the NTP settings.
13. Exit the MMC console without saving the settings.

Alpha will now synchronize with Quebec every 10 minutes. Domain computers will utilize the Windows Time Service to periodically synchronize with Alpha.

Securing the Domain with Security Templates and Group Policy

1 Security Templates

In this section we will be establishing policy settings that we will apply to the entire domain. This is the baseline security policy that will be applied to every machine within the domain thus it is important to establish policy settings that will secure machines while still providing a high degree of functionality. We will create a security template and then apply it to our domain, but we need to know a little about Group Policy.

Group Policy settings can and do conflict at times. In this case the policy set furthest down in the tree will take precedence. So a group policy setting for an OU will over ride the settings for the Domain. This is true EXCEPT in the case of Account Settings in which the Domain setting takes precedence.

1.1 Open security template editor

Security templates allow administrators to centrally configure and control the security settings on host systems. These templates are saved as .inf files and can be edited with a normal text editor. We will use Microsoft's Management Console.

Login to the Windows Domain Controller (Alpha.aia.class) with the Administrator Account:

Username = **Administrator**

Password = **tartans@1**

Click on the 'Start' button and Select 'Run'. Type **`MMC`** and click 'OK'.

From within the Microsoft Management Console, Click 'File' and select 'Add/Remove Snap-In'.

In the Available snap-ins panel, scroll down and select the 'Security Templates' and then click 'Add'. Click 'OK'.

Expand 'Security Templates' in the console and click 'C:\Users\Administrator\Documents\Security\Templates'. You will notice that there are no templates listed.

1.2 Install Security Templates

Windows Server 2008 R2 does not come with any predefined templates so we are going to use a set of templates provided by Microsoft's Windows Server 2008 Security Configuration Guide. We must first copy them from the course CD to the machine.

1. Click 'Start' and then 'Computer'.
2. Navigate to 'D:\Tools\Windows\Security Templates'.

3. Press `[Ctrl]-[A]` to highlight all 4 of the security templates and then `[Ctrl]-[C]` to copy them.
4. Navigate to 'C:\Users\Administrator\My Documents\Security\Templates'.
5. Press `[Ctrl]-[V]` to paste the templates into this folder.
6. Close 'Windows Explorer'.

1.3 Edit Domain security template

1. Back in the Microsoft Management Console, right click on 'C:\Users\Administrator\Documents\Security\Templates' and select 'Refresh'. You should now see the templates that we just copied.

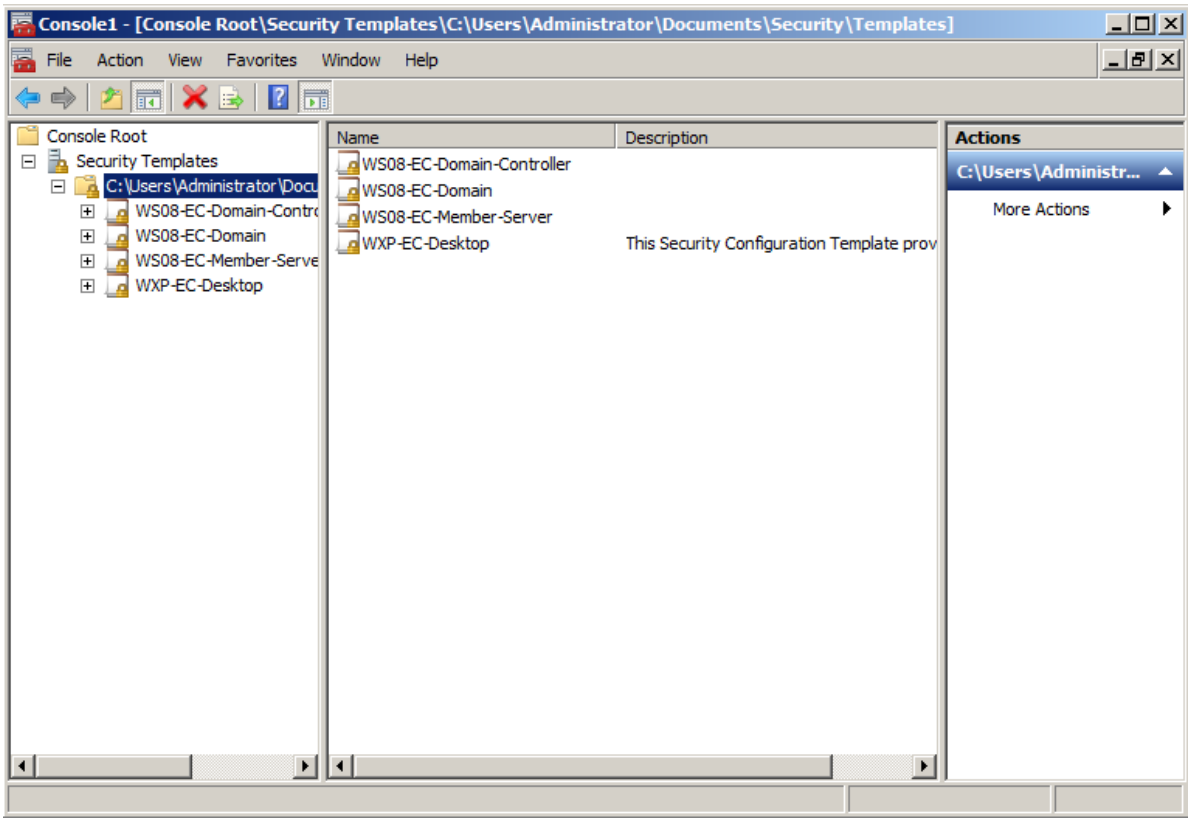


Figure 1: Installed Templates

We are going to add log on banners to all Windows boxes in the AIA domain. Banners can be set to anything from legal disclaimers, to appropriate use reminders, to daily greetings. Each time a user attempts to log on, they will see this message banner.

2. Double-click 'WS08-EC-Domain' in the right pane.
3. Double-click 'Local Policies'.
4. Double-click 'Security Options' in the right pane and then double-click 'Interactive logon: Message text for users attempting to log on'.

When the template policy window opens, check 'Define this policy setting in the template' and in the text field, type: `Warning!  This computer is for official use only!`

5. Click 'OK'.

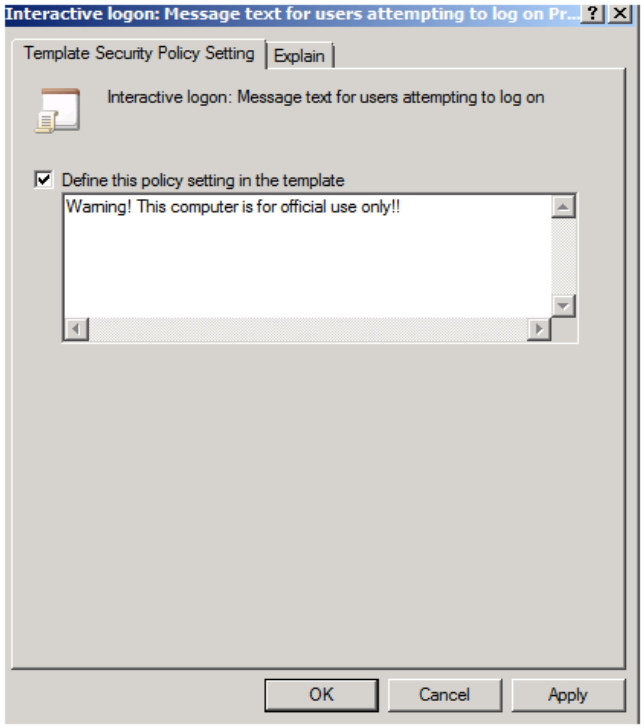


Figure 2: Creating the logon banner

6. Double-click 'Interactive logon: Message title for users attempting to log on'.
7. Check 'Define this policy setting in the template' and in the text field, type: `Log on Warning!`
8. Click 'OK'.

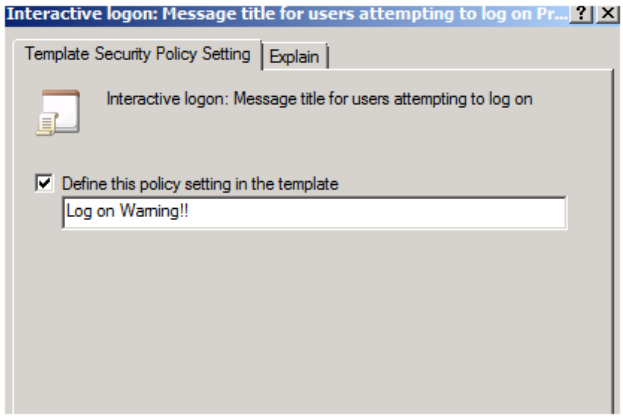


Figure 3: Creating the logon banner

9. Now right click the 'WS08-EC-Domain' template as select 'Save'.

2 Importing templates into Group Policy

2.1 Import security templates into Domain Policy GPO

In order to apply our newly edited security template, we will import it into the group policy object for the default domain policy for the aia.class domain. Before that, we need to create a Domain Group Policy object for the domain.

1. On Alpha, click ‘Start’ -> ‘Administrative Tools’ -> ‘Group Policy Management’.
2. Create Domain Group Policy Objects. In the left panel, Expand Group Policy Management->Forest->Domains->aia.class using the plus icon. Right-click “Group Policy Objects” and select “New”.

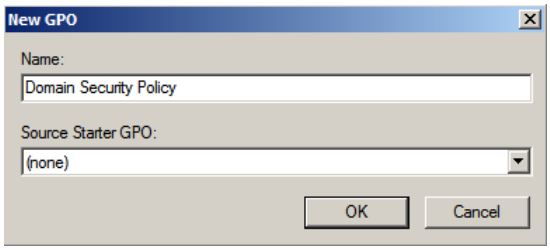


Figure 4: Creating a new GPO

Enter ‘Domain Security Policy’ as the name of new GPO and click ‘OK’.

3. Import Domain Security Policy Templates. Expand ‘Group Policy Objects’ and right-click ‘Domain Security Policy’, the newly created GPO, and select ‘Edit’. This will open ‘Group Policy Management Editor’.

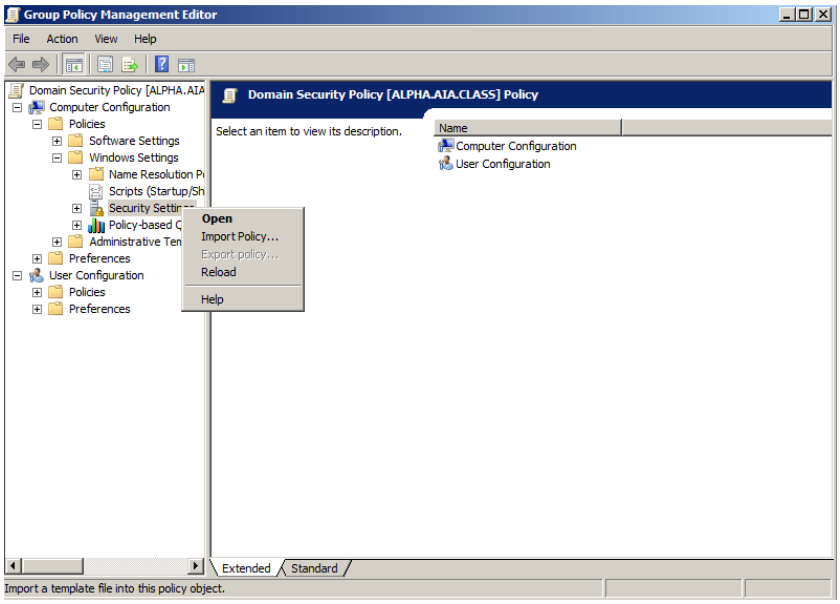


Figure 5: Import Policy to the GPO

Expand ‘Domain Security Policy’ -> ‘Computer Configuration’ -> ‘Policies’ -> ‘Windows Settings’ using the plus icon. Right-click ‘Security Settings’ and select ‘Import Policy’.

Note: The security template's policy will be applied to every user assigned to the aia.class domain.

4. In the 'Import Policy From' screen, make sure the 'Clear this database before importing' checkbox is checked and then click 'WS08-EC-Domain' and click 'Open'.

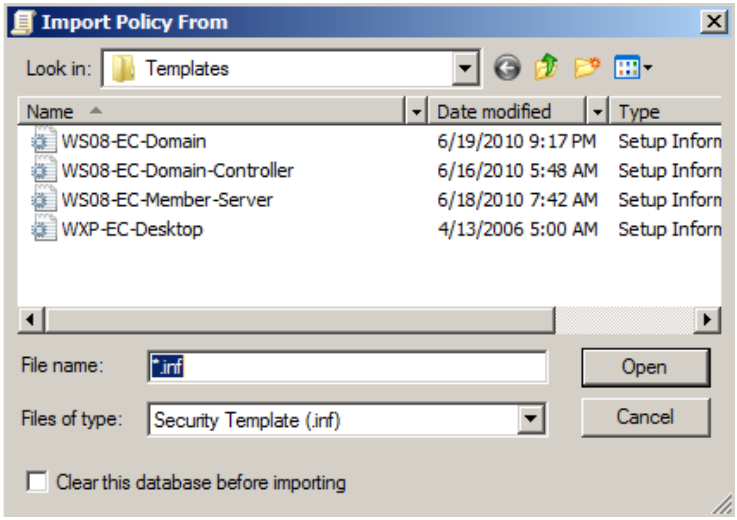


Figure 6: Importing WS08-EC-Domain Template

5. Close the 'Group Policy Management Editor'.
6. Link the GPO to the domain.

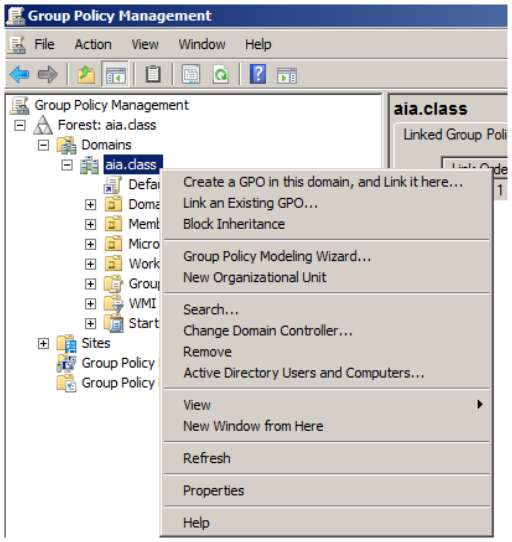


Figure 7: Link the GPO to the domain – aia.class

The GPO "Domain Security Policy" is the root policy for all in our domain. To link it to our domain, right click *'aia.class'* in Group Policy Management Console, and select "Link an Existing GPO…"

7. In Select GPO dialog, choose the GPO we just created “Domain Security Policy” and click OK. Now the GPO is linked to our domain.

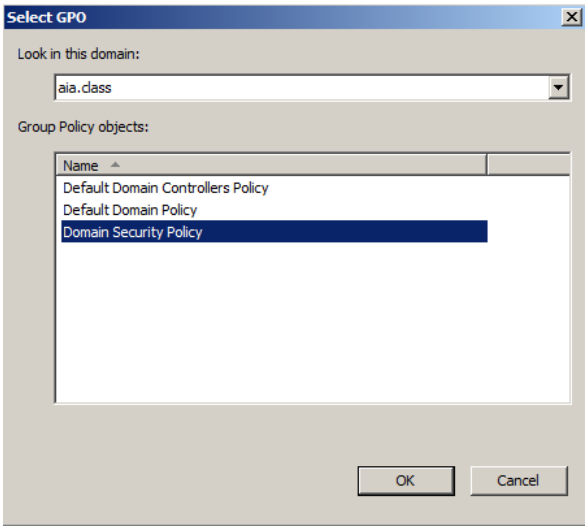


Figure 8: Select the GPO

8. Click *aia.class* again to verify that GPO is linked.

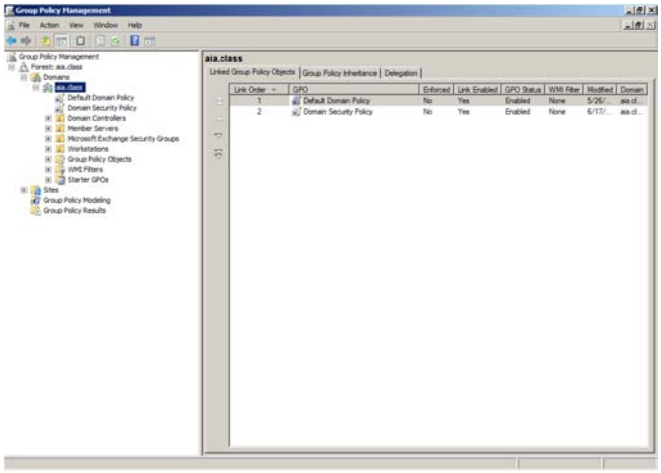


Figure 9: Verify whether the GPO is linked

9. Close all windows and do not save settings to the console.

Note: After these Security Group Policy settings are applied and each server is rebooted, you will be asked for Administrator credentials every time a configuration console is opened.

Applying Windows Domain Security

1 Creating Windows Organizational Units (OUs) and moving appropriate computers into these OUs

1.1 Create 2 new Organizational Units

Windows domains allow for the creation of OUs that enable more granular application of security policies by placing users and/or computers into isolated containers. New OUs will be created for Windows Member Servers and for Workstations.

1. Login to the Windows Domain Controller (Alpha.aia.class) with the Administrator Account:

   Username: **Administrator**

   Password: **tartans@1**

2. Click 'Start' -> 'Administrative Tools' and Open up the 'Active Directory Users and Computers'

3. Right click on the 'aia.class' domain and select 'New' -> 'Organizational Unit'.

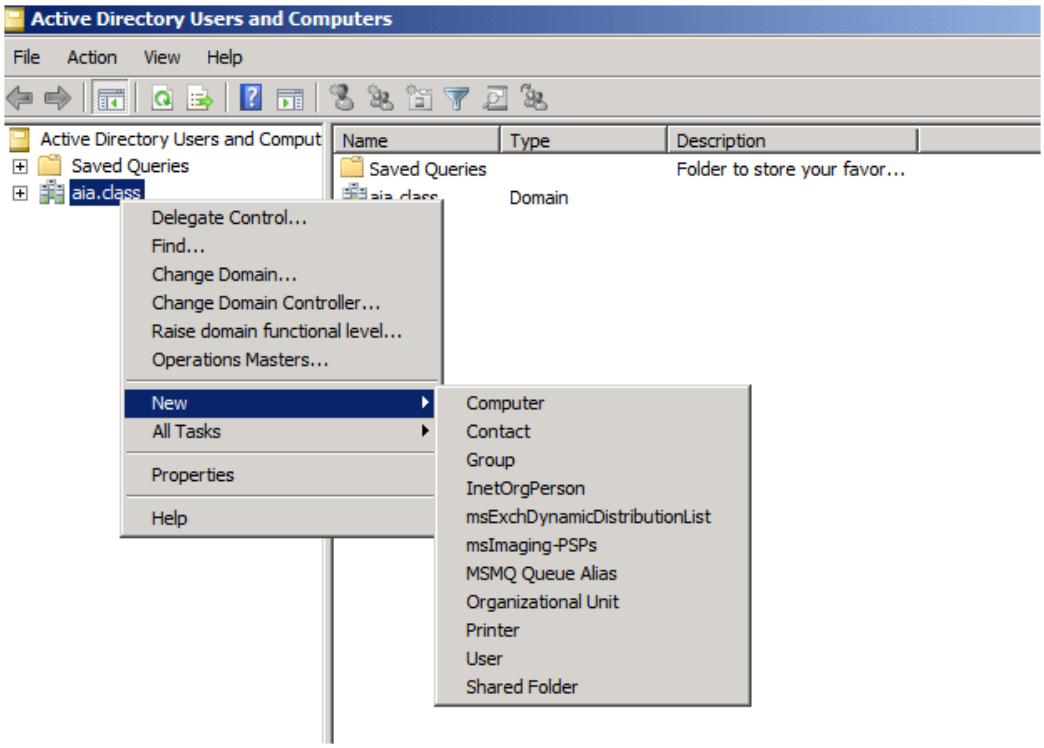


Figure 1: Creating a New OU

4. Name the new OU: `Member Servers`

5. Now create another OU and call it: `Workstations`

1.2 Move appropriate computers into new OUs

1. From within the Active Directory Users and Computers OU, click on the 'Computers' folder. Use the 'Ctrl' key to select the 3 servers, right click, select 'Move' and then select the 'Member Servers' OU.

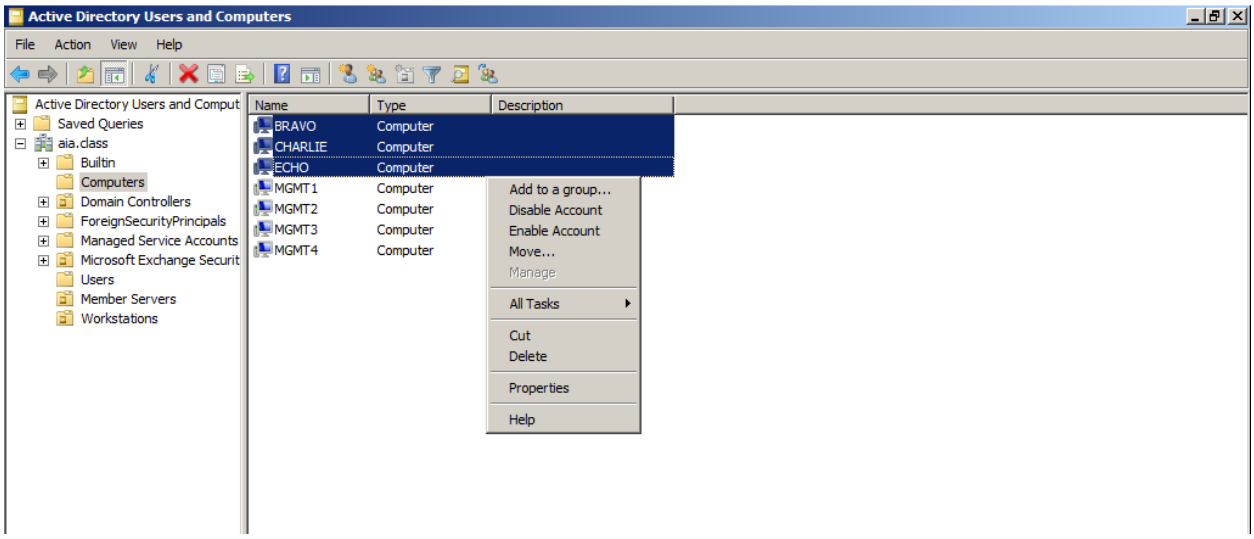


Figure 2: Moving computers into an OU

Note: It is always a good idea to separate systems and users by roles within the Active Directory Structure. Security policies can be applied with granularity in this manner.

2. Now move all of the Users and Management computers into the newly created 'Workstations' OU.

3. Close the Active Directory window.

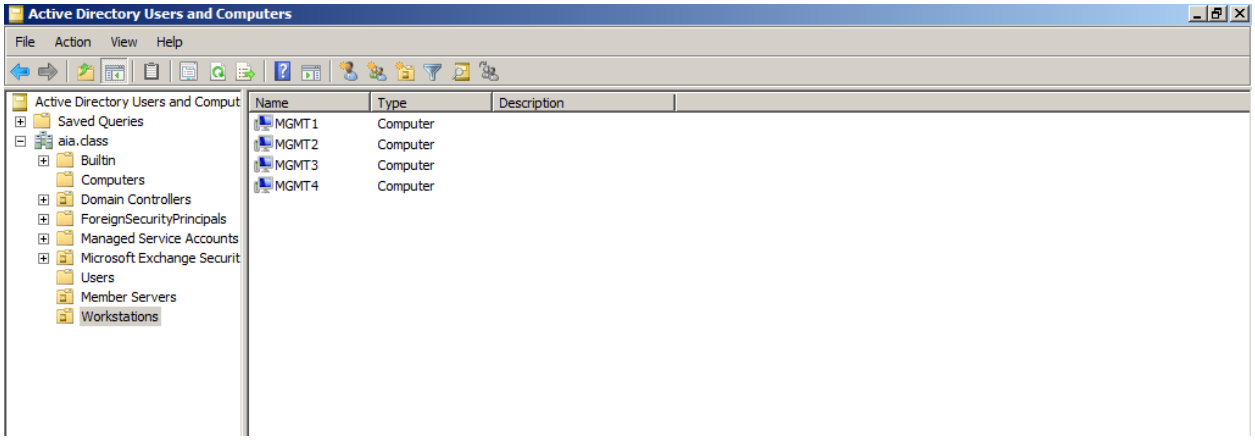


Figure 3: Contents of Workstations OU

Applying a Security Template to Member Servers

1 Security Templates

1.1 Open security template editor via MMC

Security templates allow administrators to centrally configure and control the security settings on host systems. These templates are saved as .inf files and as such can be edited with a text editor. We will be using the Microsoft Management Console to do our editing.

1. Login to the Windows Domain Controller (Alpha.aia.class) with the Administrator Account:

   Username = **Administrator**

   Password = **tartans@1**

2. Click on the 'Start' button and Select 'Run'. Type `MMC` and click 'OK'.

3. From within the Microsoft Management Console, Click 'File' and select 'Add/Remove Snap-In'. In the available snap-ins, scroll down and select the 'Security Templates Snap-In' and then click 'Add'. Click 'OK'.

1.2 Edit Member Servers Template

Now we will edit the security template for our Member Servers so that unnecessary services will be disabled and the local administrator account will be renamed. Note: In normal production environments, care should be taken when disabling services and thorough testing should be conducted prior to implementation.

1. Expand 'Security Templates' and 'C:\Users\Administrator\Documents\Security\Templates'.

2. Click on the 'WS08-EC-Member-Server' template and in the right pane, double click on 'System Services' folder.

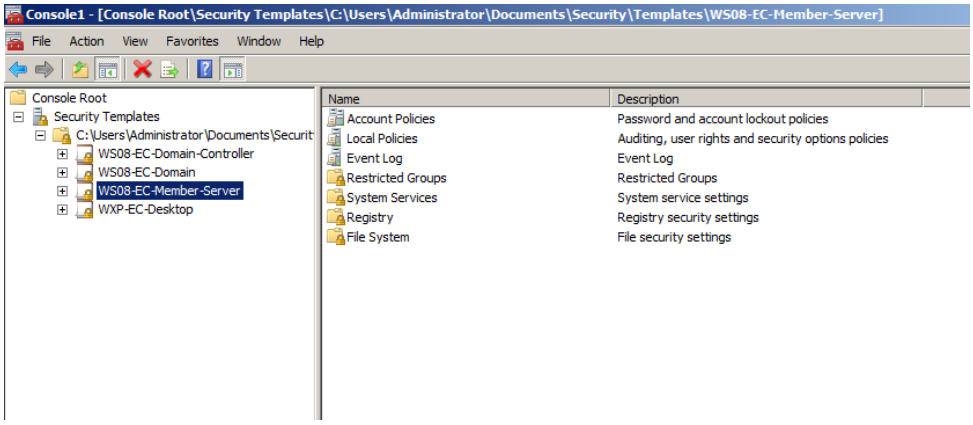


Figure 1: Editing Member Servers Security Template

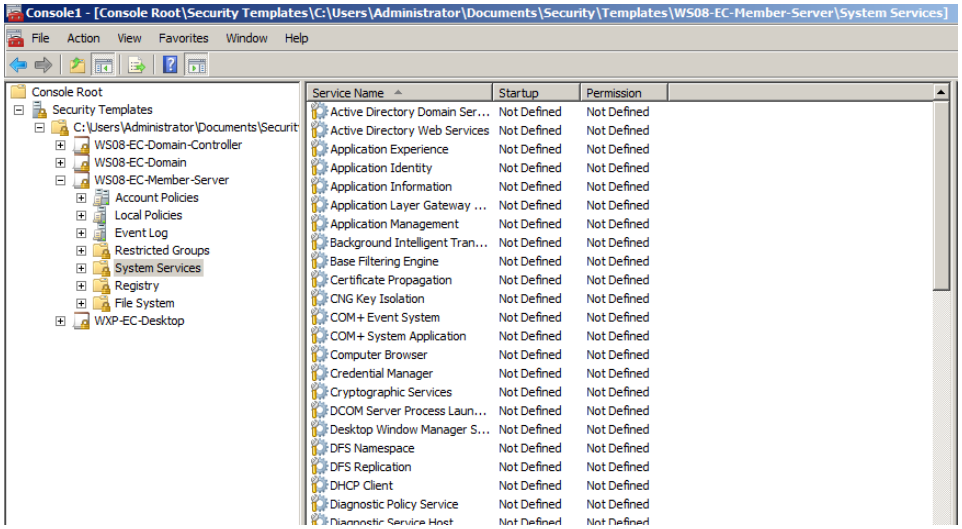


Figure 2: Member Servers – Systems Services template

We will be disabling the Routing and Remote Access service on our Windows member servers:

Note: This service represents one of the most important to lock down in a production environment. This step is used as an example of how to disable a service for an entire Organizational Unit. We will be using the Windows Security Configuration Wizard on each server individually to lock down services further. When implementing this configuration in production, you should review all services and minimize any that are not appropriate for your environment.

3. Double click the 'Routing and Remote Access' Service and then check the 'Define this policy' checkbox. Assure that Disabled is selected.
4. Click 'OK'.

   Now you will configure the security template to rename the local administrator account for all of the member servers. This is done to obfuscate this built-in privileged account and supports the defense-in-depth goal.

5. Click on the 'Local Policies' icon from within the Security Templates MMC and then double click the 'Security Options' icon in the right-hand pane.
6. Click on the 'Accounts: Rename Administrator Account', click the 'Define this policy setting in the template' check box and type `acarnegie` in the box. Click 'OK'.

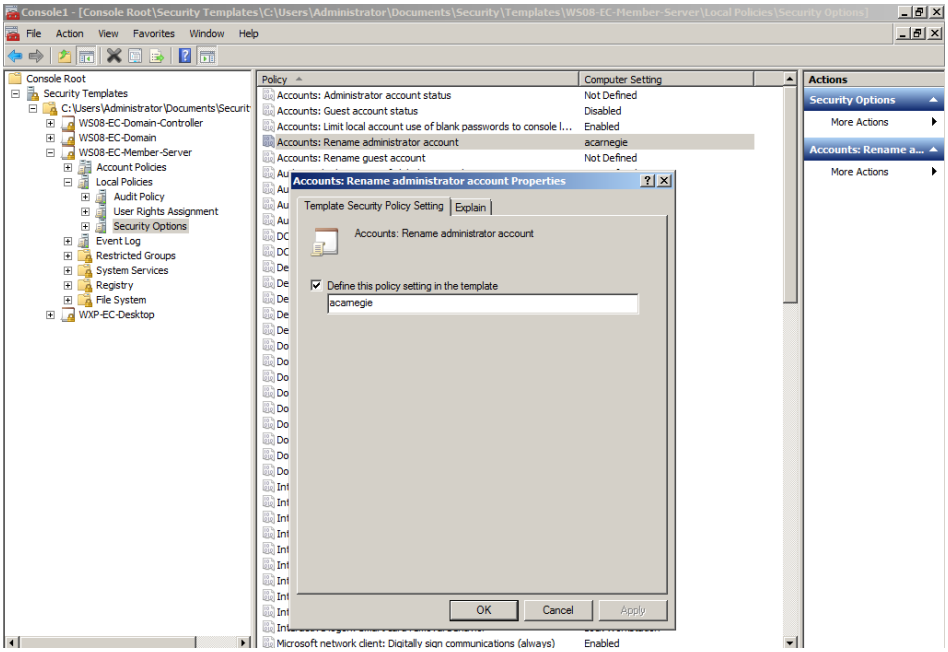


Figure 3: Renaming administrator account with Security Templates

We are also going to add log on banners to all Windows boxes in the AIA domain. Banners can be set to anything from legal disclaimers, to appropriate use reminders, to daily greetings. Each time a user attempts to log on, they will see this message banner.

7. In the 'Security Options' pane on the right, double-click 'Interactive logon: Message text for users attempting to log on'.
8. When the template policy window opens, check 'Define this policy setting in the template' and in the text field, type: `Warning!  This computer is for official use only!` Click 'OK'.

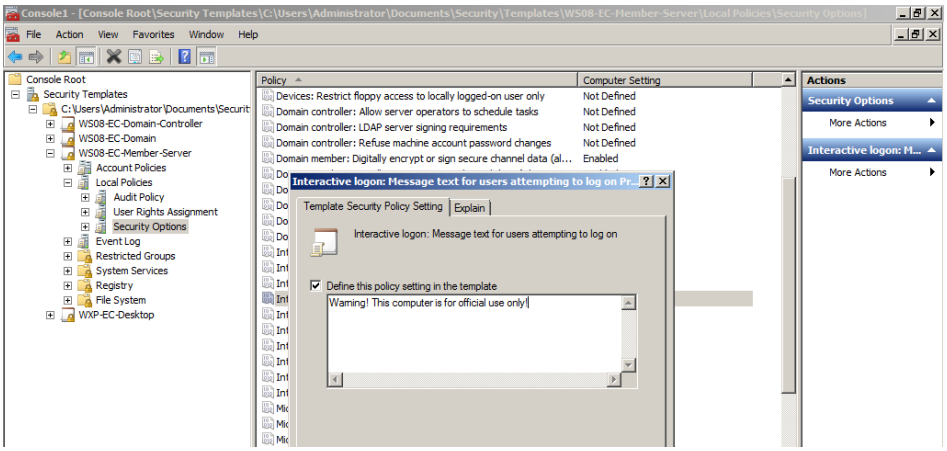


Figure 4: Creating the logon banner

9. Double-click ‘Interactive logon: Message title for users attempting to log on’. Check ‘Define this policy setting in the template’ and in the text field, type: `Log on Warning!` Click ‘OK’.

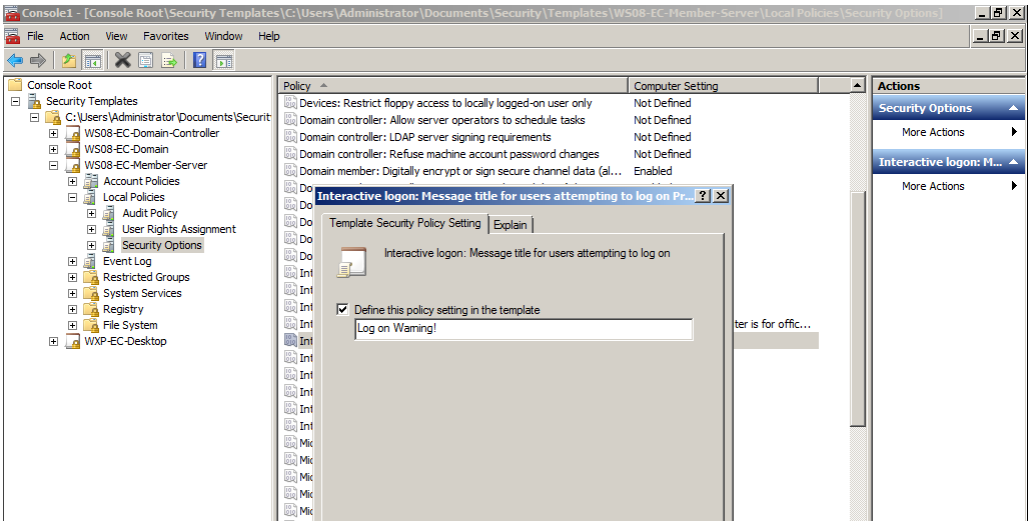


Figure 5: Creating the logon banner

The Windows Security Configuration Guide policies increase the amount of auditing done on machines which can be very beneficial to analyze system performance and security issue. We will make some modifications and decrease the amount of auditing as our Virtual Machines have very limited hard drive space and high logging will fill that up quickly.

10. Select ‘Audit Policy’ then double click on ‘Audit object Access’ , check ‘Define these policy settings in the template’, check ‘Failure’ and click ‘OK’

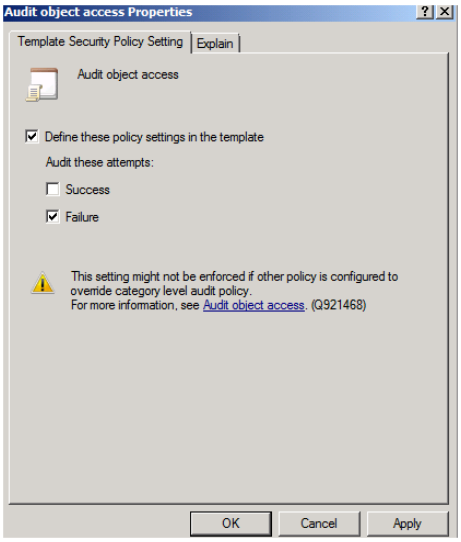


Figure 6: Properties for a security policy

Edit the settings for the other policies in Audit Policy and eventually your Audit Policy settings should look like the figure below.

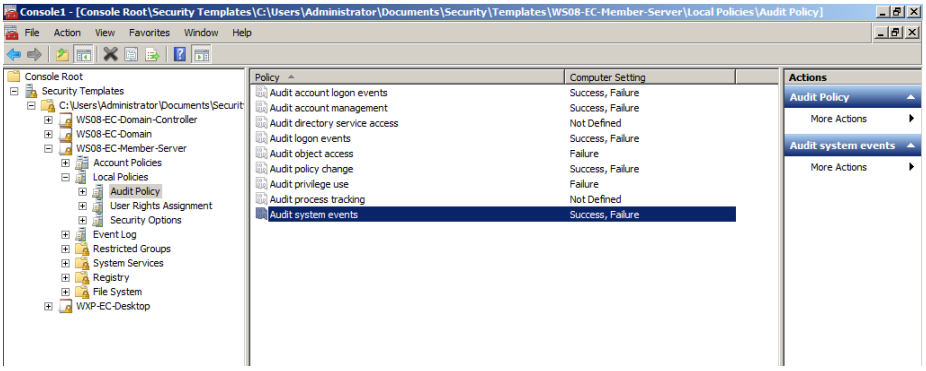


Figure 7: Final Audit Policy settings

Finally, we need to change the default method of Event Log retention in order to avoid problems caused by the limited available hard drive space on our virtual environment systems. We are going to set Event Log to overwrite events as needed if the allowed space for the Event Log is full. Note that this may not be the best option for a production network since an attacker could potentially flood the Event Log with worthless data in order to overwrite any Event Log entries that might document their break-in. However, because of the disk space constraints on our virtual environment systems, overwriting as needed will be necessary.

11. Click on ‘Event Log’ under ‘WS08-EC-Member-Server’. Then double-click ‘Retention method for application log’. Check the ‘Define this policy setting in the template’ checkbox.
12. Change the setting to ‘Overwrite events as needed’.

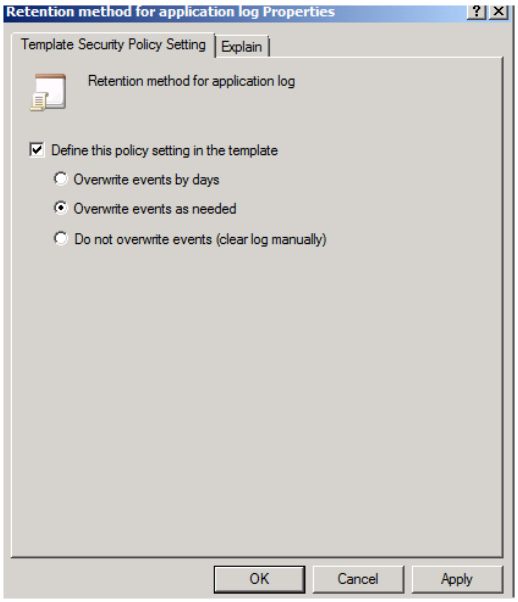


Figure 8: Properties for a security policy

13. Click ‘OK’.
14. Edit the Event Log policies such that eventually the policy settings for Event Log should be similar to the figure below:

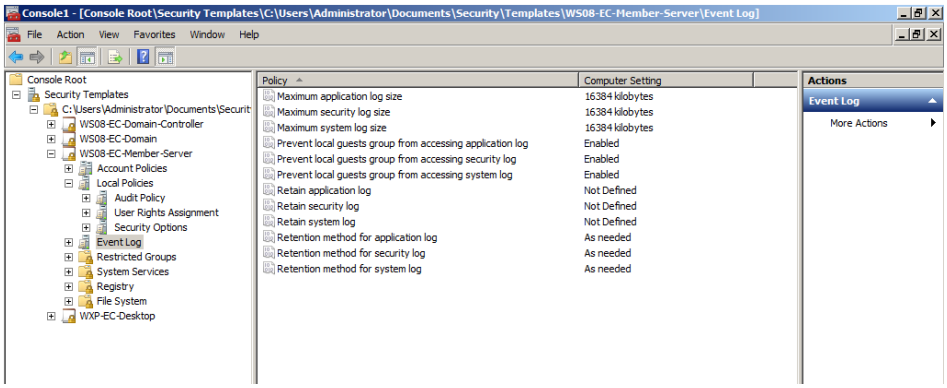


Figure 9: Final Event Log settings

15. Now right click on the ‘WS08-EC-Member-Server’ template file and select ‘Save’.
16. Open ‘Group Policy Management Console’. Click ‘Start’->’Administrative Tools’ and then select ‘Group Policy Management’.

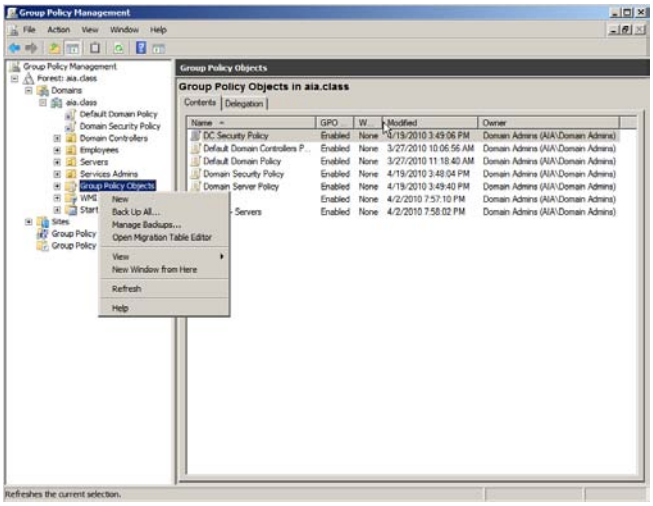


Figure 10: Group Policy Management

17. Create Member Servers Group Policy Objects. In the left panel, Expand ‘Group Policy Management’ -> ‘Forest’ -> ‘Domains’ -> ‘aia.class’, using the plus icon. Right-click ‘Group Policy Objects’ and select ‘New’.

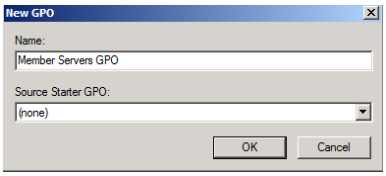


Figure 11: Creating a new GPO

Enter `Member Servers GPO` as the name of new GPO, click ‘OK’.

18. Import Domain Security Policy Templates. Expand ‘Group Policy Objects’ and right-click ‘Member Servers GPO’, the newly created GPO, and select ‘Edit’. This will open ‘Group Policy Management Editor’.

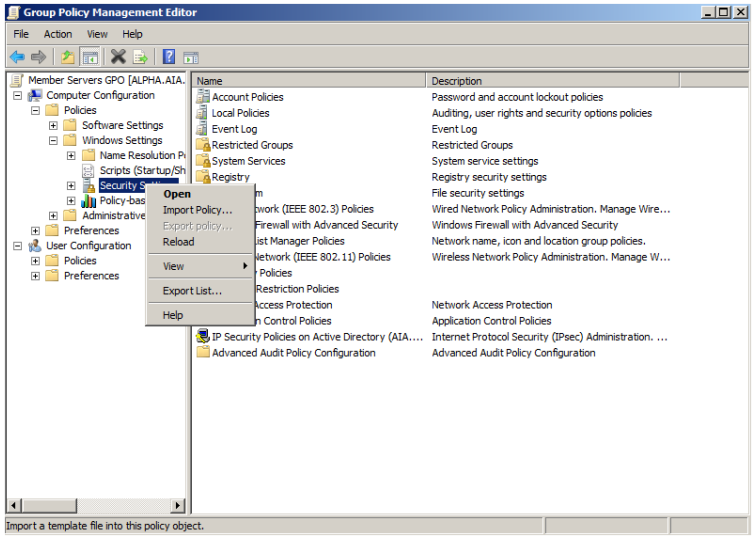


Figure 12: Import Policy

Expand ‘Member Servers GPO’ -> ‘Computer Configuration’ -> ‘Policies’ -> ‘Windows Settings’ using the plus icon. Right-click ‘Security Settings’ and select ‘Import Policy’.

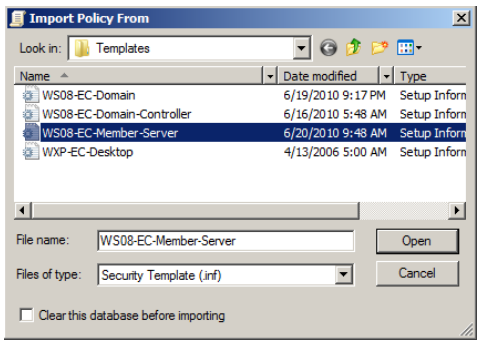


Figure 13: Importing the Member Servers security template

In the ‘Import Policy From’ screen, make sure the ‘Clear this database before importing’ box is checked and then click on ‘WS08-EC-Member-Server’ and click ‘Open’. Then, close ‘Group Policy Management Editor’.

19. Link GPO to Organization Units

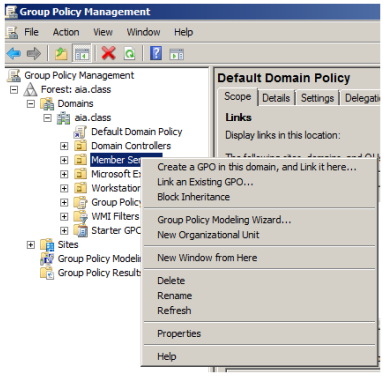


Figure 14: Link the GPO to the OU

Right click ‘Member Servers’ in Group Policy Management Console, and select

‘Link an Existing GPO…’

In Select GPO dialog, choose the GPO we just created ‘Member Servers GPO’ and click ‘OK’. Now the GPO is linked to our domain.

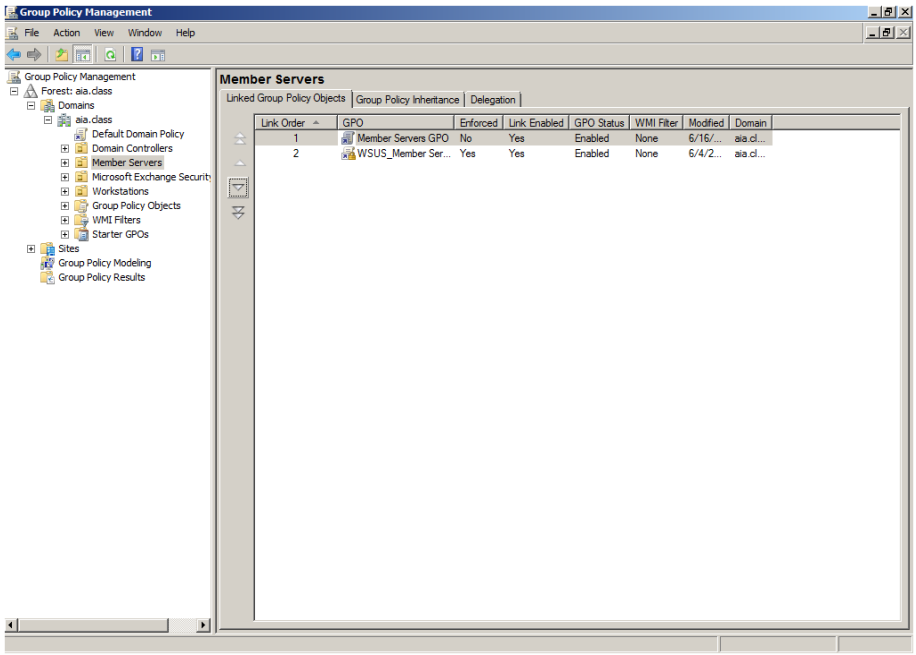


Figure 15: Verify whether the GPO is linked

Click “Member Servers” again to verify that GPO is linked.

20. Close all open windows and do not save settings to the console.

Note: After these Security Group Policy settings are applied and each server is rebooted, you will be asked for Administrator credentials every time a configuration console is opened.

Applying a Security Template to Windows Workstations

1 Security Templates

1.1 Open Security Template Editor

Logon to the Windows Domain Controller (Alpha.aia.class) with the Administrator Account:

Username = **Administrator**

Password = **tartans@1**

Click on the 'Start' button and Select 'Run'. Type `MMC` and click 'OK'.

From within the Microsoft Management Console, Click 'File' and select 'Add/Remove Snap-In'. Scroll down and select the 'Security Templates' Snap-In and then click 'Add'. Click 'Close' and then click 'OK'.

1.2 Edit Workstation security template

Now we will edit the security template for our workstations so that the local administrator account will be renamed and logon banners will be added.

1. Expand 'Security Templates', click on 'C:\Users\Administrator\Documents\Security\Templates' and double-click on 'WXP-EC-Desktop' in the right pane.

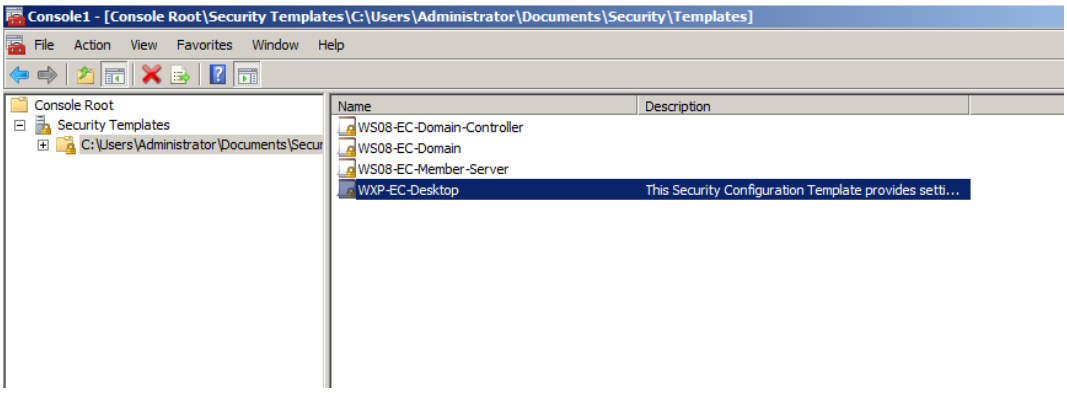


Figure 1: Workstation template

Now you will configure the security template to rename the local administrator account for all of the member servers. This is done to obfuscate this built-in privileged account and supports the defense-in-depth goal.

2. Double-click on the 'Local Policies' icon from within the Security Templates MMC and then double click the 'Security Options' icon in the right-hand pane.
3. Click on the 'Accounts: Rename Administrator Account Policy', click the 'Define this policy in the template' check box and type `acarnegie` in the box. Click 'OK'.

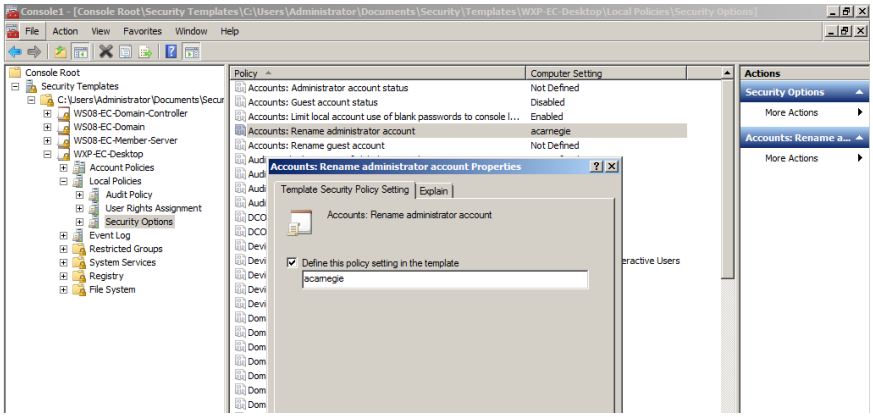


Figure 2: Renaming administrator account with Security Templates

We are also going to add log on banners to all Windows boxes in the AIA domain. Banners can be set to anything from legal disclaimers, to appropriate use reminders, to daily greetings. Each time a user attempts to log on, they will see this message banner.

4. Double-click 'Interactive logon: Message text for users attempting to log on'.
5. When the template policy window opens, change the text field to: `Warning! This computer is for official use only!` Click 'OK'.

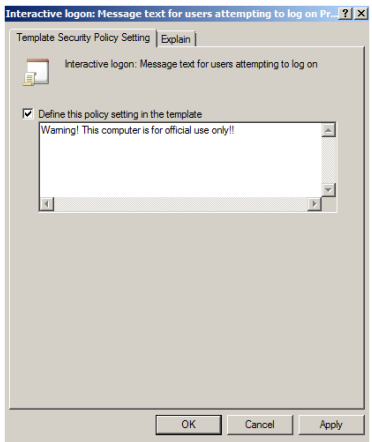


Figure 3: Creating the logon banner

6. Double-click 'Interactive logon: Message title for users attempting to log on'. Change the text field to: `Log on Warning!` Click 'OK'.

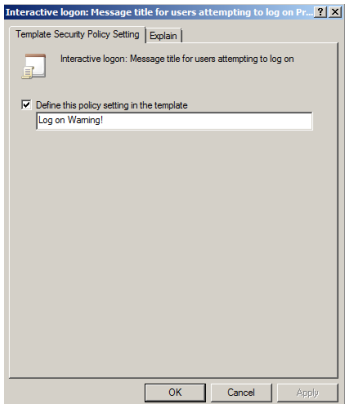


Figure 4: Creating the logon banner

7. Now right-click on the 'WXP-EC-Desktop' template file and select 'Save'.

2 Importing templates into Group Policy

2.1 Import Workstation template into Workstations OU GPO

In order to apply our newly edited security template, we will import it into the group policy object for the Workstations organizational unit.

1. Click ‘Start’ -> ‘Administrative Tools’ -> ‘Group Policy Management’.
2. Expand the ‘aia.class’ domain by clicking the ‘+’ sign.
3. Right click on ‘Group Policy Objects’ and click ‘New’
4. Type in **`Workstations GPO`** in ‘New GPO’ window as the name, click 'OK'.

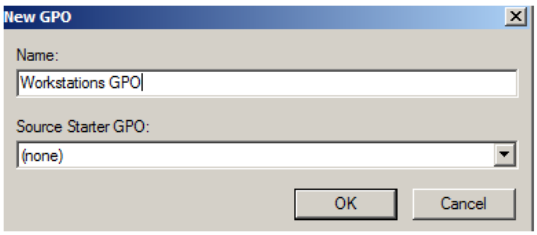


Figure 5: Naming the new Group Policy Object (GPO)

5. Expand ‘Group Policy Objects’, right click on the ‘Workstations GPO’ and select ‘Edit’.

   Note: The security template’s policy will be applied to every computer assigned to the Workstations OU. It is important to recognize that individual servers have different requirements for System Services and other components; therefore you must apply your policies in layers to account for these differences. This means that local system templates can be applied in combination with templates from group policy.

6. Expand ‘Workstations GPO\Computer Configuration\Policies\Windows Settings’ and then in the right pane, right click ‘Security Settings’ and click ‘Import Policy’.

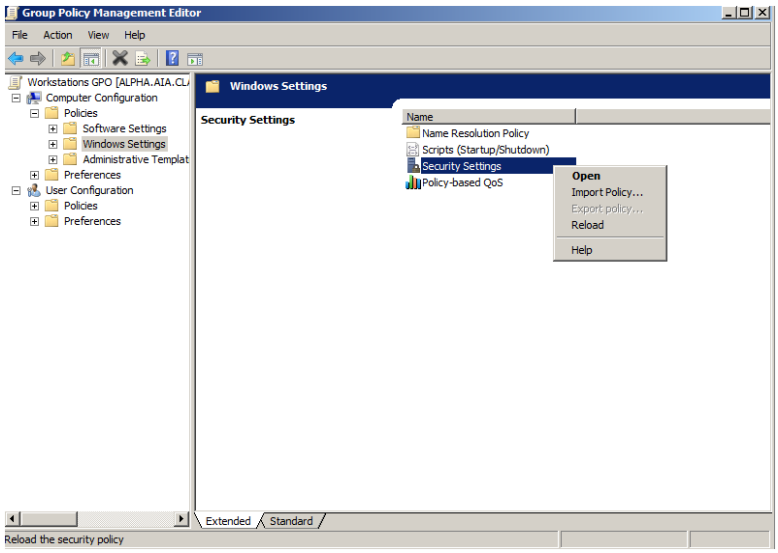


Figure 6: Import Policy into The OU’s Security Settings

7. Select 'WXP-EC-Desktop' (**make sure the Clear this database before importing checkbox is checked**) and click the 'Open' button. Then close the 'Group Policy Management Editor'.

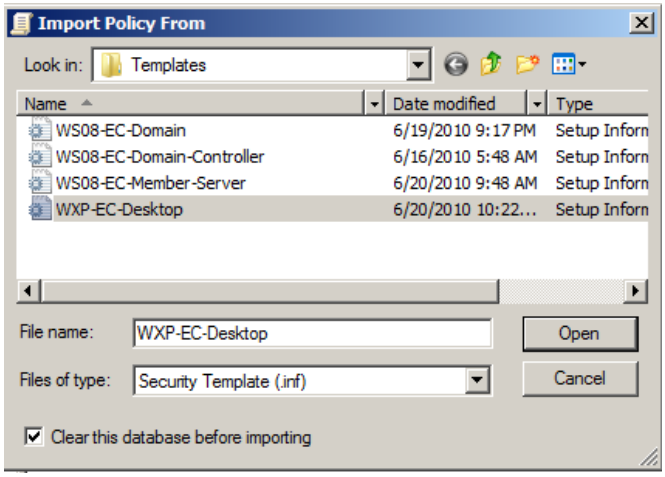


Figure 7: Import the created security template

8. Then right click on 'Workstations OU' and select 'Link an Existing GPO…'.

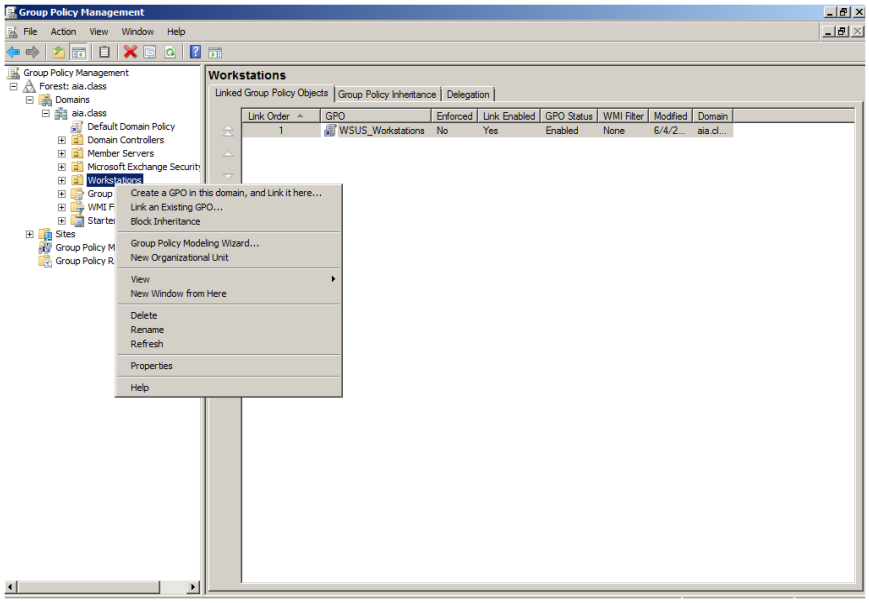


Figure 8: Link the GPO to the OU

9. Select 'Workstations GPO' from the group Policy Objects list and click 'OK'.
10. Close all open windows and do not save settings to the console.

Note: After these Security Group Policy settings are applied and each server is rebooted, you will be asked for Administrator credentials every time a configuration console is opened.

Applying Security Templates to Domain Controllers

1 Security Templates

1.1 Open security template editor via MMC

Security templates allow administrators to centrally configure and control the security settings on host systems. These templates are saved as *.inf* files and as such can be edited with a text editor. We will be using the Microsoft Management Console to do our editing.

1. Login to the Windows Domain Controller (Alpha.aia.class) with the Administrator Account:

   Username = **`Administrator`**

   Password = **`tartans@1`**

2. Click on the 'Start' button and Select 'Run'. Type `MMC` and click 'OK'.

3. From within the Microsoft Management Console, Click 'File' and select 'Add/Remove Snap-In'. In the available snap-ins, scroll down and select the 'Security Templates Snap-In' and then click 'Add'. Click 'OK'.

1.2 Edit Domain Controller security template

Now we will edit the Domain Controller security template so that unnecessary services will be disabled and the local administrator account will be renamed. Note: In normal production environments, care should be taken when disabling services and thorough testing should be conducted prior to implementation.

1. Expand Security Templates, click on 'C:\Users\Administrator\Documents\Security\Templates' and then double-click on 'WS08-EC-Domain-Controller' in the right-pane.

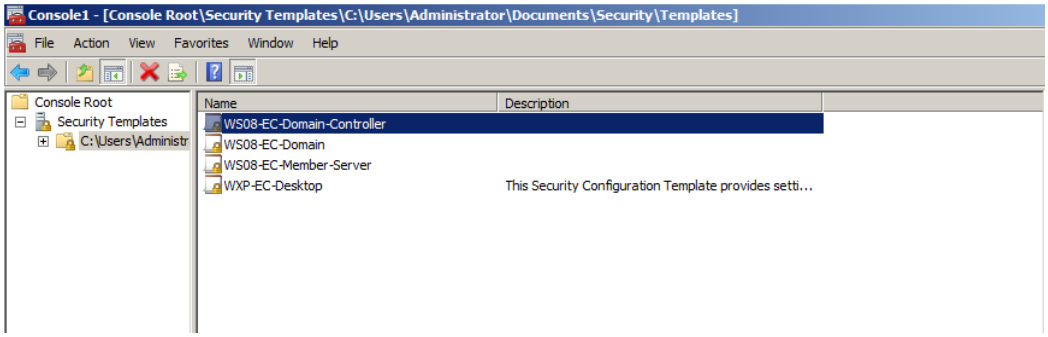


Figure 1: **Navigating to Domain Controller Security Template**

2. Double-click on the ‘System Services’ folder.

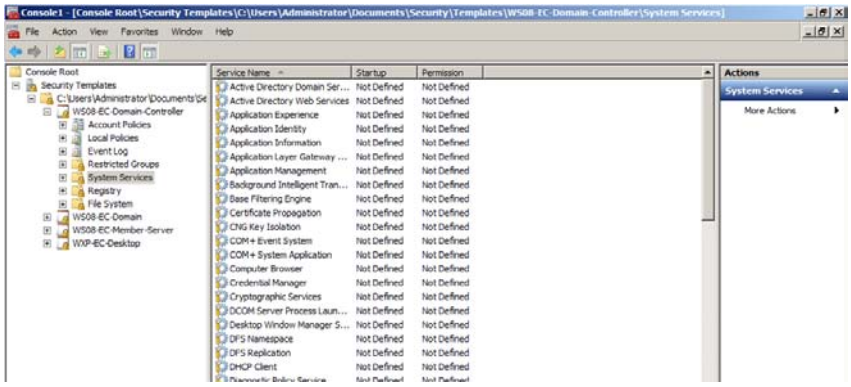


Figure 2: Domain Controller – Systems Services template

We will be disabling the Routing and Remote Access service on our Windows Domain Controllers servers:

Note: This service represents one of the most important to lock down in a production environment. This step is used as an example of how to disable a service for an entire Organizational Unit. We will be using the Windows Security Configuration Wizard on each server individually to lock down services further. When implementing this configuration in production, you should review all services and minimize any that are not appropriate for your environment.

3. Double click the ‘Routing and Remote Access’ Service and then check the ‘Define this policy’ checkbox. Assure that ‘Disabled’ is selected.
4. Click ‘OK’.
5. Expand ‘Local Policies’ and click on ‘Security Options’ in the left pane.
6. Double-click ‘Interactive logon: Message text for users attempting to log on’ in the right pane.
7. When the template policy window opens, check ‘Define this policy setting in the template’ and in the text field, type: `Warning! This computer is for official use only!` Click ‘OK’.

Figure 3: Creating the logon banner

8. Double-click ‘Interactive logon: Message title for users attempting to log on’. Check ‘Define this policy setting in the template’ and in the text field, type: `Log on Warning!` Click ‘OK’.

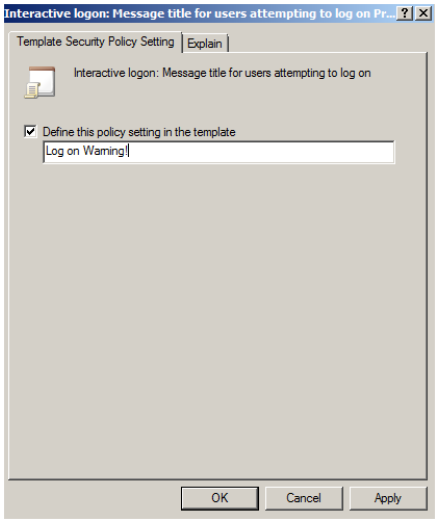


Figure 4: Creating the logon banner

For our virtual environment we will disable auditing of process tracking in order to cut down on the amount of data that will be logged to our syslog server Foxtrot. This should make it simpler to review the logs on Foxtrot by cutting down on the amount of information recorded. Whether or not you should do this in a production environment depends on what particular system information you deem critical to capture.

9. Click on ‘Local Policies’ under ‘WS08-EC-Domain-Controller’ and then expand ‘Audit Policy’

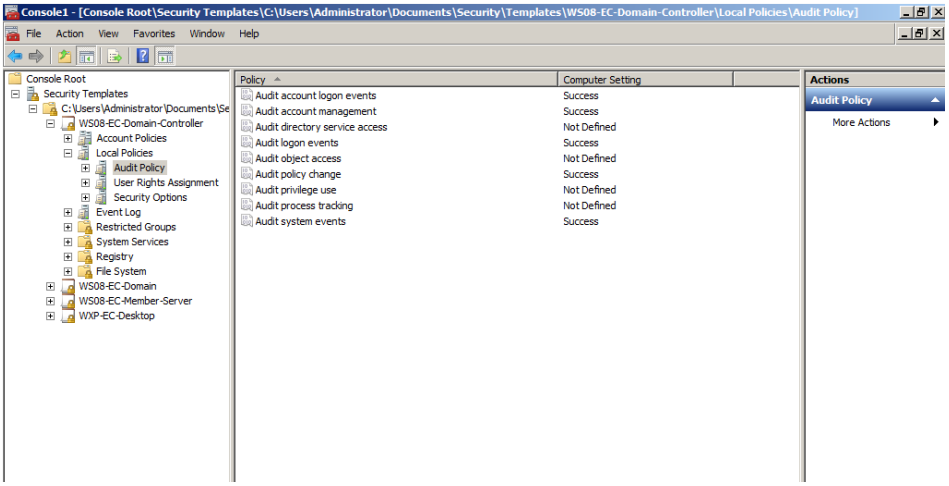


Figure 5: Audit Policy settings

10. Double-click ‘Audit directory service access’. Check the box ‘Define these policy settings in the template’ and check ‘Failure’.

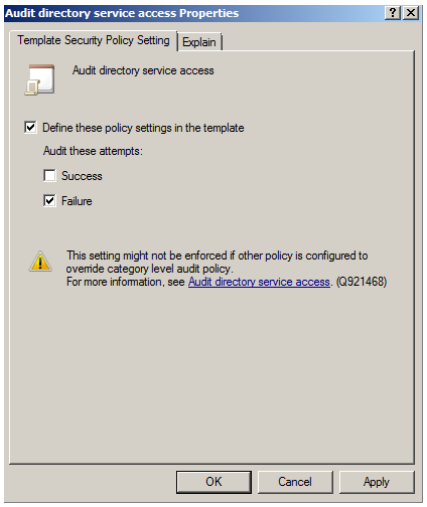


Figure 6: Properties for a security policy

11. Click ‘OK’.

12. Modify the all the policies under ‘Audit Policy’ such that at the end, it should look like the following:

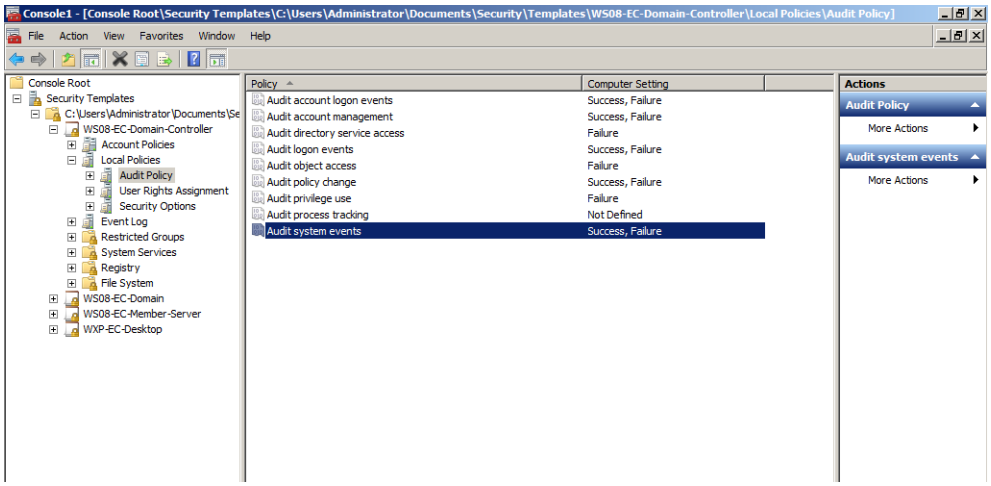


Figure 7: Final Audit Policy settings

Finally, we need to change the default method of Event Log retention in order to avoid problems caused by the limited available hard drive space on our virtual environment systems. We are going to set Event Log to overwrite events as needed if the allowed space for the Event Log is full. Note that this may not be the best option for a production network since an attacker could potentially flood the Event Log with worthless data in order to overwrite any Event Log entries that might document their break-in. However, because of the disk space constraints on our virtual environment systems, overwriting as needed will be necessary.

13. Click on ‘Event Log’ under ‘WS08-EC-Domain-Controller’. Then double-click ‘Retention method for application log’. Check the ‘Define this policy setting in the template’ checkbox.
14. Change the setting to ‘Overwrite events as needed’

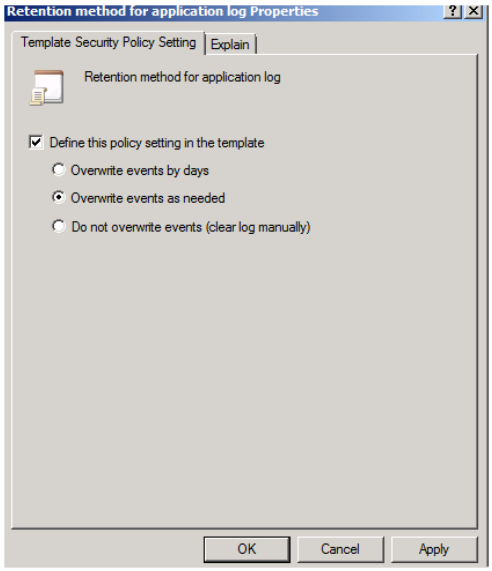


Figure 8: Properties for a security policy

15. Click ‘OK’
16. Edit the Event Log policies such that eventually the policy settings for Event Log should be similar to the figure below:

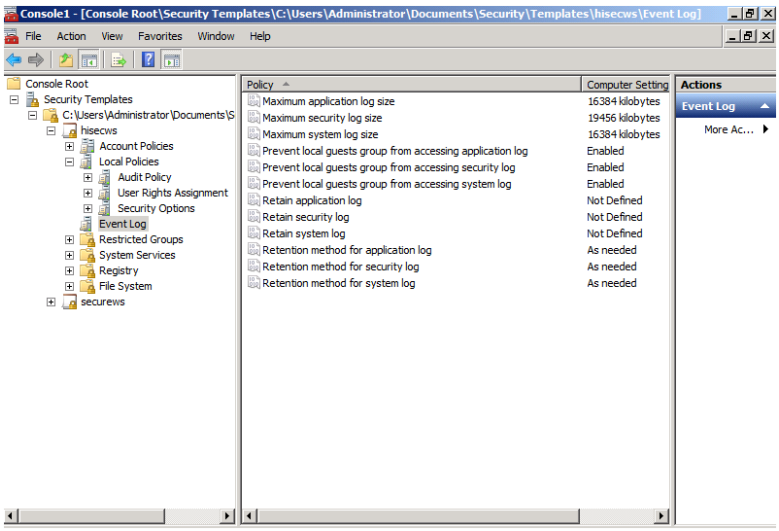


Figure 10: Final Event Log settings

17. Now right click on the ‘WS08-EC-Domain-Controller’ template file and select ‘Save’.

18. Open “Group Policy Management Console”. Click ‘Start’ -> ‘Administrative Tools’ and then select ‘Group Policy Management’.

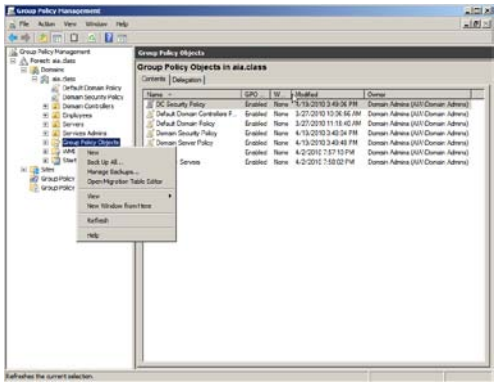


Figure 9: Group Policy Management

19. Create Domain Controllers Group Policy Objects. In the left panel, Expand ‘Group Policy Management’ -> ‘Forest’ -> ‘Domains’ -> ‘aia.class’ using the plus icon. Right-click ‘Group Policy Objects’ and select ‘New’.

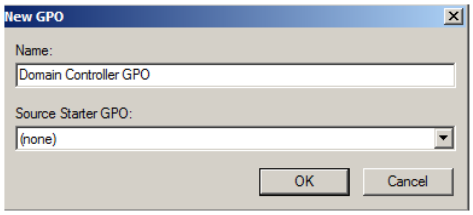


Figure 10: Creating a new GPO

Enter “Domain Controller GPO” as the name of new GPO, click ‘OK’.

20. Import Domain Security Policy Templates. Expand ‘Group Policy Objects’ and right-click “Domain Controller GPO”, the newly created GPO, and select ‘Edit’. This will open ‘Group Policy Management Editor’.

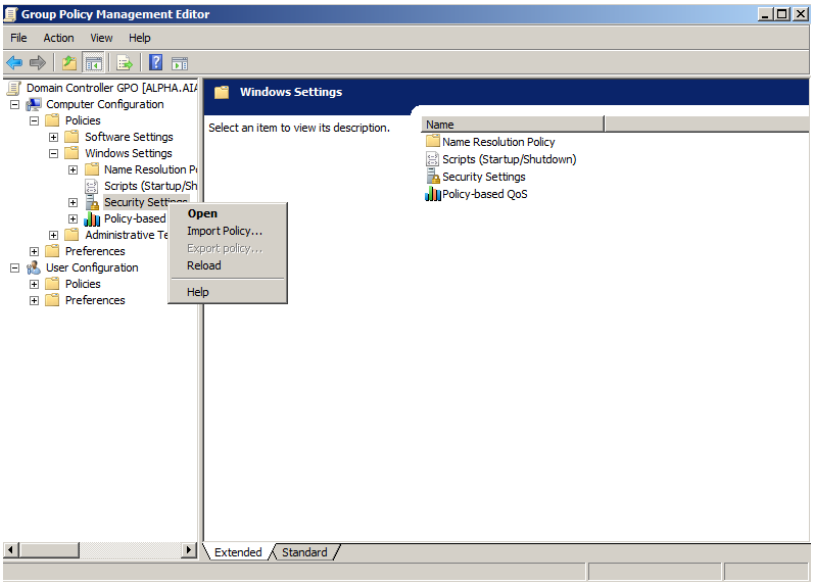


Figure 11: Import Policy

Expand 'Domain Controller GPO' -> 'Computer Configuration' -> 'Policies' -> 'Windows Settings' using the plus icon. Right-click 'Security Settings' and select 'Import Policy'.

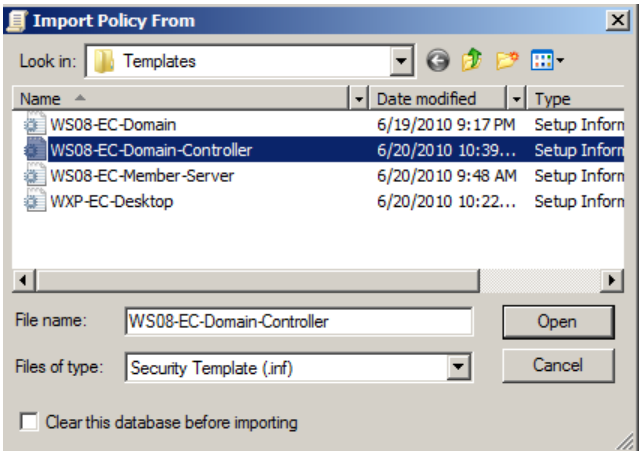


Figure 12: Importing the Domain Controller security template

In the 'Import Policy From' screen, select 'WS08-EC-Domain-Controller' and click 'Open'. (***Make sure the Clear this database before importing checkbox is checked***) Then, close 'Group Policy Management Editor'.

21. Link GPO to Organization Units

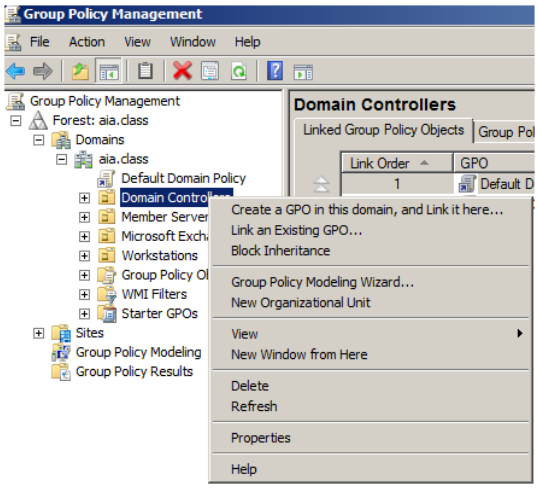


Figure 13: Link the GPO to the OU

Right click the 'Domain Controllers' OU in Group Policy Management Console, and select 'Link an Existing GPO…'

In Select GPO dialog, choose the GPO we just created 'Domain Controller GPO' and click 'OK'. Now the GPO is linked to our domain.

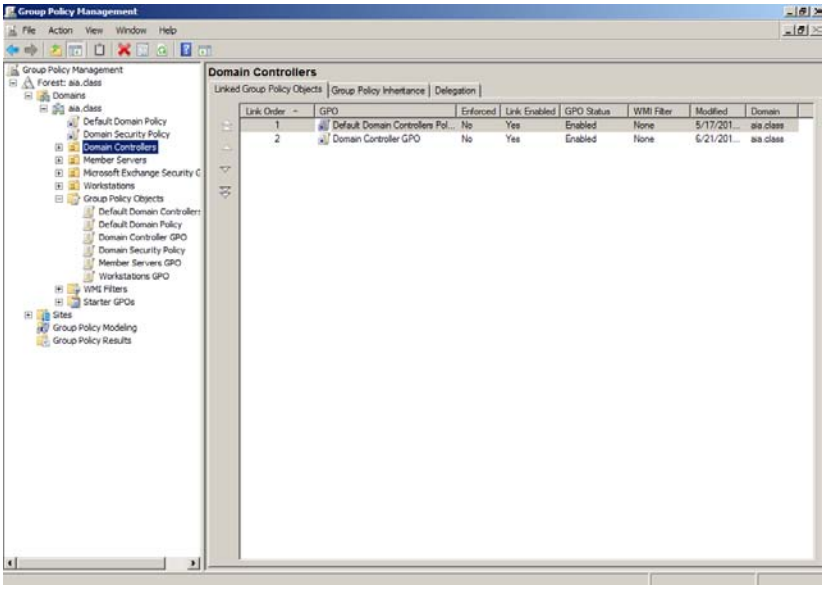


Figure 14: Verify whether the GPO is linked

Click ‘Domain Controllers OU’ again to verify that GPO is linked.

22. Close all open windows and do not save settings to the console.
23. Reboot the server.

    Note: After these Security Group Policy settings are applied and each server is rebooted, you will be asked for Administrator credentials each time a configuration console is opened.

Open Source Security (OSSEC) Agent

OSSEC agents will be installed on each Linux and Windows server and will send events to the OSSEC server that is running on Foxtrot. The OSSEC server processes events and generates warnings from alerts sent by the agents. *Before installing any OSSEC agents, make sure that you have successfully deployed the OSSEC server on Foxtrot.*

1 OSSEC Agent setup

1.1 Installation

1. Open Windows Explorer and navigate to path 'D:\Tools\Windows\OSSEC':

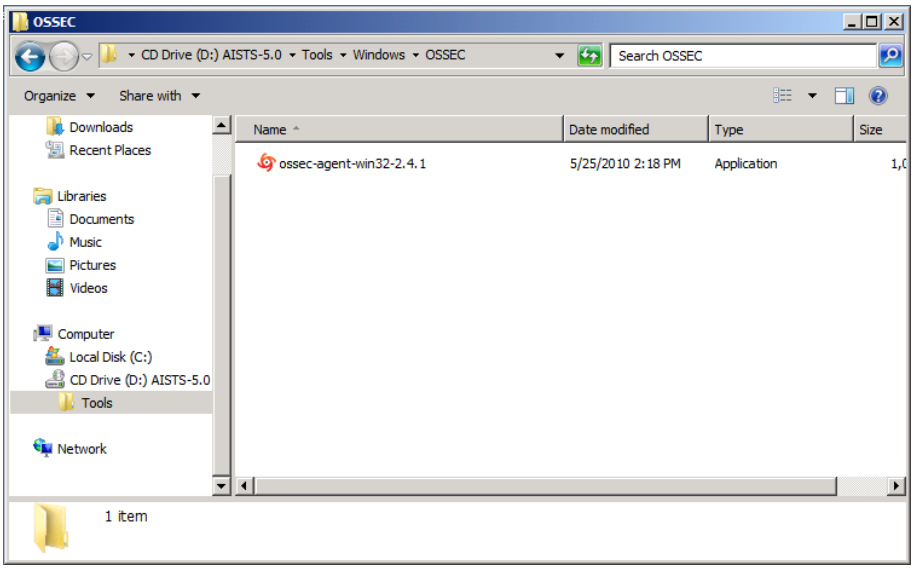


Figure 1: Setup File

2. Double click on the 'ossec-agent-win32-2.4.1' setup file and start installation:

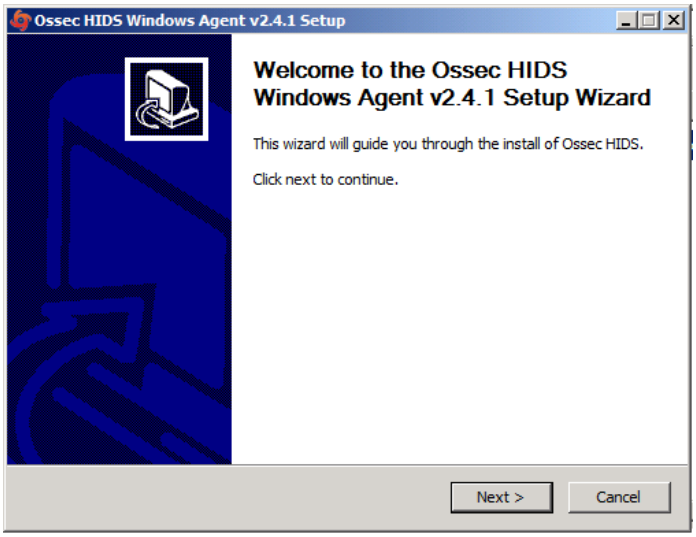


Figure 2: Welcome Screen of OSSEC Installation

3. Click ‘Next’ and accept the license agreement by pressing ‘Agree’ button:

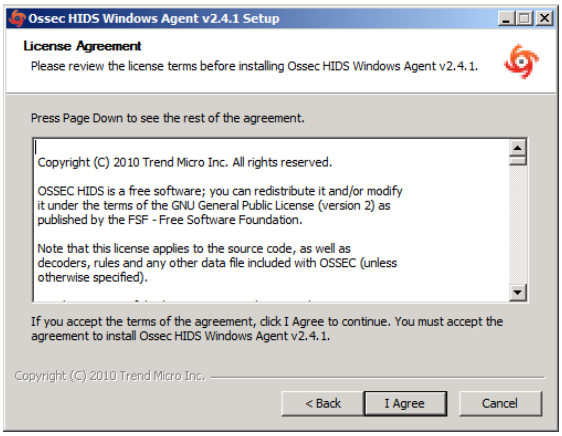


Figure 3: License Agreement window

4. Accept the default installation options and click ‘Next’:

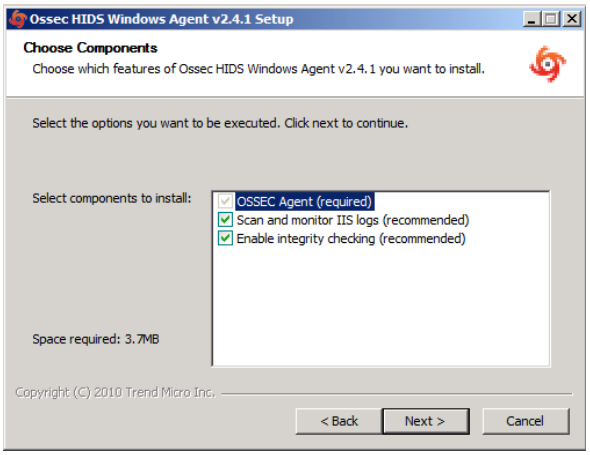


Figure 4: Choose default settings for components

5. Proceed with the installation by pressing the ‘Install’ button:

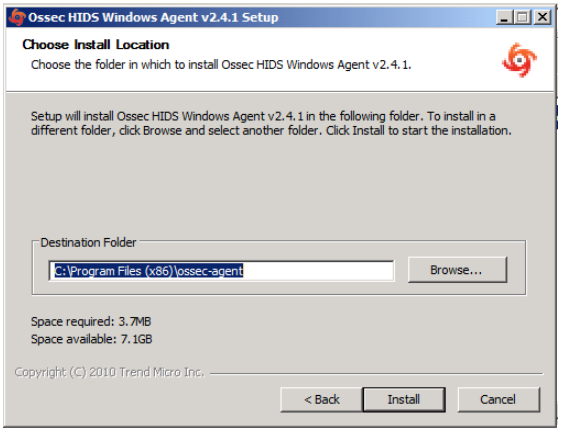


Figure 5: Location path

6. After the installation has finished you should see the following screen. Complete the installation by clicking on ‘Finish’:

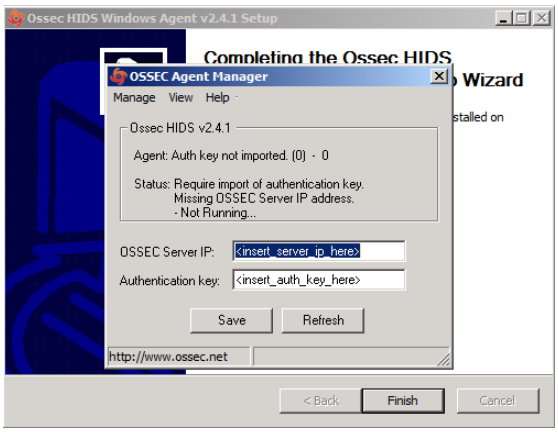


Figure 6: End of OSSEC installation

1.2 Configuration

1. Now we are going to setup a shared key between Alpha and Foxtrot. In order to do this, go back into the CD contents and execute ‘Putty’ from ‘D:\Tools\Windows\Putty’.
2. Enter **`‘10.0.4.2’`** (Foxtrot’s IP address) in the ‘Host Name’ field and click ‘Open’:

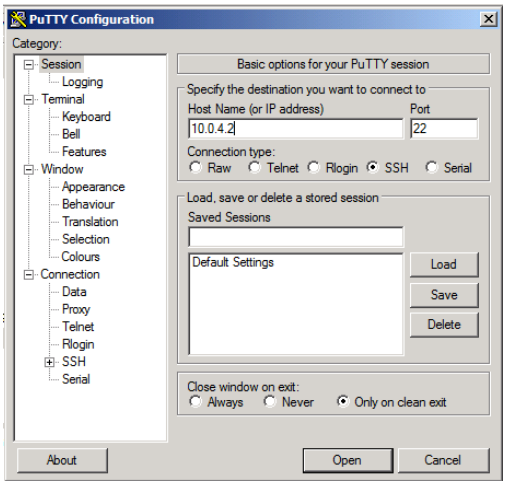


Figure 7: Setting up Putty

3. Accept the warning by clicking ‘Yes’:

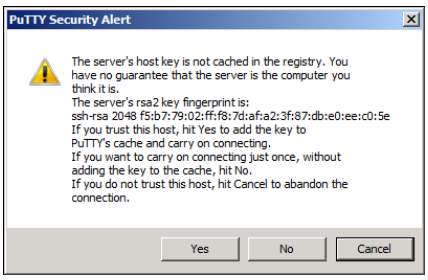


Figure 8: Accept the warning

4. Type **`root`** for the login name and press `[Enter]` then type **`tartans@1`** as the password and press `[Enter]`:

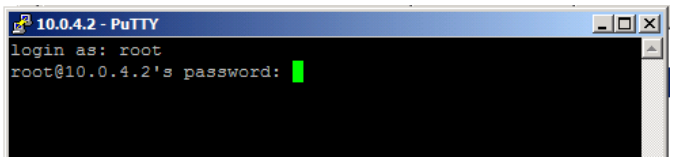


Figure 9: Login

5. Once you have logged into Foxtrot start the OSSEC agent manager by executing the following command:

```
# /var/ossec/bin/manage_agents
```

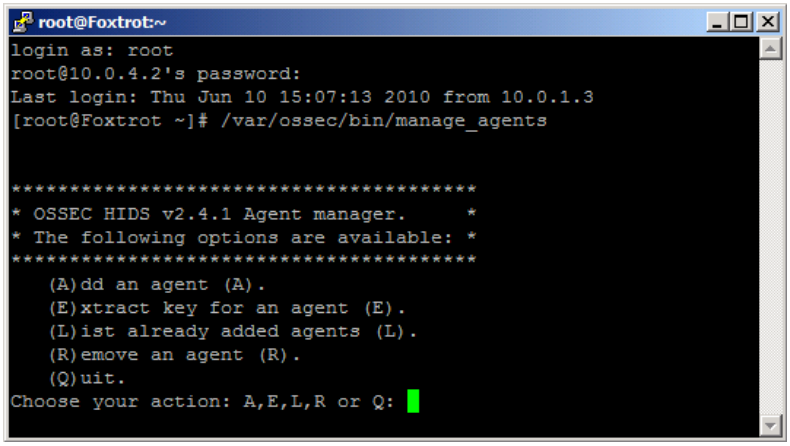


Figure 10: OSSEC Agent Manager window

6. Add an agent by typing A and pressing `[Enter]`.

7. Enter Alpha's information as shown below and press `[Enter]`:

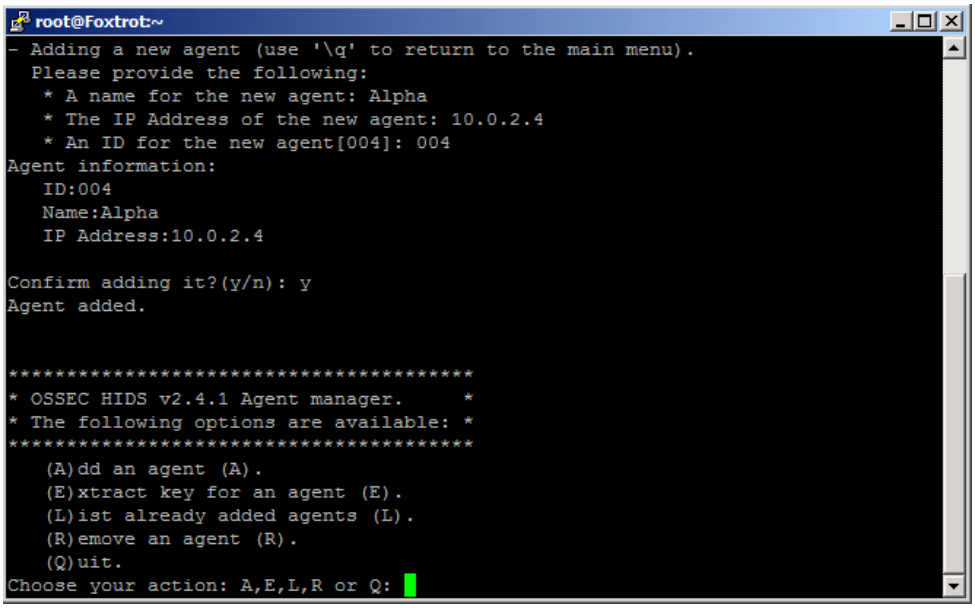


Figure 11: Select an option

8. Now type `E` and press `[Enter]` to extract shared key for Alpha, and enter `004` when the OSSEC agent manager asks for an agent ID. Please note that the key will not be the same as shown in the following screenshot, because the shared key is generated randomly each time an OSSEC agent is added:

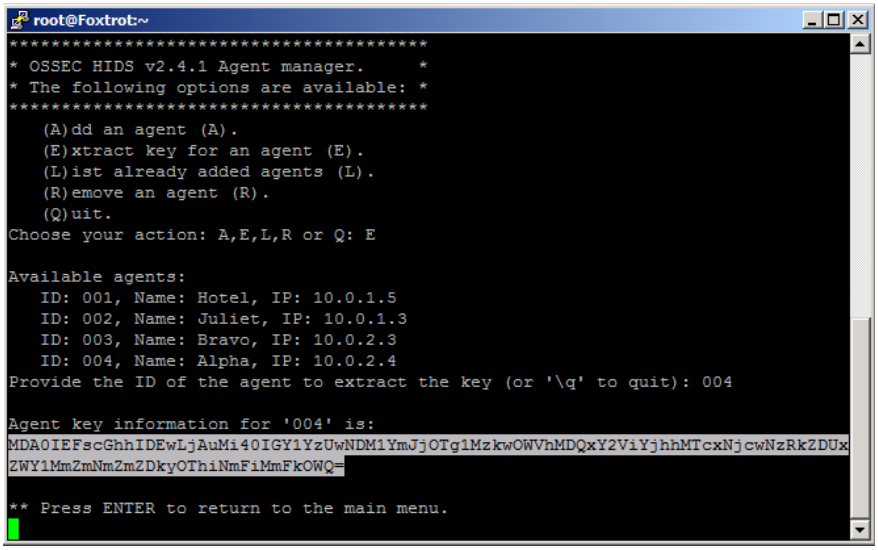


Figure 12: Randomly key generated

9. Copy the shared key by highlighting it and paste it into OSSEC agent as shown below.

10. Enter `10.0.4.2` as the server address and then click ‘Save’ then ‘OK’:

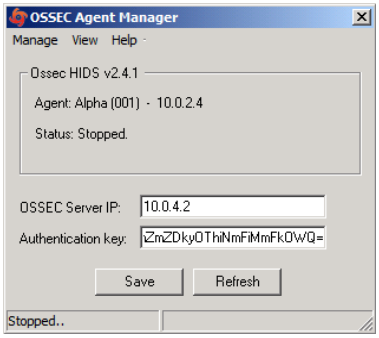


Figure 13: Enter the parameters

Figure 14: Confirm the settings

11. Choose ‘Manage -> ‘Start OSSEC’ to start the OSSEC agent:

Figure 15: Starting OSSEC

12. Switch back to the Putty SSH command shell window. Type `Q` then press `[Enter]` to quit from the agent manager then type `exit` and press `[Enter]` to end the SSH session and exit from Putty.
13. Close the OSSEC Agent Manager and Windows Explorer.
14. Click ‘Finish’ to close the OSSEC wizard.

2 Group Policy Exclusion

Now we need to add a group policy rule to allow member servers to run the OSSEC agent. Without this rule, the initial OSSEC installation will succeed, but our security policies will not allow the OSSEC Agent Manager to be launched again if OSSEC needs to be reconfigured in the future.

1. Go to ‘Start -> ‘Administrative Tools’ -> ‘Group Policy Management’.
2. Right-click ‘Domain Security Policy’ and click ‘Edit…’.

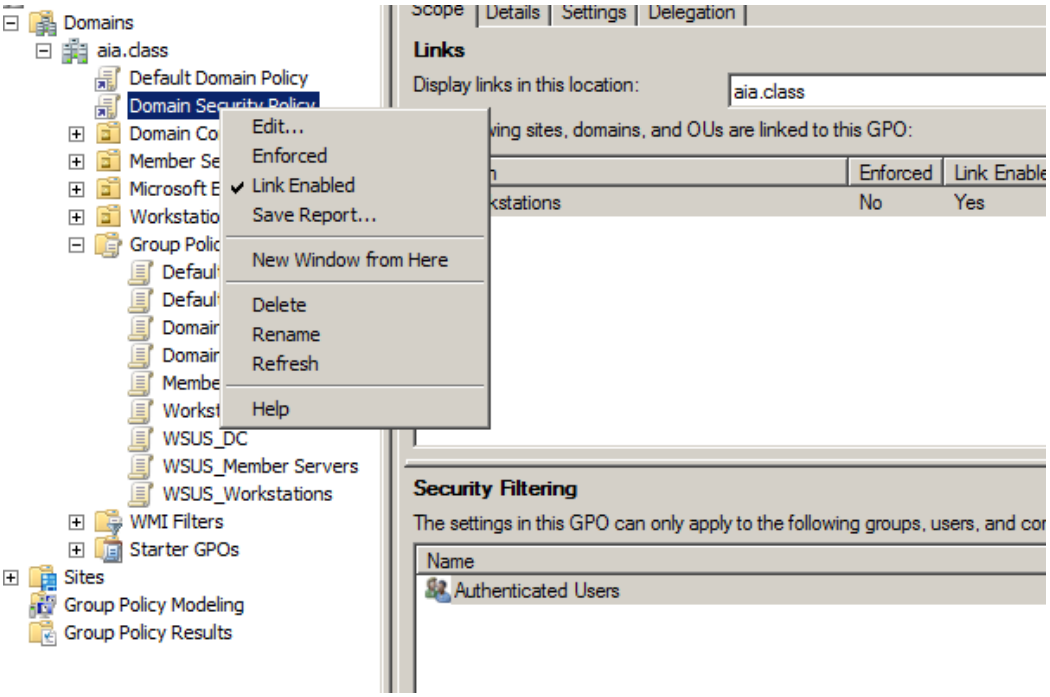


Figure 16: Edit the group policy

3. Expand ‘Computer Configuration’ -> ‘Policies’ -> ‘Windows Settings’ -> ‘Security Settings’ and click on ‘File System’.
4. Right-click on the white space in the right pane and choose ‘Add file…’.
5. Navigate to C:/Program Files (x86)/ossec-agent.
6. Click ‘OK’ twice.
7. Select ‘Replace existing…’ and click ‘OK’.
8. Close all open windows.

Windows Security Configuration Wizard

1 Run the SCW

1. Click ‘Start’ -> ‘Administrative Tools’ -> ‘Security Configuration Wizard’.
2. Click ‘Next’, on the Welcome screen.
3. Click ‘Next’, to Create a new Security Policy
4. Click ‘Next’**,** on the Select Server dialog. We will not be importing a configuration from a different server.
5. Once the Processing of the Security Configuration Database is complete click ‘Next’ to continue.
6. Click ‘Next’, on the ‘Role-Based Service Configuration’ dialog

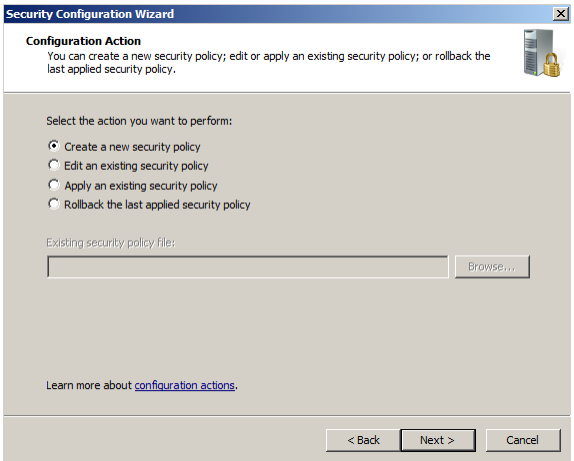


Figure 1: Create a new security policy

7. A list of currently installed roles will be presented. For Alpha, select only the following:
   - DFS Namespace
   - DFS Replication
   - DNS Server
   - Domain Controller
   - File Server
   - Middle-tier application server (COM+/DTC)

   Click **‘**Next’
8. The default Client Features are appropriate for our configuration. Click ‘Next’

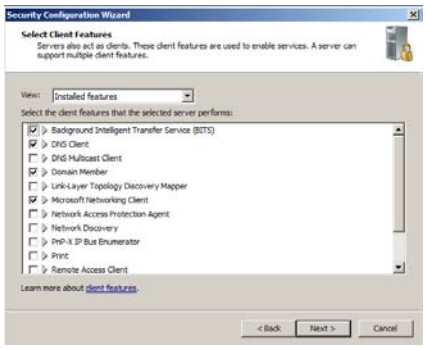


Figure 2: Client features settings

9. Administration and Other Options, select only:
   - .NET Framework 3.0
   - Application Experience Lookup Service
   - Browse Master
   - Error reporting
   - Local application installation
   - Performance Logs and Alerts
   - Remote desktop
   - Windows User Mode Driver Framework

   Click ‘Next’
10. Additional Services: Make sure only ‘OSSEC Hids’ is checked. Click ‘Next’.
11. The default handling option is ‘Do not change the startup mode of the service’ for any unspecified services. Click ‘Next’.
12. Review the list of service changes before clicking ‘Next’.
13. Click ‘Next’ to begin the Network Security Configuration
14. The SCW attempts to identify the necessary ports that the server will need open for your previous selections. However, we will minimize even further by disabling unnecessary rules. Uncheck the following:
    - Core Networking –IPv6 (IPv6-In)
    - Core Networking – IPv6 (IPv6-Out)
15. Click ‘Next’ on Network Security Rules window.
16. Click ‘Next’, when the Registry Wizard Begins.
17. Click ‘Next’, to accept the default SMB security settings.
18. Click ‘Next’, to confirm the default setting for LDAP Signing.
19. Click ‘Next’, to confirm the default setting for Outbound Authentication Methods.
20. Click ‘Next’, to confirm the default setting for Outbound Authentication using Domain Accounts.

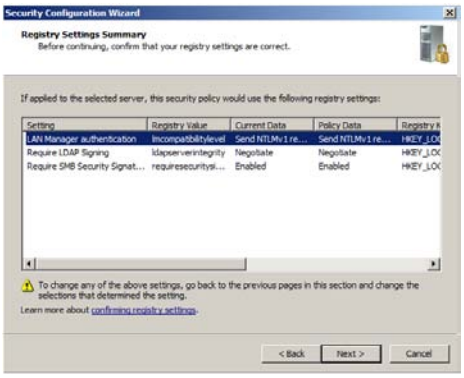


Figure 3: Review the registry settings

21. Review the Registry Settings Summary and click 'Next'.
22. Check ‘Skip this section’ to bypass configuration of the Audit Policy as this is configured using Group Policy and click ‘Next’

Figure 4: Ensure the box is checked

23. Click 'Next', to proceed to the Save Policy dialog.
24. Save the current configuration by appending the server name to the displayed path and click ‘Next’.

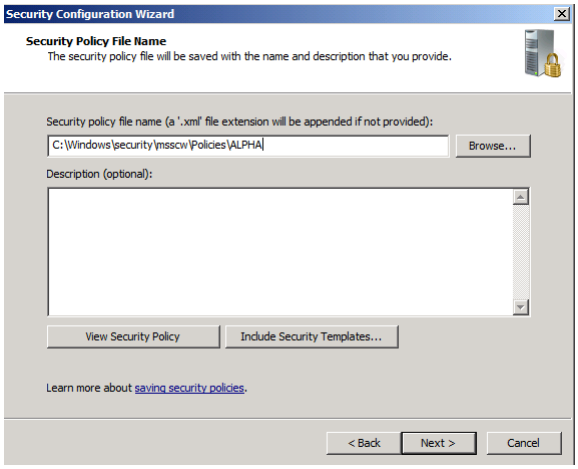


Figure 5: Append ‘ALPHA’ to the path

25. Select the option to ‘Apply Now’ and then click ‘Next’.
26. Once the wizard has completed the necessary changes, click ‘Next’, and then ‘Finish’.
27. Reboot the server.

This page left intentionally blank for pagination purposes

Bravo High Level Description

Bravo is a Windows Server with Microsoft Exchange Server and will function as the mail server for the AIA domain. This system will be configured to accept inbound mail from the mail relay/scanner (Quebec), and will be configured to forward all outbound mail directly to the Internet. Bravo will also be running Internet Information Services (IIS) to allow users to connect to their mail account through a web browser and Outlook Web Access (OWA).

Following are descriptions of Bravo's specific hands-on tasks that students must complete:

Task 1. Windows Host System Hardening

Students will be minimizing non-essential services and unnecessary network configurations - the network interface will be hardened by removing Internet Protocol (IP) version 6 and disabling NetBIOS name resolution. Students will follow security best practices to harden Windows.

Task 2. Exchange Server Hardening

Students will be hardening the Exchange server by first verifying unnecessary services and ports have been disabled through the Windows Host Hardening task. This will be followed by locking down Exchange specific services including setting up storage quotas and configuring Diagnostic and Resource monitoring.

Task 3. Configuring OSSEC Agent

Students will install and configure the OSSEC Agent, which will then send information about security events to the syslog/OSSEC server (Foxtrot).

Task 4. Windows Security Configuration Wizard

The Windows SCW wizard will take students through a series of questions which will help them harden the server as per industry best practices. Unnecessary services will be disabled, auditing functions are enabled, the windows firewall is configured, and if necessary, IIS will be hardened.

This page left intentionally blank for pagination purposes

Windows Server Baseline Hardening Steps

1 Harden Network Interfaces

1.1 Remove Unnecessary Protocols

By default, Microsoft Windows network interfaces are enabled with unnecessary protocols and services. These should be unbound from the interface (if not uninstalled completely). If your server is intended to provide these services, obviously you would NOT disable it.

1. If you have not already done so, log on to the machine using:

   Username: **`AIACLASS\Administrator`** Password: **`tartans@1`**

2. Open the 'Start' menu and right-click on 'Network' and select 'Properties' to open the 'Network and Sharing Center'.
3. Click on the 'Local Area Connection 2' and then click 'Properties'.
4. Clear the box next to 'Internet Protocol Version 6 (TCP/IPv6)'. Then click 'OK'.

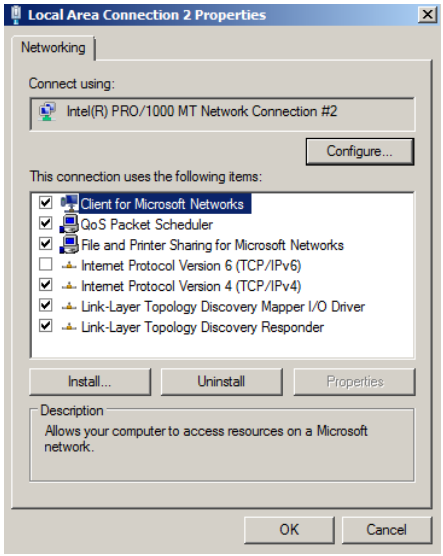


Figure 1: Remove IPv6

2 Harden TCP/IP Properties

2.1 Disable NetBIOS name resolution

As part of our defense-in-depth strategy, it is import to minimize even those parts of the environment that are normally not utilized. Since our network will be entirely native mode Windows 2000 or higher, NetBIOS name resolution would not normally be utilized, however we will eliminate the possibility of it being used altogether (NetBIOS name resolution is chatty and can divulge network information).

1. If the Properties window for your Local Area Connection is not still open, open it by following steps 1 and 2 from the section above.
2. From within the ‘Properties’ of your ‘Local Area Connection’, select the ‘Internet Protocol Version 4 (TCP/IPv4)’ item (leave it checked), and click on the ‘Properties’ button, then click the ‘Advanced’ button.
3. Next click on the ‘WINS’ tab at the top of the window.

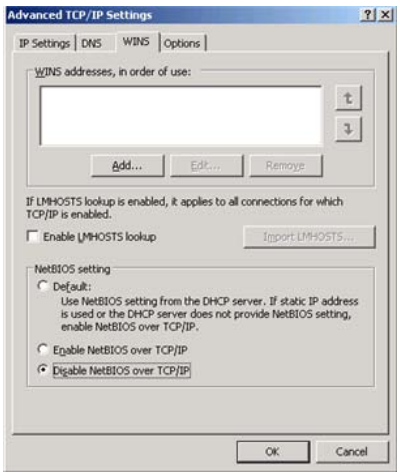


Figure 2: Minimize NetBIOS services

4. Uncheck ‘Enable LMHOSTS lookup’.
5. Select the radio button ‘Disable NetBIOS over TCP/IP’.
6. Click ‘OK’ to accept these settings.
7. Click ‘OK’ to confirm all ‘TCP/IP Properties’ changes.
8. Click ‘OK’ to confirm all ‘Local Area Connection Properties’ changes.
9. Close the ‘Local Area Connection 2 Properties’ and ‘Status’ windows.
10. Close the ‘Network and Sharing Center’ to return to the Desktop.

3 Install ClamWin for Anti-Virus Protection

3.1 Installation

1. Open the Course CD by clicking ‘Start’ -> ‘Computer’, right click ‘CD Drive (D:) AISTS’ and select ‘Open’.
2. Navigate to ‘Tools\Windows\ClamWin’ and double-click the ‘clamwin-0.96.1-setup’ icon.
3. Click ‘Next’.

Figure 3: Install ClamWin Antivirus

4. Accept the license agreement and click ‘Next’.
5. Accept the default option to install for ‘Anyone who uses this computer (all users)’ and click ‘Next’.
6. Select the default installation path and click ‘Next’.
7. At the ‘Select Components’ prompt, accept the default option of ‘Typical Installation’ and click ‘Next’.
8. Click ‘Next’ to create the default start menu folder.
9. Uncheck ‘Download Virus Database Files’ and click ‘Next’.

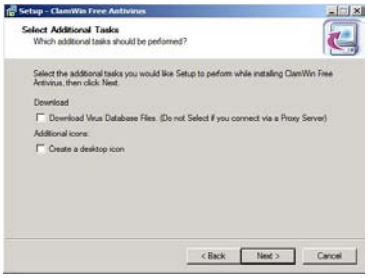


Figure 4: ClamWin Setup

10. Click ‘Install’ to install the program.
11. Click ‘Finish’ to complete the installation.
12. Close Windows Explorer.

3.2 Configuration

1. Click the upward facing arrow in the taskbar and then double-click on the ClamWin icon.

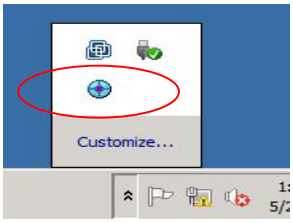


Figure 5: ClamWin Icon

2. Choose 'No' if asked to update the virus database.
3. Select ‘Tools’ from the menu, and click on ‘Preferences’.

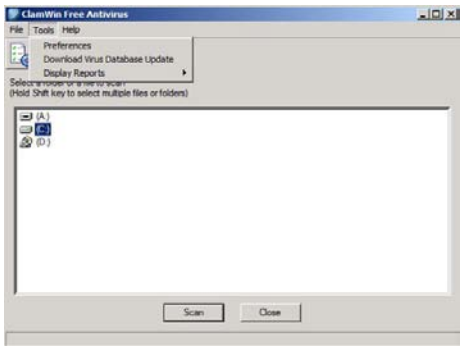


Figure 6: ClamWin Configuration

4. Click on the ‘Internet Updates’ tab. Leave the updates to be done daily, but change the time to 2:30:00 AM.

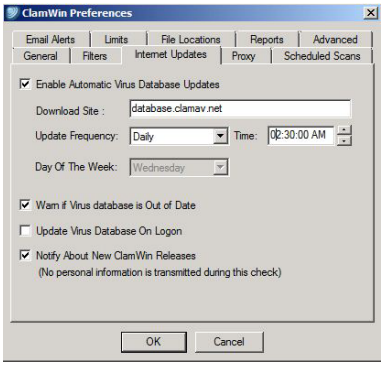


Figure 7: ClamWin Internet Updates

5. Click on the ‘Scheduled Scans’ tab. Click ‘Add’. Choose the scanning frequency to be done Daily at 3:30:00 AM. Enter `C:\` as the folder to scan. Enter a description, such as `Nightly Virus Scan`. Click ‘OK’.

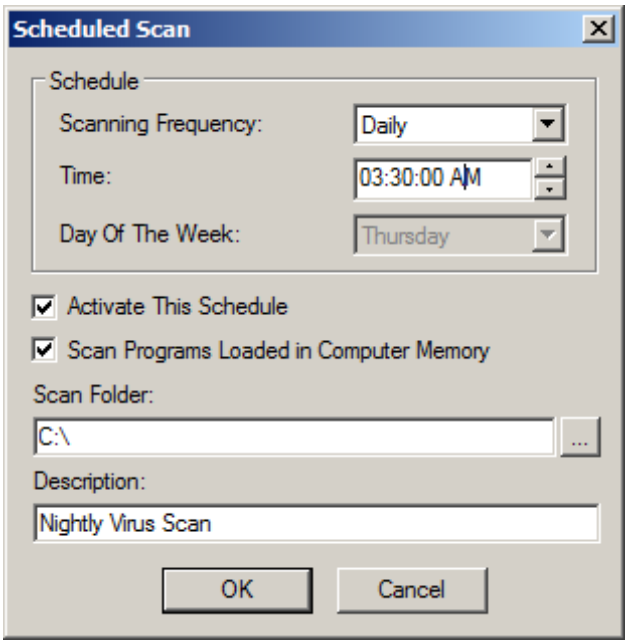


Figure 8: ClamWin Scheduled Scan

6. Click on the 'Email Alerts' tab. Check the box labeled 'Send Email On Virus Detection'. Enter in the following information:

   Mail Server – **`10.0.2.3`**

   From – **`clamwin@Bravo`**

   To – **`eventwatch@aia.class`**

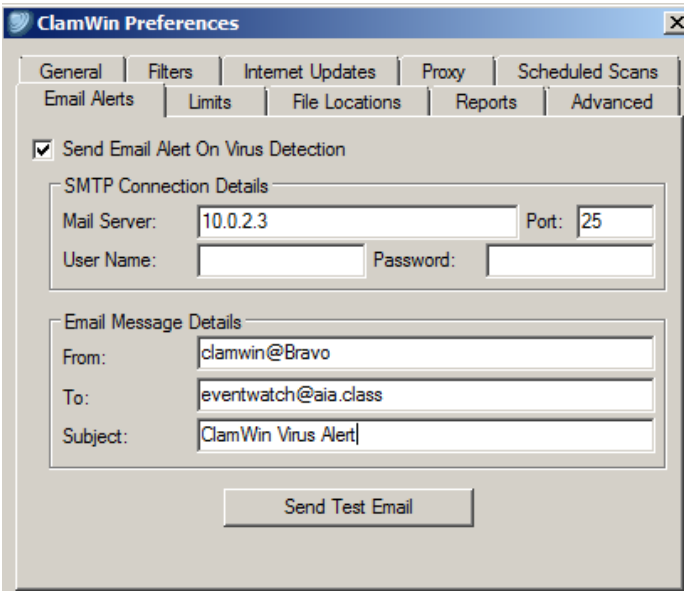


Figure 9: ClamWin Email Alerts

7. Click on the 'Proxy' tab. Enter in the IP address of the Squid Proxy server, Quebec, which is **`10.0.2.1`**. Ensure that the port is **3128**.

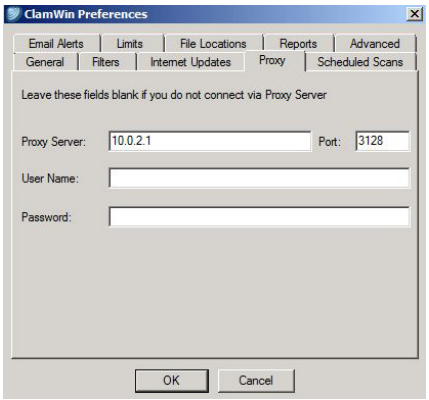


Figure 10: ClamWin Proxy Settings

8. Click 'OK' to accept all changes.
9. Choose 'No' if asked to update the database.
10. Click 'Close' to close the ClamWin window.

This page left intentionally blank for pagination purposes

Exchange Server Hardening

1 Limit User Storage Quota and Message Size

1.1 Restrict Mailbox Storage Limits

To help prevent DoS attacks, or unintentional server overloads, restrict user storage limits for mailboxes. Excessive amounts of mail stored by a number of users may cause large storage demands and lead to lengthy backup and restore processes, affecting the availability and reliability of the mail server.

1. Open the 'Exchange Management Console' from 'Start' Menu -> 'All Programs' -> 'Microsoft Exchange Server 2010'.
2. Expand 'Microsoft Exchange On-Premises (bravo.aia.class) -> 'Organization Configuration' and click on 'Mailbox'.
3. On the right pane, select the 'Database Management' tab. In the 'Create Filter' panel, right click on 'Mailbox Database 0875276437' and select 'Properties'.

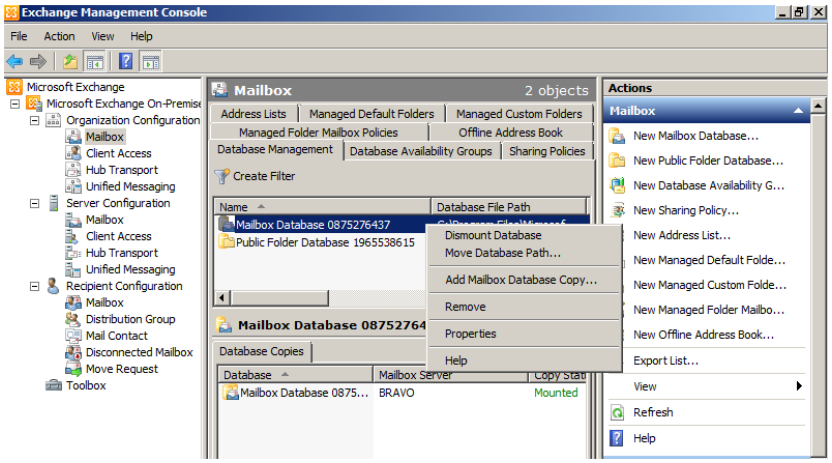


Figure 1: Navigating to configure Storage limits

4. Select the 'Limits' tab and set the following limits:

   Issue warning at (KB): ***90000***

   Prohibit send at (KB): ***100000***

   Prohibit send and receive at (KB): ***150000***

   Keep deleted items for (days): **7**

   Keep deleted mailboxes for (days): **30**

5. Click 'OK' to return.

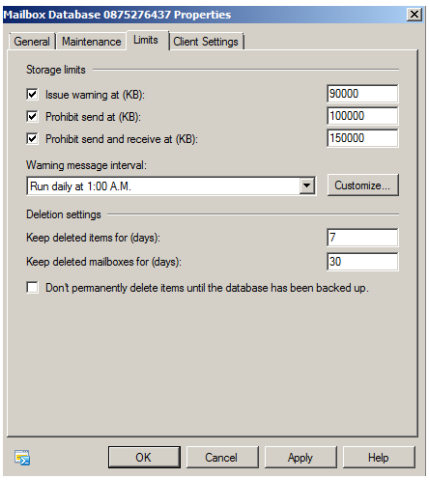


Figure 2: Restricting the storage limits

1.2 Limit Storage Size for Incoming and Outgoing Mail

1. In the 'Exchange Management Console', expand 'Organization Configuration' and click on 'Hub Transport'.
2. On the right panel, select the 'Global Settings' tab. Right click on 'Transport Settings' and select 'Properties'.

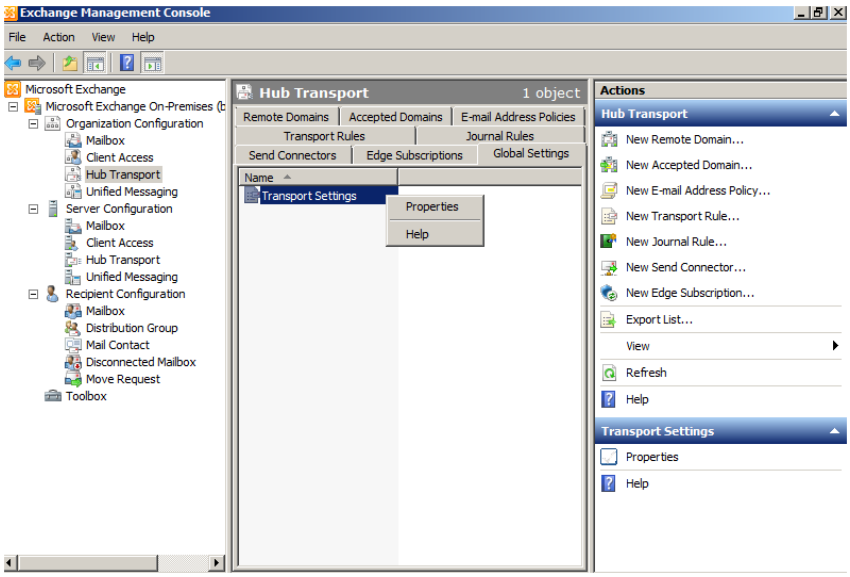


Figure 3: Navigating to configure mail size

3. In the 'General' tab, configure the following limits:

   Maximum receive size (KB): ***10000***
   Maximum send size (KB): ***10000***
   Maximum number of recipients: ***1000***

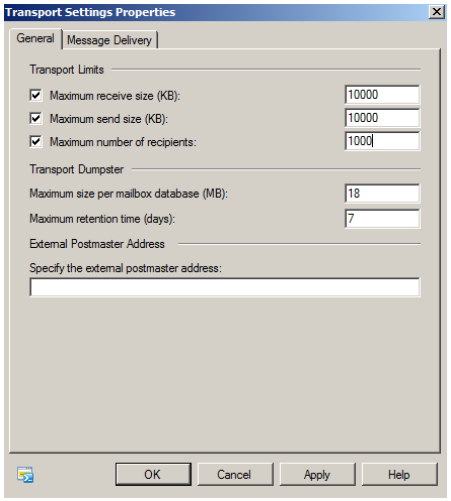


Figure 4: Restricting the incoming/outgoing mail size

4. Select 'Apply' and click 'OK' to exit the recipient properties window.

2 Auditing Exchange

2.1 Configuring Diagnostic Logging

Proactive auditing is a critical security measure to have in place to detect malicious activity and reduce the chance of a compromise, hence protecting the confidentiality, integrity and availability of a system.

An administrator should be able to verify that logging is active and the correct information is being captured. If an incident goes unnoticed an attacker may be able to increase his privileges and not only continue to pillage information, but potentially plant malicious executables. If no logs are available, countermeasures may not be possible.

Auditing and keeping logs also aid tremendously in troubleshooting server operating status. Collecting logs is only half the battle however, they must be reviewed daily and the administrators must know how to analyze and interpret the data.

Diagnostic Logging can be configured on an Exchange mail server. The events to be logged are assigned a level of criticalness to determine whether the event should be logged or not. The four levels of criticality range from *None* (least critical) to *Maximum* (most critical).

To configure Diagnostic Logging:

1. Expand ‘Microsoft Exchange On-Premises (bravo.aia.class)’ -> ‘Server Configuration’ and click on ‘Mailbox’.
2. In the right panel, right click on ‘BRAVO’ and select ‘Manage Diagnostic Logging Properties…’.

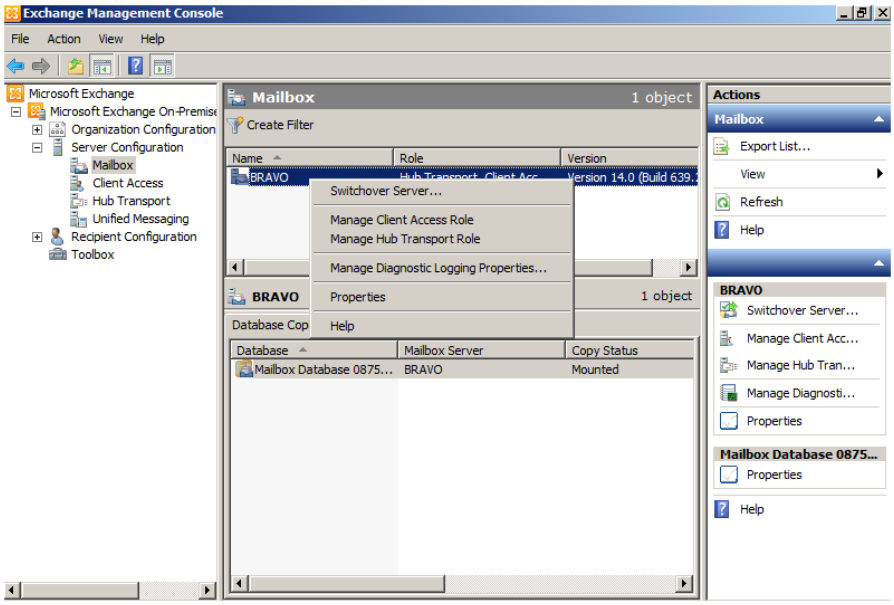


Figure 5: Navigating to configure Logging

3. Under ‘Update logging levels for services’ expand ‘MSExchangeIS’ and ‘9001 Public’. Then set each of the following to the ‘Expert’ Logging Level:

   ‘Logons’, ‘Access Control’, ‘Send On Behalf Of’, and ‘Send As’.

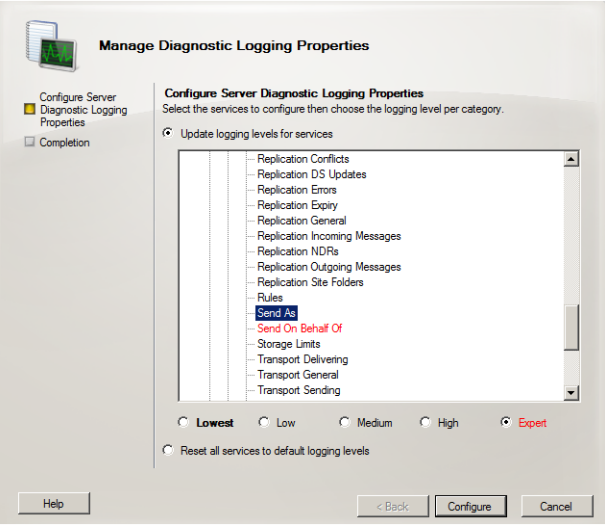


Figure 6: Configuring the Logging properties

4. Expand ‘MS Exchange IMAP4’ and set the Logging level of ‘General’ to ‘Expert’.
5. Click ‘Configure’ and once it is done, click ‘Finish’.
6. In the left panel, click ‘Server Configuration’. Then right click on ‘BRAVO’ and select ‘Properties’.

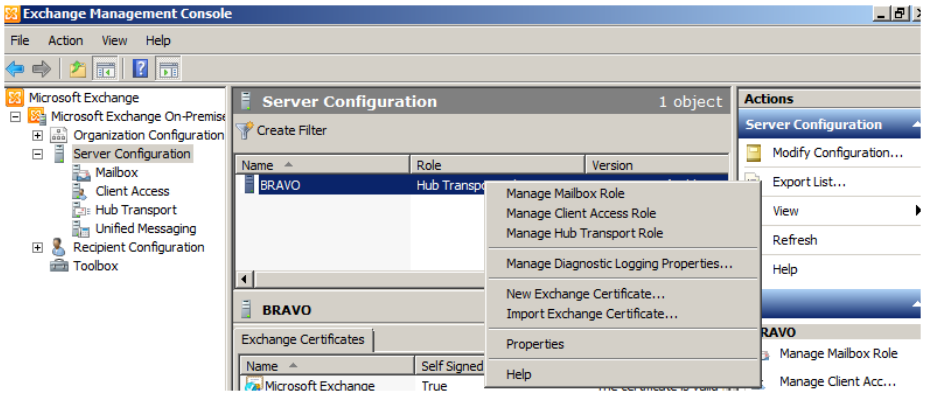


Figure 7: Navigating to Properties of BRAVO

7. On the ‘Properties’ window, select ‘Log Settings’ tab and verify both ‘Enable message tracking log’ and ‘Enable connectivity log’ are checked. Click ‘OK’.

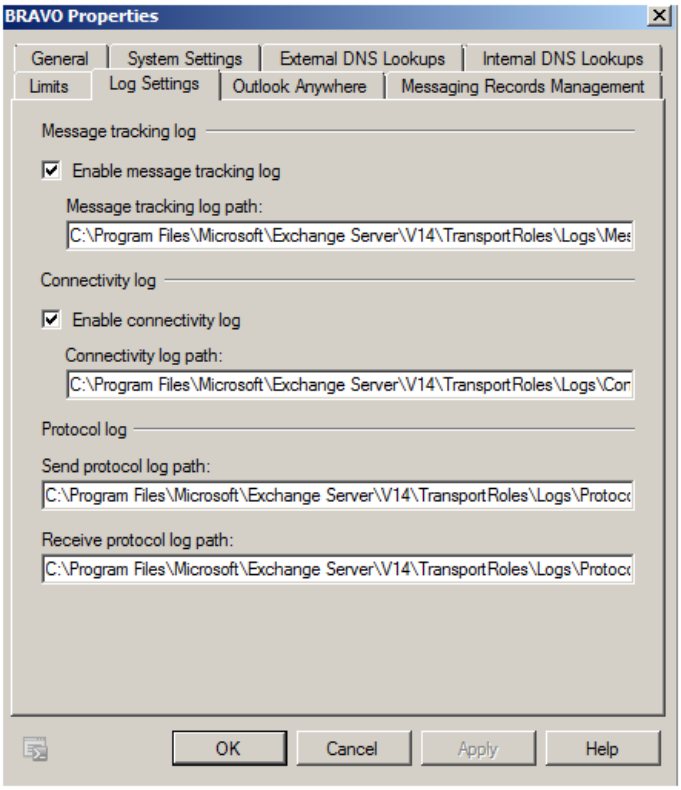


Figure 8: Logging settings

This page left intentionally blank for pagination purposes

Open Source Security (OSSEC) Agent

OSSEC agents will be installed on each Linux and Windows server and will send events to the OSSEC server that is running on Foxtrot. The OSSEC server processes events and generates warnings from alerts sent by the agents. *Before installing any OSSEC agents, make sure that you have successfully deployed the OSSEC server on Foxtrot.*

1 OSSEC Agent setup

1.1 Installation

1. Open a Windows Explorer and navigate to 'D:\Tools\Windows\OSSEC':

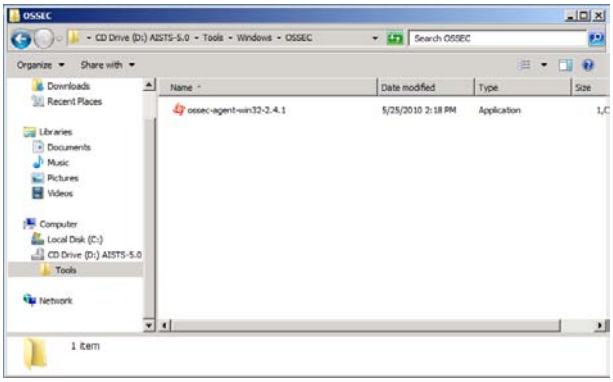


Figure 1: Setup File

2. Double click on the 'ossec-agent-win32-2.4.1' setup file and start the installation:

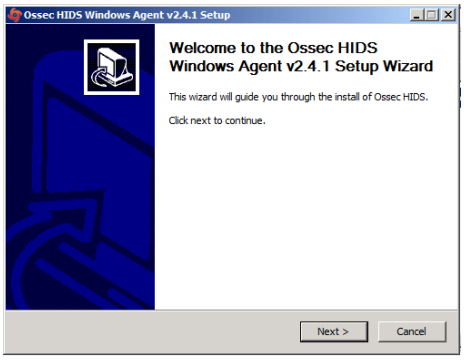


Figure 2: Welcome Screen of OSSEC Installation

3. Click 'Next' and accept the license agreement by pressing the 'I Agree' button:

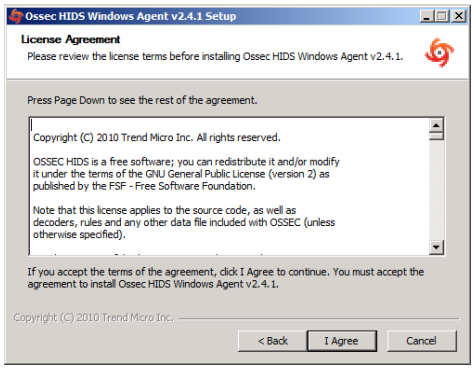


Figure 3: License Agreement window

4. Accept the default installation options and click ‘Next’:

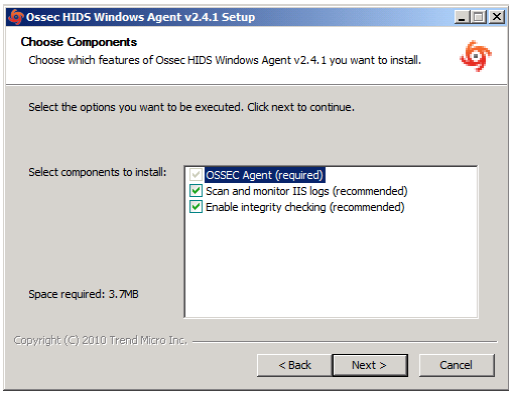


Figure 4: Choose default settings for components

5. Proceed with the installation by pressing the ‘Install’ button:

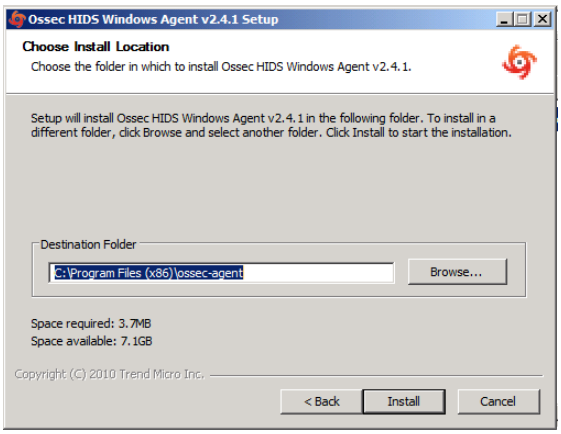


Figure 5: Location path

6. After the installation has finished you should see following screen. Complete the installation by clicking on ‘Finish’:

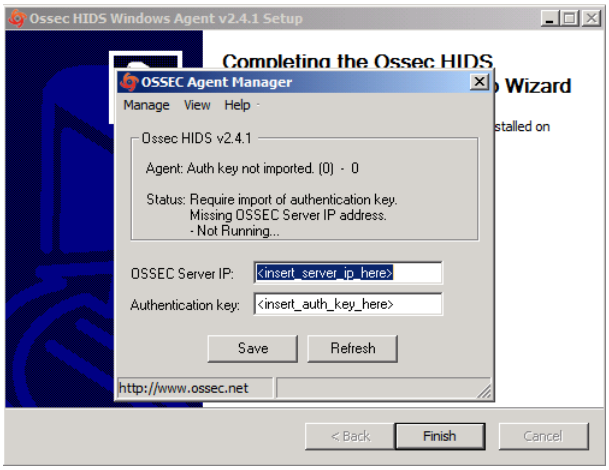


Figure 6: End of OSSEC installation

1.2 Configuration

1. Now we are going to setup a shared key between Bravo and Foxtrot. In order to do this, go back into the CD contents and execute ‘Putty’ from ‘D:\Tools\Windows\Putty’.
2. Enter `10.0.4.2` (Foxtrot’s IP Address) in the ‘Host Name’ field and click ‘Open’:

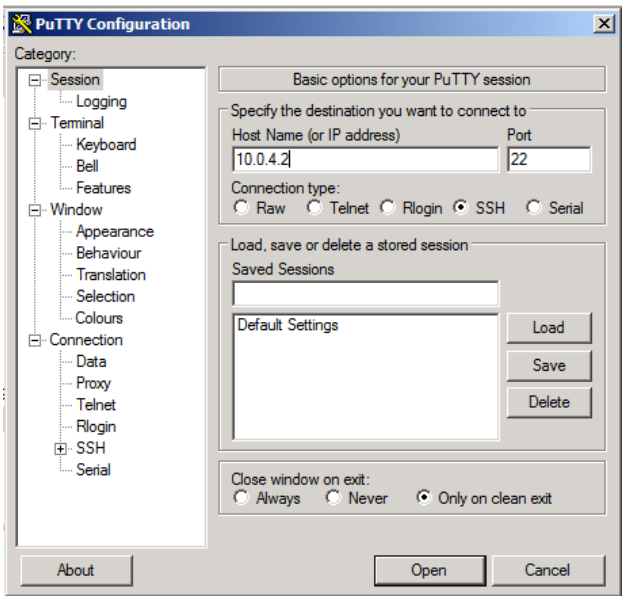


Figure 7: Setting up Putty

3. Accept the warning by clicking ‘Yes’:

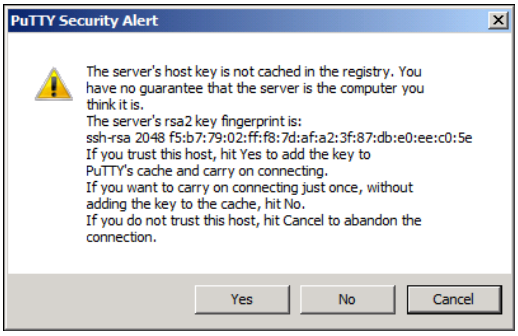


Figure 8: Accept the warning

4. Type **`root`** as the login name and press `[Enter]` then type **`tartans@1`** as the password and press `[Enter]`:

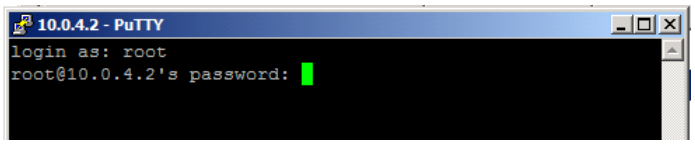


Figure 9: Login

5. Once logged into Foxtrot, start the OSSEC agent manager by executing the following command:

```
# /var/ossec/bin/manage_agents
```

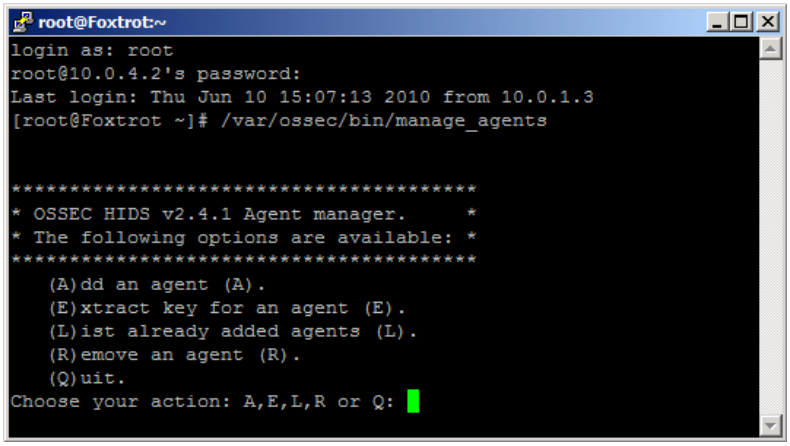


Figure 10: OSSEC Agent Manager window

6. Add an agent by typing A and pressing `[Enter]`.
7. Enter Bravo's information as shown below and press `[Enter]`:

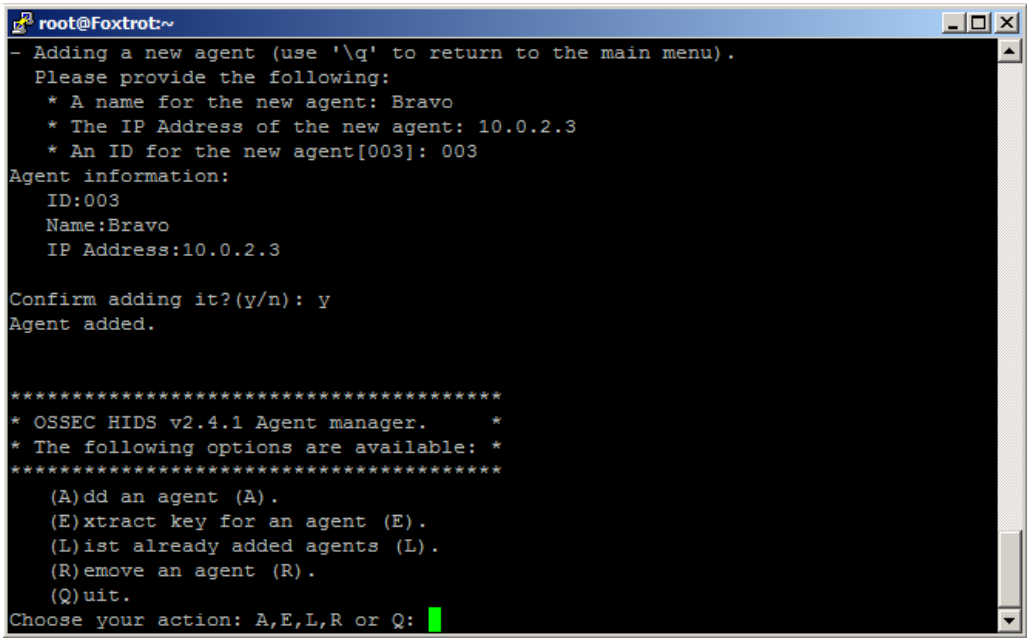


Figure 11: Select an option

8. Now type `E` and press `[Enter]` to extract the shared key for Bravo, and enter `003` when the OSSEC agent manager asks for an agent ID. Please note that the key will not be the same as shown in the following screenshot, because the shared key is generated randomly each time an OSSEC agent is added:

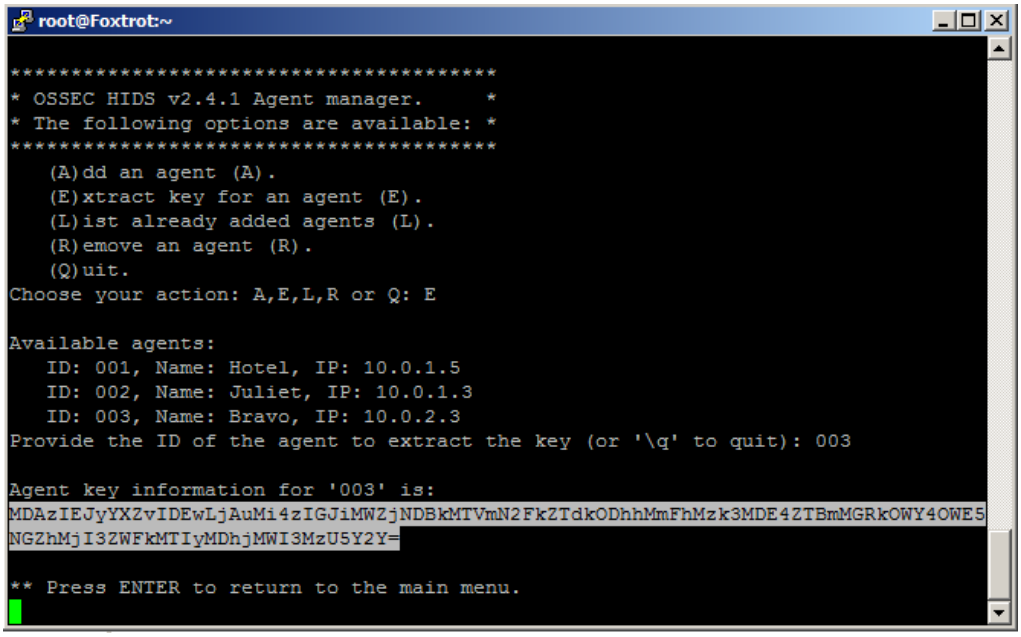


Figure 12: Random key generated

9. Copy the shared key by highlighting it and paste it into the OSSEC Agent Manager as shown below.

10. Enter `10.0.4.2` as the server address and click ‘Save’ then ‘OK’:

Figure 13: Enter the parameters

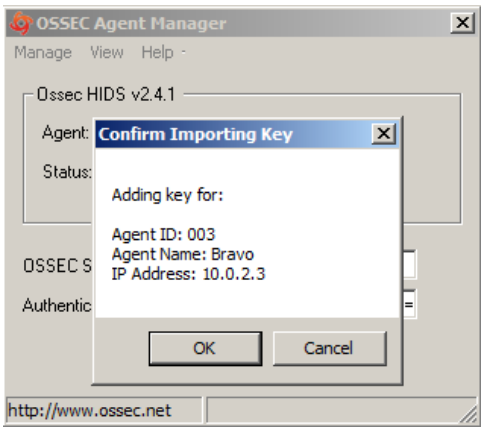


Figure 14: Confirm the settings

11. Choose ‘Manage -> ‘Start OSSEC’ to start the OSSEC agent:

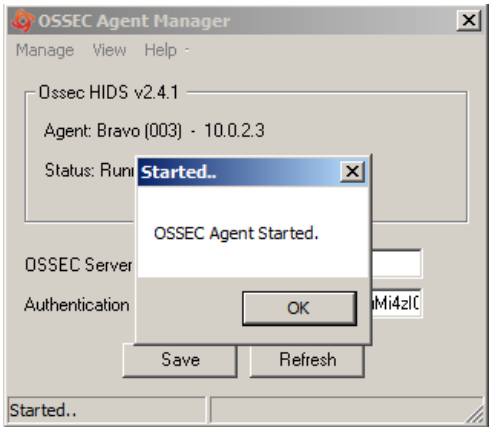


Figure 15: Starting OSSEC

12. Switch back to the Putty SSH command shell window. Type `Q` then press `[Enter]` to quit from the agent manager then type `exit` and press `[Enter]` to end the SSH session and exit from Putty.
13. Close the OSSEC Agent Manager and Windows Explorer.
14. Click ‘Finish’ to close the OSSEC wizard.

Windows Security Configuration Wizard

1 Run the SCW

1. Click ‘Start’ -> ‘Administrative Tools’ -> ‘Security Configuration Wizard’.
2. Click ‘Next’, on the Welcome screen
3. Click ‘Next’, to Create a new Security Policy
4. Click ‘Next’, on the Select Server dialog. We will not be importing a configuration from a different server.
5. Once the Processing of the Security Configuration Database is complete click ‘Next’ to continue.

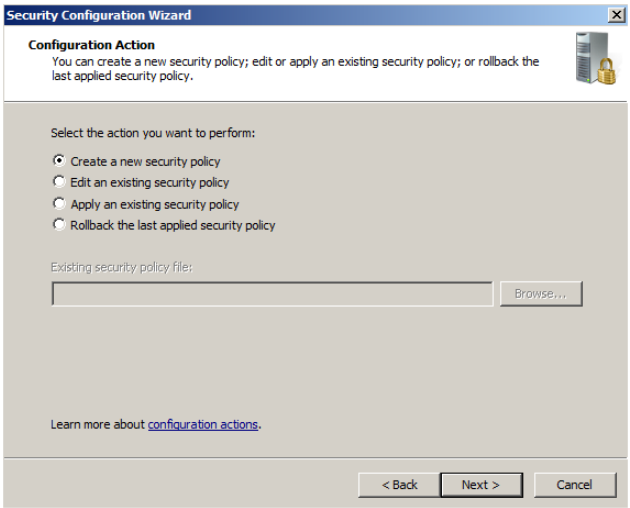


Figure 1: Create a new security policy

6. Click ‘Next’, on the Role-Based Service Configuration dialog.
7. A list of currently installed roles will be presented. Select ‘All roles’ from the ‘View’ dropdown menu and then un-check all options except:
   - ‘Application Server – Application Server Foundation’,
   - ‘Application Server – Named Pipes Activation’
   - ‘Application Server – TCP Activation’
   - ‘ASP.NET State Service’
   - ‘File Server’
   - ‘Middle-tier Application Server(COM+/DTC)’
   - SMTP Server
   - ‘Web Server’
   - ‘Windows Process Activation Service’

   Click ‘Next’.

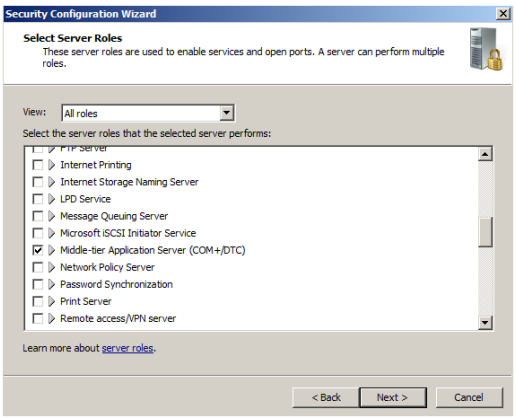


Figure 2: Server Roles settings

8. For our domain servers the default client settings are appropriate. These enable necessary services for accessing internal and Internet servers. Click ‘Next’.

9. Enable only the listed options below for the Administration and Other Options dialog:
    - .NET Framework 3.0
    - Application Experience Lookup Service
    - Error reporting
    - Local application installation
    - Performance Logs and Alerts
    - Remote desktop
    - Windows User Mode Driver Framework
10. Click ‘Next’.
11. Uncheck the following unnecessary services:
    - ‘Application Identity’
    - ‘Credential Manager’
    - ‘Disk Defragmenter’
    - ‘Encrypting File System (EFS)’
    - ‘Performance Counter DLL Host’
    - ‘Power’
    - ‘VMWare Tools Service’
    - ‘VMWare Upgrade Helper’
    - ‘Windows Font Cache Service’
12. The default handling option is ‘Do not change the start mode of the service’ for any unspecified services. Click ‘Next’.
13. Review the list of service changes before clicking ‘Next’.

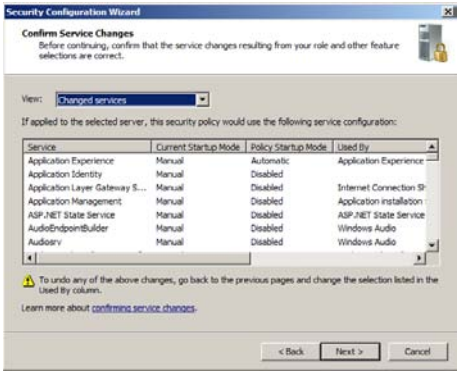


Figure 3: Review Service settings

14. Click ‘Next’ to begin the Network Security Configuration

15. The SCW attempts to identify the necessary ports that the server will need open for your previous selections. However, we will minimize even further by disabling unnecessary rules. Uncheck the following:
    - Core Networking – Ipv6 (IPv6-In)
    - Core Networking – Ipv6 (IPv6-Out)
16. Click ‘Add…’ to add a rule to listen for STMP connections.
17. Enter ‘Listen for SMTP’ in the ‘Name’ field.
18. Select ‘Inbound’ and ‘Allow the connections’.

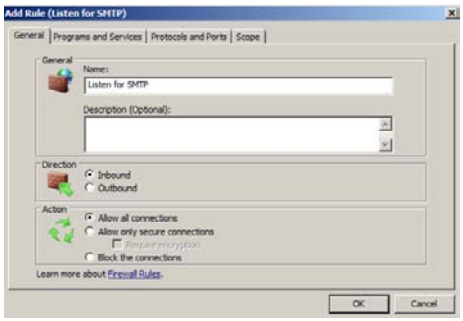


Figure 4: Adding rules

19. Go to the ‘Protocols and Ports’ tab.
20. Select ‘TCP’ under ‘Protocol Type’.
21. Select ‘Specific Ports’ and then enter ‘25’ under ‘Local Port’.
22. Click ‘OK’.
23. Click ‘Next’ to continue past the Network Security Rules window.
24. Click ‘Next’, when the Registry Wizard Begins
25. Click ‘Next’, to accept the default SMB security settings.
26. Click ‘Next’, to confirm the requirement for Domain Account authentication for outbound connections
27. Click ‘Next’, to confirm that we are using domain controllers that use the necessary LAN Manager Authentication level.

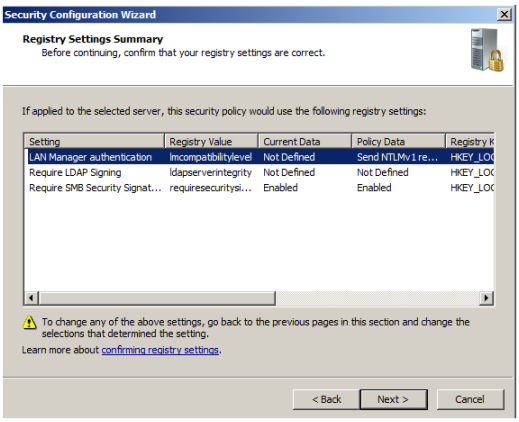


Figure 5: Review Registry settings

28. Confirm the registry settings and then click ‘Next’.
29. Check ‘Skip this section’ as all auditing is configured through Group Policy templates.
30. Click ‘Next’.
31. Click ‘Next’ to save the security policy.
32. Enter the server name and click ‘Next’.

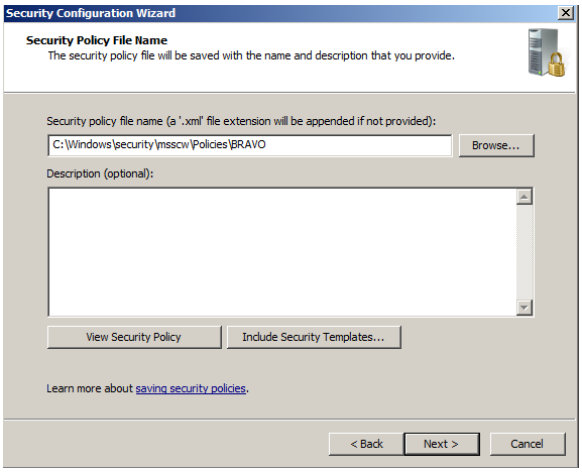


Figure 6: Append ‘BRAVO’ to the path

33. Select the option to ‘Apply Now’ and then click ‘Next’.
34. Once the wizard has completed the necessary changes, click ‘Next’, then click ‘Finish’.
35. Reboot the server.

Charlie High Level Description

Charlie is the network's WSUS server, which offers a "patch management" solution to the network. Moreover, it is also the File and Print server of the network.

The students will protect Charlie from unauthorized public access by reducing unnecessary services and limiting network connectivity. It will further be configured to send logs to the remote syslog server over an encrypted channel and will have host-based IDS and firewall.

Following are descriptions of Charlie's specific hands-on tasks that students must complete:

Task 1. Windows Host System Hardening

The network interface will be hardened by removing Internet Protocol (IP) version 6 and disabling NetBIOS name resolution. Students will follow security best practices to harden.

Task 2. Configuring WSUS

Software patches are downloaded to this server and then pushed out to the rest of the network on a scheduled basis. This eliminates the need to trust users to apply current patches to the many hosts that make up the network. It also reduces Internet bandwidth demands by downloading all patches to only one host on the network instead of every host downloading patches individually.

Task 3. Implementing WSUS with Group Policy for Member Servers

Students will create and edit a new Active Directory group policy object that enables member servers to update themselves with critical patches, hotfixes, and service packs by connecting to the aia.class Windows Server Update Services (WSUS) server-- Charlie.

Task 4. Implementing WSUS with Group Policy for Workstations

Students will create and edit a new Active Directory group policy object that enables workstations to update themselves with critical patches, hotfixes, and service packs by connecting to the aia.class WSUS server-- Charlie.

Task 5. Implementing WSUS with Group Policy for Domain Controllers

Students will create and edit a new Active Directory group policy object that enables domain controllers to update themselves with critical patches, hotfixes, and service packs by connecting to the aia.class WSUS server-- Charlie.

Task 6. Configuring OSSEC Agent

Students will install and configure OSSEC Agent, which will then send information about security events to the syslog/OSSEC server (Foxtrot).

Task 7. Windows Security Configuration Wizard

The Windows SCW wizard will take students through a series of questions which will help them harden the server as per industry best practices. Unnecessary services will be disabled, the windows firewall is configured, and if necessary IIS will be hardened.

Windows Server Baseline Hardening Steps

1 Harden Network Interfaces

1.1 Remove Unnecessary Protocols

By default, Microsoft Windows network interfaces are enabled with unnecessary protocols and services. These should be unbound from the interface (if not uninstalled completely). If your server is intended to provide these services, obviously you would NOT disable it.

1. If you have not already done so, log on to the machine using:
   Username: **AIACLASS\Administrator** Password: **tartans@1**
2. Open the 'Start' menu and right-click on 'Network' and select 'Properties' to open the 'Network and Sharing Center'.
3. Click on the 'Local Area Connection 2' and then click 'Properties'.
4. Clear the box next to 'Internet Protocol Version 6 (TCP/IPv6)'. Then click 'OK'.

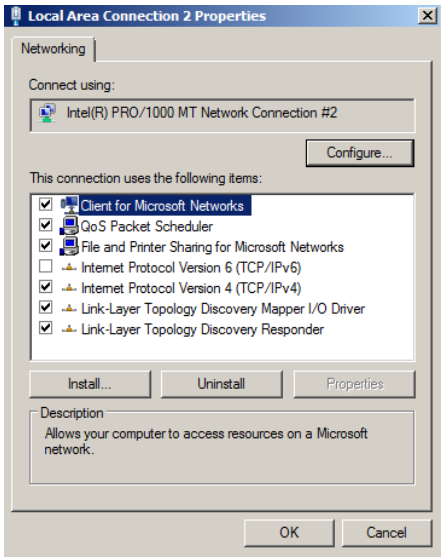


Figure 1: Remove IPv6

2 Harden TCP/IP Properties

2.1 Disable NetBIOS name resolution

As part of our defense-in-depth strategy, it is import to minimize even those parts of the environment that are normally not utilized. Since our network will be entirely native mode Windows 2000 or higher, NetBIOS name resolution would not normally be utilized, however we will eliminate the possibility of it being used altogether (NetBIOS name resolution is chatty and can divulge network information).

1. If the Properties window for your Local Area Connection is not still open, open it by following steps 1 and 2 from the section above.
2. From within the ‘Properties’ of your ‘Local Area Connection’, select the ‘Internet Protocol Version 4 (TCP/IPv4)’ item (leave it checked), and click on the ‘Properties’ button, then click the ‘Advanced’ button.
3. Next click on the ‘WINS’ tab at the top of the window.

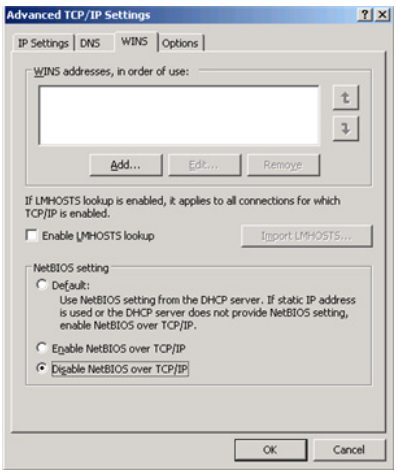


Figure 2: Minimize NetBIOS services

4. Uncheck ‘Enable LMHOSTS lookup’.
5. Select the radio button ‘Disable NetBIOS over TCP/IP’.
6. Click ‘OK’ to accept these settings.
7. Click ‘OK’ to confirm all ‘TCP/IP Properties’ changes.
8. Click ‘OK’ to confirm all ‘Local Area Connection Properties’ changes.
9. Close the ‘Local Area Connection 2 Properties’ and ‘Status’ windows.
10. Close the ‘Network and Sharing Center’ to return to the Desktop.

3 Install ClamWin for Anti-Virus Protection

3.1 Installation

1. Open the Course CD by clicking ‘Start’ -> ‘Computer’, right click ‘CD Drive (D:) AISTS’ and select ‘Open’.
2. Navigate to ‘Tools\Windows\ClamWin’ and double-click the ‘clamwin-0.96.1-setup’ icon.
3. Click ‘Next’.

Figure 3: Install ClamWin Antivirus

4. Accept the license agreement and click ‘Next’.

5. Accept the default option to install for ‘Anyone who uses this computer (all users)’ and click ‘Next’.
6. Select the default installation path and click ‘Next’.
7. At the ‘Select Component’s prompt, accept the default option of ‘Typical Installation’ and click ‘Next’.
8. Click ‘Next’ to create the default start menu folder.
9. Uncheck ‘Download Virus Database Files’ and click ‘Next’.

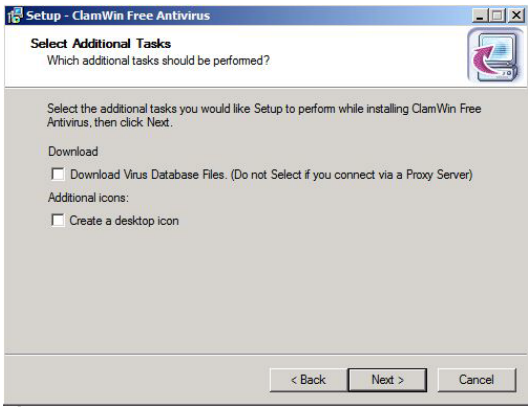


Figure 4: ClamWin Setup

10. Click ‘Install’ to install the program.
11. Click ‘Finish’ to complete the installation.
12. Close Windows Explorer.

3.2 Configuration

1. Click the upward facing arrow in the taskbar and then double-click on the ClamWin icon.

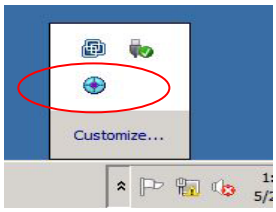


Figure 5: ClamWin Icon

2. Choose ‘No’ if asked to update the virus database.
3. Select ‘Tools’ from the menu, and click on ‘Preferences’.

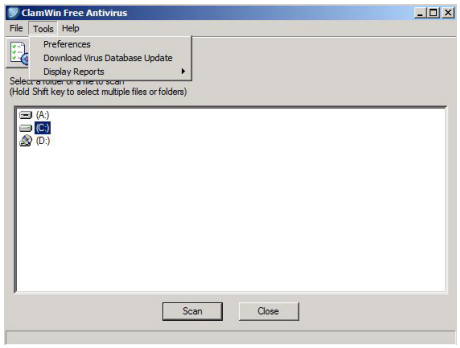


Figure 6: ClamWin Configuration

4. Click on the ‘Internet Updates’ tab. Leave the

updates to be done daily, but change the time to 2:30:00 AM.

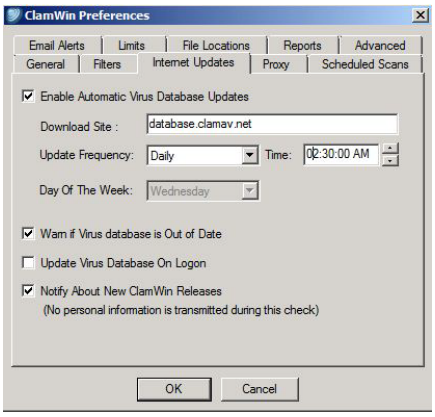


Figure 7: ClamWin Internet Updates

5. Click on the 'Scheduled Scans' tab. Click 'Add'. Choose the scanning frequency to be done Daily at 3:30:00 AM. Enter `C:\` as the folder to scan. Enter a description, such as `Nightly Virus Scan`. Click 'OK'.

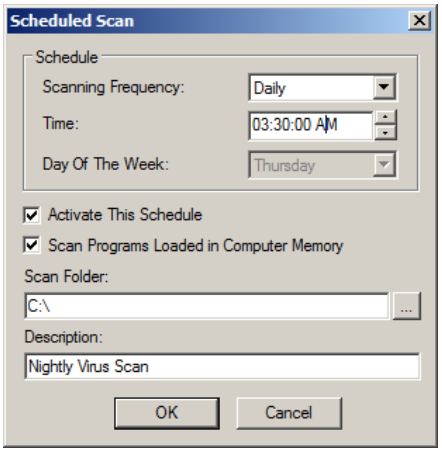


Figure 8: ClamWin Scheduled Scan

6. Click on the 'Email Alerts' tab. Check the box labeled 'Send Email On Virus Detection'. Enter in the following information:

   Mail Server – `10.0.2.3`

   From – `clamwin@Charlie`

   To – `eventwatch@aia.class`

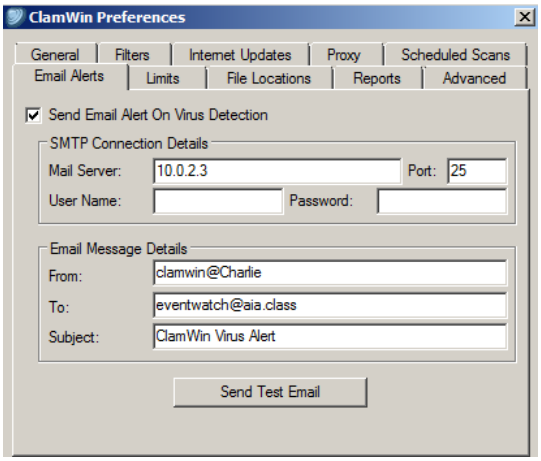


Figure 9: ClamWin Email Alerts

7. Click on the ‘Proxy’ tab. Enter in the IP address of the Squid Proxy server, Quebec, which is **10.0.2.1**. Ensure that the port is **3128**.

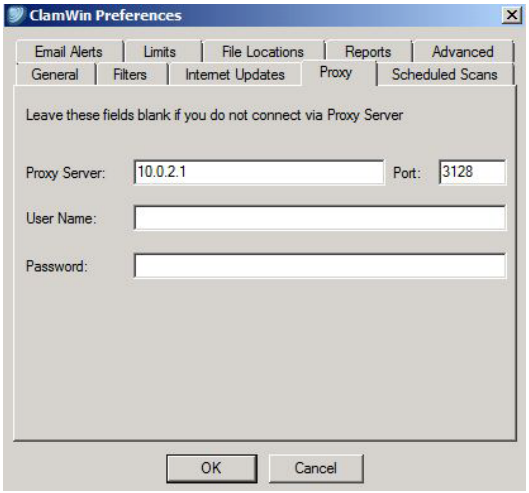


Figure 10: ClamWin Proxy Settings

8. Click ‘OK’ to accept all changes.
9. Choose ‘No’ if asked to update the virus database.
10. Click ‘Close’ to close the ClamWin window.

This page left intentionally blank for pagination purposes

Windows Software Update Services

This task will install and configure the Windows Server Update Services (WSUS) from Microsoft to manage patches on the user network and the administrative (management) systems. Windows Software Update Services (WSUS) is a free utility available from Microsoft that allows administrators to centrally manage software patching of Windows systems. It is available for download at: http://www.microsoft.com/wsus

Group Policies allow administrators to configure computer settings and user rights and permissions with extremely granular controls. Windows also allows you to standardize windows update configurations on computers by applying these group policies. In later tasks you will create Member Servers and Workstation groups within a Windows Active Directory and then configure WSUS with a unique update policy for these computer groups.

1 Install WSUS

1. Open the Course CD by clicking 'Start' -> 'Computer', right click 'CD Drive (D:) AISTS' and select 'Open'.
2. Navigate to 'Tools\Windows\WSUS' and double click on 'WSUS30-KB972455-x64' to install the WSUS on the PC.
3. Click 'Next' on the welcome screen.
4. Leave the default settings for Installation Mode Selection window as 'Full Server installation including Administration Console' and click 'Next'.
5. 'Accept' the terms of License agreement and click 'Next'.
6. Click 'Next' on the required Components to use administration UI window.
7. For Update Source, ensure Store updates locally' is checked, Select **`C:\WSUS`** for the installation path and click 'Next'. (Note: 6GB Free Disk Space volume required)
8. Leave the default settings for Database Options and click 'Next'.
9. Use the default setting for Website preference as 'Use the existing IIS Default Web Site' and click 'Next'.
10. Click 'Next' to install.
11. Once the installation is complete, click 'Finish'.
12. Open the WSUS configuration interface by clicking 'Start' -> 'Administrative Tools' -> 'Windows Server Update Services'.

2 Initial WSUS synchronization

2.1 Synchronization settings

1. Click ‘Cancel’ if the Welcome Wizard opens.
2. Navigate through ‘Update Services’ -> ‘CHARLIE’ -> ‘Options’.

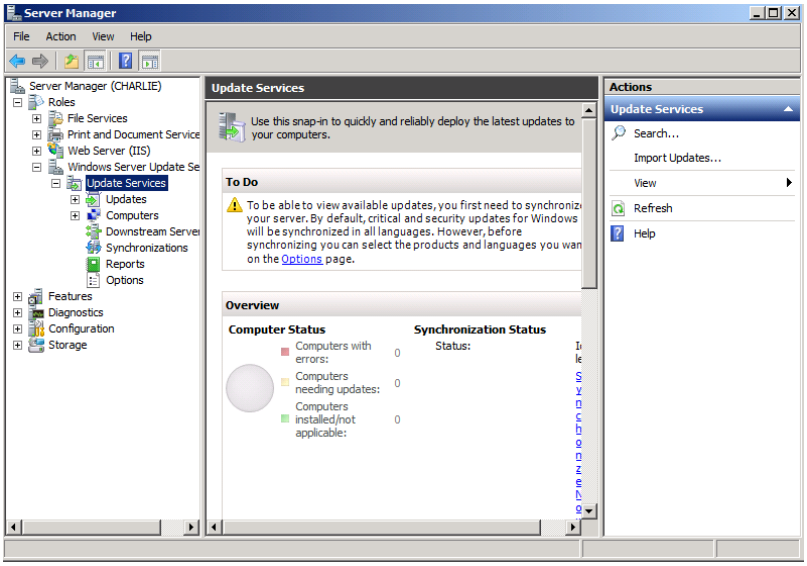


Figure 1: Update Services Management window

3. Select ‘Synchronization Schedule’.
4. Click on ‘Synchronize automatically’ and accept the default timings.

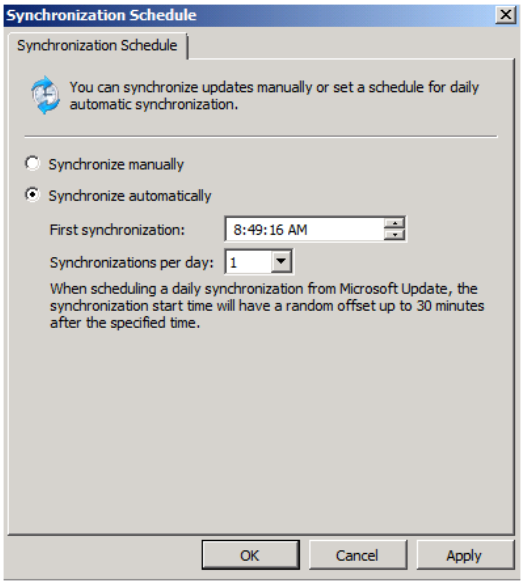


Figure 2: Setting up the synchronization

5. Click on ‘Apply’ and then ‘OK’ to close the window.
6. Select ‘Update Files and Languages’.

7. In the ‘Update Files’ settings, ensure that ‘Store update files locally on this server’ is selected. Underneath that, ensure ‘Download update files to this server only when updates are approved’.
8. Move onto ‘Update Languages’ tab.
9. Select ‘Download updates only in these languages:’. Click ‘OK’ on the prompt.
10. Check ‘English’ and click ‘OK’.

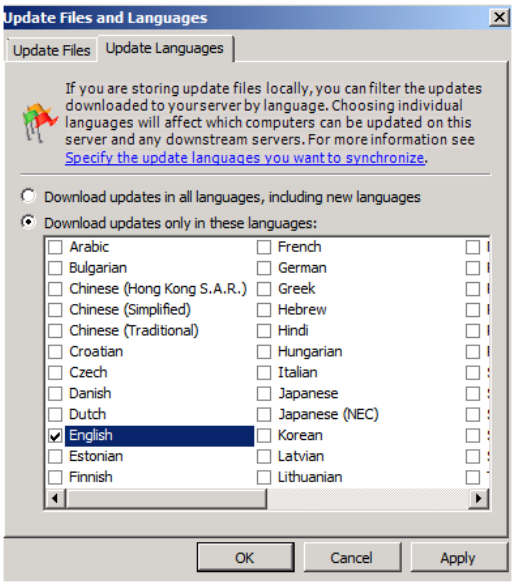


Figure 3: Language Settings

11. Click on ‘Update Source and Proxy Server’.
12. Click on ‘Proxy Server’ tab.
    a. Check ‘Use a proxy server when synchronizing’
    b. Server name: **10.0.2.1**
    c. Port number: **3128**

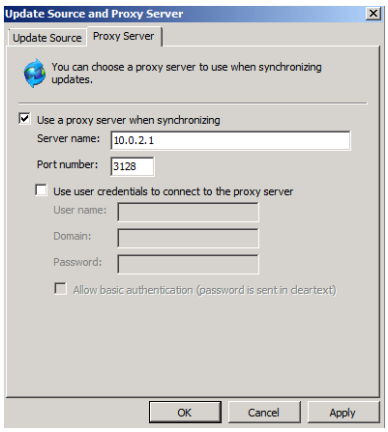


Figure 4: Proxy Server Settings

13. Click the ‘Update Source’ tab. Select ‘Synchronize from another Windows Server Update Services server’.
    - Server Name: **192.168.30.14**
    - Port number: **80**

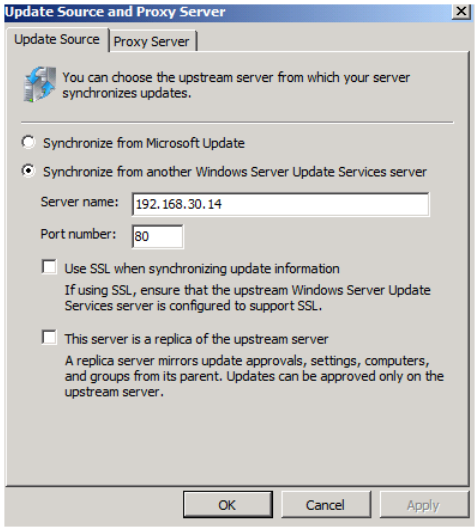


Figure 5: Update Source Settings

Note: WSUS can synchronize updates using several methods, including an upstream WSUS server. Alternately synchronization can happen directly with Microsoft servers, or even imported from an off-line repository if the local WSUS server is not connected to the Internet. To minimize the amount of time required to update Charlie we will use a *chained server deployment* and select an upstream WSUS server.

When updating from an upstream WSUS server, the Products, Categories, and Advanced options are unavailable. Instead these settings are inherited from the upstream server.

14. Click ‘OK’.

2.2 Configuring WSUS

By default, each computer is already assigned to the All Computers group. Computers will also be assigned to the Unassigned Computers group until you assign them to another group. Regardless of the group you assign a computer, it will also remain in the All Computers group. A computer can be in only one other group in addition to the All Computers group.

You can assign computers to computer groups by using one of two methods, *server-side* or *client-side targeting*. With server-side targeting, you use the ‘Move the selected computer’ task on the Computers page to move one or more client computers to one computer group at a time. With client-side targeting, you use Group Policy or edit the registry settings on client computers to enable those computers to automatically add themselves into the

computer groups. You must specify which method you will use by selecting one of the two options on the Computers Options page.

Regardless of the method you use to assign client computers to computer groups, you must first create the computer groups in the WSUS console. You do this by running the Create a computer group task on the Computers page in the WSUS console.

With ***server-side targeting***, you use the WSUS console to both create groups and then assign computers to the groups. Server-side targeting is an excellent option if you do not have many client computers to update, and you want to move client computers into computer groups manually.

With ***client-side targeting***, you enable client-computers to add themselves to the computer groups you create in the WSUS console. You can enable client-side targeting through Group Policy (in an Active Directory network environment) or by editing registry entries (in a non-Active Directory network environment) for the client computers. When the client computers connect to the WSUS server, they will add themselves into the correct computer group. Client-side targeting is an excellent option if you have many client computers and want to automate the process of assigning them to computer groups.

2.3 Enable client-side targeting

1. On the left panel, expand ‘Computers’ and then right click on ‘All Computers’.
2. Click on ‘Add Computer Group’.
3. Enter ‘**`Member Servers`**’ and click ‘Add’.

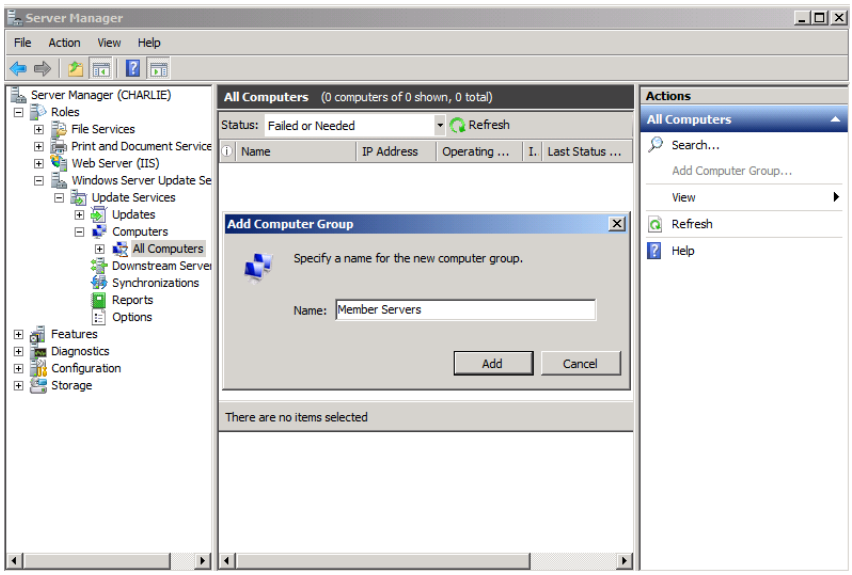


Figure 6: Adding a Computer Group

Note: This group name must match the name which will be the Organizational Unit name of the desired computers

4. Repeat step 2-3 to create Computer groups: **`Workstations`** and **`Domain Controllers`**.

5. Select the ‘Options’ on the left panel and click on ‘Computers’.
6. Select the ‘Use Group Policy or registry settings on computers’ option.

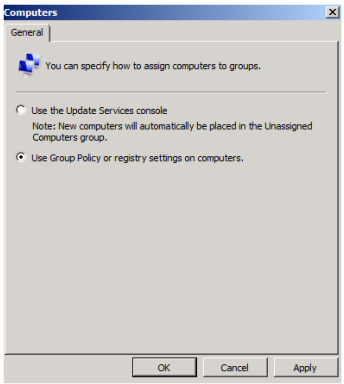


Figure 7: Configuring the settings to assign the computers

7. Click ‘OK’.

2.4 Configure automatic approval for Member Servers

1. Select the ‘Options’ on the left panel and click on ‘Automatic Approvals’.
2. Check the box for ‘Default Automatic Approval Rule’.
3. In the Rule Properties window, click on ‘all computers’.
4. Uncheck ‘Unassigned Computers’ and ‘Domain Controllers’.
5. Click ‘OK’.
6. Click ‘OK’ to close the Automatic Approvals window.

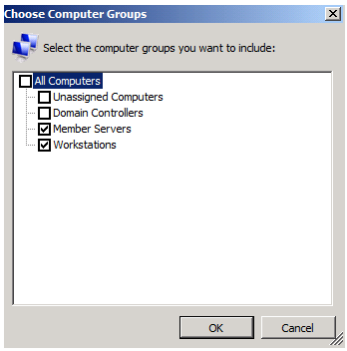


Figure 8: Selecting the Computer Groups

7. On the left panel, right click on ‘Synchronizations’ and select ‘Synchronize Now’ to synchronize with the upstream WSUS server.

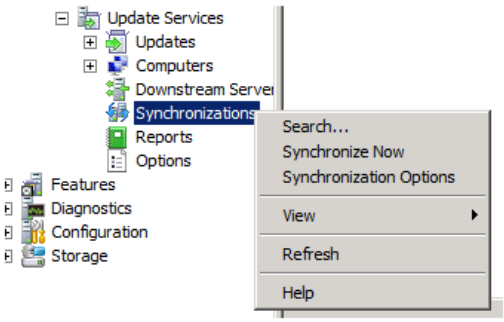


Figure 9: Start Synchronization

Implementing WSUS with Group Policy for Organizational Units(OUs)

1 Enable WSUS through Group Policy Object (GPO) for Member Servers Organizational Unit (OU)

1.1 Create new GPO and edit to enable WSUS

1. Login to Alpha using:
   Username: **AIACLASS\Administrator** Password: **tartans@1**.
2. On your management system, click 'Start' -> 'Administrative Tools' -> 'Group Policy Management'.
3. Expand the following: 'Forest:aia.class' -> 'Domains' -> 'aia.class' domain by clicking the '+' sign.
4. Right click on the 'Member Servers' OU and click on 'Create a GPO in this domain, and Link it here…'.
5. Type in '**`WSUS_Member Servers`**' as the name and click 'OK'.

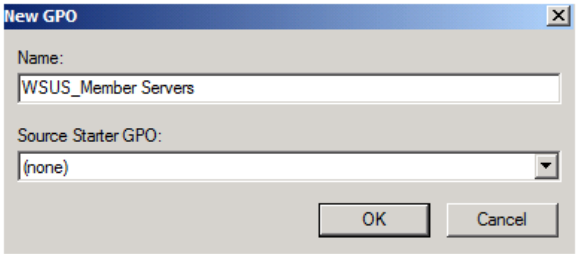


Figure 1: Create a new GPO

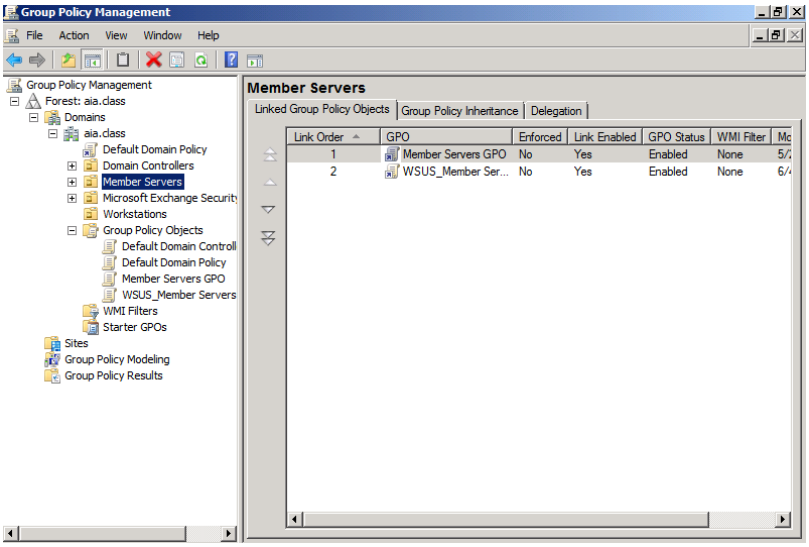


Figure 2: Member Servers OU

2 Configure WSUS Group Policy for Automatic Updates

2.1 Edit Windows Update Settings

1. Expand ‘Group Policy Objects’ and right click on ‘WSUS_Member Servers’ and click ‘Edit’.
2. On the left panel, expand through ‘Computer Configuration’ -> ‘Policies’ -> ‘Administrative Templates’ -> ‘Windows Components’ and select ‘Windows Update’.

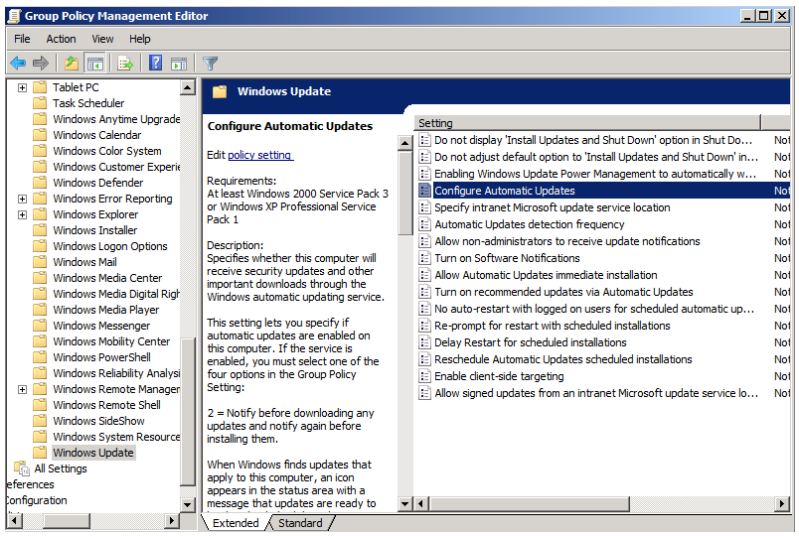


Figure 3: Configure WSUS Policy settings

3. Double click on ‘Configure Automatic Updates’.
4. Click the ‘Enabled’ radio button and select ‘4 – Auto Download and schedule the install’. Change the Scheduled install time to 04:00 and then click ‘Next Setting’.

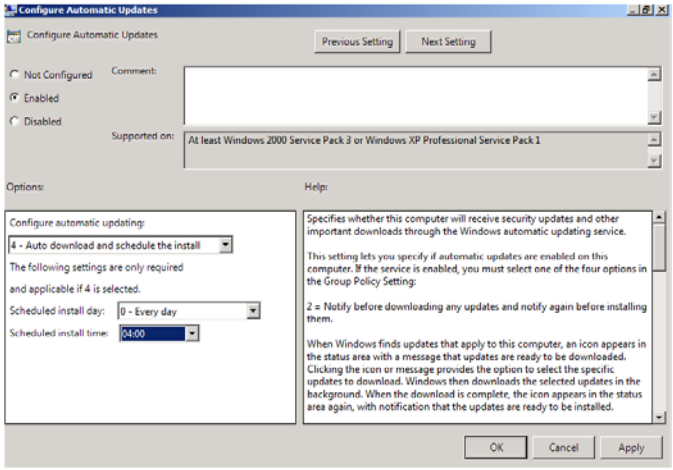


Figure 4: Configure Scheduled Updates/Installs

5. Now click on the 'Enabled' radio button and enter '`http://CHARLIE.aia.class`' in both location boxes. Then click 'OK'.

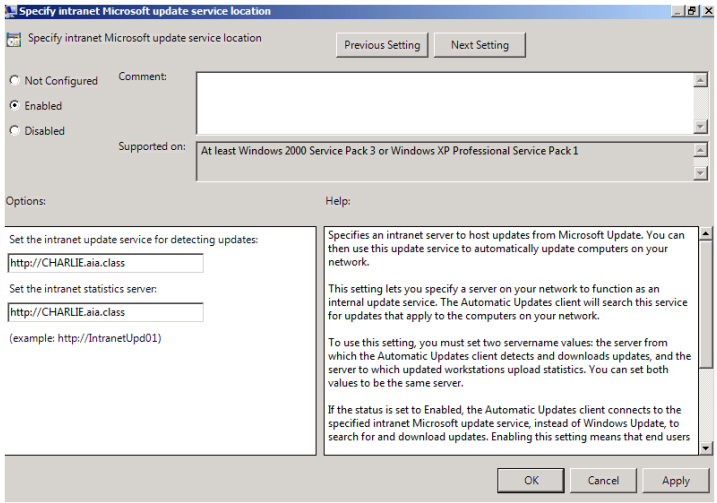


Figure 5: Configure location of SUS service

6. Click 'OK'.

7. From the list of settings, double click on 'Enable client-side targeting'.

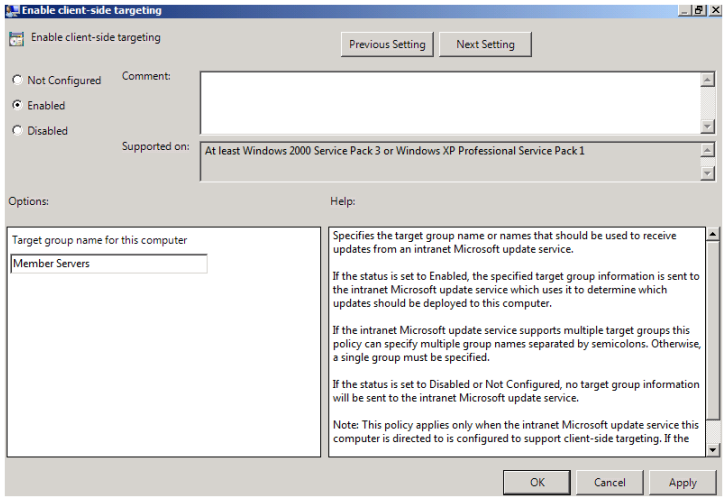


Figure 6: Configure client-side targeting group

8. Now click on the ‘Enabled’ radio button and enter `‘Member Servers’` in the target group name for this computer. This field is case sensitive and must match exactly the group name entered during the WSUS installation/configuration. Then click ‘OK’.

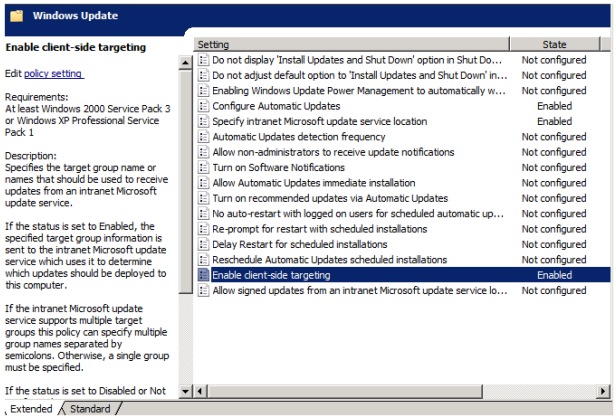


Figure 7: Final WSUS Policy settings

9. Close the Group Policy Management Editor and then close the Group Policy Management.

   Note: An alias record must be created in DNS to map http://Charlie.aia.class to the 10.0.2.6 Intranet server that happens to be running the WSUS service for this class. This has already been done by the instructors.

Implementing WSUS with Group Policy for Workstations

1 Enable WSUS through Group Policy Object (GPO) for Workstations Organizational Unit (OU)

1.1 Create new GPO and edit to enable WSUS

1. Login to Alpha
2. On your management system, click ‘Start’ -> ‘Administrative Tools’ -> ‘Group Policy Management’.
3. Expand the following: ‘Forest:aia.class’ -> ‘Domains’ -> ‘aia.class’ domain by clicking the ‘+’ sign.
4. Right click on the ‘Workstations’ OU and click on ‘Create a GPO in this domain, and Link it here..’
5. Type in **`‘WSUS_Workstations’`** as the name and click ‘OK’.

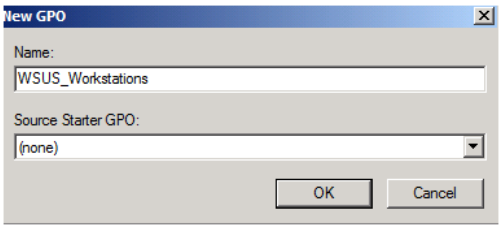


Figure 1: Create a new GPO

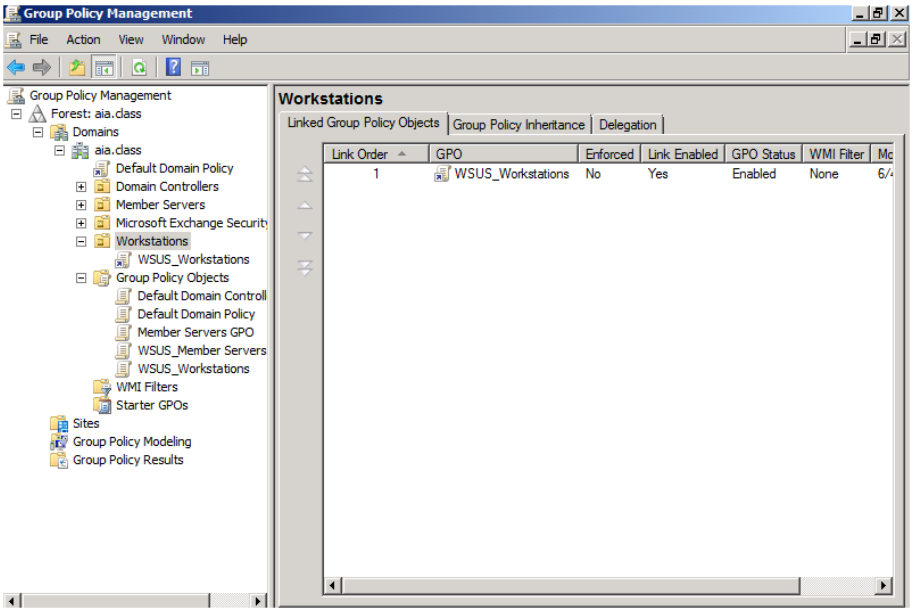


Figure 2: Workstations OU

2 Configure WSUS Group Policy for Automatic Updates

2.1 Edit Windows Update Settings

1. Expand ‘Group Policy Objects’, right click on ‘WSUS_Workstations’ and click ‘Edit’.
2. On the left panel, expand through ‘Computer Configuration’ -> ‘Policies’ -> ‘Administrative Templates’ -> ‘Windows Components’ and select ‘Windows Update’.

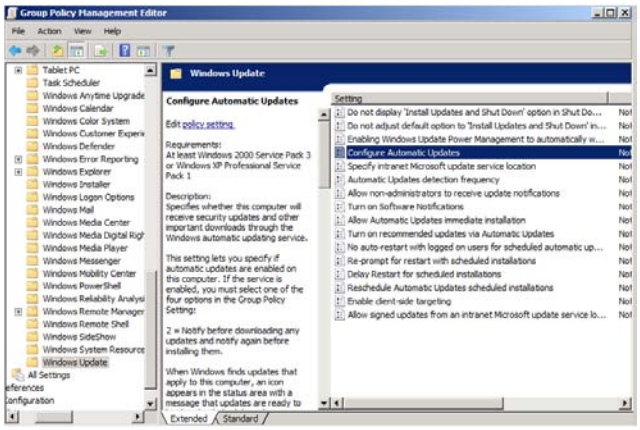


Figure 3: Configure WSUS Policy settings

3. Double click on ‘Configure Automatic Updates’.
4. Click the ‘Enabled’ radio button and select ‘4 – Auto Download and schedule the install’. Change the Scheduled install time to 04:00 and then click ‘Next Setting’.

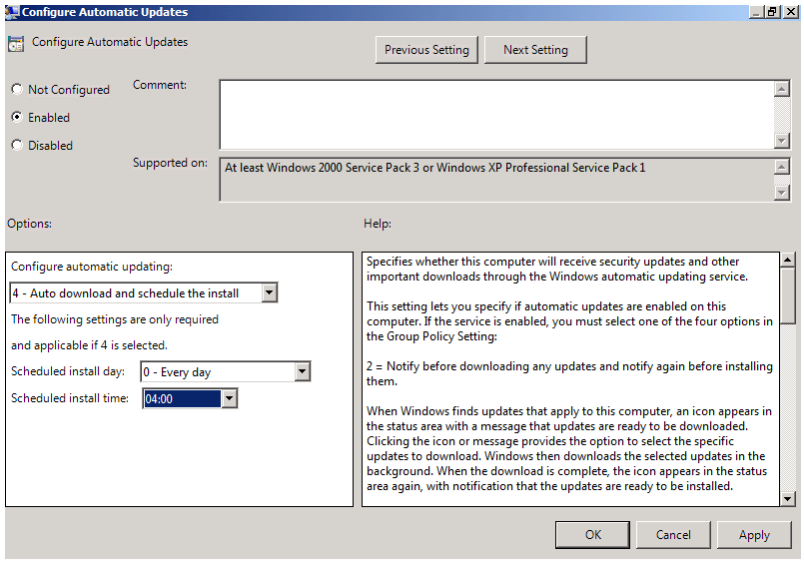


Figure 4: Configure Scheduled Updates/Installs

5. Now click on the 'Enabled' radio button and enter **`'http://CHARLIE.aia.class'`** in both location boxes. Then click 'OK'.

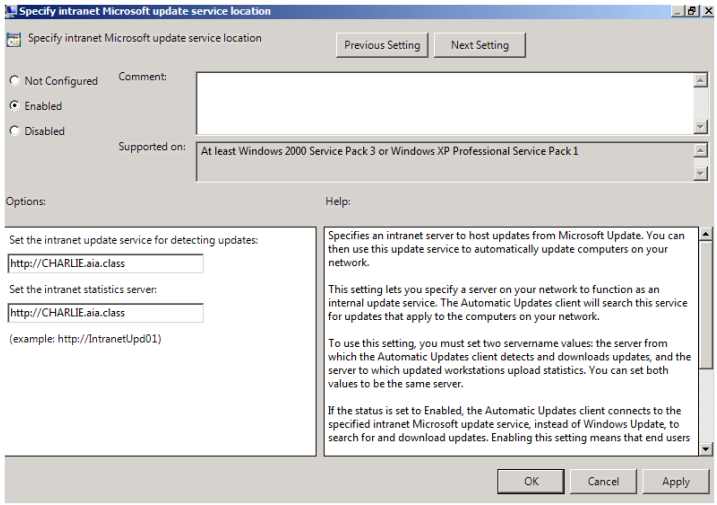


Figure 5: Configure location of SUS service

6. Click 'OK'.

7. From the list of settings, double click on 'Enable client-side targeting'.

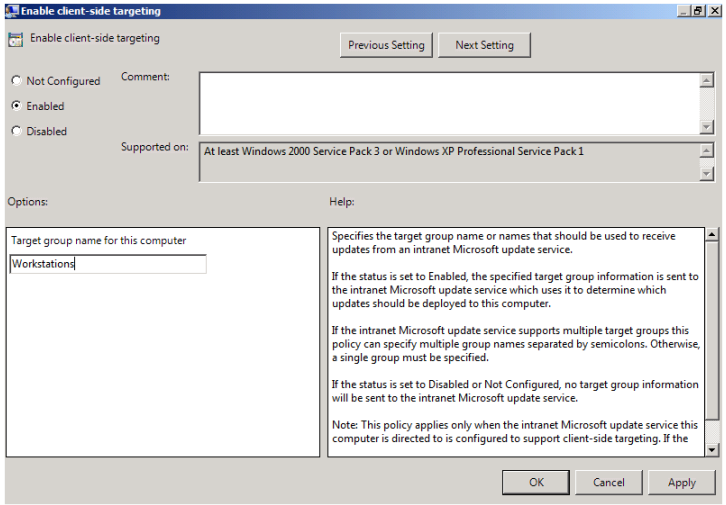


Figure 6: Configure client-side targeting group

8. Now click on the 'Enabled' radio button and enter **`'Workstations'`** in the target group name for this computer. This field is case sensitive and must match exactly the group name entered during the WSUS installation/configuration. Then click 'OK'.

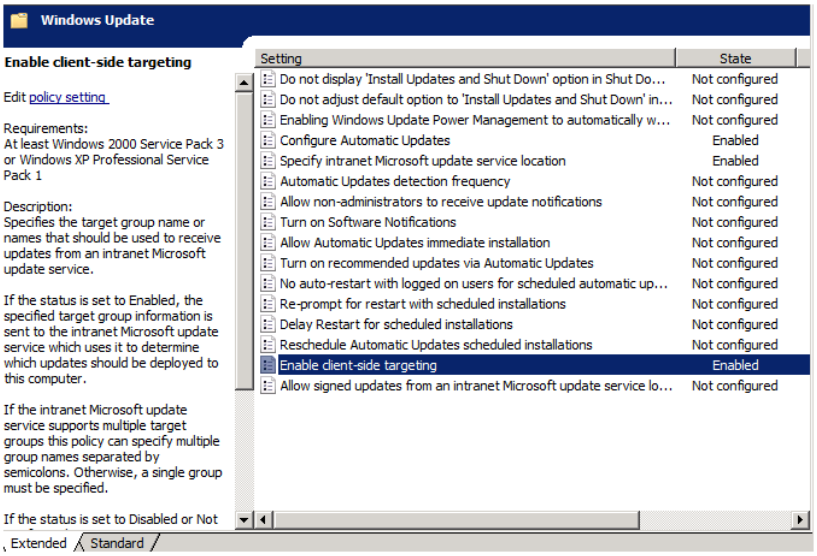


Figure 7: Final WSUS Policy settings

9. Close the Group Policy Management Editor and then close the Group Policy Management.

   Note: An alias record must be created in DNS to map http://Charlie .aia.class to the 10.0.2.6 Intranet server that happens to be running the WSUS service for this class. This has already been done by the instructors.

Implementing WSUS with Group Policy for Domain Controllers

1 Enable WSUS through Group Policy Object (GPO) for Domain Controllers Organizational Unit (OU)

1.1 Create new GPO and edit to enable WSUS

1. Login to Alpha.
2. On your management system, click ‘Start’ -> ‘Administrative Tools’ -> ‘Group Policy Management’.
3. Expand the following: ‘Forest:aia.class’ -> ‘Domains’ -> ‘aia.class’ domain by clicking the ‘+’ sign.
4. Right click on the ‘Domain Controllers’ OU and click on ‘Create a GPO in this domain, and Link it here…’.
5. Type in ‘WSUS_DC’ as the name and click ‘OK’.

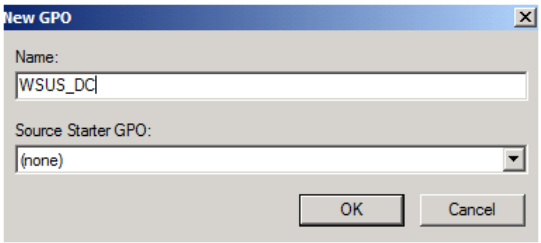


Figure 1: Create a new GPO

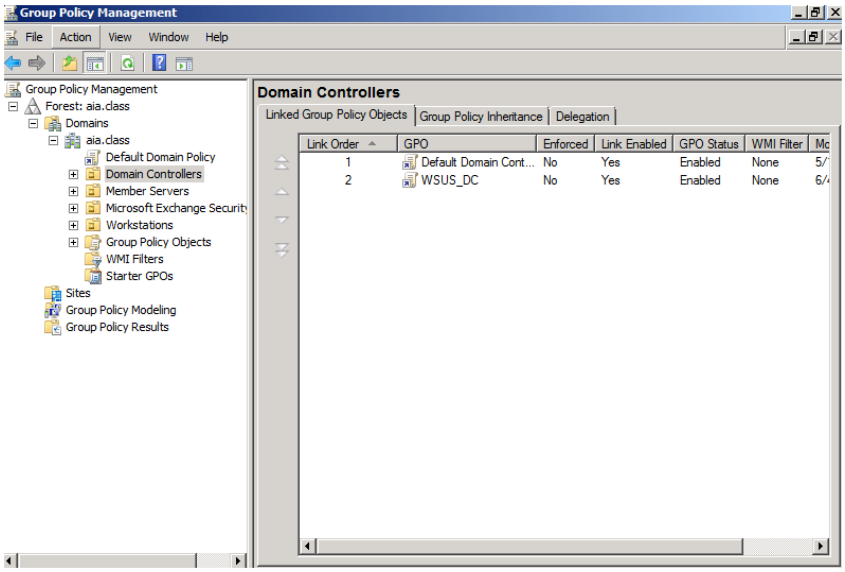


Figure 2: Domain Controllers OU

2 Configure WSUS Group Policy for Automatic Updates

2.1 Edit Windows Update Settings

1. Expand ‘Group Policy Objects’, right click on ‘WSUS_DC’ and click ‘Edit’.
2. On the left panel, expand through ‘Computer Configuration’ -> ‘Policies’ -> ‘Administrative Templates’ -> ‘Windows Components’ and select ‘Windows Update’.

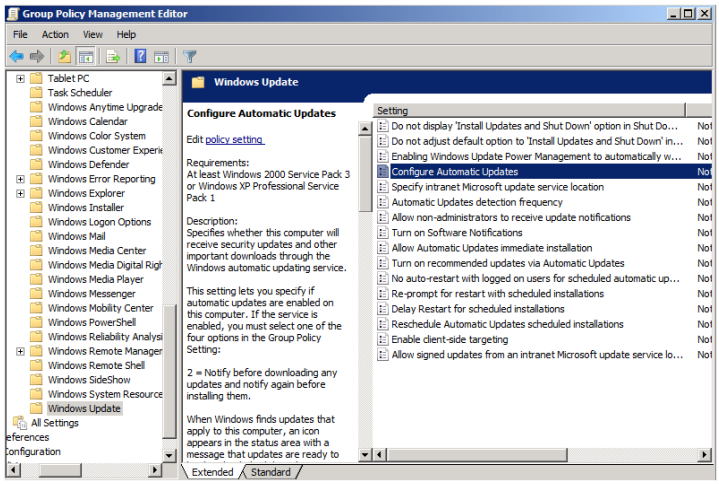


Figure 3: Configure WSUS Policy settings

3. Double click on ‘Configure Automatic Updates’.
4. Click the ‘Enabled’ radio button and select ‘4 – Auto Download and schedule the install’. Change the Scheduled install time to 04:00 and then click ‘Next Setting’.

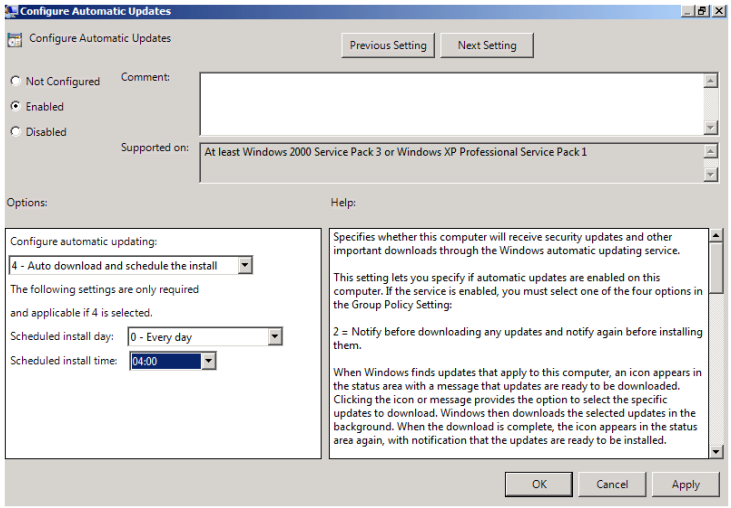


Figure 4: Configure Scheduled Updates/Installs

5. Now click on the ‘Enabled’ radio button and enter `‘http://CHARLIE.aia.class’` in both location boxes. Then click ‘OK’.

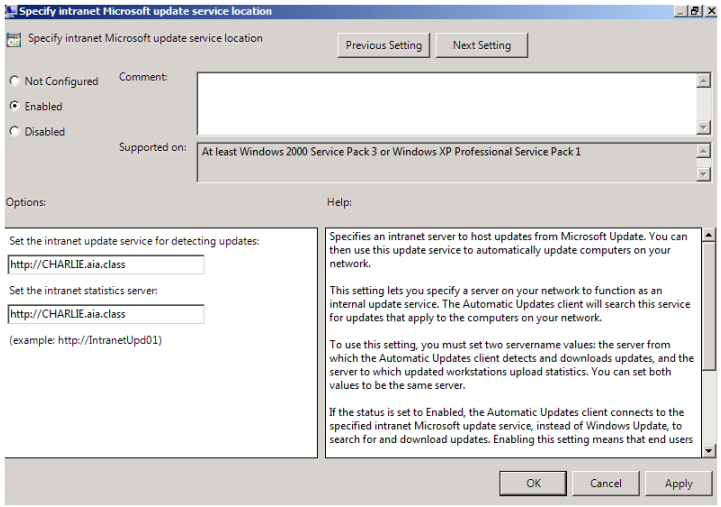


Figure 5: Configure location of SUS service

6. Click ‘OK’.

7. From the list of settings, double click on ‘Enable client-side targeting’.

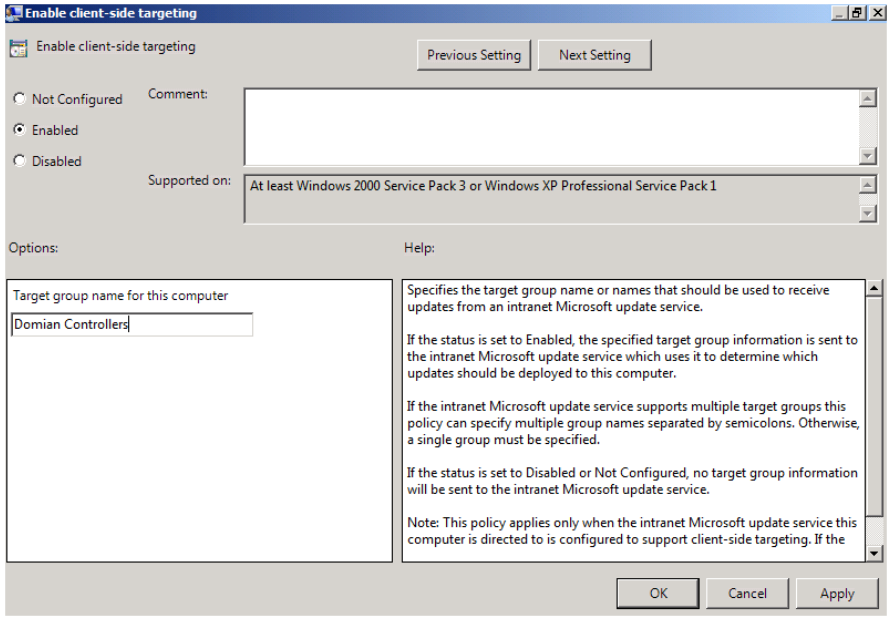


Figure 6: Configure client-side targeting group

8. Now click on the 'Enabled' radio button and enter **'Domain Controllers'** in the target group name for this computer. This field is case sensitive and must match exactly the group name entered during the WSUS installation/configuration. Then click 'OK'.

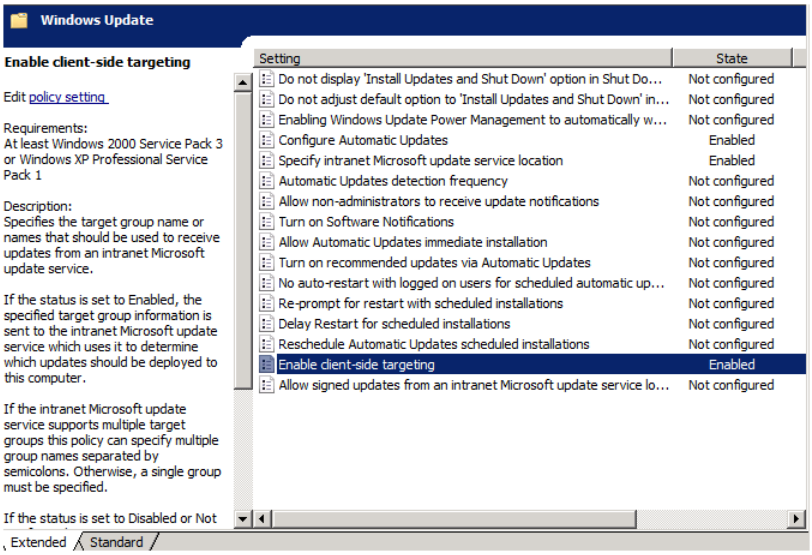


Figure 7: Final WSUS Policy settings

9. Close the Group Policy Management Editor and then close the Group Policy Management.

   Note: An alias record must be created in DNS to map http://Charlie .aia.class to the 10.0.2.6 Intranet server that happens to be running the WSUS service for this class. This has already been done by the instructors.

Open Source Security (OSSEC) Agent

OSSEC agents will be installed on each Linux and Windows server and will send events to the OSSEC server that is running on Foxtrot. The OSSEC server processes events and generates warnings from alerts sent by the agents. *Before installing any OSSEC agents, make sure that you have successfully deployed the OSSEC server on Foxtrot.*

1 OSSEC Agent setup

1.1 Installation

1. Open Windows Explorer and navigate to 'D:\Tools\Windows\OSSEC':

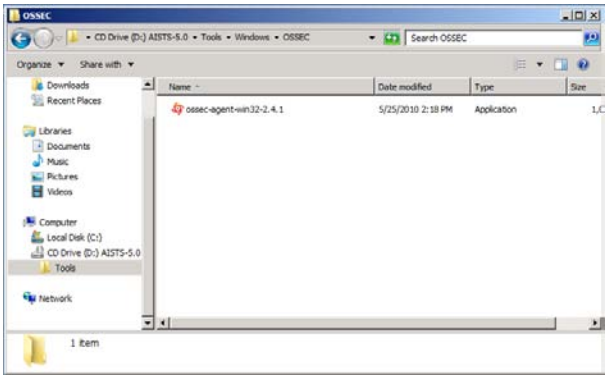


Figure 1: Setup File

2. Double click on the 'ossec-agent-win32-2.4.1' setup file and start the installation:

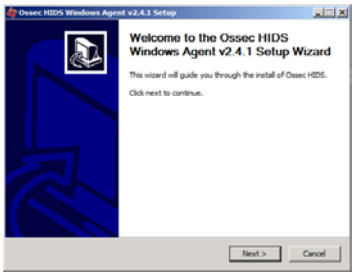


Figure 2: Welcome Screen of OSSEC Installation

3. Click 'Next' and accept the license agreement by pressing the 'Agree' button:

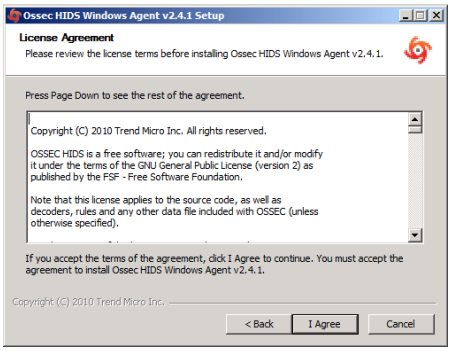


Figure 3: License Agreement window

4. Accept the default installation options and click ‘Next’:

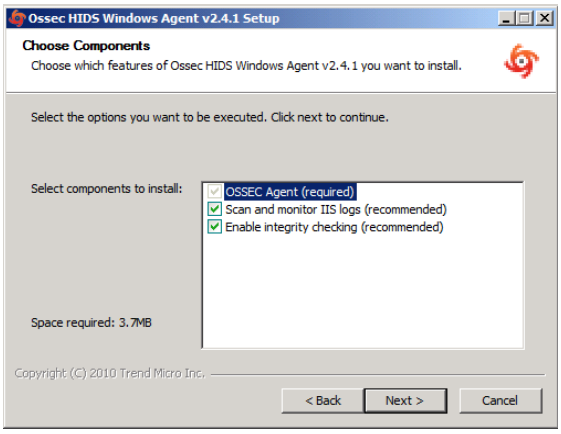


Figure 4: Choose default settings for components

5. Proceed with the installation by pressing the ‘Install’ button:

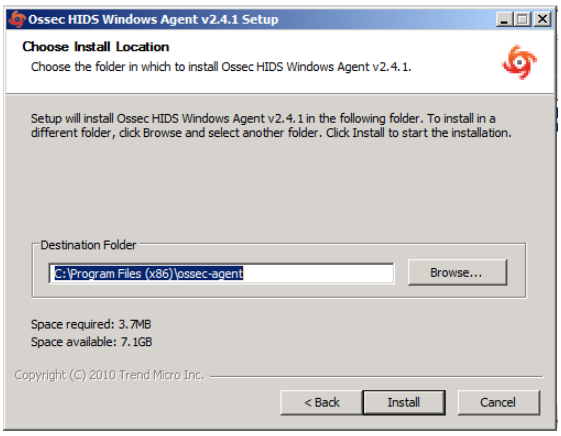


Figure 5: Location path

6. After the installation has finished you should see following screen. Complete the installation by clicking on ‘Finish’:

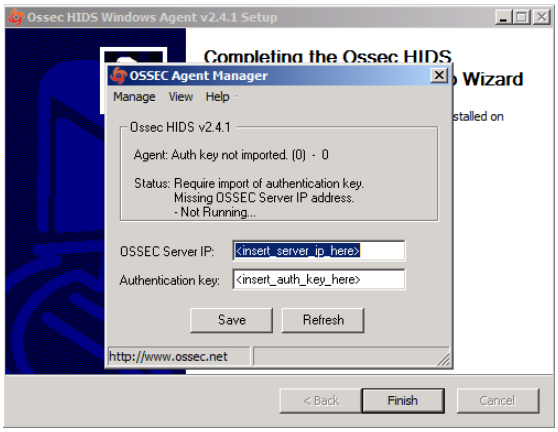


Figure 6: End of OSSEC installation

1.2 Configuration

1. Now we are going to setup a shared key between Charlie and Foxtrot. In order to do this, go back into the CD contents and execute 'Putty' from 'D:\Tools\Windows\Putty'
2. Enter `10.0.4.2` (Foxtrot's IP Address) in the 'Host Name' field and click 'Open':

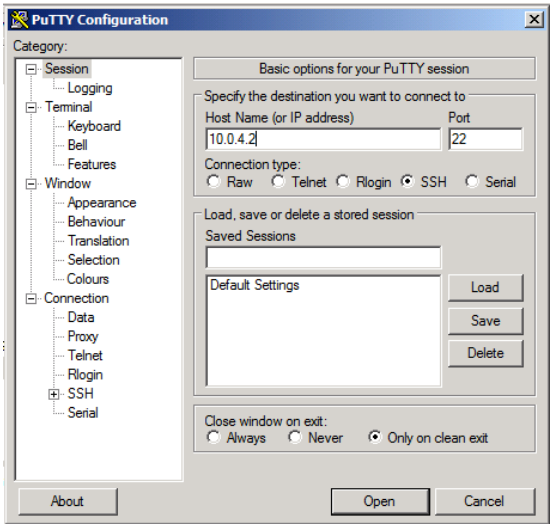


Figure 7: Setting up Putty

3. Accept the warning by clicking 'Yes':

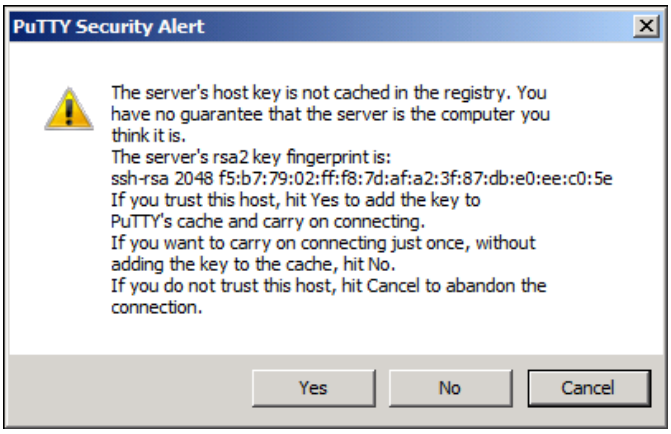


Figure 8: Accept the warning

4. Type **`root`** as the login name and press `[Enter]` then type **`tartans@1`** as the password and press `[Enter]`:

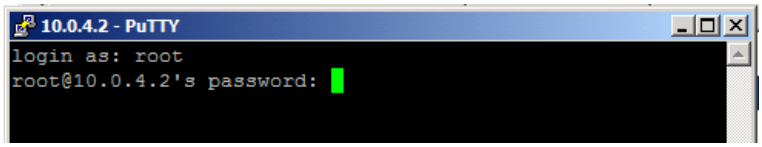


Figure 9: Login

5. Once logged into Foxtrot, start the OSSEC agent manager by executing the following command:

```
# /var/ossec/bin/manage_agents
```

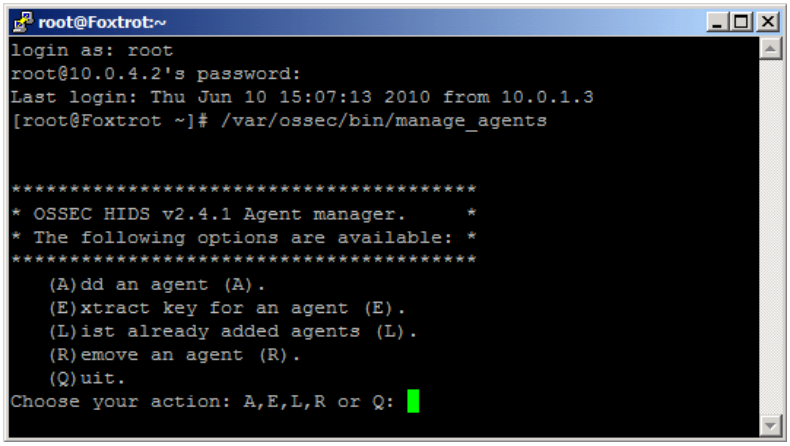


Figure 10: OSSEC Agent Manager window

6. Add an agent by typing A and pressing `[Enter]`.
7. Enter Charlie's information as shown below and press `[Enter]`:

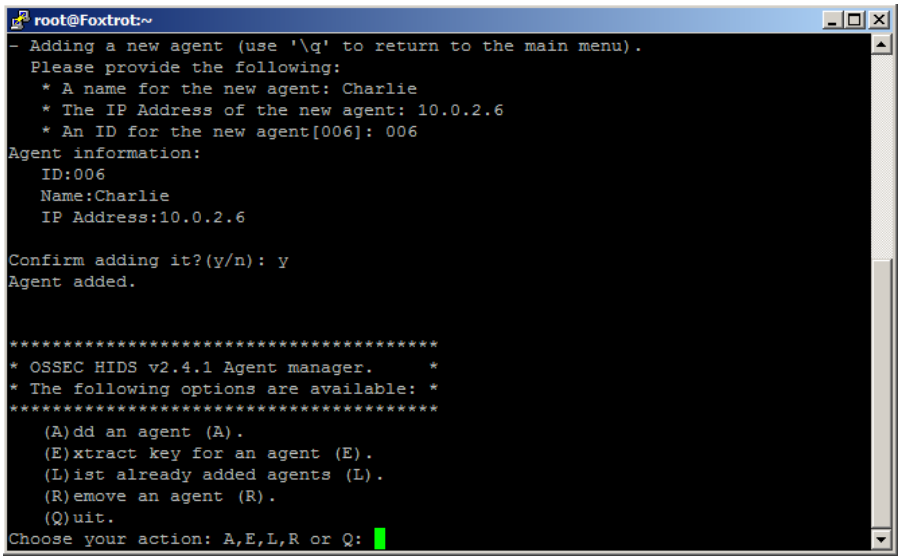


Figure 11: Select an option

8. Now type `E` and press `[Enter]` to extract the shared key for Charlie, and enter `006` when the OSSEC agent manager asks for an agent ID. Please note that key will not be the same as shown in the following screenshot, because the shared key is generated randomly each time an OSSEC agent is added:

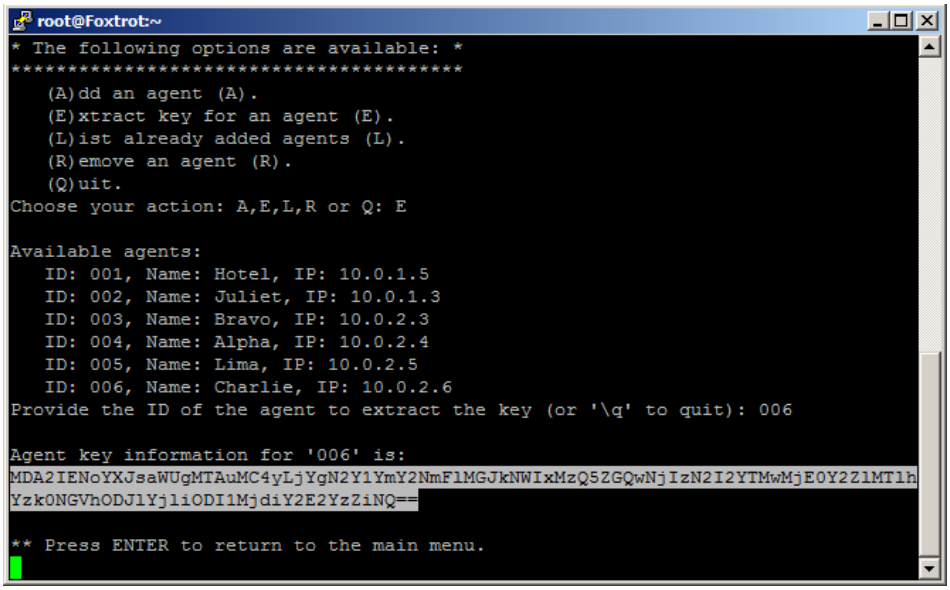


Figure 12: Random key generated

9. Copy the shared key by highlighting it and paste it into the OSSEC Agent Manager as shown below.

10. Enter `10.0.4.2` as the server address and then click ‘Save’ then ‘OK’:

Figure 13: Enter the parameters

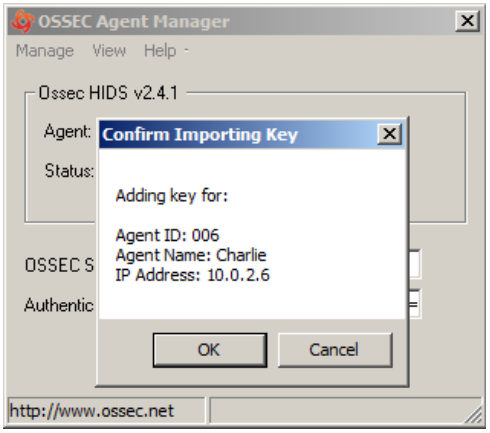


Figure 14: Confirm the settings

11. Choose ‘Manage -> Start OSSEC’ to start the OSSEC agent:

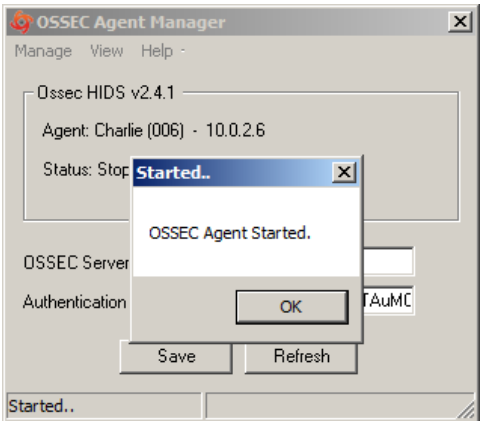


Figure 15: Starting OSSEC

12. Switch back to the Putty SSH command shell window. Type `Q` then press `[Enter]` to quit from the agent manager and type `exit` and press `[Enter]` to end the SSH session and exit from Putty.
13. Close the OSSEC Agent Manager and Windows Explorer,
14. Click ‘Finish’ to close the OSSEC wizard.

Windows Security Configuration Wizard

1 Run the SCW

1. Click ‘Start’ -> ‘Administrative Tools’ -> ‘Security Configuration Wizard’
2. Click ‘Next’, on the Welcome screen
3. Click ‘Next’, to Create a new Security Policy

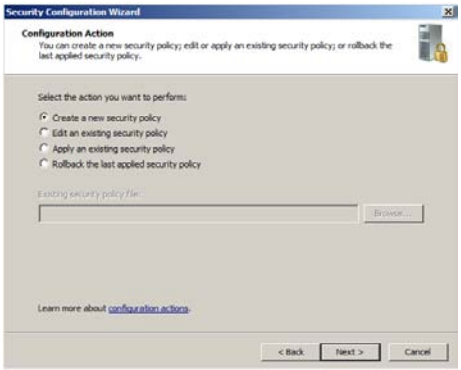


Figure 1: Create a new security policy

4. Click ‘Next’**,** on the Select Server dialog. We will not be importing a configuration from a different server.
5. Once the Processing of the Security Configuration Database is complete click ‘Next’ to continue.
6. Click ‘Next’, on the Role-Based Service Configuration dialog.
7. A list of currently installed roles will be presented. For ‘Charlie’, Select ‘All roles’ from the ‘View’ menu and then select only the following server roles:
    - ‘ASP.NET State Service’
    - ‘DFS Namespace’
    - ‘DFS Replication’
    - ‘File Server’
    - ‘File Server Resource Manager’
    - ‘Volume Shadow Copy’
    - ‘Web Server’
    - ‘Windows Process Activation Service’
    - ‘Windows System Resource Management’
8. Click **‘**Next’.

9. For our domain servers the default client settings are appropriate. These enable necessary services for accessing internal and Internet servers. Click ‘Next’.

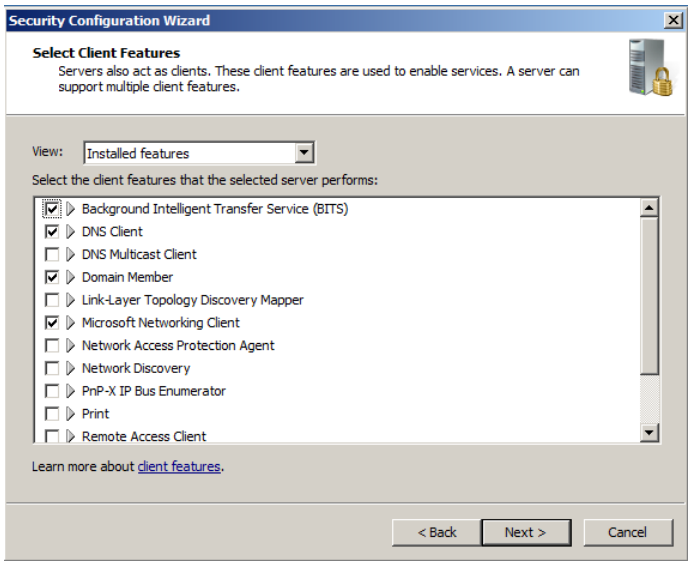


Figure 2: Client Features Settings

10. Administration and Other Options, select:
    - ‘Application Experience Lookup Service’
    - ‘Browse Master’
    - ‘Error reporting’
    - ‘Local application installation’
    - ‘Performance Logs and Alerts’
    - ‘Remote Desktop’
    - ‘Windows User Mode Driver Framework’

    Click ‘Next’.
11. Additional Services, select only:
    - ‘OSSEC Hids’
    - ‘Update Services’
    - ‘WSusCertServer’

    Click ‘Next’.
12. Accept the default option of ‘Do not change the startup mode of the service’ for any unspecified services. Click ‘Next’.
13. Review the list of service changes before clicking ‘Next’.
14. Click ‘Next’ to begin the Network Security Configuration.

15. The SCW attempts to identify the necessary ports that the server will need open for your previous selections. However, we will minimize even further by disabling unnecessary rules. Uncheck the following:
    - Core Networking – Ipv6 (IPv6-In)
    - Core Networking – Ipv6 (IPv6-Out)
16. Click ‘Next’.
17. Click ‘Next’ to begin the ‘Registry Wizard’.
18. Click ‘Next’, to accept the default SMB security settings.
19. Click ‘Next’ to confirm the default Outbound Authentication Methods.
20. Click ‘Next’ to confirm the requirement for Domain Account authentication for outbound connections.
21. Click ‘Next’ to confirm that we are using domain controllers that use the necessary LAN Manager Authentication level.

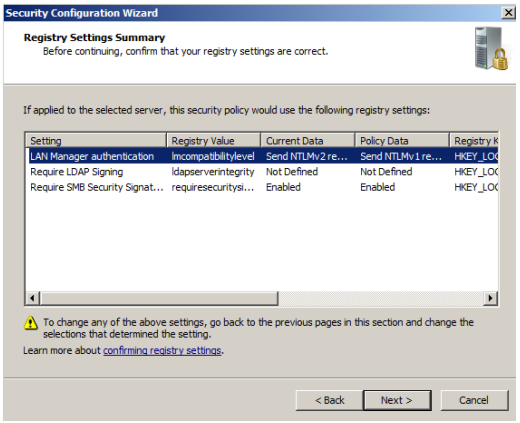


Figure 2: Review the registry settings

22. Check ‘Skip this section’ to bypass configuration of the Audit Policy as this is configured using Group Policy and click ‘Next’.

Figure 3: Ensure the box is checked

23. Save the current configuration by appending the server name to the displayed path and click ‘Next’.

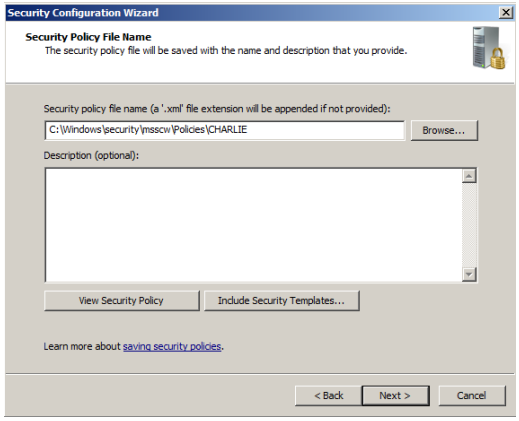


Figure 4: Append ‘CHARLIE’ to the path

24. Select the option to ‘Apply Now’ and then click ‘Next’.
25. Once the wizard has completed the necessary changes, click ‘Next’, and then ‘Finish’.
26. Reboot the server.

Echo High Level Description

Echo is a Windows server running SQL Server. Echo serves as the ‘back-end’ for Web applications running on Hotel (DMZ Web Server).

Following are descriptions of Echo's specific hands-on tasks that students must complete:

Task 1. Windows Host System Hardening

Students will be minimizing non-essential services and unnecessary network configurations - the network interface will be hardened by removing Internet Protocol (IP) version 6 and disabling NetBIOS name resolution. Students will follow security best practices to harden.

Task 2. SQL Server Hardening

If installed using default selections, SQL Server will run under LocalSystem credentials, which is unnecessarily high for a typical database server configuration. Students will create a new local machine user account on Echo and set the SQL Server process to run under the credentials of that account.

Task 3. SQL Server Event Log Auditing

By default, SQL Server logging is disabled. Students will enable logging for failure events and other problems.

Task 4. Configuring OSSEC Agent

Students will install and configure OSSEC Agent, which will then send information about security events to the syslog/OSSEC server (Foxtrot).

Task 5. Windows Security Configuration Wizard

The Windows SCW wizard will take students through a series of questions which will help them harden the server as per industry best practices. Unnecessary services will be disabled, the windows firewall will be configured, and if necessary IIS will be hardened.

This page left intentionally blank for pagination purposes

Windows Server Baseline Hardening Steps

1 Harden Network Interfaces

1.1 Remove Unnecessary Protocols

By default, Microsoft Windows network interfaces are enabled with unnecessary protocols and services. These should be unbound from the interface (if not uninstalled completely). If your server is intended to provide these services, obviously you would NOT disable it.

1. If you have not already done so, log on to the machine using: Username: **`AIACLASS\Administrator`** Password: **`tartans@1`**
2. Open the 'Start' menu and right-click on 'Network' and select 'Properties' to open the 'Network and Sharing Center'.
3. Click on the 'Local Area Connection 2' and then click 'Properties'.
4. Clear the box next to 'Internet Protocol Version 6 (TCP/IPv6)'. Then click 'OK'.

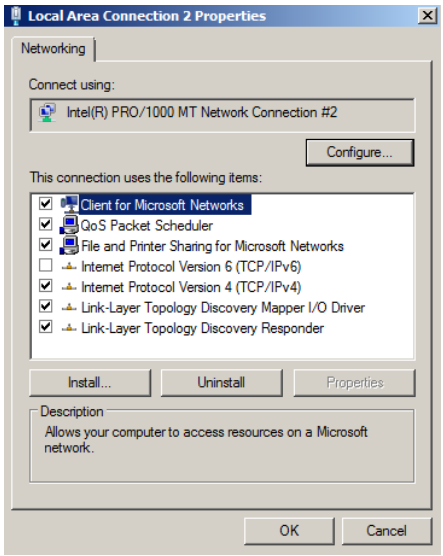


Figure 1: Remove IPv6

2 Harden TCP/IP Properties

2.1 Disable NetBIOS name resolution

As part of our defense-in-depth strategy, it is import to minimize even those parts of the environment that are normally not utilized. Since our network will be entirely native mode Windows 2000 or higher, NetBIOS name resolution would not normally be utilized, however we will eliminate the possibility of it being used altogether (NetBIOS name resolution is chatty and can divulge network information).

1. If the Properties window for your Local Area Connection is not still open, open it by following steps 1 and 2 from the section above.
2. From within the ‘Properties’ of your ‘Local Area Connection’, select the ‘Internet Protocol Version 4 (TCP/IPv4)’ item (leave it checked), and click on the ‘Properties’ button, then click the ‘Advanced’ button.
3. Next click on the ‘WINS’ tab at the top of the window.

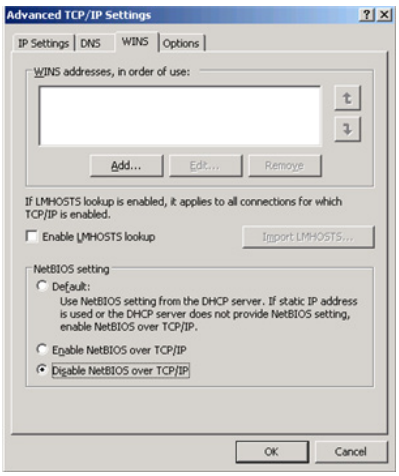


Figure 2: Minimize NetBIOS services

4. Uncheck ‘Enable LMHOSTS lookup’.
5. Select the radio button ‘Disable NetBIOS over TCP/IP’.
6. Click ‘OK’ to accept these settings.
7. Click ‘OK’ to confirm all ‘TCP/IP Properties’ changes.
8. Click ‘OK’ to confirm all ‘Local Area Connection Properties’ changes.
9. Close the ‘Local Area Connection 2 Properties’ and ‘Status’ windows.
10. Close the ‘Network and Sharing Center’ to return to the Desktop.

3 Install ClamWin for Anti-Virus Protection

3.1 Installation

1. Open the Course CD by clicking ‘Start’ -> ‘Computer’, right click ‘CD Drive (D:) AISTS’ and select ‘Open’.
2. Navigate to ‘Tools\Windows\ClamWin’ and double-click the ‘clamwin-0.96.1-setup’ icon.
3. Click ‘Next’.

Figure 3: Install ClamWin Antivirus

4. Accept the license agreement and click ‘Next’.

5. Accept the default option to install for ‘Anyone who uses this computer (all users)’ and click ‘Next’.
6. Select the default installation path and click ‘Next’.
7. At the ‘Select Component’s prompt, accept the default option of ‘Typical Installation’ and click ‘Next’.
8. Click ‘Next’ to create the default start menu folder.
9. Uncheck ‘Download Virus Database Files’ and click ‘Next’.

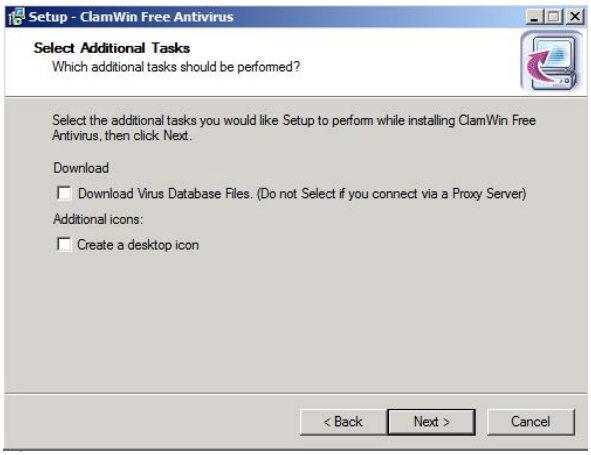


Figure 4: ClamWin Setup

10. Click ‘Install’ to install the program.
11. Click ‘Finish’ to complete the installation.
12. Close Windows Explorer.

3.2 Configuration

1. Click the upward facing arrow in the taskbar and then double-click on the ClamWin icon.

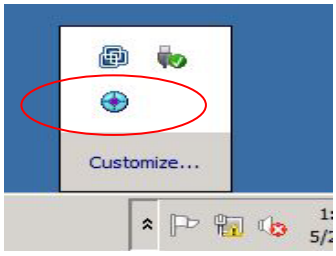


Figure 5: ClamWin Icon

2. Choose ‘No’ if asked to update the virus database.

3. Select ‘Tools’ from the menu, and click on ‘Preferences’.

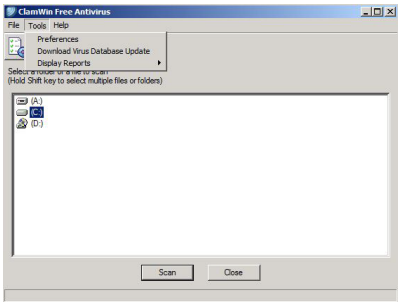


Figure 6: ClamWin Configuration

4. Click on the ‘Internet Updates’ tab. Leave the updates to be done daily, but change the time to 2:30:00 AM.

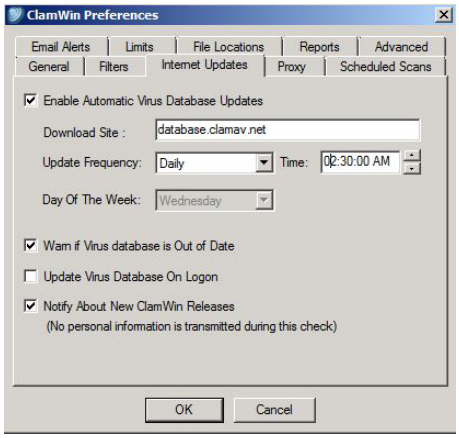


Figure 7: ClamWin Internet Updates

5. Click on the ‘Scheduled Scans’ tab. Click ‘Add’. Choose the scanning frequency to be done Daily at 3:30:00 AM. Enter `C:\` as the folder to scan. Enter a description, such as `‘Nightly Virus Scan’`. Click ‘OK’.

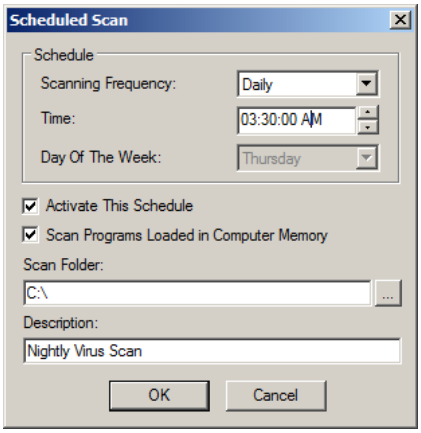


Figure 8: ClamWin Scheduled Scan

6. Click on the 'Email Alerts' tab. Check the box labeled 'Send Email On Virus Detection'. Enter in the following information:

   Mail Server – **`10.0.2.3`**

   From – **`clamwin@Echo`**

   To – **`eventwatch@aia.class`**

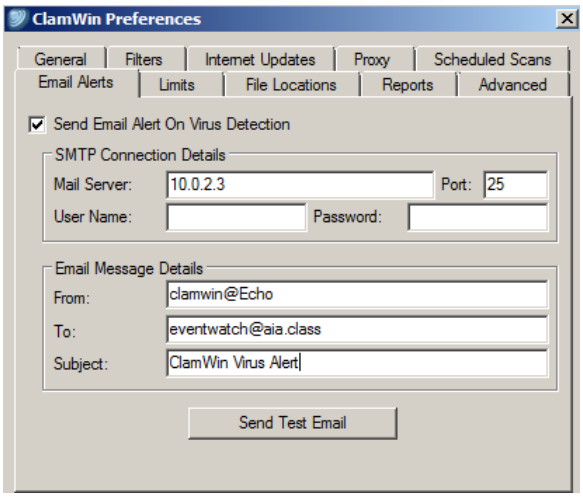


Figure 9: ClamWin Email Alerts

7. Click on the 'Proxy' tab. Enter in the IP address of the Squid Proxy server, Quebec, which is **10.0.2.1**. Ensure that the port is **3128**.

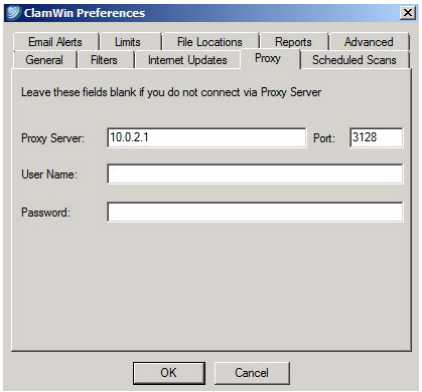


Figure 10: ClamWin Proxy Settings

8. Click 'OK' to accept all changes.
9. Choose 'No' if asked to update the virus database.
10. Click 'Close' to close the ClamWin window.

This page left intentionally blank for pagination purposes

SQL Server Hardening

1 Creating a new user account for the SQL Server process

You will add a new user to the local machine 'Users' group and deny the user rights to Log on Locally.

WARNING: Depending on the applications utilizing SQL Server and the functions that are used by the applications, changing the SQL Server process account may cause application failures. Always check vendor documentation, consult a Database Administrator (DBA), and test the change in a staging environment prior to making this change in production.

1.1 Create the User

1. Open the 'Start' menu, right-click 'Computer' and select 'Manage'.
2. Expand 'Configuration -> 'Local Users and Groups' using the plus icon.
3. Right-click 'Users' and select 'New User'.
4. Give the new user the following properties:

   Username: **sqlserversvc**
   Full Name: **SQL Server Account**
   Description: **SQL Server Service Process Account**
   Password: **Steelers!456**
   Uncheck 'User must change password at next login'
   Check 'Password never expires'

   IMPORTANT: We set the password never to expire because the SQL Server process will run using these credentials. If the password expires, the service will fail. If your organization requires password expiration, be sure you have a policy in place to audit and update passwords prior to expiration.

5. Click 'Create'.
6. Click 'Close'.

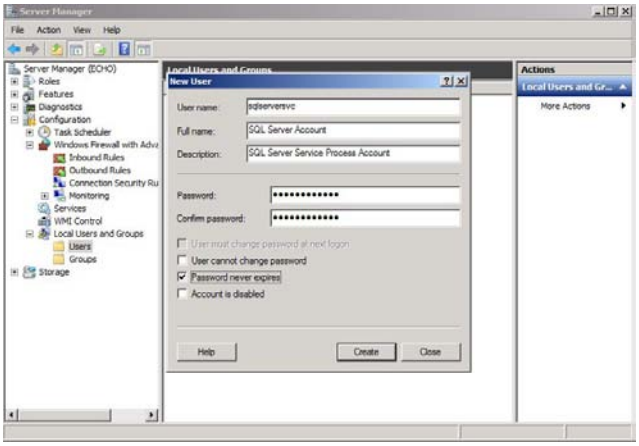


Figure 1: Creating a new user

1.2 Verify Account Permissions

We want to make sure that the account is a member only of the ‘Users’ group.

1. Select ‘Users’ in the left pane.
2. In the right panel, right-click the ‘sqlserversvc account’ and select ‘Properties’. Click the ‘Member Of’ tab.
3. Verify the only group shown is ‘Users’.
4. Click ‘Cancel’.

1.3 Deny Log On Locally Rights and Allow Log on as a Service

A Service Process Account does not need Interactive login rights.

1. Close the ‘Server Manager’ window.
2. Click ‘Start’ -> ‘Run’.
3. Enter **`secpol.msc`** and click ‘OK’.
4. Expand ‘Local Policies’ and click ‘User Rights Assignment’.
5. In the right panel, scroll until you find the entry titled ‘Deny Log on Locally’ and double-click it.
6. Click the ‘Add User or Group’ button.
7. Click the ‘Locations’ button.
8. Select the computer ‘ECHO’, and click ‘OK’.
9. Enter **`sqlserversvc`** in the object name window, and click ‘Check Names’.

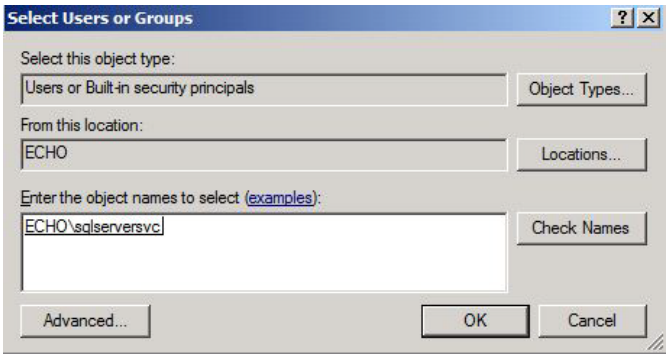


Figure 2: Select User

10. Click ‘OK’ save the user selection.
11. Click ‘OK’ to save the Deny Log on Locally properties.
12. Now find the entry titled ‘Log on as a Service’ and double-click it.
13. Click the ‘Add User or Group’ button.
14. Click the ‘Locations’ button.

15. Select the computer ‘Echo’, and click ‘OK’.
16. Enter **`sqlserversvc`** in the object name window, and click ‘Check Names’.

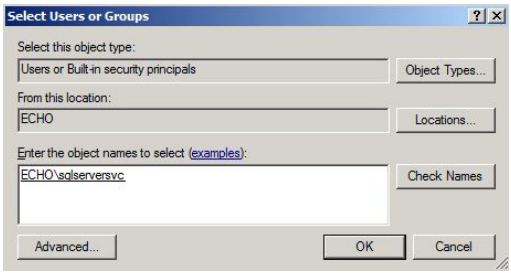


Figure 3: Select User

17. Click ‘OK’ save the user selection.

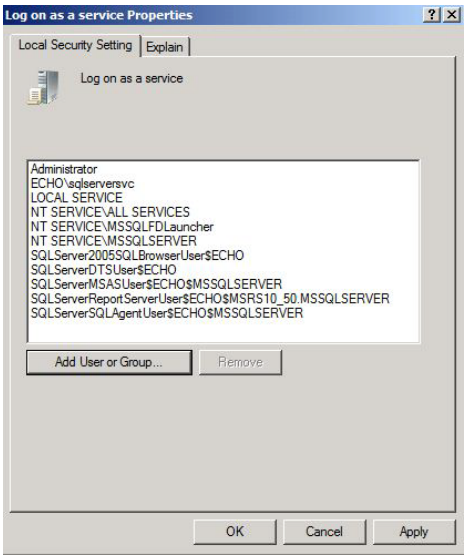


Figure 4: Review the properties

18. Click ‘OK’ to save the Log on as a service properties.
19. Close the ‘Local Security Policy’ window.

2 Assign the Process Account to SQL Server

You will now assign the new account to the SQL Server process.
IMPORTANT: When making this change on production systems outside this class, make sure you follow these instructions. Do not change the account using the Services MMC (services.msc).

1. Open SQL Server Management Studio: ‘Start’ -> ‘All Programs’ -> ‘Microsoft SQL Server 2008 R2’ -> ‘SQL Server Management Studio’.
2. Click ‘Connect’ to connect to the database.
3. Right-click the entry titled ‘ECHO (SQL Server…’ and select ‘Properties’.
4. Click the ‘Security’ tab.

5. At the bottom of the screen in the ‘Server proxy account’ section, place a check in the box to ‘Enable server proxy account’.
6. In the textboxes enter,

   Proxy account: **sqlserversvc**

   Password: **Steelers!456**

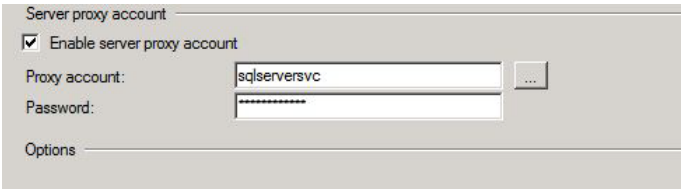


Figure 5: Server proxy account credentials

IMPORTANT: This SQL Server implementation is configured using ‘Mixed Mode’; SQL Server and Windows authentication are both enabled. Microsoft strongly recommends using Windows-only authentication. This allows SQL Server to use the security mechanisms built in to Windows. In the case of this SQL Server instance, because it is used by a Web application that is in a DMZ (and not a member of the aia.class domain), SQL Server must run in mixed mode because it cannot validate the Windows credentials of all clients that connect to it. In your production environments, if you are able to use Windows-only authentication, we recommend you do so.

7. Click ‘OK’.
8. Close ‘Server Management Studio’.
9. Now verify that the SQL Server process is running under the credentials you specified. Click ‘Start’ -> ‘Run’ and enter **`services.msc`**. Click ‘OK’.
10. Scroll the list of services until you find the service titled ‘SQL Server (MSSQLSERVER)’. Double-click it to view ‘Properties’.

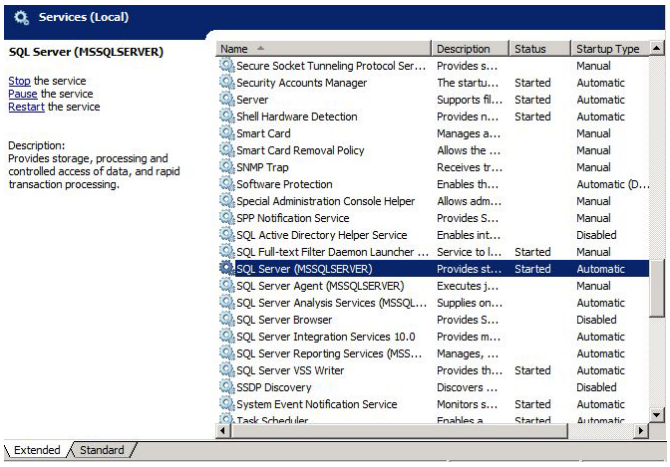


Figure 6: SQL Server properties

11. Click the ‘Log On’ tab. If the account listed is not ‘.\sqlserversvc’, change it to be so, with **Steelers!456** as the password.

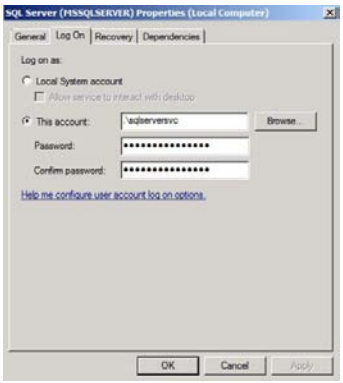


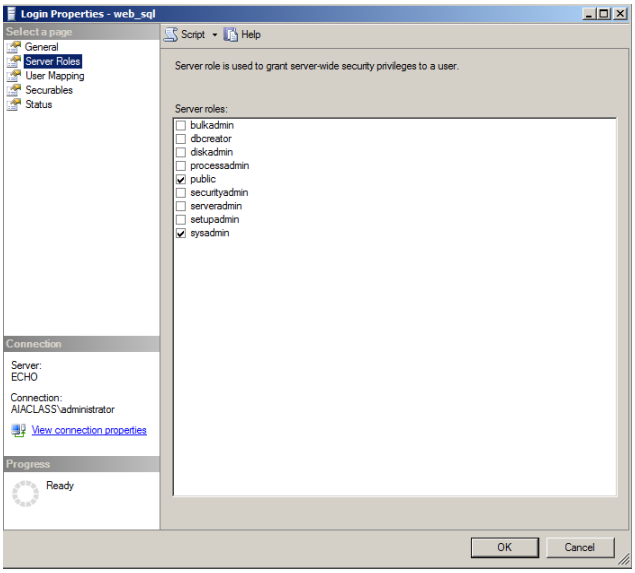
Figure 7: Verify the login credentials

12. Click ‘OK’.
13. Right-click the SQL Server service and select ‘Restart’ so that the service is running under the new credentials.
14. Close the Services MMC.

3 Remove Web App Permissions

The current login credentials that the web app running on Hotel uses to log in to the SQL database is given many more permissions than are necessary for the job. We will minimize these so as to reduce the attack surface of the database.

1. Open the SQL Server Management Studio by going to ‘Start’ -> ‘All Programs’ -> ‘Microsoft SQL Server 2008 R2’ -> ‘SQL Server Management Studio’.
2. Click ‘Connect’ to connect to the local database.
3. Expand ‘ECHO (SQL Server…)’ -> ‘Security’ -> ‘Logins’, right-click ‘web_sql’ and select ‘Properties’.
4. Click on the ‘Server Roles’ tab. Note that all roles are selected. The engineer that set up this connection must have simply given the user all roles instead of taking the time to figure out the minimum required privileges for our web app. Correct this security hole by un-checking all roles except ‘public’ and ‘sysadmin’. Click ‘OK’.



4 Rename SA Account

The built-in ‘sa’ account login is a default administrator account for the SQL Server. Since this is a known privileged account, it is an easy target for brute force and other exploit attempts to gain access to your server. It is recommended to disable or rename this account to reduce its exposure.

1. If the SQL Management Studio is not still open, re-open it using steps 1-3 above.
2. Right-click the ‘sa’ login and select ‘Rename’.
3. Enter `acarnegie` and press `[Enter]`.
4. Close the SQL Server Management Studio.

5 Disable SQL Server Agent Service

The SQL Server Agent allows SQL Server to email or page administrators based on configurable criteria. This is useful functionality, but SQL Server Agent requires Outlook to be installed on the SQL Server machine in order to function.

1. Click ‘Start’ -> ‘Run’ and enter **`services.msc`**. Click ‘OK’.
2. Find and select the service named ‘SQLSERVERAGENT’. Select it. Your windows should look like the following:

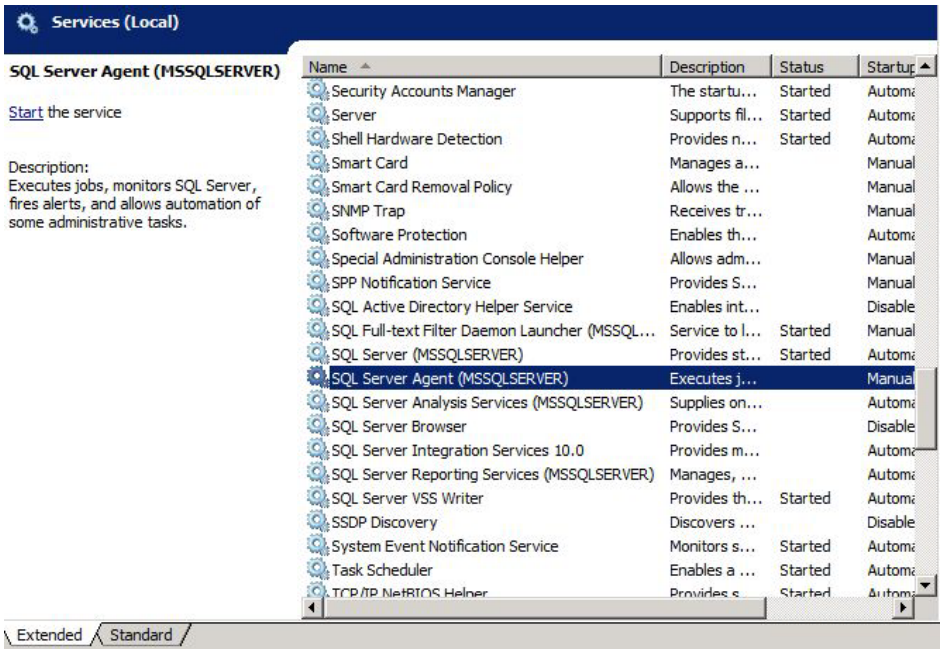


Figure 8: SQL Server Agent services

3. Right-click on the service and select ‘Properties’.
4. Find the dropdown next to ‘Startup Type’ and change it to ‘Disabled’.
5. Click ‘OK’.
6. Close the ‘Services’ window.

SQL Server Event Log Auditing

A default installation of SQL Server does not audit security events. You will make three changes to improve the auditing capabilities in SQL Server:

- Audit login attempts to the Windows Event Log
- Increase the number of stored SQL Server logs (to prevent an attacker from filling the logs to cause them to roll over, covering his/her tracks)
- Implement a SQL Server Profiler entry to log object-level security events

1 Enable Event Log Logon Auditing

1. Open SQL Server Management Studio: 'Start' -> 'All Programs' -> 'Microsoft SQL Server 2008 R2' -> 'Server Management Studio'
2. Click 'Connect'.
3. Right-click 'ECHO (SQL Server 10.50.1600 – AIACLASS\Administrator)' and select 'Properties'.
4. Click 'Security' in the upper-left pane.
5. Change the radio button for the 'Login auditing' option to 'Both failed and successful logins', as shown in Figure 1.

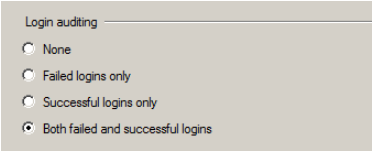


Figure 1: Security settings

6. Click 'OK'.

2 Increase the number of SQL Server Error Logs

SQL Server installs with a default of 6 error logs. You will increase this to 10 to reduce the chances that an attacker could fill the logs, causing them to roll over and hide any attack data.

1. Expand 'ECHO (SQL Server 10.50.1600 – AIACLASS\Administrator)'.
2. Expand 'Management'.
3. Right-click 'SQL Server Logs' and click 'configure'.
4. Check the box titled 'Limiting the number of the error log files before they are recycled'.
5. Increase the value of the 'Maximum number of the error log files' to 10.

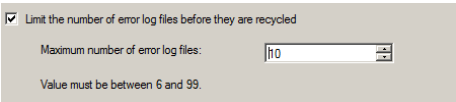


Figure 2: Setting the maximum limit for error log files

6. Click ‘OK’.
7. Close the ‘SQL Server Management Studio’.

3 Log Object Access using SQL Server Profiler

SQL Server profiler is used to run traces against database activity. It can be used for troubleshooting queries, but most importantly can be used to create logs of access attempts.

1. Open SQL Server Profiler: Click ‘Start’ -> ‘All Programs’ -> ‘Microsoft SQL Server 2008 R2’ -> ‘Performance Tools’ -> ‘SQL Server Profiler’.

3.1 Create a new Trace Template

1. Click ‘File’ -> ‘Templates’ -> ‘New Template’.
2. Select ‘Microsoft SQL Server 2008 R2’ in the ‘Select server type’ dropdown box.
3. Name the template ‘**`SQLProfiler_SecurityAudit’`**.
4. Click the ‘Events Selection’ tab.
5. Expand ‘Security Audit’ entry.
6. Check the following events:
    - Audit Add DB User Event
    - Audit Add Login to Server Role
    - Audit Add Member to DB Role
    - Audit Add Role Event
    - Audit Addlogin Event
    - Audit App Role Change Password
    - Audit Change Audit Event
    - Audit Login
    - Audit Login Change Password Event
    - Audit Login Change Property Event
    - Audit Login Failed
    - Audit Login GDR Event
    - Audit Logout
    - Audit Object Derived Permission
    - Audit Schema Object Access Event
    - Audit Statement Permission Event
7. Click ‘Save’.

3.2 Create a Trace Using the Template

1. Click ‘File’ -> ’New Trace’.
2. Click ‘Connect’ to log on to the SQL Server.
3. On the ‘General’ tab, enter **`SecurityTrace`** in the ‘Trace name’ field.
4. Click the ‘Template name’ dropdown and select the template you just created, ‘SQLProfiler_SecurityAudit’.

   Click the ‘Save to file’ checkbox. A file ‘Save As’ dialog will open. Navigate to the C:\ drive. IMPORTANT: You are saving the trace file to the C:\ root because it is the only drive on the machine. For security reasons, Trace files should be saved on a different physical drive than the SQL Server data and log files and should be protected with strong NTFS ACLs.
5. Create a new folder in the root of the C:\ and name it ‘**`Traces’.`**
6. Right click the new ‘Traces’ folder and select ‘Properties’.

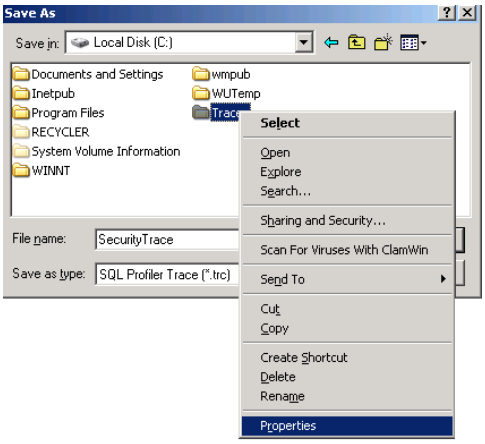


Figure 3: Navigating to the Properties of Traces folder

In the Properties window, click the Security tab.

7. Click ‘Edit’ and then ‘Add’ to add echo\sqlserversvc
8. Give the user Full Control – This is allows Profiler to write the Trace results out to a file in this folder.

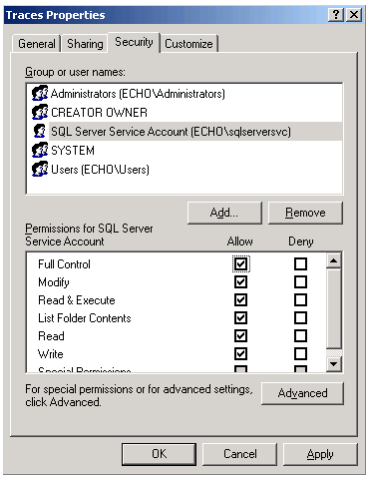


Figure 4: Security properties of Traces folder

9. Click ‘OK’.
10. In the ‘File name’ box, enter ‘\\echo\Traces\Security Trace’ and click ‘Save’.
11. Change the ‘Set maximum file size’ from 5 to 100 to prevent rollover of the log file.
12. Check the box titled ‘Server processes SQL Server trace data’.
13. When finished, your screen should look like figure 5:

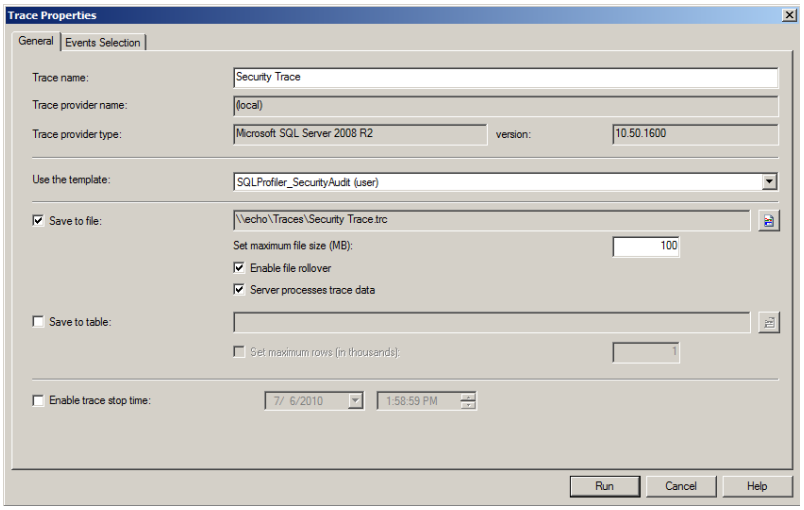


Figure 5: General Information on Traces

14. Click ‘Run’.

Notice that while the Trace runs it continuously lists out all the events that match the security events we defined in our *SQLProfiler_SecurityAudit* template. This can be very useful as a source of information when you suspect something outside the norm is happening on your SQL server.

Open Source Security (OSSEC) Agent

OSSEC agents will be installed on each Linux and Windows server and will send events to the OSSEC server that is running on Foxtrot. The OSSEC server processes events and generates warnings from alerts sent by the agents. *Before installing any OSSEC agents make sure that you have successfully deployed the OSSEC server on Foxtrot.*

1 OSSEC Agent setup

1.1 Installation

1. Open Windows Explorer and navigate to 'D:\Tools\Windows\OSSEC':

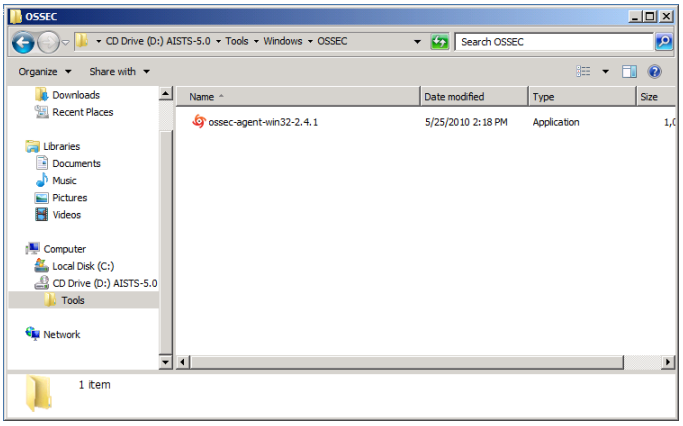


Figure 1: Setup File

2. Double click on the 'ossec-agent-win32-2.4.1' setup file and start the installation:

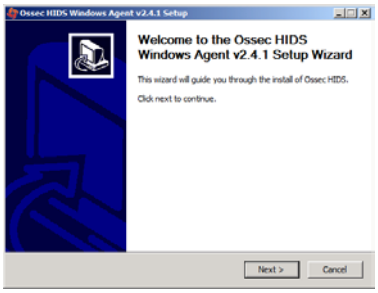


Figure 2: Welcome Screen of OSSEC Installation

3. Click 'Next' and accept the license agreement by pressing the 'I Agree' button:

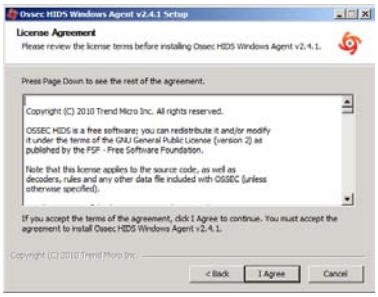


Figure 3: License Agreement window

4. Accept the default installation options and click ‘Next’:

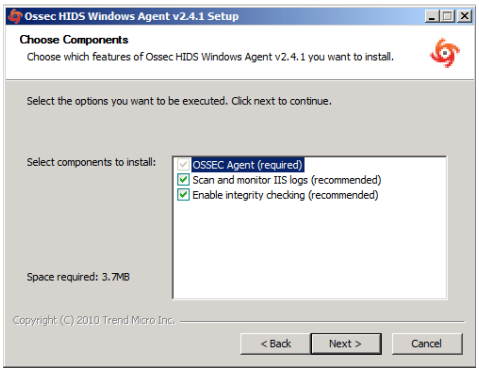


Figure 4: Choose default settings for components

5. Proceed with the installation by pressing the ‘Install’ button:

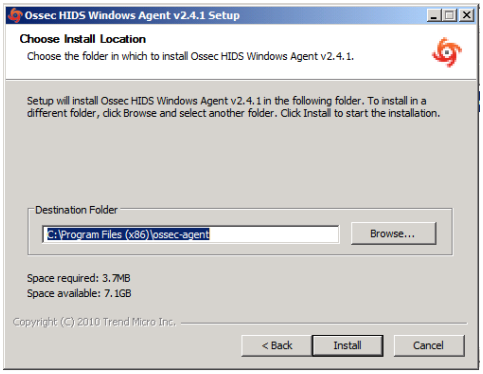


Figure 5: Location path

6. After the installation has finished you should see following screen. Complete the installation by clicking on ‘Finish’:

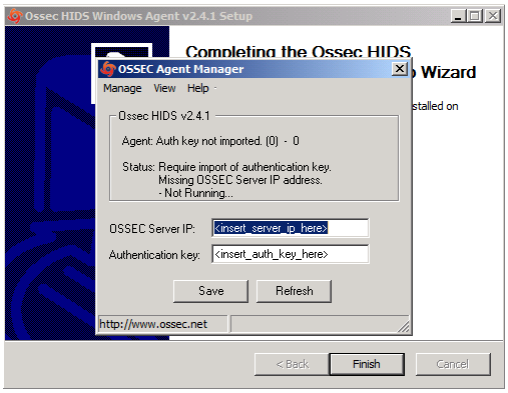


Figure 6: End of OSSEC installation

1.2 Configuration

1. Now we are going to setup a shared key between Echo and Foxtrot. In order to do this, go back into the CD contents and execute ‘Putty’ from ‘D:\Tools\Windows\Putty’
2. Enter `10.0.4.2` (Foxtrot’s IP Address) in the ‘Host Name’ field and click ‘Open’:

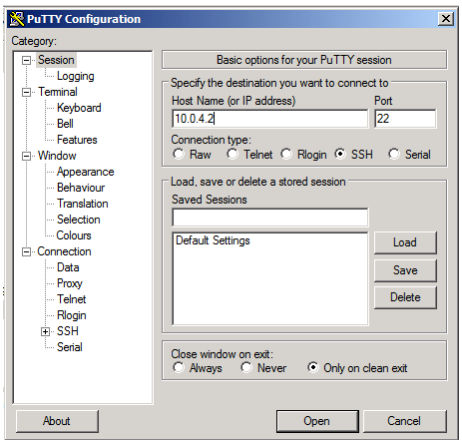


Figure 7: Setting up Putty

3. Accept the warning by clicking ‘Yes’:

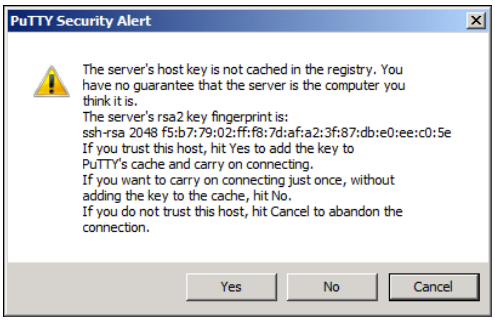


Figure 8: Accept the warning

4. Type **`root`** as the login name and press `[Enter]` then type **`tartans@1`** as the password and press `[Enter]`:

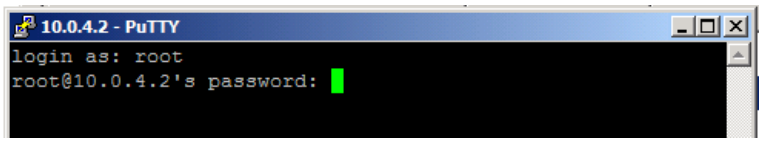


Figure 9: Login

5. Once logged into Foxtrot, start the OSSEC agent manager by executing the following command:

```
# /var/ossec/bin/manage_agents
```

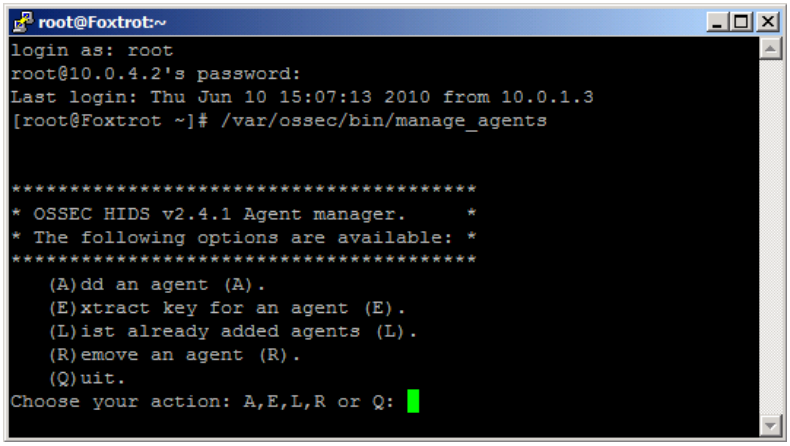


Figure 10: OSSEC Agent Manager window

6. Add an agent by typing A and pressing `[Enter]`.

7. Enter Echo's information as shown below and press `[Enter]`:

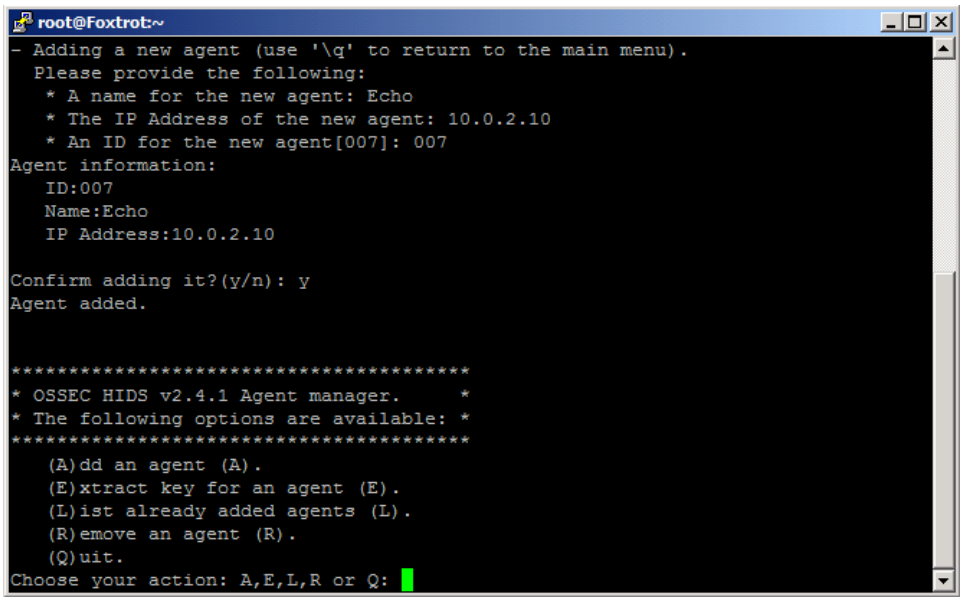


Figure 11: Select an option

8. Now type `E` and press `[Enter]` to extract the shared key for Echo, and enter `007` when the OSSEC agent manager asks for an agent ID. Please note that the key will not be the same as shown in the following screenshot, because the shared key is generated randomly each time an OSSEC agent is added:

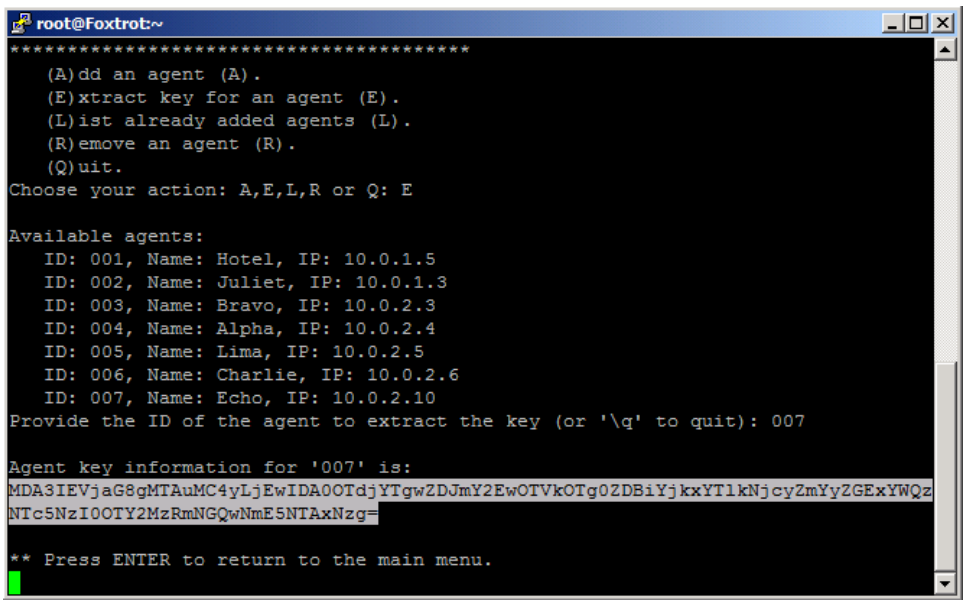


Figure 12: Random key generated

9. Copy the shared key by highlighting it and paste it into the OSSEC Agent Manager as shown below.

10. Enter `10.0.4.2` as the server address and click ‘Save’ then ‘OK’:

Figure 13: Enter the parameters

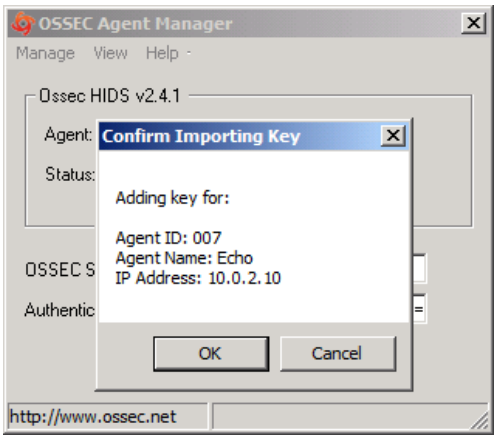


Figure 14: Confirm the settings

11. Choose ‘Manage -> Start OSSEC’ to start the OSSEC agent:

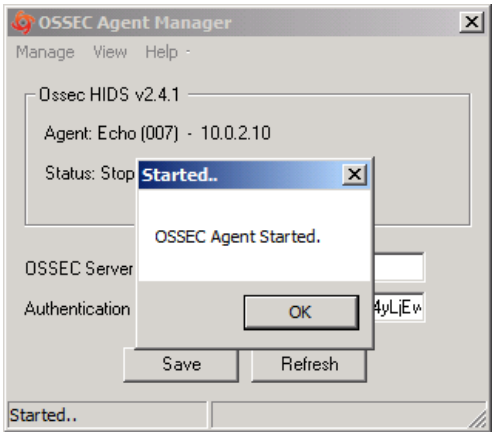


Figure 15: Starting OSSEC

12. Switch back to the Putty SSH command shell window. Type `Q` then press `[Enter]` to quit from the agent manager and type `exit` and press `[Enter]` to end the SSH session and exit from Putty.
13. Close the OSSEC Agent Manager and Windows Explorer.
14. Click ‘Finish’ to close the OSSEC wizard.

Windows Security Configuration Wizard

1 Run the SCW

1. Click ‘Start’ -> ‘Administrative Tools’ -> ‘Security Configuration Wizard’.
2. Click ‘Next’, on the Welcome screen
3. Click ‘Next’, to Create a new Security Policy
4. Click ‘Next’, on the Select Server dialog. We will not be importing a configuration from a different server.
5. Once the Processing of the Security Configuration Database is complete click ‘Next’ to continue.
6. Click ‘Next’, on the Role-Based Service Configuration dialog

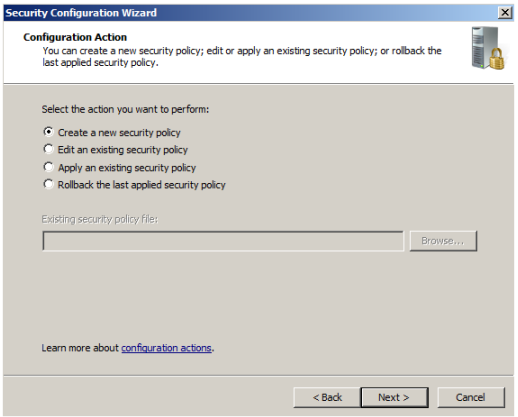


Figure 1: Create a new security policy

7. A list of currently installed roles will be presented. For Echo, Select only ‘Middle-tier application server’. Note: you may need to select ‘All roles’ from the view dropdown box. Click ‘Next’.
8. Accept the default client features and click ‘Next’.

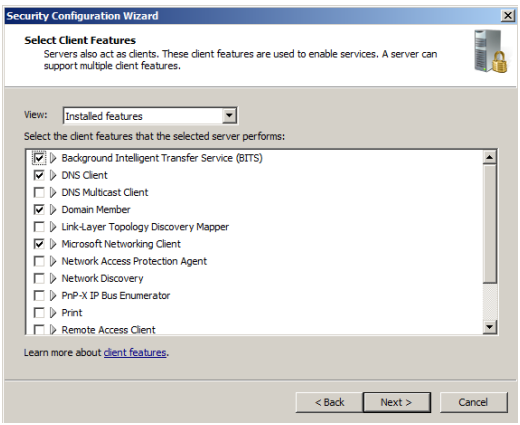


Figure 2: Client Features Settings

9. Administration and Other Options, select:
   - .Net Framework 3.0
   - ‘Application Experience Lookup Service’
   - ‘Error reporting’
   - ‘Local application installation’
   - ‘Performance Log and Alerts’
   - ‘Remote Desktop‘
   - ‘Windows User Mode Driver Framework’

   Click ‘Next’.

10. Additional Services: Enable the following:
    - ‘OSSEC Hids’
    - **‘**SQL Active Directory Helper Service’
    - ‘SQL Full-text Filter Daemon Launcher (MSSQLSERVER)’
    - ‘SQL Server (MSSQLSERVER)’
    - ‘SQL Server Analysis Services (MSSQLSERVER)’
    - ‘SQL Server Browser’
    - ‘SQL Server Integration Services 10.0’
    - ‘SQL Server Reporting Services (MSSQLSERVER)‘

    Click ‘Next’.
11. Accept the default handling option of ‘Do not change the start mode of the service’ for any unspecified services’ and click ‘Next’.
12. Review the list of service changes before clicking ‘Next’.
13. Click ‘Next’ to begin the Network Security Configuration.
14. The SCW attempts to identify the necessary ports that the server will need open for your previous selections. However, we will minimize even further by disabling unnecessary rules. Uncheck the following:
    - Core Networking – IPv6(IPv6-in)
    - Core Networking – IPv6(IPv6-Out)

    Click ‘Next’ to continue past the Network Security Rules screen.
15. Click ‘Next’, when the Registry Wizard Begins.
16. Click ‘Next’, to accept the default SMB security settings.
17. Click ‘Next’, to confirm the requirement for Domain Account authentication for outbound connections
18. Click ‘Next’, to confirm that we are using domain controllers that use the necessary LAN Manager authentication level.
19. Click ‘Next’, to begin configuration of the Audit Policy

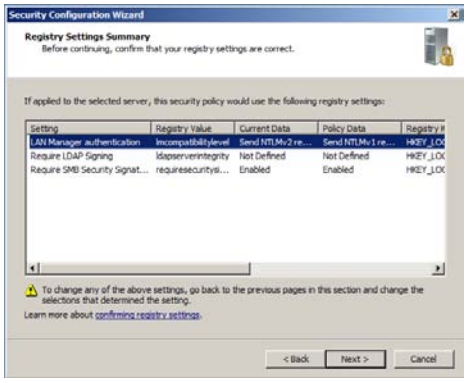


Figure 3: Review Service settings

20. Check “Skip this section” as the Auditing is configured by Group Policy and Click ‘Next’

21. Save the current configuration by appending the server name to the displayed path and Click ‘Next’.

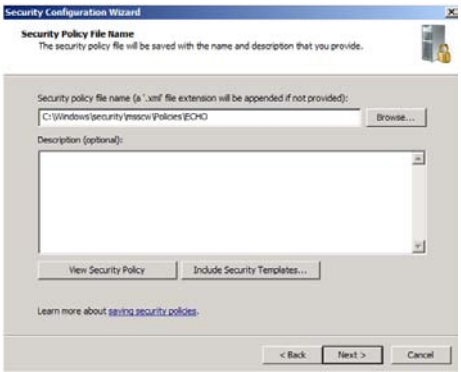


Figure 4: Append ‘ECHO’ to the path

22. Select the option to ‘Apply Now’ and then Click ‘Next’**.**
23. Once the wizard has completed the necessary changes, click ‘Next’, and then ‘Finish’.
24. Reboot the server.

2 Add Additional Firewall Rule

1. Go to ‘Start’ -> ‘Administrative Tools’ -> ‘Windows Firewall with Advanced Security’.
2. Click on ‘Inbound Rules’ in the left pane.
3. Click ‘New Rule…’ on the right.
4. Select ‘Custom’ and click ‘Next’.
5. Click ‘Next’.
6. Select ‘ICMPv4’ under ‘Protocol type’ and click ‘Next’.
7. Keep ‘Any IP address’ selected for local IP addresses and select ‘These IP addresses’ for remote IP addresses.
8. Click ‘Add…’ in the remote IP addresses section.
9. Enter Mike’s IP address: **10.0.3.2** into the ‘This IP address or subnet’ box and click ‘OK’.
10. Click ‘Next’.
11. Ensure ‘Allow the connections’ is selected and click ‘Next’.
12. Click ‘Next’.
13. Enter ‘**`Allow Ping from Mike-Nagios`**’ in the ‘Name’ field and click ‘Finish’.
14. Close the firewall window.

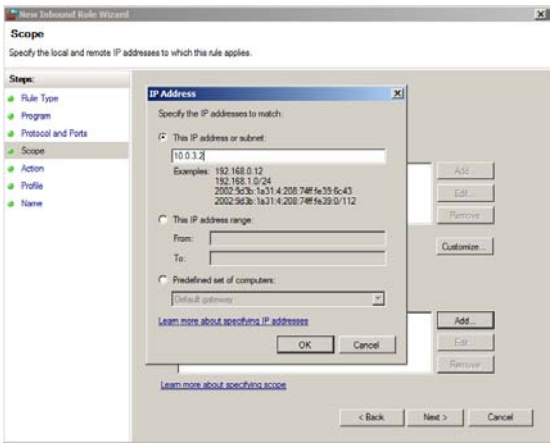


Figure 5: Assigning IP Address

This page left intentionally blank for pagination purposes

Foxtrot High Level Description

Foxtrot is a Linux centralized logging server. The purpose of this server is to collect and compile alerts sent from devices on the network. This provides the benefit of creating a backup of all important log messages for redundancy and ease of review. Foxtrot is located in a highly secure Management subnet of the network.

Students will install OSSEC server that takes care of the following: Host based IDS, syslog client, monitoring the availability of all hosts on the network, as well as the services that they are providing. OSSEC agents installed on the individual servers will send event and alert information to the OSSEC server on Foxtrot.

The students also will install and configure Splunk to manage syslog and OSSEC alerts on Foxtrot. Other services will be minimized and the network interface will be hardened.

Following are descriptions of Foxtrot's specific hands-on tasks that students must complete:

Task 1. Linux Host System Hardening

Students will be minimizing non-essential services (e.g., xinetd, portmap) as well as extraneous default users and groups. Also, students will create a non-privileged administrator account to provide an audit trail for all administrative access.

Task 2. Configuring Time Synchronization

Network Time Protocol (NTP) is used to synchronize the host computer's time to a local time server—in this deployment it is the Internet firewall (Quebec).
Alpha will synchronize to Quebec every ten minutes; the Linux hosts will synchronize with Quebec every ten minutes; and the Window hosts will synchronize with Alpha every forty-five minutes until three good synchronizations occur, then once every eight hours. With all the hosts' time across the network synchronized, the cross examination of multiple hosts' logs or the logs at the syslog Server become more meaningful and easier to examine.

Task 3. Configuring Bastille

The Bastille hardening system is a user-configurable script that attempts to lock down Linux/UNIX operating systems. The Bastille script embodies recommendations from every major reputable source on Linux/UNIX security. We will use pre-configured Bastille templates to lock down weak system settings such as maximum password age, user privileges, etc.

Task 4. Configuring IPTables

IPTables is a Linux firewall application that can be configured to perform packet filtering on network firewalls or host systems. IPTables will be configured on this host as a host-based firewall to allow only valid packets to and from this host. To do this, you will set up INPUT and OUTPUT rules that specifically allow known-good packets into and out of the host and will create default LOG rules and DROP rules.

Task 5. OSSEC Server Setup

OSSEC is a scalable, multi-platform, open source host-based intrusion detection system (HIDS) which runs on most operating systems including Linux, OpenBSD, FreeBSD, MacOS, Solaris, and Windows. It has a powerful correlation and analysis engine that integrates log analysis, file integrity checking, Windows registry monitoring, centralized policy enforcement, rootkit detection, real-time alerting, and active response. You will install and configure the OSSEC server.

Task 6. Splunk Syslog Server Setup

Splunk is a free IT search engine that can be used to index, search, alert, and report real-time log data. OSSEC will be integrated into Splunk so that it receives and indexes all OSSEC agent alerts from the hosts on the network. Having a centralized logging server allows the system administrator to collect and view the important messages from many hosts on the network in one secure location.

Linux Host System Hardening

1 Remove Zeroconf Route

1. If you have not already done so, log on to the machine using:

   Username: **root** Password: **tartans@1**

2. Open a terminal window by going to 'Applications' -> 'Accessories' -> 'Terminal'.

By default Linux adds a "zeroconf" route at boot time. This is a static route that designates the 169.254/16 prefix as local. This is unnecessary on our network, so we will remove the route.

3. Specify to not use zeroconf at boot time:

NOTE: In this and all subsequent Linux documents, the '#' at the beginning of each line should not be typed in as part of the command. It is simply meant to represent a command prompt.

```
# echo "NOZEROCONF=yes" >> /etc/sysconfig/network
```

2 Linux Kernel Upgrade

One of the most essential hardening tasks for Linux systems is to ensure that the latest kernel version is being used. The kernel is the core of the operating system and every effort should be made to ensure that the most current version is in use. Most versions of Linux include some automated means for updating software, including the kernel. We will use a tool called YUM (Yellowdog Updater Modified) to download updates from an external web server hosting our YUM repository.

2.1 Apply latest updates to Kernel and other installed packages

1. Edit the yum config file using vi:

```
# vi /etc/yum.repos.d/CentOS-Base.repo
```

2. There are six sections of the file, which are denoted by names in brackets. You will edit 3 of these sections and disable the other 3. Press [Insert] or [i] to edit the file and scroll down to the first section, '[base]'. Comment out the line beginning with 'mirrorlist=' by typing a # at the beginning of the line. Next, uncomment the line below it beginning with 'baseurl=' and edit the URL to point to our trusted yum repository at http://192.168.30.14/centos/5.4/os/i386/

   The updated lines will be as follows:

```
[base]
name=CentOS-$releasever - Base
#mirrorlist=http://mirrorlist.centos.org/?release=$releasever&arch=$basearch&rep
o=os
baseurl=http://192.168.30.14/centos/5.4/os/i386/
gpgcheck=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-CentOS-5
```

Figure 1: Configuring YUM base repository

3. Repeat the above steps for the second section, '[updates]', pointing it to the URL http://192.168.30.14/centos/5.4/updates/i386/

```
#released updates
[updates]
name=CentOS-$releasever - Updates
#mirrorlist=http://mirrorlist.centos.org/?release=$releasever&arch=$basearch&rep
o=updates
baseurl=http://192.168.30.14/centos/5.4/updates/i386/
gpgcheck=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-CentOS-5
```

Figure 2: Configuring YUM updates repository

4. Scroll down to the next section, '[addons]' and add enabled=0 underneath the last line of the section to disable it. The updated lines will be as follows:

```
#packages used/produced in the build but not released
[addons]
name=CentOS-$releasever - Addons
mirrorlist=http://mirrorlist.centos.org/?release=$releasever&arch=$basearch&repo
=addons
#baseurl=http://mirror.centos.org/centos/$releasever/addons/$basearch/
gpgcheck=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-CentOS-5
enabled=0
```

Figure 3: Disabling YUM addons repository

5. Scroll down to the next section, '[extras]', comment out the 'mirrorlist' line, and point the 'baseurl' to the trusted yum repository: http://192.168.30.14/centos/5.4/extras/i386/

```
#additional packages that may be useful
[extras]
name=CentOS-$releasever - Extras
#mirrorlist=http://mirrorlist.centos.org/?release=$releasever&arch=$basearch&rep
o=extras
baseurl=http://192.168.30.14/centos/5.4/extras/i386/
gpgcheck=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-CentOS-5
```

Figure 4: Configuring YUM extras repository

We will leave the remaining two sections at their default setting of disabled.

6. Press [Esc], then type :wq and press[Enter] to save the changes and exit VI.
7. Add a variable to '/etc/yum.conf' so that all future updates use the HTTP proxy. Edit '/etc/yum.conf' with vi:

```
# vi /etc/yum.conf
```

8. To configure yum to use the web proxy server we need to add a line to the '/etc/yum.conf file'. Add the following line to the end of the '[main]' section of the file:

```
proxy=http://10.0.2.1:3128
```

```
[main]
cachedir=/var/cache/yum
keepcache=0
debuglevel=2
logfile=/var/log/yum.log
distroverpkg=redhat-release
tolerant=1
exactarch=1
obsoletes=1
gpgcheck=1
plugins=1
proxy=http://10.0.2.1:3128
```

Figure 5: Configuring YUM proxy server

Press [Esc] then type :wq and press [Enter] to save the changes and exit VI.

NOTE: In order to access the Internet or our trusted update server, routing will need to be enabled on Quebec and Romeo. Once the access control lists are in place on these two router/firewall machines, very few devices will be able to access external networks directly. You may need to wait until these tasks are completed—check with your teammates on this.

9. Run yum in update mode:

```
# yum update
```

10. Type y then press [Enter] when prompted to download the updates.
11. Type y then press [Enter] when prompted to import the CentOS 5 GPG key.

    A number of packages will be downloaded and installed, including a newer kernel.

    This step may take several minutes to complete. Press [Ctrl] + [Shift] + [T] to open a new terminal tab if you want to move on to the next steps while the updates take place.

3 Service Minimization

3.1 Removing Unnecessary Services

By default Linux runs many services that a standalone server does not need. Extraneous services are dangerous because they provide possible attack vectors.

The services that need to be removed from this system are:

- anacron
- apmd
- atd
- autofs
- cpuspeed
- cups
- gpm
- irqbalance
- mdmonitor
- mdmpd
- microcode_ctl
- netfs
- nfslock
- portmap
- rawdevices
- rpcgssd
- rpcsvcgssd
- rpcidmapd
- sendmail
- xinetd

1. Terminate the 'anacron' service properly by using the following command:

```
# service anacron stop
```

2. Remove the 'anacron' startup routine using the following command:

```
# chkconfig --del anacron
```

```
Stopping anacron:                                          [  OK  ]
```

Figure 6: Removing a service

3. Repeat steps #1 and #2 for each service listed above. (ADVANCED: see the 'Bash Script' ADDENDUM located on the last two pages of this section to automate these repetitive steps.)

   Note: On some systems, some of the services may not be started and may not return the 'OK' or return a 'Failed' message when stopped. If this is the case, it is sufficient to simply delete the service.

4. To check that the appropriate services have been removed, use the following two commands from a terminal window:

```
# netstat -ntap | grep -i listen
```

```
tcp        0      0 :::22                   :::*                    LIST
EN      3134/sshd
```

Figure 7: Confirming service removal

```
# chkconfig --list | grep on | sort
```

```
acpid           0:off   1:off   2:on    3:on    4:on    5:on    6:off
auditd          0:off   1:off   2:on    3:on    4:on    5:on    6:off
avahi-daemon    0:off   1:off   2:off   3:on    4:on    5:on    6:off
avahi-dnsconfd  0:off   1:off   2:off   3:off   4:off   5:off   6:off
conman          0:off   1:off   2:off   3:off   4:off   5:off   6:off
crond           0:off   1:off   2:on    3:on    4:on    5:on    6:off
firstboot       0:off   1:off   2:off   3:on    4:off   5:on    6:off
haldaemon       0:off   1:off   2:off   3:on    4:on    5:on    6:off
hidd            0:off   1:off   2:on    3:on    4:on    5:on    6:off
ip6tables       0:off   1:off   2:on    3:on    4:on    5:on    6:off
iptables        0:off   1:off   2:on    3:on    4:on    5:on    6:off
lvm2-monitor    0:off   1:on    2:on    3:on    4:on    5:on    6:off
mcstrans        0:off   1:off   2:on    3:on    4:on    5:on    6:off
messagebus      0:off   1:off   2:off   3:on    4:on    5:on    6:off
netconsole      0:off   1:off   2:off   3:off   4:off   5:off   6:off
network         0:off   1:off   2:on    3:on    4:on    5:on    6:off
pcscd           0:off   1:off   2:on    3:on    4:on    5:on    6:off
readahead_early 0:off   1:off   2:on    3:on    4:on    5:on    6:off
readahead_later 0:off   1:off   2:off   3:off   4:off   5:on    6:off
restorecond     0:off   1:off   2:on    3:on    4:on    5:on    6:off
sendmail        0:off   1:off   2:on    3:on    4:on    5:on    6:off
sshd            0:off   1:off   2:on    3:on    4:on    5:on    6:off
syslog          0:off   1:off   2:on    3:on    4:on    5:on    6:off
vmware-tools    0:off   1:off   2:on    3:on    4:off   5:on    6:off
wdaemon         0:off   1:off   2:off   3:off   4:off   5:off   6:off
xfs             0:off   1:off   2:on    3:on    4:on    5:on    6:off
```

Figure 8: Results of service removals

5. If your results are *similar* to the output shown above, the services have been removed successfully.

4 User / Group Account Minimization

It is important to disable all default vendor accounts that will be unused. Typically a default account, e.g., gopher or news, is created only when the respective service is also installed; however, many default accounts will exist even if you have not installed the related services on your system. In our case, we will not use many of the default accounts and so we will remove them. The more accounts you have, the easier it is for outsiders to access your system.

4.1 Remove Default User Accounts

The users we will need to remove are:

- adm
- apache
- ftp
- games
- gopher
- halt
- lp
- mail
- mailnull
- news
- nfsnobody
- nobody
- nscd
- operator
- rpcuser
- rpc
- shutdown
- smmsp
- uucp
- vcsa
- xfs

1. Remove the ‘adm’ user account using the following command:

```
# userdel adm
```

2. Repeat the previous step for each account listed above. Verify removal by executing the following command:

```
# cat /etc/passwd
```

```
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
distcache:x:94:94:Distcache:/:/sbin/nologin
webalizer:x:67:67:Webalizer:/var/www/usage:/sbin/nologin
dovecot:x:97:97:dovecot:/usr/libexec/dovecot:/sbin/nologin
squid:x:23:23::/var/spool/squid:/sbin/nologin
mysql:x:27:27:MySQL Server:/var/lib/mysql:/bin/bash
pcap:x:77:77::/var/arpwatch:/sbin/nologin
ntp:x:38:38::/etc/ntp:/sbin/nologin
dbus:x:81:81:System message bus:/:/sbin/nologin
avahi:x:70:70:Avahi daemon:/:/sbin/nologin
named:x:25:25:Named:/var/named:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
haldaemon:x:68:68:HAL daemon:/:/sbin/nologin
avahi-autoipd:x:100:102:avahi-autoipd:/var/lib/avahi-autoipd:/sbin/nologin
gdm:x:42:42::/var/gdm:/sbin/nologin
user:x:500:500:User:/home/user:/bin/bash
```

Figure 9: Results of removing unnecessary default user accounts

3. If the default user accounts have been successfully removed, your /etc/passwd file will look *similar* to the output shown in the figure above.

4.2 Remove Default Groups

Now that we have removed all unnecessary accounts from the /etc/passwd file, we will clean up the /etc/groups file.

The groups that we will remove are:

- adm
- dip
- lock
- lp
- mail
- news
- uucp

Removing a group account is similar to the process of removing a user shown above.

1. Delete the ‘adm’ group using the following command:

```
# groupdel adm
```

2. Repeat the previous step for each group listed above.

3. Verify removal by executing the following command:

```
# cat /etc/group
```

```
root:x:0:root
bin:x:1:root,bin,daemon
daemon:x:2:root,bin,daemon
sys:x:3:root,bin
tty:x:5:
disk:x:6:root
mem:x:8:
kmem:x:9:
wheel:x:10:root
man:x:15:
users:x:100:
utmp:x:22:
utempter:x:35:
audio:x:63:gdm
distcache:x:94:
floppy:x:19:
webalizer:x:67:
dovecot:x:97:
squid:x:23:
mysql:x:27:
pcap:x:77:
slocate:x:21:
ntp:x:38:
ecryptfs:x:101:
dbus:x:81:
avahi:x:70:
named:x:25:
sshd:x:74:
haldaemon:x:68:
avahi-autoipd:x:102:
gdm:x:42:
user:x:500:
```

Figure 10: Results of removing unnecessary default groups

4. If the default groups have been successfully removed, the /etc/group file will look similar to the output shown in the figure above.

4.3 Create the 'Admin' User

The last account management task we will perform manually is to create an 'admin' user for daily administration tasks once the initial setup is complete.

1. Add the admin user using the following command:

```
# useradd admin
```

2. Set the password for the 'admin' account:

```
# passwd admin
```

3. When prompted for a password use the following: steelers

   The output will resemble that shown below:

```
Changing password for user admin.
New UNIX password:
BAD PASSWORD: it is based on a dictionary word
Retype new UNIX password:
passwd: all authentication tokens updated successfully.
```

Figure 11: Creating an Admin user

Note: In a real production environment you should always choose a strong password or passphrase that is sufficiently long and contains a combination of letters, numbers, and special characters. The above password is used for demonstration purposes only.

5 Installing ClamAV

1. Copy the ClamAV tarball from the course CD to the /root directory:

```
# cp /media/AISTS/Tools/Linux/ClamAV/clamav-0.96.1.tar.gz /root
```

2. Untar ClamAV:

```
# cd /root
# tar xvzf clamav-0.96.1.tar.gz
```

3. We need to install a few prerequisite packages before installing ClamAV. We will use our trusted yum repository that we set up earlier in this task to install zlib-devel. Additionally, in order to compile ClamAV and other tools in later tasks from source code we will need a compiler installed on the machine. This distribution of CentOS does not come with a compiler pre-installed so we will install the gcc compiler ourselves.

   Make sure to remove this compiler when all of this machine's tasks have been completed as it can be leveraged by an attacker to compile malicious code if they were to gain access to the system.

```
# yum install gcc zlib-devel
```

4. Type y then press [Enter] when prompted to confirm the download.
5. Change into the clamav-0.96.1 directory and install ClamAV:

```
# cd clamav-0.96.1
# adduser clamav
# ./configure --sysconfdir=/etc
# make
# make install
```

6. Use the VI editor to open the clamav.conf file in order to configure ClamAV:

```
# vi /etc/clamd.conf
```

7. Press [Insert] to enter edit mode. Comment out the line near the beginning of the file containing 'Example':

```
# Comment or remove the line below.
#Example
```

Figure 12: Editing clamd.conf

8. Find and uncomment the following lines by removing the '#' in front of them:
   a. 'LogFile /tmp/clamd.log'
   b. 'LogTime yes'
   c. 'LogSyslog yes'
   d. 'LocalSocket /tmp/clamd.socket'
9. Save and exit the file. Press [Esc] and type :wq then press [Enter].

10. The ClamAV updater (freshclam) needs to be pointed to our internal proxy (10.0.2.1) in order to be able to update virus definitions. Use the VI editor to open the freshclam.conf file:

```
# vi /etc/freshclam.conf
```

11. Comment out the line near the beginning of the file containing 'Example':

```
# Comment or remove the line below.
#Example
```

Figure 13: Editing freshclam.conf

12. Find the proxy settings. Uncomment and make the following changes to indicate the IP of the proxy server and the port number to use:

```
HTTPProxyServer 10.0.2.1
HTTPProxyPort 3128
```

Note: *Although freshclam has been configured, it probably won't successfully run yet. The Squid Proxy server may still need to be set up.*

13. Save and exit the file. Press [Esc] and type :wq then press [Enter].
14. Enable the ClamAV daemon to start automatically as a service:

```
# cp /media/AISTS/Tools/Linux/ClamAV/clamd /etc/init.d/
# chkconfig --add clamd
# service clamd start
```

15. Setup cron jobs for Virus definition updates and nightly virus scans:

```
# crontab –u root -e
```

16. Add the following two lines to the file:

```
15 2 * * * /usr/local/bin/freshclam --quiet
15 3 * * * /usr/local/bin/clamdscan --quiet /
```

17. Save and exit the cron file. Press [Esc] and type :wq then press [Enter].
18. Remove ClamAV installation files (they contain test signatures that will be found on every scan if we don't remove them) then reboot the server.

```
# cd /root
# rm -rf clamav-0.96*
# reboot
```

ADDENDUM Bash Script: 'for loop'

Create a file containing the list of items

1. If you would like to automate the task of removing the unwanted services, users, and groups; you can write a Bash script to loop through the list of items and process them one by one. First, start by creating a text file containing the list of items that you want to process. Enter the following command to create the text file:

```
# cat > deletedSvcList
```

2. After you typed the previous command and hit the [Enter] key, notice that there is no prompt ('#') at the cursor. The file is now open and you can enter the list of items that you want to process. Enter each item on a separate line, hitting the [Enter] key to move to the next line.
3. When all of the items have been entered into the file, press [Ctrl+d] to save and close the file. Notice that the prompt ('#') has returned to the shell.

Write the 'for loop'

1. Now we will create a 'for loop' that will read the items in the deletedSvcList file one by one and stop each service. Enter the following script as it appears below to stop the unwanted services:

```
# for str in $(cat deletedSvcList); do service $str stop; done
```

   A simple modification makes sure that those services do not start on bootup:

```
# for str in $(cat deletedSvcList); do chkconfig --del $str; done
```

2. Notice that the script is in three sections, separated by semi-colons (';'). The first section of this script creates a variable, named 'str', and assigns to it the first item in the file. The second section inserts the value of the variable, 'str', into the shell command. The command is executed and then the process is repeated for each item in the file. When there are no more items in the file, the third section of the script ends the process and returns control back to the shell.

   As you go through the steps, you will have to create three separate files for services, users, and groups. Then you must modify the file name in the first section of the script. Likewise, you will have to modify the command in the second section to perform the action that you want.

   Here are the files and scripts that should be created to remove the following items:

   Users:

```
# cat > deletedUserList
```

```
# for str in $(cat deletedUserList); do userdel $str; done
```

   Groups:

```
# cat > deletedGrpList
```

```
# for str in $(cat deletedGrpList); do groupdel $str; done
```

Linux Network Time Protocol Daemon (ntpd) Client

1 Setup Linux ntpd Client Service

1.1 Installation

1. If you have not already done so, log on the console using:

   Username: **root** Password: **tartans@1**

2. Open a terminal window by going to 'Applications' -> 'Accessories' -> 'Terminal'.
3. The Network Time Protocol Daemon (ntpd) is installed with most Linux distributions. You will create a cron job that will cause the Linux ntpd to periodically query Quebec's ntp server and update the system time.

1.2 Configuration

1. Run the following command to see the current local system time. Hopefully, it is significantly different from the time server's system time as this will explicitly demonstrate when the client becomes synchronized with the server:

```
# date
```

2. If the date is not significantly different from the time server's system time, you can change the local client's system time manually by entering the following command (you can change the system date and time to whatever you want):

```
# date -s "Fri Sep 12 14:38:19 EDT 2003"
```

3. The ntp configuration file must be modified to tell it which time server to use to update the system time. This file is located in the '/etc' directory. To open the config file in the 'vi' text editor, enter:

```
# vi /etc/ntp.conf
```

4. In order to modify the file in the 'vi' editor, the `[Insert]` or `[i]` key must be pressed before trying to add or change text.
5. Scroll down to the section beginning with "# Use public servers" which is excerpted here:

```
# Use public servers from the pool.ntp.org project.
# Please consider joining the pool (http://www.pool.ntp.org/join.html).
server 0.centos.pool.ntp.org
server 1.centos.pool.ntp.org
server 2.centos.pool.ntp.org
```

Figure 1: Default NTP configuration file

Comment out the previous servers and add the following two lines at the end of this section:

```
restrict 10.0.2.1 mask 255.255.255.255 nomodify notrap noquery
server 10.0.2.1 prefer
```

Your section should look similar to the following:

```
# Use public servers from the pool.ntp.org project.
# Please consider joining the pool (http://www.pool.ntp.org/join.html).
#server 0.centos.pool.ntp.org
#server 1.centos.pool.ntp.org
#server 2.centos.pool.ntp.org
restrict 10.0.2.1 mask 255.255.255.255 nomodify notrap noquery
server 10.0.2.1 prefer
```

Figure 2: Edited NTP configuration file

6. Save and exit the file. Press `[Esc]` and type `:wq` then press `[Enter]`.
7. Now we need to cause ntpd to update to the ntp server time by modifying /etc/ntp/step-tickers to run ntpdate when ntpd is started. Do this by running these two commands:

```
# echo "10.0.2.1" > /etc/ntp/step-tickers
```

8. The 'step-tickers' file should now contain only the ntp server's IP address. The file contents can be viewed by entering this command:

```
# cat /etc/ntp/step-tickers
```

9. Enter the date command to see that the date is still incorrect.
10. If the ntpd service is not currently running, it must be started by entering the following command. If the service is currently running, replace 'start' with `restart`. NOTE: Once the service is running, always remember to 'restart' after making any changes to the ntp config file. Otherwise, the service will continue to run according to the previous config file settings until the service is restarted. Later, we will be creating a cron job to periodically restart the service. For now, enter this command:

```
# service ntpd start
```

11. You should see these two messages:

```
ntpd: Synchronizing with time server:                    [  OK  ]
Starting ntpd:                                           [  OK  ]
```

Figure 3: Starting the NTP service

12. Enter the date command again to see that the time has been synchronized.

    Note: This will only be successful after Quebec's time server has been configured properly. Check with your teammates for its status.

13. The service can be verified and the current pid identified by entering:

```
# service ntpd status
```

14. Now, you are going to make sure that ntpd updates the system time regularly. Skew the local system time again by entering the following command that you entered earlier (up arrow to find this command and press enter):

```
# date -s "Fri Sep 12 14:38:19 EDT 2003"
```

15. A cron job must be created to cause the ntpd service to periodically query the time server and update the local system time accordingly. Enter this command to create the cron job file:

```
# crontab –u root –e
```

16. This file should automatically open using the 'vi' text editor again, so you must press the `[Insert]` or `[i]` key before you can add or modify text.

17. Insert the following line at the top of the file to set up a cron job that will execute every 10 minutes. You can review the 'man 5 crontab' pages to understand the crontab fields in more depth after you are done with this task. After the ntpd is verified to be up and running correctly, the first set of numbers can be changed to a '0' to cause the cron job to run at the top of every hour (0th minute of every hour) instead.

    Make sure that there is a space after the 50 and between each '*' and the '/' character following them. There are no spaces between the initial set of numbers.

```
0,10,20,30,40,50 * * * * /etc/rc.d/init.d/ntpd restart
```

18. Press the `[Enter]` key at the end of the line to make sure that there is a blank line at the bottom of the file.

19. Now Save and exit the file. Press `[Esc]` and type `:wq` then press `[Enter]`.

20. Entering the following command will create init scripts at run levels 3-5 to start the ntpd service every time the system is started up.

```
# chkconfig --level 345 ntpd on
```

21. Use the following command to verify that the ntpd service is turned on at run levels 3, 4, and 5:

```
# chkconfig --list | grep ntpd
```

22. Make sure that it looks like this:

```
ntpd            0:off   1:off   2:off   3:on    4:on    5:on    6:off
```

Figure 4: NTP service startup run levels

23. Now, use the date command to see if the cron job has updated the system time. If not, wait a few more minutes and try again.

24. Once the remote centralized syslog server is installed and configured, we can review the logs that are generated from the Network Time Server process, which will show each time the client is updated and the offset amount by which it is updated.

This page left intentionally blank for pagination purposes

Installing and Configuring Bastille-Linux

You have already performed preliminary hardening (by removing users, groups, etc) and now you will use Bastille-Linux to finish the task. Bastille allows you to easily modify many OS settings. In this task, you will apply a previously configured Bastille template file (analogous to the Security Configuration templates used on Windows) to our system.

1 Bastille Configuration

1.1 Install Bastille

1. If you have not already done so, log on to the machine using:

   Username: **root**

   Password: **tartans@1**

2. Open a terminal window by clicking on:

   Applications->Accessories->Terminal.

3. There are two modules that are required to implement Bastille:

   perl-Curses-1.12-1.2.el4.rf.i386.rpm

   Bastille-3.0.8-1.0.noarch.rpm

   Copy the required modules to the /root directory with this command:

```
# cp /media/AISTS/Tools/Linux/Bastille/* /root
```

4. Using the following commands, change to the /root directory and get a directory listing to confirm all of the Bastille files copied:

```
# cd /root
# ls -l
```

5. Install perl-Curses module:

```
# rpm -ivh perl-Curses-1.28-1.el5.rf.i386.rpm
```

6. Install Bastille module:

```
# rpm -ivh Bastille-3.0.9-1.0.noarch.rpm
```

1.2 Run Bastille

1. Copy Foxtrot's Bastille template to the Bastille configuration directory (this command should be typed as one continuous line with a space after 'cp' and after 'bastille-ids-config'):

```
# cp
/media/AISTS/Tools/Linux/Config_Files/Foxtrot_10.0.4.2/bast
ille-syslog-config /etc/Bastille/config
```

2. Run Bastille in batch mode to apply the preconfigured template:

```
# bastille -b -n 2>/dev/null
```

Note: The template generates error messages about the CentOS version, but the settings will be applied successfully. These messages are not important, so we divert all error messages for this command to /dev/null (the trash).

```
NOTE:    Entering Critical Code Execution.
         Bastille has disabled keyboard interrupts.


NOTE:    Bastille is scanning the system configuration...

NOTE:    Bastille is now locking down your system in accordance with your
         answers in the "config" file.  Please be patient as some modules
         may take a number of minutes, depending on the speed of your
         machine.
NOTE:    Executing Firewall Specific Configuration
NOTE:    Executing File Permissions Specific Configuration
NOTE:    Executing Account Security Specific Configuration
NOTE:    Executing Boot Security Specific Configuration
NOTE:    Executing Inetd Specific Configuration
NOTE:    Executing PAM Specific Configuration
NOTE:    Executing Logging Specific Configuration
NOTE:    Executing Daemon Specific Configuration
NOTE:    Executing Sendmail Specific Configuration
NOTE:    Executing Apache Specific Configuration
NOTE:    Executing FTP Specific Configuration
NOTE:    Executing Temporary Directory Specific Configuration
```

Figure 1: Bastille Output

2 Bastille Configuration

1. The template you applied has been previously configured as follows.

   Enter the following command to view the new Bastille security settings:

```
# cat /etc/Bastille/config | less
```

2. Now you can scroll up and down to view the entire file. When you are finished reviewing the file, press the `[Q]` key to quit viewing the file and return to the shell prompt.

3. After reviewing the config file, *reboot* the system by typing `reboot`. You will now have to login with the admin account that was created in the Linux Host System Hardening task. *Make sure that the admin account was created before rebooting the system or you will not be able to login.*

   You may need to reset the screen resolution to 1024x768 the first time you log on to the admin account. You can do this by going to ‘System’ -> ‘Preferences’ -> ‘Screen Resolution’.

   The remaining sections of this document detail the previously configured template that you applied. Note that you will *NOT* need to actually perform any tasks in the following sections; it is merely here for your edification. After reviewing, you can move on to the next task.

2.1 File Permissions

- Disallow non-root access to ping, usernetctl, mount/umount, and at
- Disable the r-tools (rsh, rlogin, etc), which are troublesome due to their use of weak authentication.

```
# Q:  Would you like to set more restrictive permissions on the administration u
tilities? [N]
FilePermissions.generalperms_1_1="Y"

# Q:  Would you like to disable SUID status for mount/umount?
FilePermissions.suidmount="Y"

# Q:  Would you like to disable SUID status for ping? [Y]
FilePermissions.suidping="Y"

# Q:  Would you like to disable SUID status for at? [Y]
FilePermissions.suidat="Y"

# Q:  Would you like to disable the r-tools? [Y]
FilePermissions.suidrtool="Y"

# Q:  Would you like to disable SUID status for usernetctl? [Y]
FilePermissions.suidusernetctl="Y"
```

Figure 2: File Permissions

2.2 Account Security Settings

- Enforce password aging
- Restrict cron (scheduler) to the root user
- Disallow root from direct login. After you apply this template all administrators must log in using the ‘admin’ account and then su to root.
- Set permissions on all user-created files so that the file is only readable by the user who created it.

```
# Q:  Should Bastille disable clear-text r-protocols that use IP-based authentic
ation? [Y]
AccountSecurity.protectrhost="Y"

# Q:  Would you like to enforce password aging? [Y]
AccountSecurity.passwdage="Y"

# Q:  Do you want to set the default umask? [Y]
AccountSecurity.umaskyn="Y"

# Q:  What umask would you like to set for users on the system? [077]
AccountSecurity.umask="077"

# Q:  Should we disallow root login on tty's 1-6? [N]
AccountSecurity.rootttylogins="N"
```

Figure 3: Account Security Settings

2.3 Boot Security Settings

- Disable CTRL-ALT-DELETE rebooting so that a user must have a valid username and password to reboot the machine.
- Password protect single user mode to require the root password. Single user mode is equivalent to run level 1. You are granted root access, but networking is disabled.

```
# Q:  Would you like to password-protect the GRUB prompt? [N]
BootSecurity.protectgrub="N"

# Q:  Would you like to disable CTRL-ALT-DELETE rebooting? [N]
BootSecurity.secureinittab="Y"

# Q:  Would you like to password protect single-user mode? [Y]
BootSecurity.passsum="Y"
```

Figure 4: Boot Security Settings

2.4 Securing inetd and TCP Wrappers

- Disable telnet and ftp
- Create authorized use banners that will be displayed before the user can log in
- You do not set default deny on TCP wrappers in this configuration. Later on, you will configure an IPtables firewall that will handle this.

```
# Q:  Would you like to set a default-deny on TCP Wrappers and xinetd? [N]
SecureInetd.tcpd_default_deny="N"

# Q:  Would you like to display "Authorized Use" messages at log-in time? [Y]
SecureInetd.banners="Y"

# Q:  Who is responsible for granting authorization to use this machine?
SecureInetd.owner="administrator@aia.class"
```

Figure 5: Securing inetd and TCP Wrappers

2.5 Configure PAM

- Set limits on resources. Users will only be allowed to start 150 concurrently running processes and will be unable to open core system (kernel) files.
- Only allow admin to log in at the console

```
# Q:  Would you like to put limits on system resource usage? [N]
ConfigureMiscPAM.limitsconf="Y"

# Q:  Should we restrict console access to a small group of user accounts? [N]
ConfigureMiscPAM.consolelogin="Y"

# Q:  Which accounts should be able to login at console? [root]
ConfigureMiscPAM.consolelogin_accounts="admin"
```

Figure 6: PAM Settings

2.6 Logging Settings

- You will configure logging in a later module, therefore you will not configure logging through Bastille

```
# Q:  Would you like to set up process accounting? [N]
Logging.pacct="N"
```

Figure 7: Logging Settings

2.7 Sendmail Settings

- Prevent sendmail from running in daemon mode. This machine will not be a mail server, so sendmail does not need to listen for connections

```
# Q:  Do you want to stop sendmail from running in daemon mode? [Y]
Sendmail.sendmaildaemon="Y"
```

Figure 8: Sendmail Settings

2.8 Miscellaneous Daemons

```
# Q:  Would you like to disable acpid and/or apmd? [Y]
MiscellaneousDaemons.apmd="Y"

# Q:  Would you like to disable GPM? [Y]
MiscellaneousDaemons.gpm="Y"

# Q:  Would you like to deactivate the HP OfficeJet (hpoj) script on this machin
e?
MiscellaneousDaemons.disable_hpoj="Y"

# Q:  Would you like to deactivate the ISDN script on this machine?
MiscellaneousDaemons.disable_isdn="Y"
```

Figure 9: Miscellaneous Deamons

2.9 Apache Web Server Settings

```
# Q:  Would you like to bind the Web server to listen only to the localhost? [N]
Apache.bindapachelocal="N"

# Q:  Would you like to bind the web server to a particular interface? [N]
Apache.bindapachenic="N"

# Q:  Would you like to deactivate the following of symbolic links? [Y]
Apache.symlink="N"
```

Figure 10: Apache Web Server Settings

2.10 Tempdir Scripts

- This system is not a multi-user system and therefore you will not be very concerned with the temporary (shared) directories

```
# Q:  Would you like to install TMPDIR/TMP scripts? [N]
TMPDIR.tmpdir="N"
```

Figure 11: Tempdir Scripts

2.11 Packet Filtering Firewall

- You will configure a firewall in a later module, therefore you will not use Bastille's firewall configuration

```
# Q:  Would you like to run the packet filtering script? [N]
Firewall.ip_intro="N"
```

Figure 12: Packet Filtering Firewall

2.12 FTP Settings

```
# Q:  Would you like to disable anonymous download? [N]
FTP.anonftp="Y"

# Q:  Would you like to disable user privileges on the FTP daemon? [N]
FTP.userftp="Y"
```

Figure 13: FTP Settings

Configuring IPTables as a Host Based Firewall on Linux Systems

The host based firewall for Linux, iptables, can be configured by accessing the console directly or via SSH from a management workstation. Iptables has six pre-defined "chains" that are available with the ability to create user defined chains as well. The default chains are:

- INPUT
- OUTPUT
- INPUT
- FORWARD
- PREROUTING
- POSTROUTING

The table below lists various options that can be used when configuring iptables rules. Additional information is available by typing `iptables --help` at the Linux command line or by reviewing the iptables man page (type: `man iptables`).

--table -t	Description
filter	Default table. This is used if not specified
nat	Network address translation
mangle	Used for Quality Of Service (QOS) and preferential treatment
raw	Enables optimization. i.e. Ignore firewall state matching for port 80 for enhanced speed due to less processing. Requires kernel patch

Command (Use one)	Description
-A --append	Append rule to chain
-D --delete	Delete rule from chain
-I --insert	Insert rule at beginning or at specified sequence number in chain.
-R --replace	Replace rule
-F --flush	Flush all rules
-Z --zero	Zero byte counters in all chains
-L --list	List all rules. Add option --line-numbers for rule number.
-N --new-chain	Create new chain
-X --delete-chain	Delete user defined chain
-P --policy	Set default policy for a chain
-E --rename-chain	Rename a chain

Command Option	Description
-s --source	Source address of packet
-d --destination	Destination address of packet
-i --in-interface	Interface packet is arriving from
-o --out-interface	Interface packet is going to
-p --protocol	Protocol: °tcp --sport port[:port] --dport port[:port] --syn °udp °icmp °mac ...
-j --jump	Target to send packet to
-f --fragment	Fragment matching
-c --set-counters	Set packet/byte counter
-m tcp --match tcp	°--source-port port[:port] (port # or range ##) °--destination-port port[:port] °--tcp-flags
-m state --match state	--state °ESTABLISHED °RELATED °NEW °INVALID (Push content, not expected to recieve this packet.)

Defined Policies	Description
ACCEPT	Let packet through
DROP	Deny packet with no reply
REJECT	Deny packet and notify sender
RETURN	Handled by default targets
MARK	Used for error response. Use with option --reject-with type
MASQUERADE	Used with nat table and DHCP.
LOG	Log to file and specify message: °--log-level # °--log-prefix "prefix" °--log-tcp-sequence °--log-tcp-options °--log-ip-options
ULOG	Log to file and specify userpace logging messages
SNAT	Valid in PREROUTING chain. Used by nat.
REDIRECT	Used with nat table. Output.
DNAT	Valid in POSTROUTING chain. Output.
QUEUE	Pass packet to userspace.

Figure 1: IPtables Options

1 Creating Inbound and Outbound Filtering Rules

The filtering rules for this server will be set up to allow the following traffic into and out of the system:

Source Address	Destination Address	Proto	Source Ports	Destination Port	Direction	Purpose
10.0.4.0/24	10.0.4.2/32	ANY	ANY	ANY	Inbound	Management
10.0.3.2/32	10.0.4.2/32	ANY	ANY	ANY	Inbound	Mike-Nagios
10.0.2.0/24	10.0.4.2/32	UDP	ANY	1514	Inbound	Services network
10.0.1.5/32	10.0.4.2/32	UDP	ANY	1514	Inbound	Hotel
10.0.1.3/32	10.0.4.2/32	UDP	ANY	1514	Inbound	Juliet
10.0.2.1/32	10.0.4.2/32	UDP	ANY	514	Inbound	Quebec
10.0.2.0/24	10.0.4.2/32	TCP	ANY	22	Inbound	Services network
10.0.1.5/32	10.0.4.2/32	TCP	ANY	22	Inbound	Hotel
10.0.1.3/32	10.0.4.2/32	TCP	ANY	22	Inbound	Juliet
127.0.0.1/32	127.0.0.1/32	*	*	*	Inbound	Loopback
Log All Denied						
10.0.4.2/32	10.0.4.0/24	ANY	ANY	ANY	Outbound	Management
10.0.4.2/32	10.0.2.3/32	TCP	ANY	25	Outbound	SMTP
10.0.4.2/32	10.0.2.4/32	UDP	ANY	53	Outbound	DNS
10.0.4.2/32	10.0.2.1/32	UDP	ANY	123	Outbound	NTP
10.0.4.2/32	10.0.2.1/32	TCP	ANY	3128	Outbound	Squid Proxy
127.0.0.1/32	127.0.0.1/32	*	*	*	Outbound	Loopback
Log All Denied						

1. If you have not already done so, log on to the machine using the newly enforced admin account:

   Username: **admin** Password: **steelers**

2. Open a terminal window by going to ‘Applications’ -> ‘Accessories’ -> ‘Terminal’.
3. Elevate to root level privileges by typing the following command and entering the root password **tartans@1**

```
# su -
```

4. Ensure iptables is stopped.

```
# service iptables stop
```

5. Clear all existing iptables rules.

```
# iptables --flush
```

6. Set the default policy for the FORWARD chain to DROP all packets.

```
# iptables -P FORWARD DROP
```

7. Create the iptables file that will be used to save firewall rules.

```
# iptables-save > /etc/sysconfig/iptables
# vi /etc/sysconfig/iptables
```

8. Remove the last two lines. Move the cursor to each line and press the [D] key twice. This will delete the current line in VI. The file should look like the following when completed:

```
# Generated by iptables-save v1.3.5 on Mon Jun 14 10:52:10 2010
*filter
:INPUT ACCEPT [5:420]
:FORWARD DROP [0:0]
:OUTPUT ACCEPT [5:420]
```

9. Add the remaining rules to the iptables file as listed below. Comments/remarks are identified with a '#' at the beginning of the line. These lines are used to identify what the rules beneath them are used for. Although they are not required, it is a good practice to describe the rules, their intent, who added the rule, and potentially the date when the rule was added or modified. Use the cursor to go to the bottom of the file. Simultaneously press the [Shift] and [A] keys to append text to the end of the last line. Press [Enter] to add a new line. Enter the following lines:

```
# Allow all inbound traffic from the MGMT network
-A INPUT -s 10.0.4.0/24 -d 10.0.4.2/32 -i eth0 -j ACCEPT

# Allow all inbound traffic from Mike-Nagios
-A INPUT -s 10.0.3.2/32 -d 10.0.4.2/32 -i eth0 -j ACCEPT

# Allow OSSEC agent from Services network to Foxtrot
-A INPUT -s 10.0.2.0/24 -d 10.0.4.2/32 -i eth0 -p udp --dport 1514 -j ACCEPT

# Allow OSSEC agent from DMZ network
-A INPUT -s 10.0.1.5/32 -d 10.0.4.2/32 -i eth0 -p udp --dport 1514 -j ACCEPT
-A INPUT -s 10.0.1.3/32 -d 10.0.4.2/32 -i eth0 -p udp --dport 1514 -j ACCEPT

# Allow Mike's OSSEC agent
-A INPUT -s 10.0.3.2/32 -d 10.0.4.2/32 -i eth0 -p udp --dport 1514 -j ACCEPT

# Allow Syslog from Quebec
-A INPUT -s 10.0.2.1/32 -d 10.0.4.2/32 -i eth0 -p udp --dport 514 -j ACCEPT

# Allow Syslog from Romeo
-A INPUT -s 10.0.4.1/32 -d 10.0.4.2/32 -i eth0 -p udp --dport 514 -j ACCEPT

# Allow SSH from Services network
-A INPUT -s 10.0.2.0/24 -d 10.0.4.2/32 -i eth0 -p tcp --dport 22 -j ACCEPT

# Allow SSH from DMZ network
-A INPUT -s 10.0.1.5/32 -d 10.0.4.2/32 -i eth0 -p tcp --dport 22 -j ACCEPT
-A INPUT -s 10.0.1.3/32 -d 10.0.4.2/32 -i eth0 -p tcp --dport 22 -j ACCEPT

# Allow Mike access through SSH
-A INPUT -s 10.0.3.2/32 -d 10.0.4.2/32 -i eth0 -p tcp --dport 22 -j ACCEPT

# Allow all established connections
-A INPUT -i eth0 -m state --state ESTABLISHED,RELATED -j ACCEPT

# Allow all inbound traffic on the loopback interface
-A INPUT -i lo -p all -j ACCEPT

# Enable logging on INPUT chain
-A INPUT -j LOG --log-level 6

# Set the default input policy to Drop
-P INPUT DROP
```

Figure 2: IPtables Input Rules

```
# Allow outbound mail traffic to Bravo
-A OUTPUT -d 10.0.2.3/32 -o eth0 -p tcp --dport 25 -j ACCEPT

# Allow outbound DNS traffic to Alpha
-A OUTPUT -d 10.0.2.4/32 -o eth0 -p udp --dport 53 -j ACCEPT

# Allow outbound web proxy traffic to Quebec
-A OUTPUT -d 10.0.2.1/32 -o eth0 -p tcp --dport 3128 -j ACCEPT

# Allow outbound NTP traffic to Quebec
-A OUTPUT -d 10.0.2.1/32 -o eth0 -p udp --dport 123 -j ACCEPT

# Allow all outbound traffic to the MGMT network
-A OUTPUT -d 10.0.4.0/24 -o eth0 -p all -j ACCEPT

# Allow all established connections
-A OUTPUT -o eth0 -m state --state ESTABLISHED,RELATED -j ACCEPT

# Allow all outbound traffic on the loopback interface
-A OUTPUT -o lo -p all -j ACCEPT

# Enable logging on OUTPUT chain
-A OUTPUT -j LOG --log-level 6

# Set the default OUTPUT policy to Drop
-P OUTPUT DROP

# Enable rule set
COMMIT
```

Figure 3: IPtables Output Rules

10. Save and exit the file. Press `[Esc]` and type `:wq` then press `[Enter]`.

1.1 Applying the firewall rules

1. Enter the following command to start the iptables firewall:

```
# service iptables start
```

2. If the service started successfully, you should see the following:

```
Flushing firewall rules:                                   [  OK  ]
Setting chains to policy ACCEPT: filter                    [  OK  ]
Unloading iptables modules:                                [  OK  ]
Applying iptables firewall rules:                          [  OK  ]
Loading additional iptables modules: ip_conntrack_netbios_n[  OK  ]
```

Figure 4: IPtables Successful Startup

1.2 Making the iptables file immutable

1. Since we do not want the iptables file to change for ANY reason after the rules have been built without intervention from the administrator, we will make this file immutable. To do this, we will issue the following command.

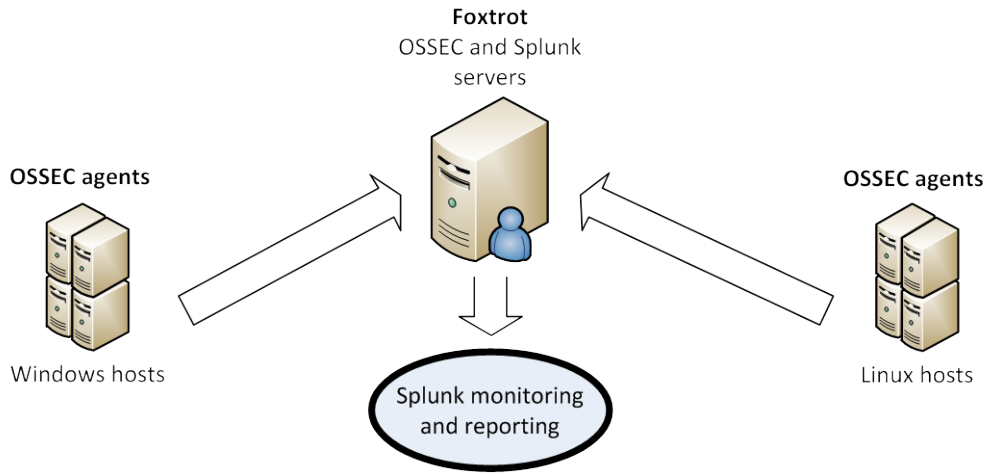
```
# chattr +i /etc/sysconfig/iptables
```

2. Relinquish the elevated root privileges by typing the following command:

```
# exit
```

OSSEC HIDS Server

OSSEC is a scalable, multi-platform, open source host-based intrusion detection system (HIDS) that runs on most operating systems, including Linux, OpenBSD, FreeBSD, MacOS, Solaris, and Windows. It has a powerful correlation and analysis engine integrating log analysis, file integrity checking, Windows registry monitoring, centralized policy enforcement, rootkit detection, real-time alerting and active response. You will integrate OSSEC with Splunk so that you can easily process and correlate all event logs and alerts through a single interface. In this case the basic architecture will be as shown below:



OSSEC agents will be installed on each Linux and Windows server and send events to the OSSEC server which is running on Foxtrot. The OSSEC server will process these events and generate warnings and alerts. Splunk will directly gather information from the OSSEC server and index all events, generating graphs and reports. OSSEC provides an additional advantage over traditional syslog agents by setting up a shared key pair between the OSSEC server and each OSSEC agent, allowing for secure, encrypted log transfer seamlessly without the need to create additional encrypted tunnels.

1 OSSEC Server Setup

1.1 Installation and configuration

1. If you have not already done so, log on to the machine using the newly enforced admin account:

   Username: **admin** Password: **steelers**

2. Open a terminal window by going to ‘Applications’ -> ‘Accessories’ -> ‘Terminal’.
3. Elevate to root level privileges by typing the following command and entering the root password **tartans@1**

```
# su -
```

4. Navigate to the Course CD by executing the following command:

```
# cd /media/AISTS/Tools/Linux/OSSEC/
```

5. Copy the OSSEC installation package:

```
# cp ossec-hids-2.4.1.tar.gz /root/
```

6. Extract installation package to the root directory:

```
# cd /root/
# tar xzvf ossec-hids-2.4.1.tar.gz
```

7. Start installation using the following command and accept the default language by pressing [Enter]:

```
# cd ossec-hids-2.4.1
# ./install.sh
```

8. Read the introduction and press [Enter]:

```
OSSEC HIDS v2.4.1 Installation Script - http://www.ossec.net

You are about to start the installation process of the OSSEC HIDS.
You must have a C compiler pre-installed in your system.
If you have any questions or comments, please send an e-mail
to dcid@ossec.net (or daniel.cid@gmail.com).

 - System: Linux Foxtrot 2.6.18-164.el5
 - User: root
 - Host: Foxtrot


 -- Press ENTER to continue or Ctrl-C to abort. --
```

9. Answer the rest of the questions as shown and hit [Enter] when you have finished:

```
1- What kind of installation do you want (server, agent, local or help)? server

  - Server installation chosen.

2- Setting up the installation environment.

 - Choose where to install the OSSEC HIDS [/var/ossec]:

    - Installation will be made at  /var/ossec .

3- Configuring the OSSEC HIDS.

  3.1- Do you want e-mail notification? (y/n) [y]:
   - What's your e-mail address? eventwatch@aia.class
   - What's your SMTP server ip/host? 10.0.2.3

  3.2- Do you want to run the integrity check daemon? (y/n) [y]:

   - Running syscheck (integrity check daemon).

  3.3- Do you want to run the rootkit detection engine? (y/n) [y]:

   - Running rootcheck (rootkit detection).
```

```
3.4- Active response allows you to execute a specific
     command based on the events received. For example,
     you can block an IP address or disable access for
     a specific user.
     More information at:
     http://www.ossec.net/en/manual.html#active-response

 - Do you want to enable active response? (y/n) [y]: n

   - Active response disabled.

3.5- Do you want to enable remote syslog (port 514 udp)? (y/n) [y]: y

 - Remote syslog enabled.

3.6- Setting the configuration to analyze the following logs:
  -- /var/log/messages
  -- /var/log/secure
  -- /var/log/maillog

- If you want to monitor any other file, just change
  the ossec.conf and add a new localfile entry.
  Any questions about the configuration can be answered
  by visiting us online at http://www.ossec.net .


  --- Press ENTER to continue ---
```

10. When installation has finished you should see following screen and hit [Enter]:

```
- System is Redhat Linux.
- Init script modified to start OSSEC HIDS during boot.

- Configuration finished properly.

- To start OSSEC HIDS:
              /var/ossec/bin/ossec-control start

- To stop OSSEC HIDS:
              /var/ossec/bin/ossec-control stop

- The configuration can be viewed or modified at /var/ossec/etc/ossec.conf


   Thanks for using the OSSEC HIDS.
   If you have any question, suggestion or if you find any bug,
   contact us at contact@ossec.net or using our public maillist at
   ossec-list@ossec.net
   ( http://www.ossec.net/main/support/ ).

   More information can be found at http://www.ossec.net

   ---  Press ENTER to finish (maybe more information below). ---
```

11. You may need to perform the following command in order to write to the OSSEC configuration file:

```
# chmod 640 /var/ossec/etc/ossec.conf
```

12. Open the default configuration file with the following command:

```
# vi /var/ossec/etc/ossec.conf
```

You will install OSSEC agents on all of the host machines, which will send logs to the OSSEC server. However, OSSEC agents cannot be installed on Quebec and Romeo, the firewall and router. These machines will use traditional syslog to send information to Foxtrot. You must configure the OSSEC server to allow syslog connections from these IP addresses.

13. Press the / key and then type ‘syslog’ and press [Enter] to search for the first occurrence of the word syslog in the file.
14. Press n to skip to the next occurrence. You should see the following:

```
<remote>
  <connection>syslog</connection>
</remote>
```

15. Edit the above section of the configuration file so that it looks like the screenshot below:

```
<remote>
  <connection>syslog</connection>
  <allowed-ips>10.0.2.1</allowed-ips>
  <allowed-ips>10.0.4.1</allowed-ips>
</remote>
```

16. Save and exit the file by pressing [Esc] and then typing `:wq` and pressing [Enter].
17. Start the OSSEC server by executing following command:

```
# /var/ossec/bin/ossec-control start
```

```
[root@Foxtrot ossec-hids-2.4.1]# /var/ossec/bin/ossec-control start
Starting OSSEC HIDS v2.4.1 (by Trend Micro Inc.)...
Started ossec-maild...
Started ossec-execd...
Started ossec-analysisd...
Started ossec-logcollector...
Started ossec-remoted...
Started ossec-syscheckd...
Started ossec-monitord...
Completed.
```

18. If you are not performing any more administrative tasks on this machine, relinquish the elevated root privileges by typing the following command:

```
# exit
```

Remote Centralized Monitoring Server

Splunk is a centralized monitoring tool that has search, monitoring, and reporting features. It collects logs, metrics, and other data from different places like applications, servers, and network devices and indexes all information in searchable repository. Also Splunk can generate graphs, SQL reports, and alerts from this indexed data repository.

1 Splunk Setup

1.1 Installation

1. If you have not already done so, log on to the machine using the newly enforced admin account:

   Username: **admin** Password: **steelers**

2. Open a terminal window by going to 'Applications' -> 'Accessories' -> 'Terminal'.
3. Elevate to root level privileges by typing the following command and entering the root password **tartans@1**

```
# su -
```

4. Navigate to the Course CS by executing following command:

```
# cd /media/AISTS/Tools/Linux/Splunk/
```

5. Execute the following command to begin installation:

```
# rpm -ivh splunk-4.1.3-80534.i386.rpm
```

```
[root@Foxtrot Splunk]# rpm -ivh splunk-4.1.3-80534.i386.rpm
warning: splunk-4.1.3-80534.i386.rpm: Header V3 DSA signature: NOKEY, key ID 653fb112
Preparing...                ########################################### [100%]
   1:splunk                 ########################################### [100%]
-----------------------------------------------------------------------
Splunk has been installed in:
        /opt/splunk

To start Splunk, run the command:
        /opt/splunk/bin/splunk start

To use the Splunk Web interface, point your browser at:
        http://Foxtrot:8000

Complete documentation is at http://www.splunk.com/r/docs
-----------------------------------------------------------------------
[root@Foxtrot Splunk]#
```

6. Splunk requires a current version of Flash Player so you will install it by executing the following command:

```
# rpm -ivh flash-plugin-10.0.32.18-0.2.el5.rf.i386.rpm
```

7. Copy the OSSEC application for Splunk to the /opt/splunk/etc/apps directory, extract it, and remove archive:

```
# cp ossec.tgz /opt/splunk/etc/apps/
# cd /opt/splunk/etc/apps/
# tar -xzvf ossec.tgz
# rm -f ossec.tgz
```

8. Now start Splunk by executing following command:

```
# /opt/splunk/bin/splunk start
```

9. Press `[Space]` to reach end of the 'License Agreement' and accept the license by typing `y`.

```
SPLUNK INC.

SOFTWARE LICENSE AGREEMENT

THIS SPLUNK SOFTWARE LICENSE AGREEMENT (THE "AGREEMENT") GOVERNS ALL SOFTWARE
PROVIDED BY SPLUNK INC. ("SPLUNK") INCLUDING FREE SPLUNK SOFTWARE ("FREE
SOFTWARE") AND SOFTWARE PURCHASED THROUGH SPLUNK'S ONLINE STORE OR OTHER
CHANNELS ("PURCHASED SOFTWARE"), COLLECTIVELY THE SPLUNK SOFTWARE ("SOFTWARE")
AND ANY AND ALL UPDATES, UPGRADES, AND MODIFICATIONS THERETO. CONFIRMATION OF
YOUR ORDERS ("ORDER CONFIRMATION") WILL BE DEEMED INCORPORATED INTO AND MADE
PART OF THIS AGREEMENT.

YOU WILL BE REQUIRED TO INDICATE YOUR AGREEMENT TO THESE TERMS AND CONDITIONS IN
ORDER TO DOWNLOAD THE SOFTWARE AND REGISTER WITH SPLUNK IN ORDER TO OBTAIN
LICENSE KEYS NECESSARY TO COMPLETE THE INSTALLATION PROCESS FOR PURCHASED
SOFTWARE.  BY CLICKING ON THE "YES" BUTTON, DOWNLOADING OR INSTALLING THE
SOFTWARE, OR USING ANY MEDIA THAT CONTAINS THE SOFTWARE, YOU ARE CONSENTING TO
BE BOUND BY THIS AGREEMENT.

IF YOU AGREE TO THESE TERMS ON BEHALF OF A BUSINESS, YOU REPRESENT AND WARRANT
THAT YOU HAVE AUTHORITY TO BIND THAT BUSINESS TO THIS AGREEMENT, AND YOUR
AGREEMENT TO THESE TERMS WILL BE TREATED AS THE AGREEMENT OF THE BUSINESS.  IN
THAT EVENT, "YOU" AND "YOUR" REFER HEREIN TO THAT BUSINESS.

 "Splunk Developer API" means the documentation and functionality enabling the
 creation of extensions to the Software. "Example Modules" means the source code
 and binary form of examples that use the Splunk Developer API.

--More--(7%)


 GENERAL. This Agreement shall be governed by and construed in accordance with
 the laws of the State of California, as if performed wholly within the state
 and without giving effect to the principles of conflict of law. Any legal
 action or proceeding arising under this Agreement will be brought exclusively
 in the federal or state courts located in the Northern District of California
 and the parties hereby consent to personal jurisdiction and venue therein. If
 any portion hereof is found to be void or unenforceable, the remaining
 provisions of this Agreement shall remain in full force and effect. Neither
 party may assign this Agreement, in whole or in part, except in connection with
 an internal reorganization or a sale of the business with which this Agreement
 is associated without Splunk's prior written consent, and any attempt to assign
 this Agreement other than as permitted above will be null and void. This
 Agreement is intended for the sole and exclusive benefit of the parties and is
 not intended to benefit any third party. Only the parties to this Agreement may
 enforce it. This Agreement and any Order Confirmations constitute the complete
 and exclusive understanding and agreement between the parties regarding their
 subject matter and supersede all prior or contemporaneous agreements or
 understandings, written or oral, relating to their subject matter. Any waiver,
 modification or amendment of any provision of this Agreement will be effective
 only if in writing and signed by duly authorized representatives of both
 parties.

 EACH PARTY SIGNING BELOW REPRESENTS AND WARRANTS THAT THEY HAVE THE AUTHORITY
 TO BIND THAT BUSINESS TO THIS AGREEMENT, AND THEIR AGREEMENT TO THESE TERMS
 WILL BE TREATED AS THE AGREEMENT OF THE BUSINESS.  IN THAT EVENT, "YOU" AND
 "YOUR" REFER HEREIN TO THAT BUSINESS.

Do you agree with this license? [y/n]: y
```

10. If Splunk has successfully started then you should see the following screen:

```
Starting splunk server daemon (splunkd)... Done.Starting splunkweb... /opt/splunk/share/splunk/ce
rts does not exist. Will create
Generating certs for splunkweb server
Generating a 1024 bit RSA private key
.......................................................................+++++++
...................+++++++
writing new private key to 'privkeySecure.pem'
-----
Signature ok
subject=/CN=Foxtrot/O=SplunkUser
Getting CA Private Key
writing RSA key
                                                            [  OK  ]
Done.
If you get stuck, we're here to help.
Look for answers here: http://www.splunk.com/base/Documentation

The Splunk web interface is at http://Foxtrot:8000
```

11. Set Splunk to start on system boot:

```
# /opt/splunk/bin/splunk enable boot-start
```

1.2 Configuration

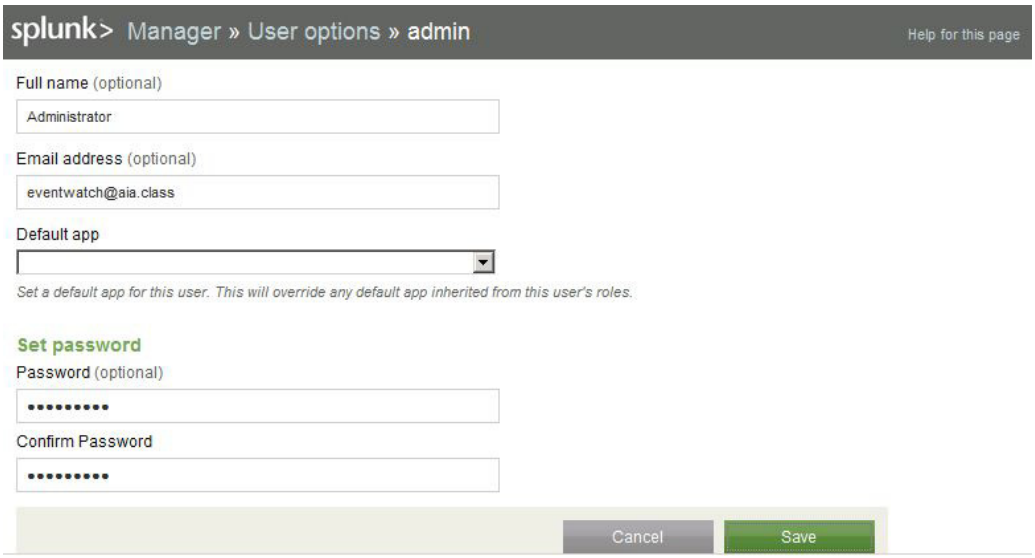
Once the Splunk service is started you can access Splunk at http://foxtrot.aia.class:8000 (or http://10.0.4.2:8000). The commercial version of Splunk allows for many more control options. These include the use of SSL to securely access the console and the ability to setup multiple users with numerous access roles. The free version that you are using does not provide these same options.

1. Open Internet Explorer on a management workstation and navigate to `http://foxtrot.aia.class:8000`.
2. Click 'Add' twice and then 'Close' if prompted with the Internet Explorer Enhanced Security Configuration prompt.
3. If the 'Welcome to Internet Explorer 8' screen appears, click 'Ask me Later' and close the tab to the Microsoft website that opens.
4. At the Splunk login page, login with the following Splunk default credentials:

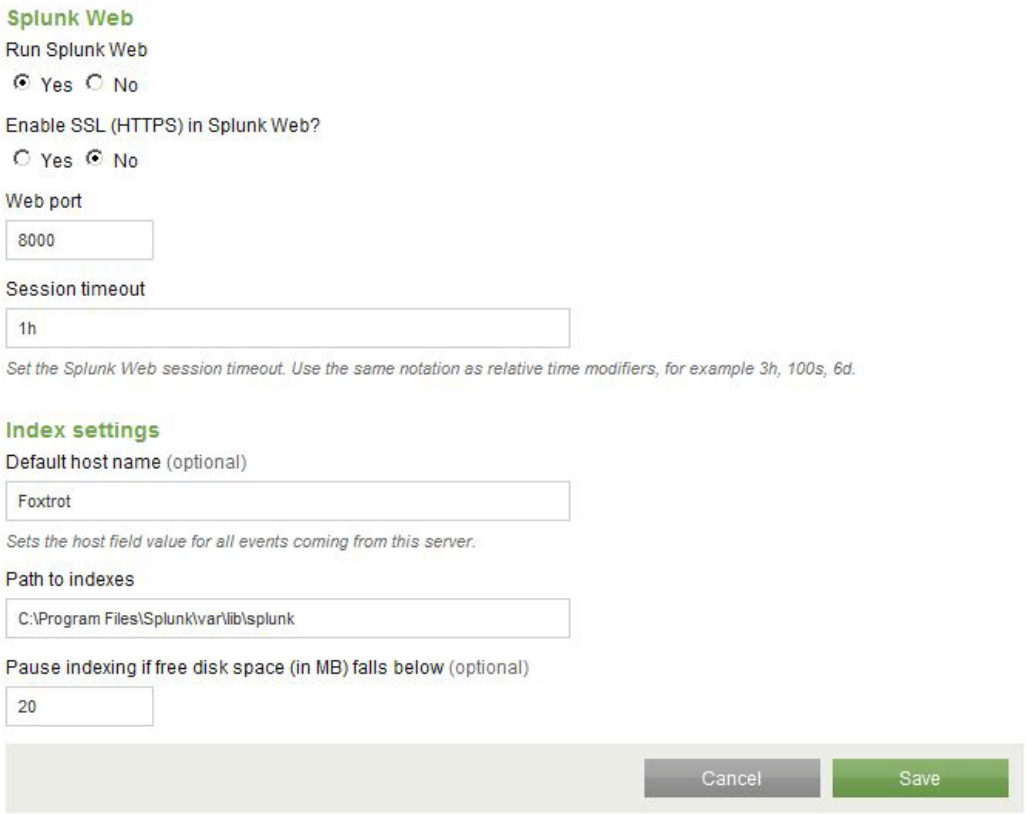
   Username: **admin**

   Password: **changeme**
5. Once at the Splunk welcome screen, click on the 'Manager' link.
6. Scroll to the bottom of the page and click on the 'User options' link.

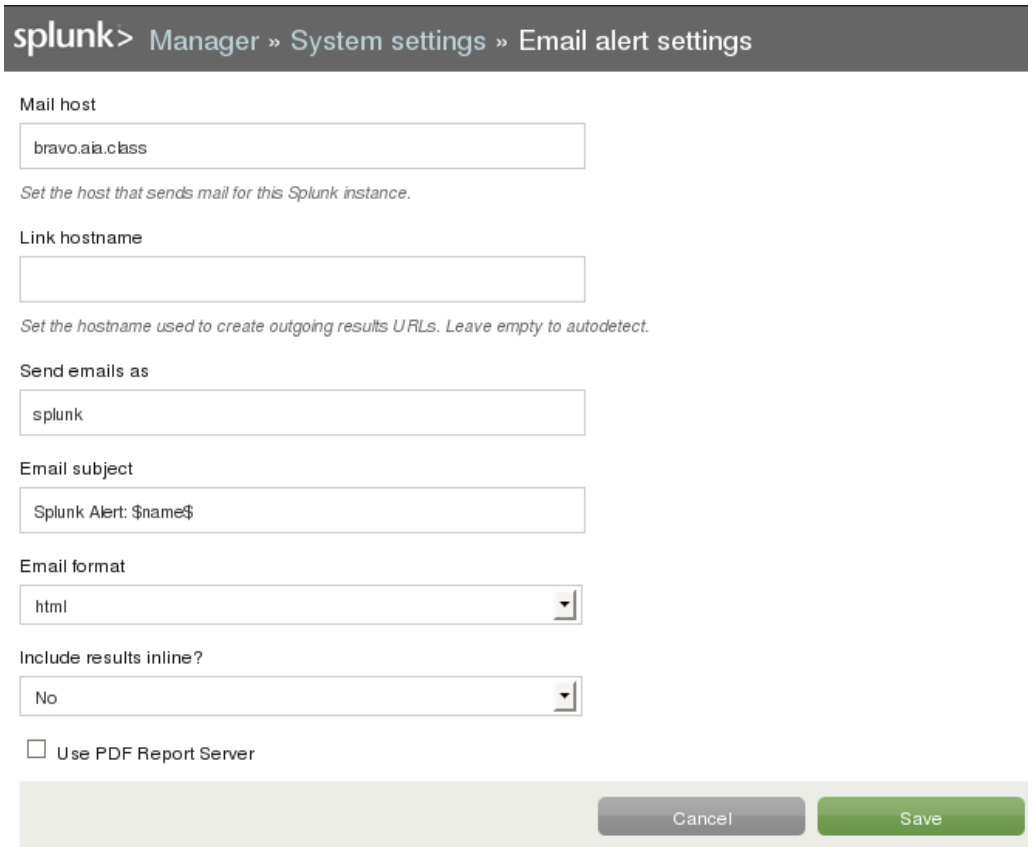
7. Change the email address to `eventwatch@aia.class` and set the password to `tartans@1` and click 'Save'.



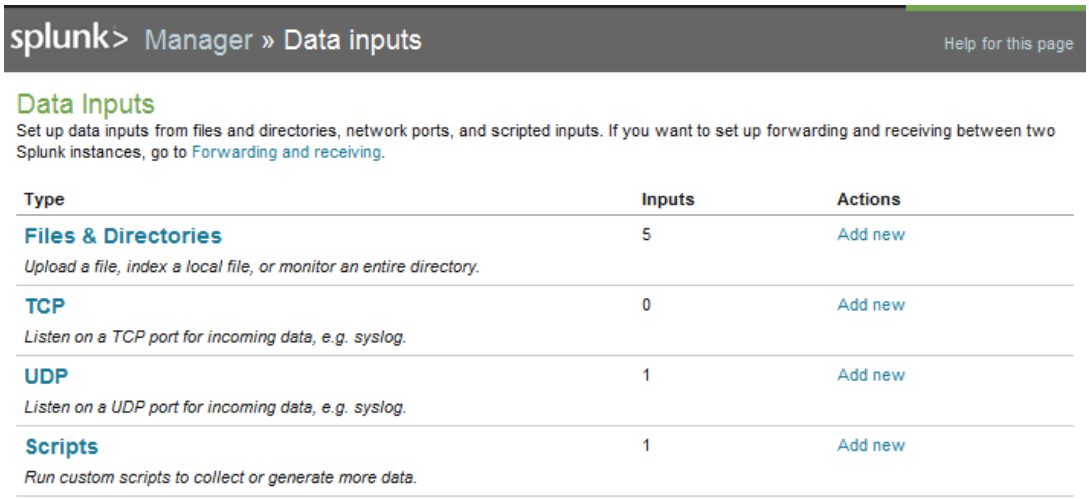
8. Click on the 'System settings' link on the Manager page and go to "General settings'.
9. Verify the Splunk server name and Web Port #. In the 'Index settings' section change the value of the 'Pause indexing if free disk space (in MB) falls below' field to 20 MB. Click 'Save'.



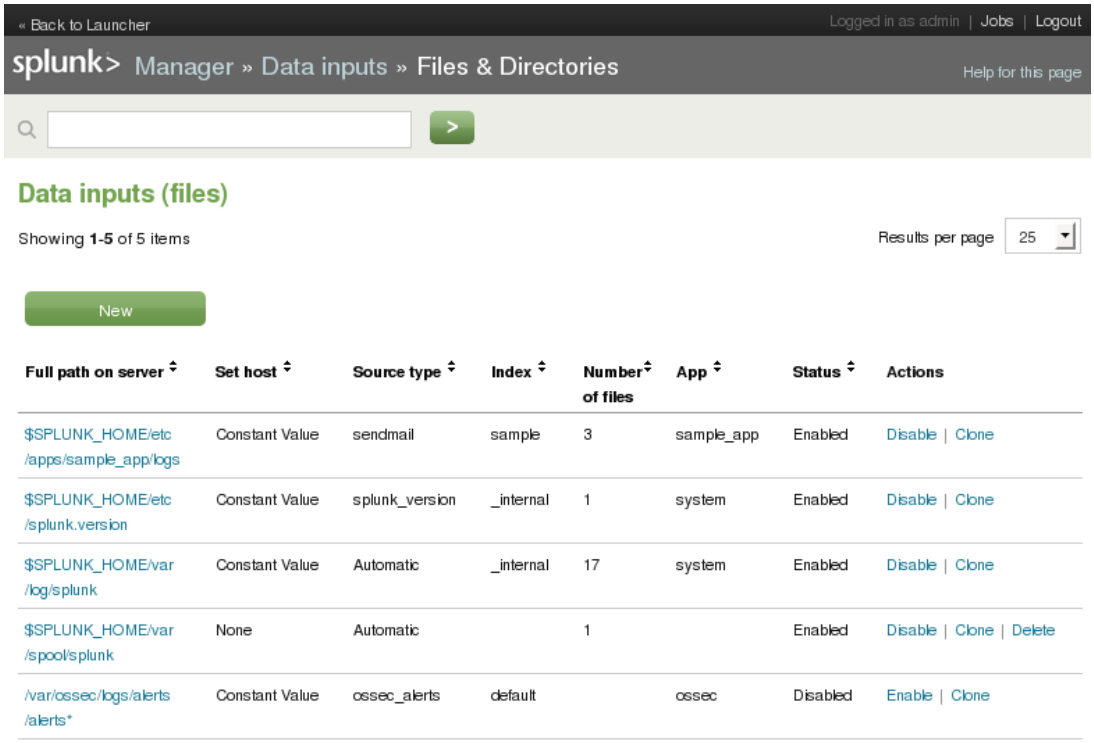
10. Go back into ‘System Settings’ page click on email alert settings and type `bravo.aia.class` in the mail host field. Click ‘Save’.



11. Go back to ‘Manager’ page and click on ‘Data inputs’. You should see following web page and then go to ‘Files & Directories’.



12. If you have successfully installed OSSEC application for Splunk then you should see the following page. The last entry indicates OSSEC for Splunk has been integrated into Splunk. Click ‘Enable’ from the ‘Actions’ row and Splunk is now ready to process OSSEC alert logs.



Full path on server	Set host	Source type	Index	Number of files	App	Status	Actions
$SPLUNK_HOME/etc /apps/sample_app/logs	Constant Value	sendmail	sample	3	sample_app	Enabled	Disable | Clone
$SPLUNK_HOME/etc /splunk.version	Constant Value	splunk_version	_internal	1	system	Enabled	Disable | Clone
$SPLUNK_HOME/var /log/splunk	Constant Value	Automatic	_internal	17	system	Enabled	Disable | Clone
$SPLUNK_HOME/var /spool/splunk	None	Automatic		1		Enabled	Disable | Clone | Delete
/var/ossec/logs/alerts /alerts*	Constant Value	ossec_alerts	default		ossec	Disabled	Enable | Clone

13. Click the ‘Manager’ link.
14. You need to restart Splunk for the changes to take effect. Select ‘Server controls’ and click ‘Restart Splunk’.
15. Click ‘OK’ to restart Splunk.
16. When it is done restarting, click ‘OK’ and close Internet Explorer.
17. If you are not performing any more administrative tasks on this machine, relinquish the elevated root privileges by typing the following command:

```
# exit
```

Golf High Level Description

Golf is the Intrusion Detection System (IDS) located on the Management network, with a sniffer interface to monitor the DMZ. It will provide network administrators information regarding the traffic going to and from the DMZ hosts. Golf's rules are configured to view all addresses as hostile except the DMZ hosts. This configuration allows network administrators to see reconnaissance and attack traffic originating from the external network or the internal network (which would indicate an internal compromise).

Golf will also serve as a central collection point for IDS alerts from sensors residing on the services network (Lima) and the user network (Mike). Snort will be installed on Golf, Lima, and Mike. Each of those sensors will log alerts to a MySQL database that resides on Golf. Administrators will use the Basic Analysis Security Engine (BASE) to view alerts and correlate events. BASE and its' prerequisites will be installed and configured on Golf.

Following are descriptions of Golf's specific hands-on tasks that students must complete:

Task 1. Linux Host System Hardening

Students will be minimizing non-essential services (e.g., xinetd, portmap) as well as extraneous default users and groups. As a standalone system running Snort, Golf does not require these components and so students will follow security best practices in removing them. Also, students will create a non-privileged administrator account to provide an audit trail for all administrative access.

Task 2. Configuring Time Synchronization

Network Time Protocol (NTP) is used to synchronize the host computer's time to a local time server, in this deployment it is the Internet firewall (Quebec).

Alpha will synchronize to Quebec every ten minutes; the Linux hosts will synchronize with Quebec every ten minutes; and the Window hosts will synchronize with Alpha every forty-five minutes until three good synchronizations occur, then once every eight hours. With all the hosts' time across the network synchronized, the cross examination of multiple hosts' logs, or the logs at the syslog Server, become more meaningful and easier to examine.

Task 3. Configuring Bastille

The Bastille hardening system is a user-configurable script that attempts to lock down Linux/UNIX operating systems. The Bastille script embodies recommendations from every major reputable source on Linux/UNIX security. We will use pre-configured Bastille templates to lock down such weak system settings as maximum password age, user privileges, etc.

Task 4. Configuring IPTables

IPTables is a Linux firewall application which can be configured to do packet filtering on network firewalls or on host systems. IPTables will be configured on this host as a host-based firewall to allow only valid packets to and from this host. To do this, we will set up INPUT and OUTPUT rules to specifically allow known-good packets into and out of the host, and will create default LOG rules and DROP rules.

Task 5. Installing the IDS

Students will install and configure Snort, MySQL, BASE and the necessary supporting applications.

Task 6. Configuring OSSEC Agent

Students will install and configure OSSEC Agent, which will then send information about security events to the syslog/OSSEC server (Foxtrot).

Linux Host System Hardening

1 Remove Zeroconf Route

1. If you have not already done so, log on to the machine using:

   Username: **root** Password: **tartans@1**

2. Open a terminal window by going to ‘Applications’ -> ‘Accessories’ -> ‘Terminal’.

By default Linux adds a "zeroconf" route at boot time. This is a static route that designates the 169.254/16 prefix as local. This is unnecessary on our network, so we will remove the route:

3. Specify to not use zeroconf at boot time:

NOTE: In this and all subsequent Linux documents, the ‘#’ at the beginning of each line should *not* be typed in as part of the command. It is simply meant to represent a command prompt.

```
# echo "NOZEROCONF=yes" >> /etc/sysconfig/network
```

2 Linux Kernel Upgrade

One of the most essential hardening tasks for Linux systems is to ensure that the latest kernel version is being used. The kernel is the core of the operating system and every effort should be made to ensure the most current updated and/or patched version is in use. Most versions of Linux include some automated means for updating software, including the kernel. We will use a tool called YUM (Yellowdog Updater Modified) to download updates from an external web server hosting our YUM repository.

2.1 Apply latest updates to Kernel and other installed packages

1. Edit the yum config file using vi:

```
# vi /etc/yum.repos.d/CentOS-Base.repo
```

2. There are six sections of the file denoted by names in brackets. You will edit 3 of these sections and disable the other 3. Press `[Insert]` or `[i]` to edit the file and scroll down to the first section, ‘[base]’. Comment out the line beginning with ‘mirrorlist=’ by typing a # at the beginning of the line. Next, uncomment the line below it beginning with ‘baseurl=’ and edit the URL to point to our trusted yum repository at `http://192.168.30.14/centos/5.4/os/i386/`. The updated lines will be as follows:

```
[base]
name=CentOS-$releasever - Base
#mirrorlist=http://mirrorlist.centos.org/?release=$releasever&arch=$basearch&rep
o=os
baseurl=http://192.168.30.14/centos/5.4/os/i386/
gpgcheck=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-CentOS-5
```

Figure 1: Configuring YUM base repository

3. Repeat the above steps for the second section, '[updates]', pointing it to the URL `http://192.168.30.14/centos/5.4/updates/i386/`.

```
#released updates
[updates]
name=CentOS-$releasever - Updates
#mirrorlist=http://mirrorlist.centos.org/?release=$releasever&arch=$basearch&rep
o=updates
baseurl=http://192.168.30.14/centos/5.4/updates/i386/
gpgcheck=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-CentOS-5
```

Figure 2: Configuring YUM updates repository

4. Scroll down to the next section, '[addons]' and add `enabled=0` underneath the last line of the section to disable it. The updated lines will be as follows:

```
#packages used/produced in the build but not released
[addons]
name=CentOS-$releasever - Addons
mirrorlist=http://mirrorlist.centos.org/?release=$releasever&arch=$basearch&repo
=addons
#baseurl=http://mirror.centos.org/centos/$releasever/addons/$basearch/
gpgcheck=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-CentOS-5
enabled=0
```

Figure 3: Disabling YUM addons repository

5. Scroll down to the next section, '[extras]' and point it to the URL `http://192.168.30.14/centos/5.4/extras/i386/`.

```
#additional packages that may be useful
[extras]
name=CentOS-$releasever - Extras
#mirrorlist=http://mirrorlist.centos.org/?release=$releasever&arch=$basearch&rep
o=extras
baseurl=http://192.168.30.14/centos/5.4/extras/i386/
gpgcheck=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-CentOS-5
```

Figure 4: Configuring YUM extras repository

We will leave the remaining two sections at their default setting of disabled.

6. Press `[Esc]`, then type **:**`wq` and press `[Enter]` to save the changes and exit VI.
7. Add a variable to '/etc/yum.conf' so that all future updates use the HTTP proxy. Edit '/etc/yum.conf' with vi:

```
# vi /etc/yum.conf
```

8. To configure yum to use the web proxy server we need to add a line to the '/etc/yum.conf file'. Add the following line to the end of the '[main]' section of the file:

```
proxy=http://10.0.2.1:3128
```

```
[main]
cachedir=/var/cache/yum
keepcache=0
debuglevel=2
logfile=/var/log/yum.log
distroverpkg=redhat-release
tolerant=1
exactarch=1
obsoletes=1
gpgcheck=1
plugins=1
proxy=http://10.0.2.1:3128
```

Figure 5: Configuring YUM proxy server

Press `[Esc]` then type `:wq` and press `[Enter]` to save the changes and exit VI.

NOTE: In order to access the Internet, or even our trusted update server, routing will need to be enabled on Quebec and Romeo. Once the Access control lists are in place on these two router/firewall machines, very few devices will be able to access external networks directly. You may need to wait until these tasks are completed--check with your teammates on this.

9. Run yum in update mode:

```
# yum update
```

10. Type y then press `[Enter]` when prompted to download the updates.
11. Type y then press `[Enter]` when prompted to import the CentOS 5 GPG key.

    A number of packages will be downloaded and installed, including a newer kernel.

    This step may take several minutes to complete. Press `[Ctrl]` + `[Shift]` + `[T]` to open a new terminal tab if you want to move on to the next steps while the updates take place.

3 Service Minimization

3.1 Removing Unnecessary Services

By default Linux runs many services that a standalone server will not need. Extraneous services are dangerous because they provide possible attack vectors.

The services that will need to be removed from this system are:

- anacron
- apmd
- atd
- autofs
- cpuspeed
- cups
- gpm
- irqbalance
- mdmonitor
- mdmpd
- microcode_ctl
- netfs
- nfslock
- portmap
- rawdevices
- rpcgssd
- rpcsvcgssd
- rpcidmapd
- sendmail
- xinetd

1. Terminate the ‘anacron’ service properly by using the following command:

```
# service anacron stop
```

2. Remove the ‘anacron’ startup routine using the following command:

```
# chkconfig --del anacron
```

```
Stopping anacron:                                          [  OK  ]
```

Figure 6: Removing a service

3. Repeat steps #1 and #2 for each service listed above. (ADVANCED: see the ‘Bash Script’ ADDENDUM located on the last two pages of this section to automate these repetitive steps.)

   Note: On some systems, some of the services may not be started and may not return the ‘OK’ when stopped. If this is the case, it will be sufficient to simply delete the service.

4. To check that the appropriate services have been removed, use the following two commands from a terminal window:

```
# netstat –ntap | grep –i listen
```

```
tcp        0      0 :::22                   :::*                    LIST
EN      3134/sshd
```

Figure 7: Confirming service removal

```
# chkconfig --list | grep on | sort
```

```
acpid           0:off   1:off   2:on    3:on    4:on    5:on    6:off
auditd          0:off   1:off   2:on    3:on    4:on    5:on    6:off
avahi-daemon    0:off   1:off   2:off   3:on    4:on    5:on    6:off
avahi-dnsconfd  0:off   1:off   2:off   3:off   4:off   5:off   6:off
conman          0:off   1:off   2:off   3:off   4:off   5:off   6:off
crond           0:off   1:off   2:on    3:on    4:on    5:on    6:off
firstboot       0:off   1:off   2:off   3:on    4:off   5:on    6:off
haldaemon       0:off   1:off   2:off   3:on    4:on    5:on    6:off
hidd            0:off   1:off   2:on    3:on    4:on    5:on    6:off
ip6tables       0:off   1:off   2:on    3:on    4:on    5:on    6:off
iptables        0:off   1:off   2:on    3:on    4:on    5:on    6:off
lvm2-monitor    0:off   1:on    2:on    3:on    4:on    5:on    6:off
mcstrans        0:off   1:off   2:on    3:on    4:on    5:on    6:off
messagebus      0:off   1:off   2:off   3:on    4:on    5:on    6:off
netconsole      0:off   1:off   2:off   3:off   4:off   5:off   6:off
network         0:off   1:off   2:on    3:on    4:on    5:on    6:off
pcscd           0:off   1:off   2:on    3:on    4:on    5:on    6:off
readahead_early 0:off   1:off   2:on    3:on    4:on    5:on    6:off
readahead_later 0:off   1:off   2:off   3:off   4:off   5:on    6:off
restorecond     0:off   1:off   2:on    3:on    4:on    5:on    6:off
sendmail        0:off   1:off   2:on    3:on    4:on    5:on    6:off
sshd            0:off   1:off   2:on    3:on    4:on    5:on    6:off
syslog          0:off   1:off   2:on    3:on    4:on    5:on    6:off
vmware-tools    0:off   1:off   2:on    3:on    4:off   5:on    6:off
wdaemon         0:off   1:off   2:off   3:off   4:off   5:off   6:off
xfs             0:off   1:off   2:on    3:on    4:on    5:on    6:off
```

Figure 8: Results of service removals

5. If your results are *similar* to the output shown above, the services have been removed successfully.

4 User / Group Account Minimization

It is important to disable all default vendor accounts that will be unused. Typically a default account, e.g., gopher or news, is created only when the respective service is also installed; however, many default accounts will exist even if you have not installed the related services on your system. In our case, we will not use many of the default accounts and so we will remove them. The more accounts you have, the easier it is for outsiders to access your system.

4.1 Remove Default User Accounts

The users we will need to remove are:

- adm
- ftp
- games
- gopher
- halt
- lp
- mail
- mailnull
- news
- nfsnobody
- nobody
- nscd
- operator
- rpcuser
- rpc
- shutdown
- smmsp
- uucp
- vcsa
- xfs

1.

2. Remove the ‘adm’ user account using the following command:

```
# userdel adm
```

3. Repeat the previous step for each account listed above. Verify removal by executing the following command:

```
# cat /etc/passwd
```

```
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
distcache:x:94:94:Distcache:/:/sbin/nologin
webalizer:x:67:67:Webalizer:/var/www/usage:/sbin/nologin
dovecot:x:97:97:dovecot:/usr/libexec/dovecot:/sbin/nologin
squid:x:23:23::/var/spool/squid:/sbin/nologin
mysql:x:27:27:MySQL Server:/var/lib/mysql:/bin/bash
pcap:x:77:77::/var/arpwatch:/sbin/nologin
ntp:x:38:38::/etc/ntp:/sbin/nologin
dbus:x:81:81:System message bus:/:/sbin/nologin
avahi:x:70:70:Avahi daemon:/:/sbin/nologin
named:x:25:25:Named:/var/named:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
haldaemon:x:68:68:HAL daemon:/:/sbin/nologin
avahi-autoipd:x:100:102:avahi-autoipd:/var/lib/avahi-autoipd:/sbin/nologin
gdm:x:42:42::/var/gdm:/sbin/nologin
user:x:500:500:User:/home/user:/bin/bash
```

Figure 8 : Results of removing unnecessary default user accounts

4. If the default user accounts have been successfully removed, your /etc/passwd file will look *similar* to the output shown in the figure above.

4.2 Remove Default Groups

Now that we have removed all unnecessary accounts from the /etc/passwd file, we will clean up the /etc/groups file.

The groups that we will remove are:

- adm
- dip
- lock
- lp
- mail
- news
- uucp

Removing a group account is similar to the process of removing a user shown above.

1. Delete the ‘adm’ group using the following command:

```
# groupdel adm
```

2. Repeat the previous step for each group listed above.

3. Verify removal by executing the following command:

```
# cat /etc/group
```

```
root:x:0:root
bin:x:1:root,bin,daemon
daemon:x:2:root,bin,daemon
sys:x:3:root,bin
tty:x:5:
disk:x:6:root
mem:x:8:
kmem:x:9:
wheel:x:10:root
man:x:15:
users:x:100:
utmp:x:22:
utempter:x:35:
audio:x:63:gdm
distcache:x:94:
floppy:x:19:
webalizer:x:67:
dovecot:x:97:
squid:x:23:
mysql:x:27:
pcap:x:77:
slocate:x:21:
ntp:x:38:
ecryptfs:x:101:
dbus:x:81:
avahi:x:70:
named:x:25:
sshd:x:74:
haldaemon:x:68:
avahi-autoipd:x:102:
gdm:x:42:
user:x:500:
```

Figure 9: Results of removing unnecessary default groups

4. If the default groups have been successfully removed, the /etc/group file will look similar to the output shown in the figure above.

4.3 Create the 'Admin' User

The last account management task we will perform manually is to create an 'admin' user for daily administration tasks once the initial setup is complete.

1. Add the admin user using the following command:

```
# useradd admin
```

2. Set the password for the 'admin' account:

```
# passwd admin
```

3. When prompted for a password use the following: `steelers`

   The output will resemble that shown below:

```
Changing password for user admin.
New UNIX password:
BAD PASSWORD: it is based on a dictionary word
Retype new UNIX password:
passwd: all authentication tokens updated successfully.
```

Figure 10: Creating an Admin user

Note: In a real production environment you should always choose a strong password or passphrase that is sufficiently long and contains a combination of letters, numbers, and special characters. The above password is used for demonstration purposes only.

5 Installing ClamAV

1. Copy the ClamAV tarball from the course CD to the /root directory:

```
# cp /media/AISTS/Tools/Linux/ClamAV/clamav-0.96.1.tar.gz /root
```

2. Untar ClamAV:

```
# cd /root
# tar xvzf clamav-0.96.1.tar.gz
```

3. We need to install a few prerequisite packages before installing ClamAV. We will use our trusted yum repository that we set up earlier in this task to install zlib-devel. Additionally, in order to compile ClamAV and other tools in later tasks from source code we will need a compiler installed on the machine. This distribution of CentOS does not come with a compile pre-installed so we will install the gcc compiler ourselves.

   Make sure to remove this compiler when all of this machine's tasks have been completed as it can be leveraged by an attacker to compile malicious code if they were to gain access to the system.

```
# yum install gcc zlib-devel
```

4. Type `y` then press `[Enter]` when prompted to confirm the download.
5. Change into the clamav-0.96.1 directory and install ClamAV:

```
# cd clamav-0.96.1
# adduser clamav
# ./configure --sysconfdir=/etc
# make
# make install
```

6. Use the VI editor to open the clamav.conf file in order to configure ClamAV:

```
# vi /etc/clamd.conf
```

7. Press `[Insert]` to enter edit mode. Comment out the line near the beginning of the file containing 'Example':

```
# Comment or remove the line below.
#Example
```

Figure 11: Editing clamd.conf

8. Find and uncomment the following lines by removing the '#' in front of them:
   a. 'LogFile /tmp/clamd.log'
   b. 'LogTime yes'
   c. 'LogSyslog yes'
   d. 'LocalSocket /tmp/clamd.socket'
9. Save and exit the file. Press `[Esc]` and type `:wq` then press `[Enter]`.
10. The ClamAV updater (freshclam) needs to be pointed to our internal proxy (10.0.2.1) in order to be able to update virus definitions. Use the VI editor to open the freshclam.conf file:

```
# vi /etc/freshclam.conf
```

11. Comment out the line near the beginning of the file containing 'Example':

```
# Comment or remove the line below.
#Example
```

Figure 12: Editing freshclam.conf

12. Find the proxy settings. Uncomment and make the following changes to indicate the IP of the proxy server and the port number to use:

```
HTTPProxyServer 10.0.2.1
HTTPProxyPort 3128
```

Note: Although freshclam has been configured, it probably won't successfully run yet. The Squid Proxy server may still need to be set up.

13. Save and exit the file. Press `[Esc]` and type `:wq` then press `[Enter]`.
14. Enable the ClamAV daemon to start automatically as a service:

```
# cp /media/AISTS/Tools/Linux/ClamAV/clamd /etc/init.d/
# chkconfig --add clamd
# service clamd start
```

15. Setup cron jobs for Virus definition updates and nightly virus scans:

```
# crontab –u root -e
```

16. Add the following two lines to the file:

```
15 2 * * * /usr/local/bin/freshclam --quiet
15 3 * * * /usr/local/bin/clamdscan --quiet /
```

17. Save and exit the cron file. Press `[Esc]` and type `:wq` then press `[Enter]`.
18. Remove ClamAV installation files (they contain test signatures that will be found on every scan if we don't remove them) then reboot the server.

```
# cd /root
# rm -rf clamav-0.96*
# reboot
```

ADDENDUM Bash Script: 'for loop'

Create a file containing the list of items

1. If you would like to automate the task of removing the unwanted services, users and groups, you can write a Bash script to loop through the list of items and process them one by one. First, start by creating a text file containing the list of items that you want to process. Enter the following command to create the text file:

```
# cat > deletedSvcList
```

2. After you typed the previous command and hit the `[Enter]` key, notice that there is no prompt ('#') at the cursor. The file is now open and you can enter the list of items that you want to process. Enter each item on a separate line, hitting the `[Enter]` key to move to the next line.

3. When all of the items have been entered into the file, press `[Ctrl+d]` to save and close the file. Notice that the prompt ('#') has returned to the shell.

Write the 'for loop'

1. Now we will create a 'for loop' that will read the items in the deletedSvcList file one by one and stop each service. Enter the following script as it appears below to stop the unwanted services:

```
# for str in $(cat deletedSvcList); do service $str stop; done
```

A simple modification makes sure that those services do not start on bootup:

```
# for str in $(cat deletedSvcList); do chkconfig --del $str; done
```

2. Notice that the script is in three sections, separated by semi-colons (';'). The first section of this script creates a variable, named 'str', and assigns to it the first item in the file. The second section inserts the value of the variable, 'str', into the shell command. The command is executed and then the process is repeated for each item in the file. When there are no more items in the file, the third section of the script ends the process and returns control back to the shell.

As you go through the steps, you will have to create three separate files for services, users and groups. Then you must modify the file name in the first section of the script. Likewise, you will have to modify the command in the second section to perform the action that you want.

Here are the files and scripts that should be created to remove the following items:

Users:

```
# cat > deletedUserList
```

```
# for str in $(cat deletedUserList); do userdel $str; done
```

Groups:

```
# cat > deletedGrpList
```

```
# for str in $(cat deletedGrpList); do groupdel $str; done
```

Linux Network Time Protocol Daemon (ntpd) Client

1 Setup Linux ntpd Client Service

1.1 Installation

1. If you have not already done so, log on the console using:

   Username: **root** Password: **tartans@1**

2. Open a terminal window by going to 'Applications' -> 'Accessories' -> 'Terminal'.
3. The Network Time Protocol Daemon (ntpd) is installed with most Linux distributions. You will create a cron job that will cause the Linux ntpd to query the W2k ntp server on a periodic basis and update the Linux box's system time.

1.2 Configuration

1. Run the following command to see the current local system time. Hopefully, it is significantly different from the updated time server's system time as this will explicitly demonstrate when the client becomes synchronized with the server:

```
# date
```

2. If the date is not significantly different from the time server's system time, you can change the local client system's time manually by entering the following command, changing the system date and time to whatever you want:

```
# date -s "Fri Sep 12 14:38:19 EDT 2003"
```

3. The ntp configuration file must be modified to tell it which time server to use to update the system time. This file is located in the '/etc' directory. To open the config file in the 'vi' text editor, enter:

```
# vi /etc/ntp.conf
```

4. In order to be able to modify the file in the 'vi' editor, the `[Insert]` key must be pressed before trying to add or change text.
5. Scroll down to the section beginning with "# Use public servers" which is excerpted here:

```
# Use public servers from the pool.ntp.org project.
# Please consider joining the pool (http://www.pool.ntp.org/join.html).
server 0.centos.pool.ntp.org
server 1.centos.pool.ntp.org
server 2.centos.pool.ntp.org
```

Figure 1: Default NTP configuration file

Comment out the previous servers and add the following two lines at the end of this section:

```
restrict 10.0.2.1 mask 255.255.255.255 nomodify notrap noquery
server 10.0.2.1 prefer
```

Your section should look similar to the following:

```
# Use public servers from the pool.ntp.org project.
# Please consider joining the pool (http://www.pool.ntp.org/join.html).
#server 0.centos.pool.ntp.org
#server 1.centos.pool.ntp.org
#server 2.centos.pool.ntp.org
restrict 10.0.2.1 mask 255.255.255.255 nomodify notrap noquery
server 10.0.2.1 prefer
```

Figure 2: Edited NTP configuration file

6. Save and exit the file. Press `[Esc]` and type `:wq` then press `[Enter]`.
7. Now we need to cause ntpd to update to the ntp server time by modifying /etc/ntp/step-tickers to run ntpdate when ntpd is started. Do this by running these two commands:

```
# echo "10.0.2.1" > /etc/ntp/step-tickers
```

8. The 'step-tickers' file should now contain only the ntp server's IP address. The file contents can be viewed by entering this command:

```
# cat /etc/ntp/step-tickers
```

9. Enter the date command to see that the date is still incorrect.
10. Now, if the ntpd service is not currently running, it must be started by entering the following command. If the service is currently running, replace 'start' with `restart`. NOTE: Once the service is running, always remember to 'restart' after making any changes to the ntp config file. Otherwise, the service will continue to run according to the previous config file settings until the service is restarted. Later, we will be creating a cron job to periodically restart the service. For now, enter this command:

```
# service ntpd start
```

11. You should see these two messages:

```
ntpd: Synchronizing with time server:                    [  OK  ]
Starting ntpd:                                           [  OK  ]
```

Figure 3: Starting the NTP service

12. Enter the date command again to see that the time has been synchronized.

    Note: This will only be successful after Quebec's time server has been configured properly. Check with your teammates for its status.

13. The service can be verified and the current pid identified by entering:

```
# service ntpd status
```

14. Now, we are going to make sure that ntpd updates the system time regularly. Skew the local system time again by entering the following command that you entered earlier:

```
# date -s "Fri Sep 12 14:38:19 EDT 2003"
```

15. A cron job must be created to cause the ntpd service to periodically query the time server and update the local system time accordingly. Enter this command to create the cron job file:

```
# crontab –u root –e
```

16. This file should automatically open using the 'vi' text editor again, so you must press the `[Insert]` key before you can add or modify text.

17. Enter the following command to set up a cron job that will execute every 10 minutes. Review the 'man 5 crontab' pages to understand the crontab fields in more depth. After the ntpd is verified to be up and running correctly, the first set of numbers can be changed to a '0' to cause the cron job to run at the top of every hour (0th minute of every hour) instead.

    Make sure that there is a space after the 50 and between each '*' and the '/' character following them. There are no spaces between the initial set of numbers.

```
0,10,20,30,40,50 * * * * /etc/rc.d/init.d/ntpd restart
```

```
0,10,20,30,40,50 * * * * /etc/rc.d/init.d/ntpd restart
15 2 * * * /usr/local/bin/freshclam --quiet
15 3 * * * /usr/local/bin/clamdscan --quiet /
```

18. Now Save and exit the file. Press `[Esc]` and type `:wq` then press `[Enter]`.

19. Entering the following command will create init scripts at run levels 3-5 to start the ntpd service every time the system is started up.

```
# chkconfig --level 345 ntpd on
```

20. Use the following command to verify that the ntpd service is turned on at run levels 3, 4, and 5:

```
# chkconfig --list | grep ntpd
```

21. Make sure that it looks like this:

```
ntpd            0:off   1:off   2:off   3:on    4:on    5:on    6:off
```

Figure 4: NTP service startup run levels

22. Now, use the date command to see if the cron job has updated the system time. If not, wait a few more minutes and try again.

23. Once the remote centralized syslog server is installed and configured, we can review the logs that are generated from the Network Time Server process. There we will see each time that the client is updated and the offset amount by which it is updated.

This page left intentionally blank for pagination purposes

Installing and Configuring Bastille-Linux

We have already done preliminary hardening (by removing users, groups, etc) and now we will use Bastille-Linux to finish the task. Bastille allows us to easily modify many OS settings. In this task, we will apply a previously configured Bastille template file (analogous to the Security Configuration templates used on Windows) to our system.

1 Bastille Configuration

1.1 Install Bastille

1. If you have not already done so, log on to the machine using:

   Username: **root**

   Password: **tartans@1**

2. Open a terminal window by clicking on:

   Applications->Accessories->Terminal.

3. There are two modules that are required to implement Bastille:

   perl-Curses-1.12-1.2.el4.rf.i386.rpm

   Bastille-3.0.8-1.0.noarch.rpm

   Copy the required modules to the /root directory with this command:

```
# cp /media/AISTS/Tools/Linux/Bastille/* /root
```

4. Using the following commands, change to the /root directory and get a directory listing to confirm all of the Bastille files copied:

```
# cd /root
# ls –l
```

5. Install perl-Curses module:

```
# rpm –ivh perl-Curses-1.28-1.el5.rf.i386.rpm
```

6. Install Bastille module:

```
# rpm –ivh Bastille-3.0.9-1.0.noarch.rpm
```

1.2 Run Bastille

1. Copy Golf's Bastille template to the Bastille configuration directory (this command should be typed as one continuous line with a space after 'cp' and after 'bastille-ids-config'):

```
# cp /media/AISTS/Tools/Linux/Config_Files/Golf_10.0.4.4/bast
ille-ids-config /etc/Bastille/config
```

2. Run Bastille in batch mode to apply the preconfigured template:

```
# bastille –b –n 2>/dev/null
```

Note: The template generates error messages about the CentOS version, but the settings will be applied successfully. These messages are not important, and so in this command, we divert all error messages to /dev/null (the trash).

```
NOTE:    Entering Critical Code Execution.
         Bastille has disabled keyboard interrupts.


NOTE:    Bastille is scanning the system configuration...

NOTE:    Bastille is now locking down your system in accordance with your
         answers in the "config" file.  Please be patient as some modules
         may take a number of minutes, depending on the speed of your
         machine.
NOTE:    Executing Firewall Specific Configuration
NOTE:    Executing File Permissions Specific Configuration
NOTE:    Executing Account Security Specific Configuration
NOTE:    Executing Boot Security Specific Configuration
NOTE:    Executing Inetd Specific Configuration
NOTE:    Executing PAM Specific Configuration
NOTE:    Executing Logging Specific Configuration
NOTE:    Executing Daemon Specific Configuration
NOTE:    Executing Sendmail Specific Configuration
NOTE:    Executing Apache Specific Configuration
NOTE:    Executing FTP Specific Configuration
NOTE:    Executing Temporary Directory Specific Configuration
```

Figure 1: Bastille Output

2 Bastille Configuration

1. The template we applied has been previously configured as follows.

   Enter the following command to view the new Bastille security settings:

```
# cat /etc/Bastille/config | less
```

2. Now you can scroll up and down to view the entire file. When you are finished reviewing the file, press the ‘q’ key to quit viewing the file and return to the shell prompt.

3. After reviewing the config file, *reboot* the system by typing `reboot`. You will now have to login with the admin account that was created in the Linux Host System Hardening task. *Make sure that the admin account was created before rebooting the system or you will not be able to login.*

   You may need to reset the screen resolution to 1024x768 the first time you log on to the admin account. You can do this by going to ‘System’ -> ‘Preferences’ -> ‘Screen Resolution’.

   The remaining sections of this document detail the previously configured template that we applied. Note that you will *NOT* need to actually perform any tasks in the following sections; it is merely here for your edification. After reviewing, you can move on to the next task.

2.1 File Permissions

- Disallow non-root access to ping, usernetctl, mount/umount, and at
- Disable the r-tools (rsh, rlogin, etc) which are troublesome due to their use of weak authentication.

```
# Q:  Would you like to set more restrictive permissions on the administration u
tilities? [N]
FilePermissions.generalperms_1_1="N"

# Q:  Would you like to disable SUID status for mount/umount?
FilePermissions.suidmount="Y"

# Q:  Would you like to disable SUID status for ping? [Y]
FilePermissions.suidping="Y"

# Q:  Would you like to disable SUID status for at? [Y]
FilePermissions.suidat="Y"

# Q:  Would you like to disable the r-tools? [Y]
FilePermissions.suidrtool="Y"

# Q:  Would you like to disable SUID status for usernetctl? [Y]
FilePermissions.suidusernetctl="Y"
```

Figure 2: File Permissions

2.2 Account Security Settings

- Enforce password aging
- Restrict cron (scheduler) to the root user
- Disallow root from direct login. After we apply this template all administrators must login using the ‘admin’ account and then su to root.
- Set permissions on all user-created files so that the file is only readable by the user who created it.

```
# Q:  Should Bastille disable clear-text r-protocols that use IP-based authentic
ation? [Y]
AccountSecurity.protectrhost="Y"

# Q:  Would you like to enforce password aging? [Y]
AccountSecurity.passwdage="Y"

# Q:  Do you want to set the default umask? [Y]
AccountSecurity.umaskyn="Y"

# Q:  What umask would you like to set for users on the system? [077]
AccountSecurity.umask="077"

# Q:  Should we disallow root login on tty's 1-6? [N]
AccountSecurity.rootttylogins="Y"
```

Figure 3: Account Security Settings

2.3 Boot Security Settings

- Disable CTRL-ALT-DELETE rebooting so that a user must have a valid login and password to reboot the machine.
- Password protect single user mode to require the root password. Single user mode is equivalent to run level 1. You are granted root access, but networking is disabled.

```
# Q:  Would you like to password-protect the GRUB prompt? [N]
BootSecurity.protectgrub="N"

# Q:  Would you like to disable CTRL-ALT-DELETE rebooting? [N]
BootSecurity.secureinittab="Y"

# Q:  Would you like to password protect single-user mode? [Y]
BootSecurity.passsum="Y"
```

Figure 4: Boot Security Settings

2.4 Securing inetd and TCP Wrappers

- Disable telnet and ftp
- Create authorized use banners that will be displayed before the user can log in
- We do not set default deny on TCP wrappers in this configuration. Later on we will configure an IPtables firewall which will handle this for us.

```
# Q:  Would you like to set a default-deny on TCP Wrappers and xinetd? [N]
SecureInetd.tcpd_default_deny="N"

# Q:  Would you like to display "Authorized Use" messages at log-in time? [Y]
SecureInetd.banners="Y"

# Q:  Who is responsible for granting authorization to use this machine?
SecureInetd.owner="administrator@aia.class"
```

Figure 5: Securing inetd and TCP Wrappers

2.5 Configure PAM

- Set limits on resources. Users will only be allowed to start 150 concurrently running processes, and will be unable to open core system (kernel) files.
- Only allow admin to log in at the console

```
# Q:  Would you like to put limits on system resource usage? [N]
ConfigureMiscPAM.limitsconf="Y"

# Q:  Should we restrict console access to a small group of user accounts? [N]
ConfigureMiscPAM.consolelogin="Y"

# Q:  Which accounts should be able to login at console? [root]
ConfigureMiscPAM.consolelogin_accounts="admin"
```

Figure 6: PAM Settings

2.6 Logging Settings

- We will configure logging in a later module, therefore we will not configure logging through Bastille

```
# Q:  Would you like to set up process accounting? [N]
Logging.pacct="N"
```

Figure 7: Logging Settings

2.7 Sendmail Settings

- Prevent sendmail from running in daemon mode. This machine will not be a mail server, so sendmail need not listen for connections

```
# Q:  Do you want to stop sendmail from running in daemon mode? [Y]
Sendmail.sendmaildaemon="Y"
```

Figure 8: Sendmail Settings

2.8 Miscellaneous Daemons

```
# Q:  Would you like to disable acpid and/or apmd? [Y]
MiscellaneousDaemons.apmd="Y"

# Q:  Would you like to disable GPM? [Y]
MiscellaneousDaemons.gpm="Y"

# Q:  Would you like to deactivate the HP OfficeJet (hpoj) script on this machin
e?
MiscellaneousDaemons.disable_hpoj="Y"

# Q:  Would you like to deactivate the ISDN script on this machine?
MiscellaneousDaemons.disable_isdn="Y"
```

Figure 9: Miscellaneous Deamons

2.9 Apache Web Server Settings

```
# Q:  Would you like to bind the Web server to listen only to the localhost? [N]
Apache.bindapachelocal="N"

# Q:  Would you like to bind the web server to a particular interface? [N]
Apache.bindapachenic="N"

# Q:  Would you like to deactivate the following of symbolic links? [Y]
Apache.symlink="N"
```

Figure 10: Apache Web Server Settings

2.10 Tempdir Scripts

- This system is not a multi-user system, and therefore we will not be very concerned with the temporary (shared) directories

```
# Q:  Would you like to install TMPDIR/TMP scripts? [N]
TMPDIR.tmpdir="N"
```

Figure 11: Tempdir Scripts

2.11 Packet Filtering Firewall

- We will configure a firewall in a later module, therefore we will not use Bastille's firewall configuration

```
# Q:  Would you like to run the packet filtering script? [N]
Firewall.ip_intro="N"
```

Figure 12: Packet Filtering Firewall

2.12 FTP Settings

```
# Q:  Would you like to disable anonymous download? [N]
FTP.anonftp="Y"

# Q:  Would you like to disable user privileges on the FTP daemon? [N]
FTP.userftp="Y"
```

Figure 13: FTP Settings

Configuring IPTables as a Host Based Firewall on Linux Systems

The host based firewall for Linux, IPTables, can be configured by accessing the console directly or via SSH from a management workstation. IPTables has six pre-defined "chains" that are available with the ability to create user defined chains as well. The default chains are:

- INPUT
- OUTPUT
- INPUT
- FORWARD
- PREROUTING
- POSTROUTING

The table below lists various options that can be used when configuring iptables rules. Additional information is available by typing `iptables --help` at the Linux command line or by reviewing the iptables man page (type: `man iptables`).

--table -t	Description
filter	Default table. This is used if not specified
nat	Network address translation
mangle	Used for Quality Of Service (QOS) and preferential treatment
raw	Enables optimization. i.e. Ignore firewall state matching for port 80 for enhanced speed due to less processing. Requires kernel patch

Command (Use one)	Description
-A --append	Append rule to chain
-D --delete	Delete rule from chain
-I --insert	Insert rule at beginning or at specified sequence number in chain.
-R --replace	Replace rule
-F --flush	Flush all rules
-Z --zero	Zero byte counters in all chains
-L --list	List all rules. Add option --line-numbers for rule number.
-N --new-chain	Create new chain
-X --delete-chain	Delete user defined chain
-P --policy	Set default policy for a chain
-E --rename-chain	Rename a chain

Command Option	Description
-s --source	Source address of packet
-d --destination	Destination address of packet
-i --in-interface	Interface packet is arriving from
-o --out-interface	Interface packet is going to
-p --protocol	Protocol: °tcp --sport port[:port] --dport port[:port] --syn °udp °icmp °mac ...
-j --jump	Target to send packet to
-f --fragment	Fragment matching
-c --set-counters	Set packet/byte counter
-m tcp --match tcp	°--source-port port[:port] (port # or range ##) °--destination-port port[:port] °--tcp-flags
-m state --match state	--state °ESTABLISHED °RELATED °NEW °INVALID (Push content, not expected to recieve this packet.)

Defined Policies	Description
ACCEPT	Let packet through
DROP	Deny packet with no reply
REJECT	Deny packet and notify sender
RETURN	Handled by default targets
MARK	Used for error response. Use with option --reject-with type
MASQUERADE	Used with nat table and DHCP.
LOG	Log to file and specify message: °--log-level # °--log-prefix "prefix" °--log-tcp-sequence °--log-tcp-options °--log-ip-options
ULOG	Log to file and specify userpace logging messages
SNAT	Valid in PREROUTING chain. Used by nat.
REDIRECT	Used with nat table. Output.
DNAT	Valid in POSTROUTING chain. Output.
QUEUE	Pass packet to userspace.

Figure 1: IPtables Options

1 Creating Inbound and Outbound Filtering Rules

The filtering rules for this server will be set up to allow the following traffic into and out of the system:

Source Address	Destination Address	Proto	Source Ports	Destination Port	Direction	Purpose
10.0.4.0/24	10.0.4.4/32	ANY	ANY	ANY	Inbound	Management
10.0.3.2/32	10.0.4.4/32	ANY	ANY	ANY	Inbound	Mike-Nagios
10.0.2.5/32	10.0.4.4/32	TCP	ANY	3306	Inbound	Lima
10.0.2.5/32	10.0.4.4/32	UDP	ANY	3306	Inbound	Lima
10.0.3.2/32	10.0.4.4/32	UDP	ANY	3306	Inbound	Mike - Nagios
127.0.0.1/32	127.0.0.1/32	*	*	*	Inbound	Loopback
Log All Denied						
10.0.4.4/32	10.0.4.0/24	ANY	ANY	ANY	Outbound	Management
10.0.4.4/32	10.0.2.3/32	TCP	ANY	25	Outbound	SMTP
10.0.4.4/32	10.0.2.4/32	UDP	ANY	53	Outbound	DNS
10.0.4.4/32	10.0.2.1/32	UDP	123	123	Outbound	NTP
10.0.4.4/32	10.0.2.1/32	TCP	ANY	3128	Outbound	Squid Proxy
127.0.0.1/32	127.0.0.1/32	*	*	*	Outbound	Loopback
Log All Denied						

1. If you have not already done so, log on to the machine using the newly enforced admin account:

   Username: **admin** Password: **steelers**

2. Open a terminal window by going to ‘Applications’ -> ‘Accessories’ -> ‘Terminal’.
3. Elevate to root level privileges by typing the following command and entering the root password **tartans@1**

```
# su -
```

4. Ensure iptables is stopped.

```
# service iptables stop
```

5. Clear all existing iptables rules.

```
# iptables --flush
```

6. Set the default policy for the FORWARD chain to DROP all packets.

```
# iptables –P FORWARD DROP
```

7. Create the iptables file that will be used to save firewall rules.

```
# iptables-save > /etc/sysconfig/iptables
# vi /etc/sysconfig/iptables
```

8. Remove the last two lines. Move the cursor to each line and press the [D] key twice. This will delete the current line in VI. The file should look like the following when completed:

```
# Generated by iptables-save v1.3.5 on Mon Jun 14 10:52:10 2010
*filter
:INPUT ACCEPT [5:420]
:FORWARD DROP [0:0]
:OUTPUT ACCEPT [5:420]
```

9. Add the remaining rules to the iptables file as listed below. Comments/remarks are identified with a '#' at the beginning of the line. These lines are used to identify what the rules beneath them are used for. Although they are not required, it is a good practice to describe the rules, their intent, who added the rule, and potentially the date on which the rule was added or modified. Use the cursor to go to the bottom of the file. Simultaneously press the [Shift] and [A] keys to append text to the end of the last line. Press [Enter] to add a new line. Enter the following lines:

```
# Allow all inbound traffic from the MGMT network
-A INPUT -s 10.0.4.0/24 -d 10.0.4.4/32 -i eth1 -j ACCEPT

# Allow all inbound traffic from Mike-Nagios
-A INPUT -s 10.0.3.2/32 -d 10.0.4.4/32 -i eth1 -j ACCEPT

# Allow Lima Snort sensor to send alerts to BASE
-A INPUT -s 10.0.2.5/32 -d 10.0.4.4/32 -i eth1 -p tcp --dport 3306 -j ACCEPT
-A INPUT -s 10.0.2.5/32 -d 10.0.4.4/32 -i eth1 -p udp --dport 3306 -j ACCEPT

# Allow Mike Snort sensor to send alerts to BASE
-A INPUT -s 10.0.3.2/32 -d 10.0.4.4/32 -i eth1 -p tcp --dport 3306 -j ACCEPT
-A INPUT -s 10.0.3.2/32 -d 10.0.4.4/32 -i eth1 -p udp --dport 3306 -j ACCEPT

# Allow all established connections
-A INPUT -i eth1 -m state --state ESTABLISHED,RELATED -j ACCEPT

# Allow all inbound traffic on the loopback interface
-A INPUT -i lo -p all -j ACCEPT

# Enable logging on INUT chain
-A INPUT -j LOG --log-level 6

# Set the default INPUT policy to Drop
-P INPUT DROP
```

Figure 2: IPtables Input Rules

```
# Allow outbound mail traffic to Bravo
-A OUTPUT -d 10.0.2.3/32 -o eth1 -p tcp --dport 25 -j ACCEPT

# Allow outbound DNS traffic to Alpha
-A OUTPUT -d 10.0.2.4/32 -o eth1 -p udp --dport 53 -j ACCEPT

# Allow outbound web proxy traffic to Quebec
-A OUTPUT -d 10.0.2.1/32 -o eth1 -p tcp --dport 3128 -j ACCEPT

# Allow outbound NTP traffic to Quebec
-A OUTPUT -d 10.0.2.1/32 -o eth1 -p udp --dport 123 -j ACCEPT

# Allow all outbound traffic to the MGMT network
-A OUTPUT -d 10.0.4.0/24 -o eth1 -p all -j ACCEPT

# Allow all established connections
-A OUTPUT -o eth1 -m state --state ESTABLISHED,RELATED -j ACCEPT

# Allow all outbound traffic on the loopback interface
-A OUTPUT -o lo -p all -j ACCEPT

# Enable logging on OUTPUT chain
-A OUTPUT -j LOG --log-level 6

# Set the default OUTPUT policy to Drop
-P OUTPUT DROP

# Enable rule set
COMMIT
```

Figure 3: IPtables Output Rules

10. Save and exit the file. Press `[Esc]` and type `:wq` then press `[Enter]`.

1.1 Applying the firewall rules

1. Enter the following command to start the iptables firewall:

```
# service iptables start
```

2. If the service started successfully, you should see the following:

```
Flushing firewall rules:                                   [  OK  ]
Setting chains to policy ACCEPT: filter                    [  OK  ]
Unloading iptables modules:                                [  OK  ]
Applying iptables firewall rules:                          [  OK  ]
Loading additional iptables modules: ip_conntrack_netbios_n[  OK  ]
```

Figure 4: IPtables Successful Startup

1.2 Making the iptables file immutable

1. Since we do not want the iptables file to change for ANY reason after the rules have been built without intervention from the administrator, we will make this file immutable. To do this, we will issue the following command.

```
# chattr +i /etc/sysconfig/iptables
```

2. Relinquish the elevated root privileges by typing the following command:

```
# exit
```

This page left intentionally blank for pagination purposes

Installing a Linux Intrusion Detection System

Golf will be an IDS sensor for the DMZ and a central collection point for all other IDS sensors on the network. The collection database and analysis console will be installed on this server running in the management network. Access to the console requires authentication and is only available from the management network (10.0.4.0/24).

The following applications will be installed and configured:

- Snort; A popular open source IDS tool (http://www.snort.org).
- BASE; Basic Analysis Security Engine: a web based front end for SNORT Alert Analysis (http://sourceforge.net/projects/secureideas).
- MySQL; "The world's most popular open source database" (http://www.mysql.com).
- Several additional applications to support Base,
  - PHP; A server-side scripting language (http://www.php.net).
  - ADODB; the database abstraction library for PHP that enables the BASE application to communicate with the snort MySQL database, (http://adodb.sourceforge.net/).

1 Snort Installation and Configuration

The Snort Intrusion Detection System can be a powerful tool to help in protecting a network. We will be installing Snort, along with other modules that Snort requires.

1.1 Installation

Snort can log in a variety of different formats, including a few different database formats and flat text. We will be installing Snort to log to a MySQL database.

There are several prerequisites that must be installed for Snort to run. Snort uses libpcap to capture packets from the ethernet interface. There are also a number of other packages we need to install in order to configure Snort to send our alerts to the central MySQL console.

1. If you have not already done so, log on to the machine using the newly enforced admin account:

   Username: **admin** Password: **steelers**

2. Open a terminal window by going to 'Applications' -> 'Accessories' -> 'Terminal'.
3. Elevate to root level privileges by typing the following command and entering the root password **tartans@1**

```
# su -
```

4. Download and install the prerequisites from the trusted repository that was set up in the Linux Host System Hardening step by executing the following command:

```
# yum install mysql-server mysql-bench mysql-devel libpcap libpcap-
devel pcre-devel
```

5. Type `y` and press `[Enter]` when prompted to download the packages.
6. There are several files that we will need to implement Snort:

snort-2.8.6.tar.gz
snortd
snortrules-aists.tar.gz

Copy the required files to the /root directory with this command:

```
# cp /media/AISTS/Tools/Linux/Snort/* /root
```

7. Setup folders that we will use for Snort:

```
# mkdir /var/log/snort
# mkdir /etc/snort
```

8. Untar the Snort installation file and cd into the new directory:

```
# cd /root
# tar xvzf snort-2.8.6.tar.gz
# cd snort-2.8.6
```

9. Configure the installation to have Snort be compatible with MySQL, compile the code, then install the files to their final location:

```
# ./configure –-with-mysql –-enable-zlib
# make
# make install
```

10. Install the rules and configuration files:

```
# cd /root
# cp ./snortrules-aists.tar.gz /etc/snort
# cd /etc/snort
# tar xvzf snortrules-aists.tar.gz
# rm –f snortrules-aists.tar.gz
# cp etc/* .
# rm –rf etc
```

11. Copy the Snort startup script into the /etc/rc.d/init.d directory:

```
# cp /root/snortd /etc/rc.d/init.d
```

12. Configure Snort to start when the machine is booted:

```
# cd /etc/rc.d/init.d
# chmod 755 snortd
# chkconfig –-level 2345 snortd on
```

13. Use chkconfig to ensure that snort is configured to start at the correct run levels (2,3,4,5):

```
# chkconfig –-list | grep snortd
```

```
snortd          0:off   1:off   2:on    3:on    4:on    5:on    6:off
```

Figure 1: Chkconfig Output for Snort

14. The snortd file needs to be edited to ensure that snort starts after MySQL has started on bootup. Use VI to edit the snortd file:

```
# vi /etc/rc.d/init.d/snortd
```

15. During the boot, MySQL is started first, but does not complete before Snort is started, so Snort fails to start. We need to make sure that Snort is set to wait extra time before it runs. Verify that the following line has been added to the snortd file right below the line labeled “start)”:

```
sleep 3
```

This causes the Snort startup script to wait 3 seconds before continuing to run the script. It should look like the figure below:

```
# Source function library.
. /etc/rc.d/init.d/functions

# Specify your network interface here
INTERFACE=eth0

# See how we were called.
case "$1" in
  start)
        sleep 3
        echo -n "Starting snort: "
        daemon /usr/local/bin/snort -d -D \
                -c /etc/snort/snort.conf
        touch /var/lock/subsys/snort
        echo
        ;;
  stop)
        echo -n "Stopping snort: "
        killproc snort
        rm -f /var/lock/subsys/snort
        echo
        ;;
  restart)
```

Figure 2: Have Snort pause 3 seconds

16. To save and exit the VI editor, press `[Esc]` then type `:wq` and press `[Enter]`.

1.2 Configuration

1. Edit the snort configuration file

```
# vi /etc/snort/snort.conf
```

2. Scroll down to the section titled ‘Step #1: Set the network variables’. This is where we will tell Snort the layout of our network and the location of the rules that we just installed. Press `[Insert]` to edit the file. Change the following lines, making sure to include the brackets “[“ and “]” where shown when entering the info:

   var HOME_NET [10.0.1.0/24]

   var EXTERNAL_NET !$HOME_NET

   var RULE_PATH /etc/snort/rules

   var SO_RULE_PATH /etc/snort/so_rules

   var PREPROC_RULE_PATH /etc/snort/preproc_rules

   Note: When entering in the IP addresses, be sure <u>not</u> to include any spaces or carriage returns.

3. Scroll down to the section titled ‘Step #5: Configure preprocessors’. We are going remove the small_segments directive in the Snort stream5_tcp preprocessor because it can cause a large number of false positive alerts in our network. Find the line beginning with ‘preprocessor stream5_tcp:’ and remove the ‘small_segments 3 bytes 150,’ text from the line. The result should look like the following:

```
preprocessor stream5_tcp: policy windows, detect_anomalies, require_3whs 180, \
   overlap_limit 10, timeout 180, \
    ports client 21 22 23 25 42 53 79 109 110 111 113 119 135 136 137 139 143 \
        161 445 513 514 587 593 691 1433 1521 2100 3306 6665 6666 6667 6668 6669
 \
```

Figure 3: Edit Snort preprocessor

4. Next find the ‘Portscan detection’ heading in this section and enable portscan detection by removing the ‘#’ in front of the line beginning with ‘preprocessor sfportscan’ and set the sense_level to ‘medium’.

5. Add an additional logging option and a new ‘ignore_scanners’ directive to not alert us of portscan traffic coming from hosts on our network that are known to cause false positives of such alerts as shown below:

```
# Portscan detection.  For more information, see README.sfportscan
preprocessor sfportscan: proto  { all } memcap { 10000000 } sense_level { medium
 } \
ignore_scanners { 10.0.1.3/32 } \
logfile { portscan.log }
```

Figure 4: Configure Snort preprocessor

6. Scroll down to the section titled ‘Step #6: Configure output plugins’. Find the ‘# pcap’ section and add a line as follows:

```
# pcap
# output log_tcpdump: tcpdump.log
output alert_fast: alert.ids
```

Figure 5: Configure Snort Output

7. We will be configuring Snort to log to our MySQL database. Find the section beginning with '# database' and edit the second 'output database' line to look like the following:

```
# database
# output database: alert, <db_type>, user=<username> password=<password> test db
name=<name> host=<hostname>
output database: log, mysql, user=snort password=snortpw dbname=snort host=local
host sensor_name=golf
```

Figure 6: Configure Snort output database

1.3 Rules

There are many rules that are enabled by default when Snort is initially installed. Many of these may or may not be necessary depending on your particular network configuration. We will be disabling some unnecessary rules. The reason that we do this is that the more rules that are active, the more that Snort has to parse for each packet that is scanned.

1. We don't need all of the rule sets since the DMZ network doesn't have many of the services that are trying to be exploited. For example, there is no Oracle database, and telnet should be disabled on all hosts. Scroll down to the 'Step #7: Customize your rule set' section of the config file. Disable all rule sets by placing '#' at the beginning of each rule line, except for the following rules which we will leave enabled:

   include $RULE_PATH/icmp.rules

   include $RULE_PATH/sql.rules

   include $RULE_PATH/web-iis.rules

   include $RULE_PATH/web-misc.rules

   Scroll down to the 'Step #9: Customize your Shared Object Snort Rules' section of the config file. Enable the following rule sets by removing the '#' at the beginning of each of the following rule lines:

   include $SO_RULE_PATH/icmp.rules

   include $SO_RULE_PATH/sql.rules

   include $SO_RULE_PATH/web-iis.rules

   include $SO_RULE_PATH/web-misc.rules

2. Save and exit the file. Press `[Esc]` type `:wq` then press `[Enter]`.

3. Install pre-compiled shared object rules:

```
# mkdir /usr/local/lib/snort_dynamicrules
# cp /etc/snort/so_rules/precompiled/Centos-5-4/i386/2.8.6.0/* /usr/local/lib/snort_dynamicrules/
# snort -c /etc/snort/snort.conf --dump-dynamic-rules=/etc/snort/so_rules
```

```
  Finished Loading all dynamic preprocessor libs from /usr/local/lib/snort_dynam
icpreprocessor/
Dumping dynamic rules...
Dumping dynamic rules for Library icmp 1.0.1
Dumping dynamic rules for Library misc 1.0.1
Dumping dynamic rules for Library imap 1.0.1
Dumping dynamic rules for Library web-activex 1.0.1
Dumping dynamic rules for Library exploit 1.0.1
Dumping dynamic rules for Library chat 1.0.1
Dumping dynamic rules for Library bad-traffic 1.0.1
Dumping dynamic rules for Library multimedia 1.0.1
Dumping dynamic rules for Library smtp 1.0.1
Dumping dynamic rules for Library nntp 1.0.1
Dumping dynamic rules for Library web-misc 1.0.1
Dumping dynamic rules for Library web-client 1.0.1
Dumping dynamic rules for Library netbios 1.0.1
Dumping dynamic rules for Library dos 1.0.1
Dumping dynamic rules for Library web-iis 1.0.1
Dumping dynamic rules for Library sql 1.0.1
Dumping dynamic rules for Library p2p 1.0.1
  Finished dumping dynamic rules.
Snort exiting
```

Figure 7: Install Snort dynamic rules

2 Install ADODB

1. Copy the required files to the /root directory with this command:

```
# cp /media/AISTS/Tools/Linux/IDS/adodb/* /root
```

2. Unpack ADODB to the /var/www/html/ directory:

```
# cd /var/www/html
# tar xvzf /root/adodb511.tgz
# mv adodb5 adodb
# chown –R apache /var/www/html/adodb
```

3 Install and Configure BASE

3.1 Installation

3. Copy the required files to the /root directory with this command:

```
# cp /media/AISTS/Tools/Linux/IDS/BASE/* /root
```

4. Unpack BASE to the /var/www/html/ directory:

```
# cd /var/www/html
# tar xvzf /root/base-1.4.5.tar.gz
# mv base-1.4.5 base
# chown –R apache /var/www/html/base
```

3.2 Configuration

1. Copy the base_conf.php.dist configuration file to base_conf.php and open it in a text editor:

```
# cd base
# cp base_conf.php.dist base_conf.php
# chown apache base_conf.php
# vi base_conf.php
```

2. Make the following changes to the base config file:

```
Original: $BASE_urlpath = '';
Change: $BASE_urlpath = '/base';

Original: $DBlib_path = '';
Change: $DBlib_path = '/var/www/html/adodb';

Original:
  $alert_dbname = ‘snort_log';
  $alert_host = 'localhost';
  $alert_port = '';
  $alert_user = 'snort';
  $alert_password = 'mypassword';
Change to:
  $alert_dbname = 'snort';
  $alert_host = 'localhost';
  $alert_port = '';
  $alert_user = 'base';
  $alert_password = 'basepw’;

Original:
  $archive_exists = 0; # Set this to 1 if you want access to
the archive DB from BASE
  $archive_dbname = 'snort_archive';
  $archive_host = 'localhost';
```

```
  $archive_port = '';
  $archive_user = 'snort';
  $archive_password = 'mypassword';
Change to:
  $archive_exists = 1; # Set this to 1 if you want access to
the archive DB from BASE
  $archive_dbname = 'archive';
  $archive_host = 'localhost';
  $archive_port = '';
  $archive_user = 'base';
  $archive_password = 'basepw’;

Original: $show_rows = 48;
Change: $show_rows = 90;

Original: $show_expanded_query = 0;
Change: $show_expanded_query = 1;

Original: $portscan_file = '';
Change: $portscan_file = '/var/log/snort/portscan.log';

Original: $colored_alerts = 0;
Change: $colored_alerts = 1;

Original: $priority_colors = array
('FF0000','FFFF00','FF9900','999999','FFFFFF','006600');
Change: $priority_colors =
array('000000','FF0000','FF9900','FFFF00','999999');
```

3. Save and exit the file by typing `[Esc] :wq [Enter]`

4 Configure Apache

1. Edit the apache configuration file:

```
# vi /etc/httpd/conf/httpd.conf
```

2. After

   <Directory />

   Options FollowSymLinks

   AllowOverride None

   </Directory>

   Add the following

```
<Directory “/var/www/html/base”>
    AuthType Basic
    AuthName “Golf(IDS)”
    AuthUserFile “/etc/httpd/passwords/passwords”
    Require user base
</Directory>
```

3. Make these additional changes:

```
Original: #ServerName www.example.com:80
Change: ServerName golf.aia.class
Original: DirectoryIndex index.html index.html.var
Change: DirectoryIndex base_main.php
Original: Options Indexes FollowSymLinks
Change: Options -Indexes FollowSymLinks
```

4. Save and exit the file.

Create BASE user and set password

5. Create the folder for the passwords file:

```
mkdir /etc/httpd/passwords
chown apache /etc/httpd/passwords
```

6. Change directories to the apache folder:

```
cd /etc/httpd
```

7. Create the passwords file for the BASE user:

```
/usr/bin/htpasswd –c passwords/passwords base
```

8. Enter and Re-Enter the password, **tartans@1**
9. Give apache ownership of the passwords file:

```
# chown apache /etc/httpd/passwords/passwords
```

10. Configure Apache to load on startup:

```
# chkconfig –-level 2345 httpd on
```

11. Use chkconfig to ensure that Apache is configured to start at the correct run levels (2,3,4,5):

```
# chkconfig –-list | grep httpd
```

```
[root@Golf httpd]# chkconfig --level 2345 httpd on
[root@Golf httpd]# chkconfig --list | grep httpd
httpd           0:off   1:off   2:on    3:on    4:on    5:on    6:off
```

Figure 8: Chkconfig Output for Apache

5 Install and Configure PHP

5.1 Install PHP

1. Install PHP packages that we need from our trusted repository:

```
# yum install php-mysql php-gd php-pear php-pear-Net-SMTP
```

2. Type `y [Enter]` when prompted to download the packages.
3. Open the PHP configuration file in VI:

```
# vi /etc/php.ini
```

4. Make the following change

```
Original: max_execution_time = 30
Change: max_execution_time = 60
```

5. To save and exit the VI editor, press `[Esc] :wq [enter]`

5.2 Install supporting PHP modules

1. Numerous PHP add-ons can be downloaded and/or installed using PEAR. Copy the PEAR folder from the course CD to the /root directory:

```
# cp –r /media/AISTS/Tools/Linux/IDS/Pear /root
# cd /root/Pear
```

With Internet access these modules only take a minute or two to download and install. The included modules have successfully been tested with the other versions of the included applications.

2. Update existing PEAR packages:

```
# pear upgrade –-force Archive_Tar-1.3.7.tgz Console_Getopt-1.2.3.tgz PEAR-1.9.1.tgz Structures_Graph-1.0.3.tgz XML_Util-1.2.1.tgz
```

3. Install necessary PEAR packages for BASE:

```
# pear install *
```

6 Setup and Configure MySQL Databases

1. Turn on the MYSQL service:

```
# service mysqld start
```

2. Create an admin MYSQL user:

```
# mysqladmin -u root password ‘tartans@1’
```

3. Configure MYSQL to load on startup:

```
# chkconfig –-level 2345 mysqld on
```

4. Use chkconfig to ensure that mysql is configured to start at the correct run levels (2,3,4,5):

```
# chkconfig –-list | grep mysqld
```

```
[root@Golf Pear]# chkconfig --level 2345 mysqld on
[root@Golf Pear]# chkconfig --list | grep mysqld
mysqld          0:off   1:off   2:on    3:on    4:on    5:on    6:off
```

Figure 9: Chkconfig Output for MYSQL

Each of the sql scripts used below can be opened in a text editor to view the list of commands used within the MySQL console.

5. Create the Snort and Archive Databases:

```
mysql -u root -p < /media/AISTS/Tools/Linux/IDS/aists-sql/create_databases.sql
```

6. When prompted, enter the root user password: **tartans@1**
7. Create the tables for Snort Databases:

```
mysql -u root -p -D snort < /root/snort-2.8.6/schemas/create_mysql
```

8. When prompted, enter the root user password: **tartans@1**
9. Create tables to support BASE in the Snort Database:

```
mysql -u root -p -D snort < /var/www/html/base/sql/create_base_tbls_mysql.sql
```

10. When prompted, enter the root user password: **tartans@1**
11. Create tables in the Archive Database

```
mysql -u root -p -D archive  < /root/snort-2.8.6/schemas/create_mysql
```

12. When prompted, enter the root user password: **tartans@1**
13. Create tables to support BASE in the Archive Database:

```
mysql -u root -p -D archive < /var/www/html/base/sql/create_base_tbls_mysql.sql
```

14. When prompted, enter the root user password: **tartans@1**
15. Assign users to Snort and Archive Databases:

```
mysql -u root -p < /media/AISTS/Tools/Linux/IDS/aists-sql/assign_users.sql
```

16. When prompted, enter the root user password: **tartans@1**

7 Access the BASE Console

1. REBOOT Golf.
2. Once Golf has rebooted, access one of the Management workstations.
3. Browse to http://golf.aia.class/base (http://10.0.4.4/base)
4. Enter the username: **base**
5. Enter the password: **tartans@1**

Apache does support HTTPS, and SSL certificates could have been used to further secure this installation. Since access to the console is restricted to Management workstations on the same subnet this additional task will not be completed.

This page left intentionally blank for pagination purposes

OSSEC Agent

OSSEC agents will be installed on each Linux and Windows server and send events to the OSSEC server which is running on Foxtrot. OSSEC server processes events, generate warnings and alerts sent by agents. *Before installing any OSSEC agents make sure that you have successfully deployed the OSSEC server in order to connect the OSSEC agents to the OSSEC server which is running on Foxtrot.*

1 OSSEC Agent setup

1.1 Installation

1. If you have not already done so, log on to the machine using the newly enforced admin account:

   Username: **admin** Password: **steelers**

2. Open a terminal window by going to 'Applications' -> 'Accessories' -> 'Terminal'.
3. Elevate to root level privileges by typing the following command and entering the root password **tartans@1**

```
# su -
```

4. Navigate to the Course CD by executing following command:

```
# cd /media/AISTS/Tools/Linux/OSSEC/
```

5. Copy the OSSEC installation package:

```
# cp ossec-hids-2.4.1.tar.gz /root/
```

6. Extract the installation package into the root directory

```
# cd /root/
# tar -xzvf ossec-hids-2.4.1.tar.gz
```

7. Start installation using the following command and accept the default language by pressing `[Enter]`:

```
# cd ossec-hids-2.4.1
# ./install.sh
```

8. Read the introduction and press [Enter]:

```
OSSEC HIDS v2.4.1 Installation Script - http://www.ossec.net

You are about to start the installation process of the OSSEC HIDS.
You must have a C compiler pre-installed in your system.
If you have any questions or comments, please send an e-mail
to dcid@ossec.net (or daniel.cid@gmail.com).

 - System: Linux Golf 2.6.18-164.el5
 - User: root
 - Host: Golf


 -- Press ENTER to continue or Ctrl-C to abort. --
```

9. Answer the rest of the questions as shown in below and press [Enter] when you have finished:

```
1- What kind of installation do you want (server, agent, local or help)?
 agent

  - Agent(client) installation chosen.

2- Setting up the installation environment.

 - Choose where to install the OSSEC HIDS [/var/ossec]:

    - Installation will be made at  /var/ossec .

3- Configuring the OSSEC HIDS.

  3.1- What's the IP Address of the OSSEC HIDS server?: 10.0.4.2

   - Adding Server IP 10.0.4.2

  3.2- Do you want to run the integrity check daemon? (y/n) [y]: y

   - Running syscheck (integrity check daemon).

  3.3- Do you want to run the rootkit detection engine? (y/n) [y]: y
```

```
3.4 - Do you want to enable active response? (y/n) [y]: n

 - Active response disabled.

3.5- Setting the configuration to analyze the following logs:
  -- /var/log/messages
  -- /var/log/secure
  -- /var/log/maillog
  -- /var/log/httpd/error_log (apache log)
  -- /var/log/httpd/access_log (apache log)

 - If you want to monitor any other file, just change
  the ossec.conf and add a new localfile entry.
  Any questions about the configuration can be answered
  by visiting us online at http://www.ossec.net .


  --- Press ENTER to continue ---
```

10. When the installation has finished you should see following screen and press `[Enter]`:

```
- System is Redhat Linux.
- Init script modified to start OSSEC HIDS during boot.

- Configuration finished properly.

- To start OSSEC HIDS:
              /var/ossec/bin/ossec-control start

- To stop OSSEC HIDS:
              /var/ossec/bin/ossec-control stop

 - The configuration can be viewed or modified at /var/ossec/etc/ossec.c
onf


   Thanks for using the OSSEC HIDS.
   If you have any question, suggestion or if you find any bug,
   contact us at contact@ossec.net or using our public maillist at
   ossec-list@ossec.net
   ( http://www.ossec.net/main/support/ ).

   More information can be found at http://www.ossec.net

   ---  Press ENTER to finish (maybe more information below). ---
```

1.2 Configuration

1. Now we're going to setup a shared key between the OSSEC agent and OSSEC server. In order to get a shared key from the OSSEC server login to Foxtrot through SSH:

```
# ssh root@10.0.4.2
```

Accept SSH connectivity by typing `yes` and entering the password **tartans@1** and you will be connected to Foxtrot:

```
[root@Golf ~]# ssh root@10.0.4.2
The authenticity of host '10.0.4.2 (10.0.4.2)' can't be established.
RSA key fingerprint is f5:b7:79:02:ff:f8:7d:af:a2:3f:87:db:e0:ee:c0:5e.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.0.4.2' (RSA) to the list of known hosts.
root@10.0.4.2's password:
Last login: Wed Jun 16 12:03:50 2010 from 10.0.2.10
[root@Foxtrot ~]#
```

2. Start the OSSEC agent manager:

```
# /var/ossec/bin/manage-agents
```

```
[root@Foxtrot ~]# /var/ossec/bin/manage_agents


****************************************
* OSSEC HIDS v2.4.1 Agent manager.     *
* The following options are available: *
****************************************
   (A)dd an agent (A).
   (E)xtract key for an agent (E).
   (L)ist already added agents (L).
   (R)emove an agent (R).
   (Q)uit.
Choose your action: A,E,L,R or Q:
```

3. Now add Golf's OSSEC agent to the OSSEC server by entering `A`. Type `y` and press `[Enter]` when you have finished entering the information about Golf as shown below:

```
- Adding a new agent (use '\q' to return to the main menu).
  Please provide the following:
   * A name for the new agent: Golf
   * The IP Address of the new agent: 10.0.4.4
   * An ID for the new agent[008]: 008
Agent information:
   ID:008
   Name:Golf
   IP Address:10.0.4.4

Confirm adding it?(y/n): y
Agent added.
```

4. Now type `E` and press `[Enter]` to extract the shared key for Golf, and enter `008` when the OSSEC agent manager asks for an agent ID. Please note that the key will not be the same as shown in following screenshot, because the shared key is generated randomly each time when an OSSEC agent is added:

```
****************************************
* OSSEC HIDS v2.4.1 Agent manager.     *
* The following options are available: *
****************************************
   (A)dd an agent (A).
   (E)xtract key for an agent (E).
   (L)ist already added agents (L).
   (R)emove an agent (R).
   (Q)uit.
Choose your action: A,E,L,R or Q: E

Available agents:
   ID: 001, Name: Hotel, IP: 10.0.1.5
   ID: 002, Name: Juliet, IP: 10.0.1.3
   ID: 003, Name: Bravo, IP: 10.0.2.3
   ID: 004, Name: Alpha, IP: 10.0.2.4
   ID: 005, Name: Lima, IP: 10.0.2.5
   ID: 006, Name: Charlie, IP: 10.0.2.6
   ID: 007, Name: Echo, IP: 10.0.2.10
   ID: 008, Name: Golf, IP: 10.0.4.4
Provide the ID of the agent to extract the key (or '\q' to quit): 008

Agent key information for '008' is:
MDA4IEdvbGYgMTAuMC40LjQgNWVjNjZiYjJmMmZmNDMwMjRkOGZlYzY2YmJiMGU2NmM2OT
FjNjY5ZDNjNTNmYTZkYmU1NDJjMGFiYmU1NmJiYw==

** Press ENTER to return to the main menu.
```

5. Copy the shared key to your clipboard by highlighting it, right-clicking and choosing ‘Copy’.

6. Type `Q` and press `[Enter]` to quit from the OSSEC agent manager, and type `exit` and press `[Enter]` to end the SSH session:

```
****************************************
* OSSEC HIDS v2.4.1 Agent manager.     *
* The following options are available: *
****************************************
   (A)dd an agent (A).
   (E)xtract key for an agent (E).
   (L)ist already added agents (L).
   (R)emove an agent (R).
   (Q)uit.
Choose your action: A,E,L,R or Q: Q
```

7. Now you should be back in the shell of Golf. Execute following command to import the copied key.

```
# /var/ossec/bin/manage_agents
```

8. Type `I` then press `[Enter]`.

9. Paste the copied key by right-clicking and choosing ‘Paste’ to import the key and accept confirmation by typing y then pressing `[Enter]` as shown below:

```
****************************************
* OSSEC HIDS v2.4.1 Agent manager.     *
* The following options are available: *
****************************************
   (I)mport key from the server (I).
   (Q)uit.
Choose your action: I or Q: I

* Provide the Key generated by the server.
* The best approach is to cut and paste it.
*** OBS: Do not include spaces or new lines.

Paste it here (or '\q' to quit): MDA4IEdvbGYgMTAuMC40LjQgNWVjNjZiYjJmMmZ
mNDMwMjRkOGZlYzY2YmJiMGU2NmM2OTFjNjY5ZDNjNTNmYTZkYmU1NDJjMGFiYmU1NmJiYw=
=

Agent information:
   ID:008
   Name:Golf
   IP Address:10.0.4.4

Confirm adding it?(y/n): 
```

10. Exit from OSSEC manager by typing `Q` then pressing `[Enter]`:

```
Confirm adding it?(y/n): y
Added.
** Press ENTER to return to the main menu.



****************************************
* OSSEC HIDS v2.4.1 Agent manager.     *
* The following options are available: *
****************************************
   (I)mport key from the server (I).
   (Q)uit.
Choose your action: I or Q: Q

** You must restart the server for your changes to have effect.

manage_agents: Exiting ..
```

11. Start the OSSEC agent by executing the following command:

```
# /var/ossec/bin/ossec-control start
```

```
[root@Golf ~]# /var/ossec/bin/ossec-control start
Starting OSSEC HIDS v2.4.1 (by Trend Micro Inc.)...
Started ossec-execd...
Started ossec-agentd...
Started ossec-logcollector...
Started ossec-syscheckd...
Completed.
```

12. If you are not performing any more administrative tasks on this machine, relinquish the elevated root privileges by typing the following command:

```
# exit
```

This page left intentionally blank for pagination purposes

Hotel High Level Description

Hotel is a Windows server running Internet Information Services. It serves as the public (reachable from the Internet) world wide web server for the organization. Hotel hosts a web-based application which ties into the Microsoft SQL Server on Echo. Hotel is NOT in the aia.class windows domain. This is for security reasons!

Following are descriptions of Hotel' specific hands-on tasks that students must complete:

Task 1. Windows Host System Hardening

Students will be minimizing non-essential services and unnecessary network configurations - the network interface will be hardened by removing Internet Protocol (IP) version 6 and disabling NetBIOS name resolution. Students will follow security best practices to harden Windows.

Task 2. Configuring Time Synchronization

Network Time Protocol (NTP) is used to synchronize the host computer's time to a local time server, in this deployment it is the Internet firewall (Quebec).

Task 3. Configuring OSSEC Agent

Students will install and configure the OSSEC Agent, which will then send information about security events to the syslog/OSSEC server (Foxtrot).

Task 4. Windows Security Configuration Wizard

The Windows SCW wizard will take students through a series of questions, which will help them harden the server as per industry best practices. Unnecessary services will be disabled, the windows firewall will be configured, and if necessary, IIS will be hardened.

This page left intentionally blank for pagination purposes

Windows Server Baseline Hardening Steps

1 Harden Network Interfaces

1.1 Remove Unnecessary Protocols

By default, Microsoft Windows network interfaces are enabled with unnecessary protocols and services. These should be unbound from the interface (if not uninstalled completely). If your server is intended to provide these services, obviously you would NOT disable it.

1. If you have not already done so, log on to the machine using:

   Username: **`AIACLASS\Administrator`** Password: **`tartans@1`**

2. Open the 'Start' menu and right-click on 'Network' and select 'Properties' to open the 'Network and Sharing Center'.
3. Click on the 'Local Area Connection 2' and then click 'Properties'.
4. Clear the box next to 'File and Printer Sharing for Microsoft Networks' and 'Internet Protocol Version 6 (TCP/IPv6)'. Then click 'OK'.

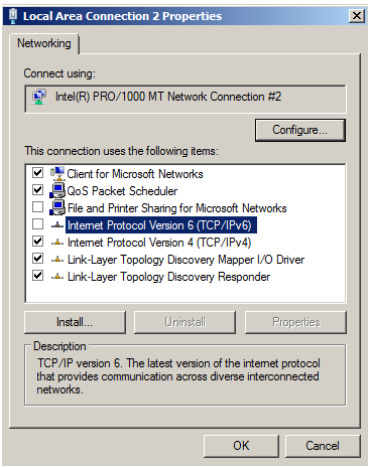


Figure 1: Remove File/Print Sharing

2 Harden TCP/IP Properties

2.1 Disable NetBIOS name resolution

As part of our defense-in-depth strategy, it is import to minimize even those parts of the environment that are normally not utilized. Since our network will be entirely native mode Windows 2000 or higher, NetBIOS name resolution would not normally be utilized, however we will eliminate the possibility of it being used altogether (NetBIOS name resolution is chatty and can divulge network information).

1. If the Properties window for your Local Area Connection is not still open, open it by following steps 1 and 2 from the section above.

2. From within the ‘Properties’ of your ‘Local Area Connection’, select the ‘Internet Protocol Version 4 (TCP/IPv4)’ item (leave it checked), and click on the ‘Properties’ button, then click the ‘Advanced’ button.
3. Next click on the ‘WINS’ tab at the top of the window.

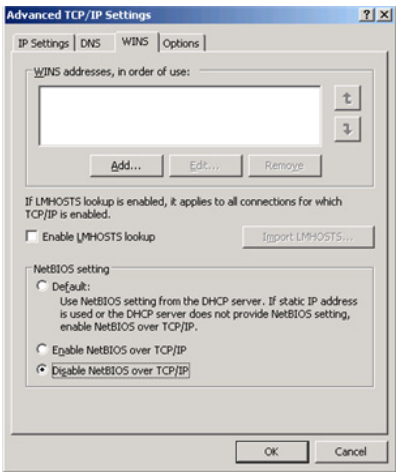


Figure 2: Minimize NetBIOS services

4. Uncheck ‘Enable LMHOSTS lookup’.
5. Select the radio button ‘Disable NetBIOS over TCP/IP’.
6. Click ‘OK’ to accept these settings.
7. Click ‘OK’ to confirm all ‘TCP/IP Properties’ changes.
8. Click ‘OK’ to confirm all ‘Local Area Connection Properties’ changes.
9. Close the ‘Local Area Connection 2 Properties’ and ‘Status’ windows.
10. Close the ‘Network and Sharing Center’ to return to the Desktop.

3 Install ClamWin for Anti-Virus Protection

3.1 Installation

1. Open the Course CD by clicking ‘Start’ -> ‘Computer’, right click ‘CD Drive (D:) AISTS’ and select ‘Open’.
2. Navigate to ‘Tools\Windows\ClamWin’ and double-click the ‘clamwin-0.96.1-setup’ icon.
3. Click ‘Next’.

Figure 3: Install ClamWin Antivirus

4. Accept the license agreement and click ‘Next’.
5. Accept the default option to install for ‘Anyone who uses this computer (all users)’ and click ‘Next’.
6. Select the default installation path and click ‘Next’.
7. At the ‘Select Components’ prompt, accept the default option of ‘Typical Installation’ and click ‘Next’.
8. Click ‘Next’ to create the default start menu folder.
9. Uncheck ‘Download Virus Database Files’ and click ‘Next’.

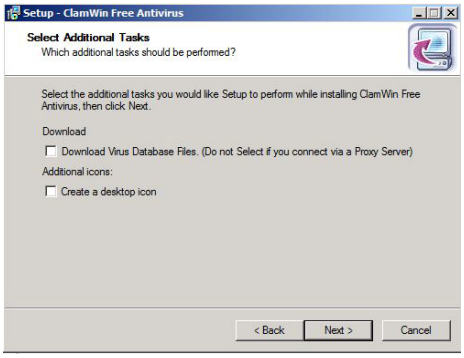


Figure 4: ClamWin Setup

10. Click ‘Install’ to install the program.
11. Click ‘Finish’ to complete the installation.
12. Close Windows Explorer.

3.2 Configuration

1. Click the upward facing arrow in the taskbar and then double-click on the ClamWin icon.

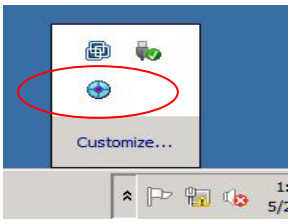


Figure 5: ClamWin Icon

2. Click ‘No’ if asked to update virus definitions now.
3. Select ‘Tools’ from the menu, and click on ‘Preferences’.

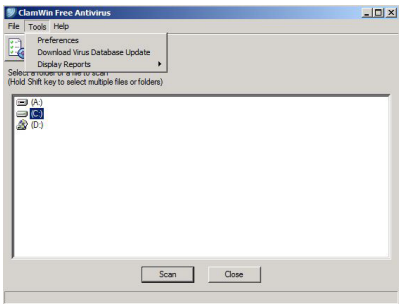


Figure 6: ClamWin Configuration

4. Click on the 'Internet Updates' tab. Leave the updates to be done daily, but change the time to **2:30:00 AM**.

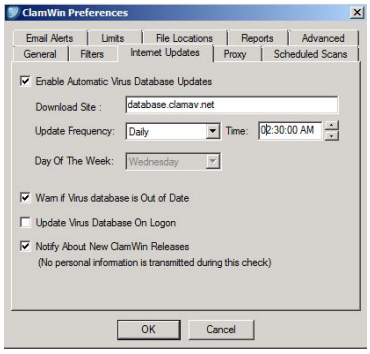


Figure 7: ClamWin Internet Updates

5. Click on the 'Scheduled Scans' tab. Click 'Add'. Choose the scanning frequency to be done Daily at 3:30:00 AM. Enter `C:\` as the folder to scan. Enter a description, such as `Nightly Virus Scan`. Click 'OK'.

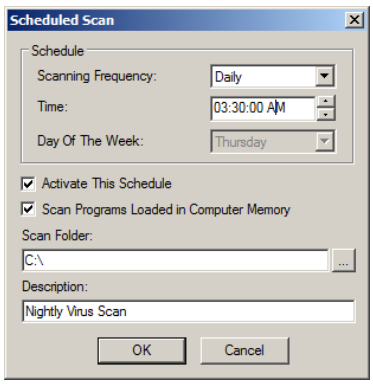


Figure 8: ClamWin Scheduled Scan

6. Click on the 'Email Alerts' tab. Check the box labeled 'Send Email On Virus Detection'. Enter in the following information:

   Mail Server – **10.0.2.3**

   From – `clamwin@Hotel`

   To – `eventwatch@aia.class`

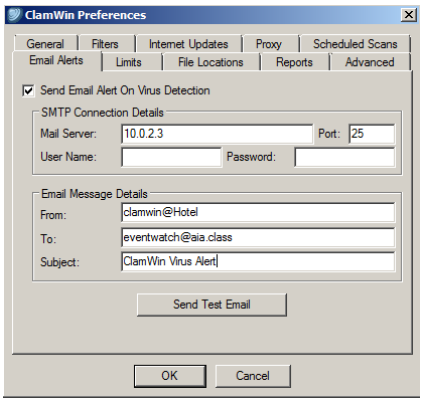


Figure 9: ClamWin Email Alerts

7. Click on the ‘Proxy’ tab. Enter in the IP address of the Squid Proxy server, Quebec, which is **10.0.1.1**. Ensure that the port is **3128**.

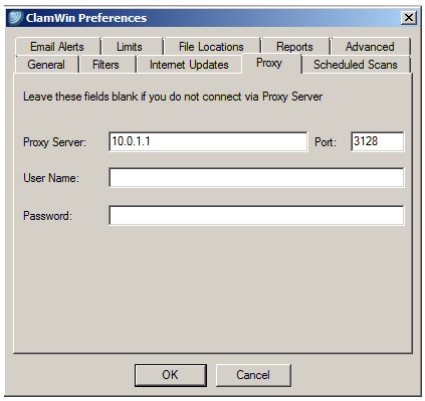


Figure 10: ClamWin Proxy Settings

8. Click ‘OK’ to accept all changes.
9. Choose ‘No’ if asked to update the virus database.
10. Click ‘Close’ to close the ClamWin window.

This page left intentionally blank for pagination purposes

Network Time Protocol (NTP) Client Setup

1 Windows 2008 Server Time Synchronization

Windows Time Service is installed by default on all computers running Windows Server 2008. Windows Time Service uses Coordinated Universal Time (UTC), which is independent of time zone.

In a domain, time synchronization takes place when Windows Time Service turns on during system startup and periodically while the system is running. Because Hotel is not part of the AIA.CLASS domain it will need to have its clock configured to synchronize to our internal time source (Alpha).

1. Click the 'Start' button and select 'Control Panel'.
2. Select 'Clock, Language, and Region'.
3. Select 'Date and Time'.
4. Click on the 'Internet Time' tab.
5. Click 'Change settings'.
6. Enter **10.0.1.1** in the server window.
7. Click 'Update Now'. If a timeout error occurs, you may need to click 'Update Now' again. When successful, you should see the following:

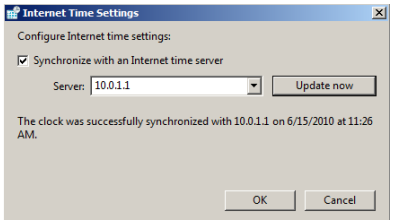


Figure 1: Time Synchronization settings

8. Click 'OK' to close the Internet Time Settings.
9. Click 'OK' again to close the Date and Time settings.

2 Windows Server 2008 Time Synchronization using Local Policy

An alternative to using the Date and Time control panel Internet Time tab is to configure time synchronization settings within the registry. Using the Local Policy snap-in for the Microsoft Management Console (MMC) these settings can easily be changed. ***This task is included for your reference and is not required for the configuration of this server.***

1. Click the 'Start' button.
2. Select 'Run'.
3. Type **`MMC`** and click 'OK'.
4. Click 'File' -> 'Add/Remove Snap-In'.

5. Select ‘Group Policy Object Editor’ from Available snap-ins, click ‘Add’ and then ‘Finish’ on the ‘Welcome to the Group Policy Wizard’ screen.
6. Click ‘OK’ to close the ‘Add Snap-In’ dialog.
7. Navigate the hierarchy to the following folder: ‘Computer Configuration\Administrative Templates\System\Windows Time Service\Time Providers’.

   Here you can enable and configure the NTP client along with configuring the computer as a NTP time server.
8. Double click the ‘Enable Windows NTP Client’.
9. Select ‘Enabled’, and click ‘OK’.
10. Double click ‘Configure Windows NTP Client’ and select the ‘Enabled’ option.
11. Set the ‘NTP Server’ to **10.0.1.1**, 0x1 (Quebec). This will set Hotel to synchronize time with the firewall. The 0x1 parameter after the IP address directs the computer to synchronize with the NTP server as per the value set with ‘SpecialPollInterval’.
12. Change the ‘Type’ to ‘NTP’. The default setting of ‘NT5DS’ is for computers participating in a windows domain. Non-domain computers should use ‘NTP’ or the ‘AllSync’ option which will try to synchronize using all available methods.
13. Change the ‘SpecialPollInterval’ to ‘600’, which is every 10 minutes.

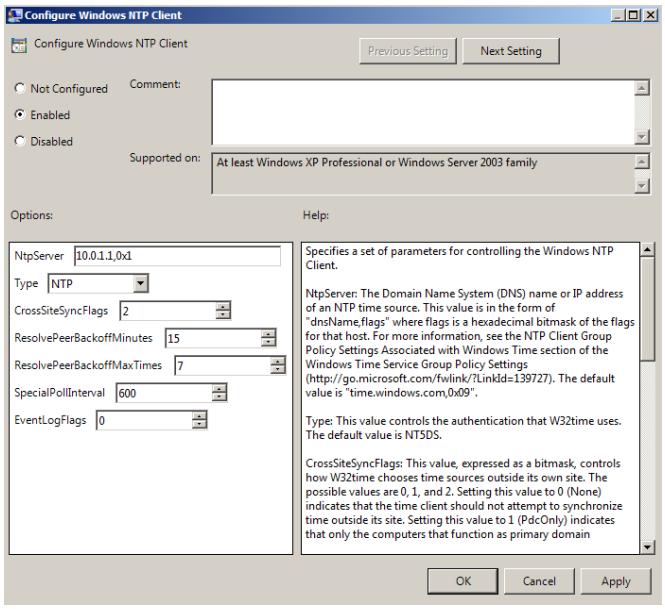


Figure 2: NTP Client Settings

14. Click ‘OK’, to save the NTP settings.
15. Exit the MMC console without saving the settings. Hotel will now synchronize with Quebec every 10 minutes.

Open Source Security (OSSEC) Agent

OSSEC agents will be installed on each Linux and Windows server and will send events to the OSSEC server that is running on Foxtrot. The OSSEC server processes events and generates warnings from alerts sent by the agents. *Before installing any OSSEC agents, make sure that you have successfully deployed the OSSEC server on Foxtrot.*

1 OSSEC Agent setup

1.1 Installation

1. Open Windows Explorer and navigate to 'D:\Tools\Windows\OSSEC':

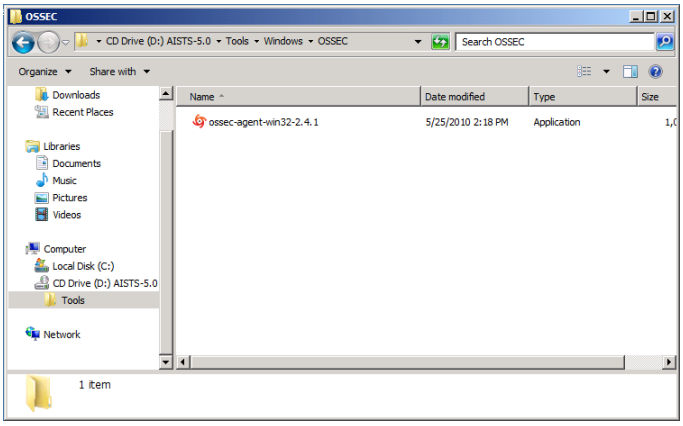


Figure 1: Setup File

2. Double click on 'ossec-agent-win32-2.4.1' setup file and start the installation:

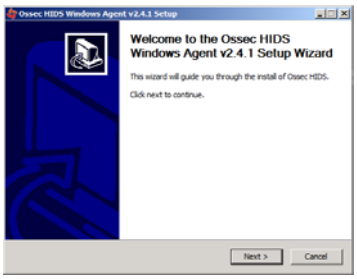


Figure 2: Welcome Screen of OSSEC Installation

3. Click 'Next' and accept the license agreement by pressing the 'I Agree' button:

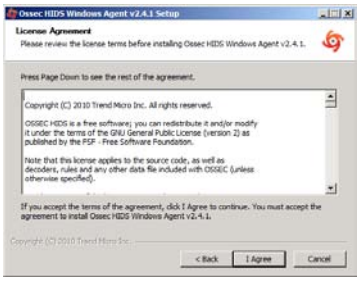


Figure 3: License Agreement window

4. Accept the default installation options and click ‘Next’:

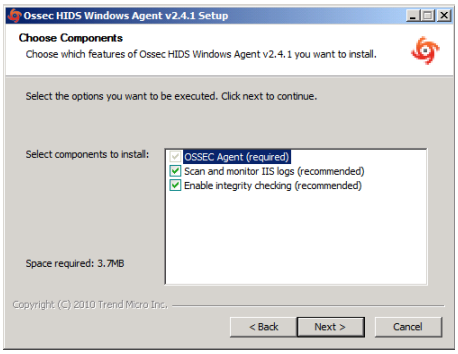


Figure 4: Choose default settings for components

5. Proceed with the installation by pressing the ‘Install’ button:

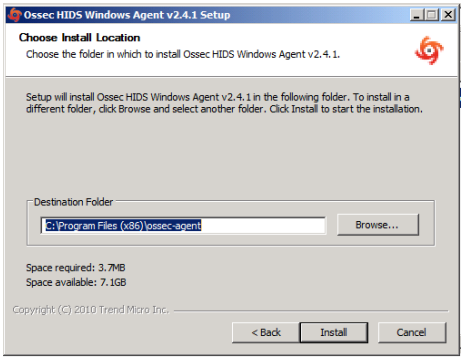


Figure 5: Location path

6. After the installation has finished you should see the following screen. Complete the installation by clicking on ‘Finish’:

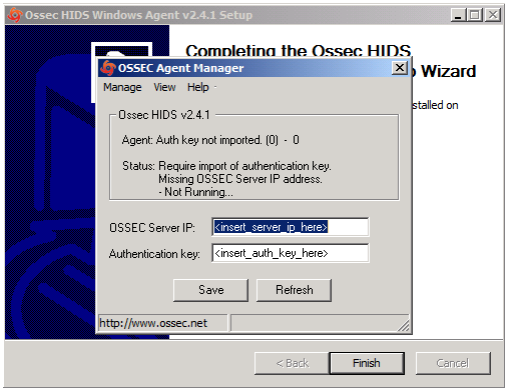


Figure 6: End of OSSEC installation

1.2 Configuration

1. Now we are going to setup a shared key between Hotel and Foxtrot. In order to do this, go back into the CD contents and execute ‘Putty’ from ‘D:\Tools\Windows\Putty’.

2. Enter 10.0.4.2 (Foxtrot's IP Address) in the 'Host Name' field and click 'Open':

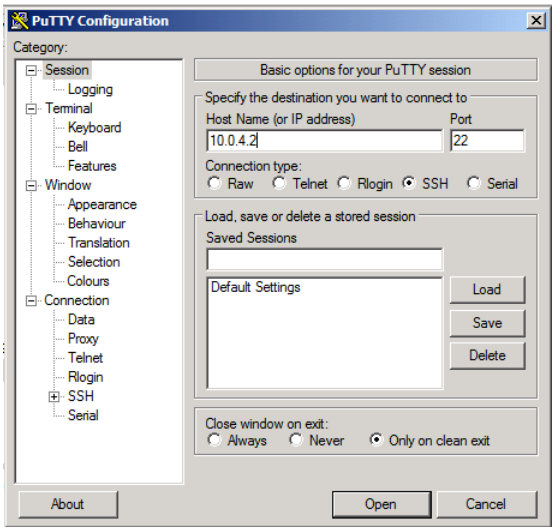


Figure 7: Setting up Putty

3. Accept the warning by clicking 'Yes':

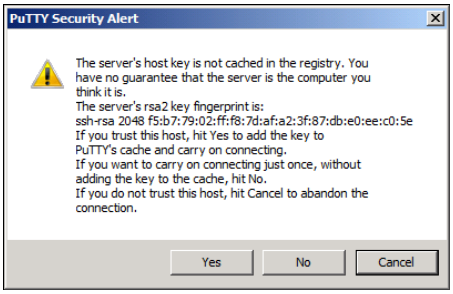


Figure 8: Accept the warning

4. Type **`root`** as the login name and press `[Enter]`then type **`tartans@1`** as the password and press `[Enter]`:

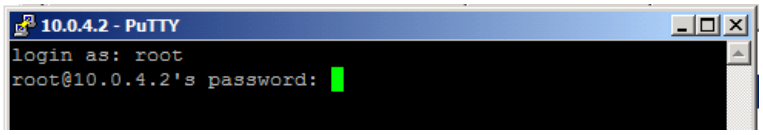


Figure 9: Login

5. Once logged into Foxtrot, start the OSSEC agent manager by executing the following command:

```
# /var/ossec/bin/manage_agents
```

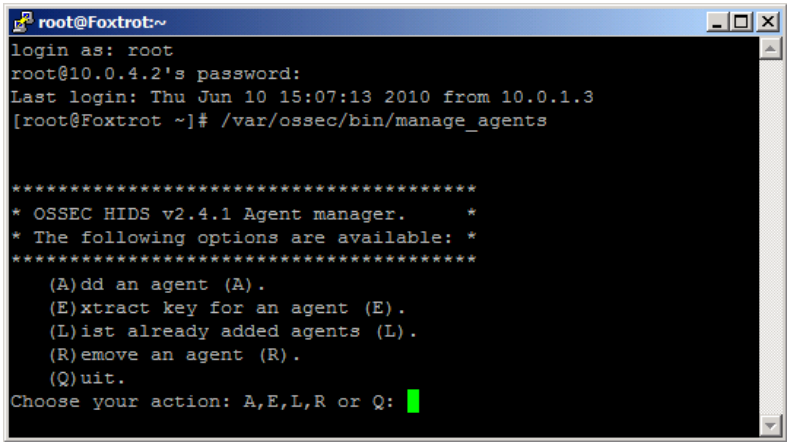


Figure 10: OSSEC Agent Manager window

6. Add an agent by typing A and pressing `[Enter]`.
7. Enter Hotel's information as shown below and press `[Enter]`:

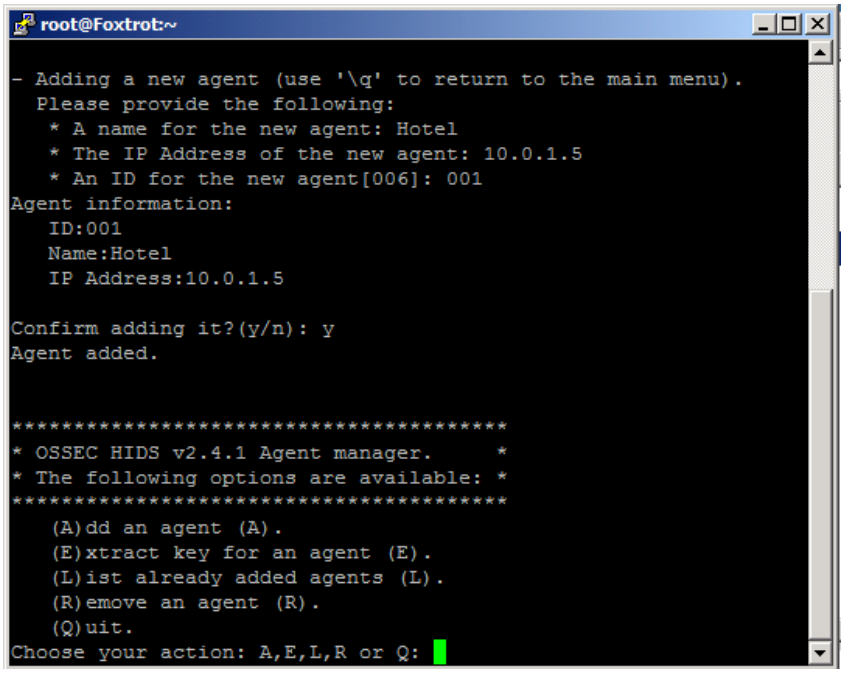


Figure 11: Select an option

8. Now type `E` and press `[Enter]` to extract the shared key for Hotel, and enter `001` when the OSSEC agent manager asks for an agent ID. Please note that the key will not be the same as shown in the following screenshot, because the shared key is generated randomly each time an OSSEC agent is added:

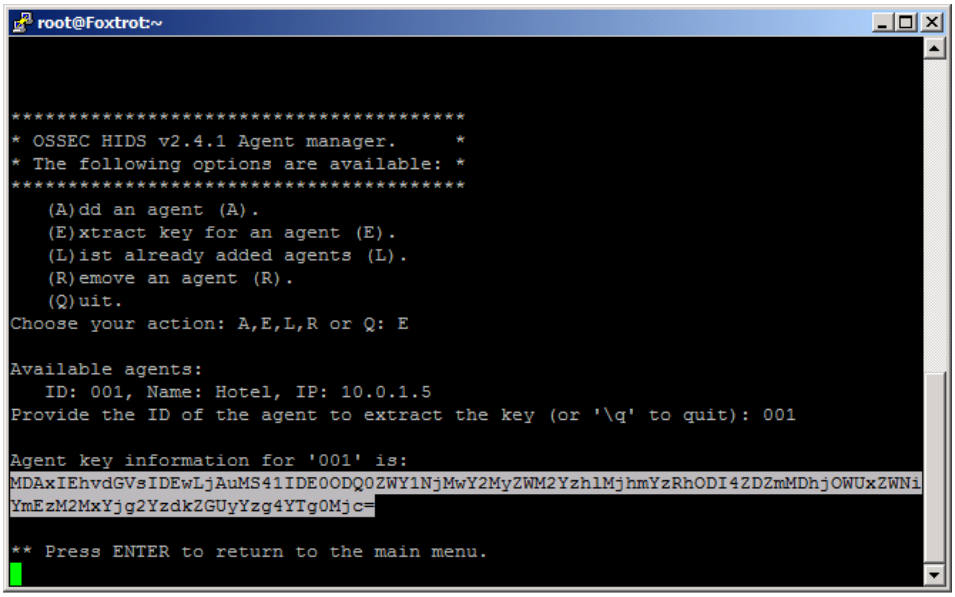


Figure 12: Random key generated

9. Copy the shared key by highlighting it and paste it into OSSEC Agent Manager as shown below.

10. Enter `10.0.4.2` as the server address and click ‘Save’ then ‘OK’:

Figure 13: Enter the parameters

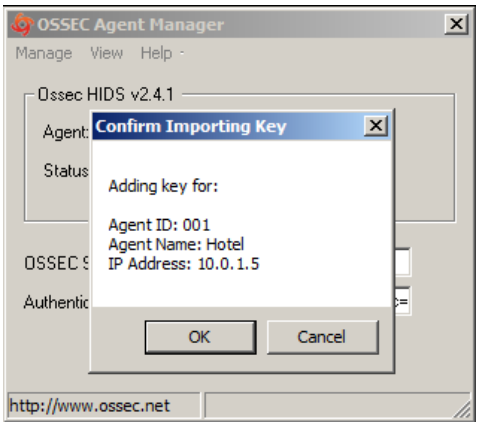


Figure 14: Confirm the settings

11. Switch back to the Putty SSH command shell window. Type `Q` then press `[Enter]` to quit from the agent manager then type `exit` and press `[Enter]` to end the SSH session and exit from Putty.

12. From the OSSEC Agent Manager, Click on ‘View’ -> ‘View Config’ to open the OSSEC Agent configuration file.

13. Take advantage of Notepad's Copy/Paste features to add/edit 2 new lines to the bottom of the file to enable additional IIS log monitoring:

```
<!-- END of Default Configuration. -->


<!-- IIS log file -->
<ossec_config>
  <localfile>
    <location>C:\Windows\System32\LogFiles\W3SVC1\ex%y%m%d.log</location>
    <log_format>iis</log_format>
  </localfile>
  <localfile>
    <location>C:\Windows\System32\LogFiles\W3SVC1\u_extend1.log</location>
    <log_format>iis</log_format>
  </localfile>
  <localfile>
    <location>C:\Windows\System32\LogFiles\W3SVC1\u_inetsv1.log</location>
    <log_format>iis</log_format>
  </local_file>
</ossec_config>


 <ossec_config>
   <client>
      <server-ip>10.0.4.2</server-ip>
   </client>
 </ossec_config>
```

Figure 15: IIS Log File

14. Close the file and choose 'Save'.

15. Choose 'Manage' -> 'Start OSSEC' to start the OSSEC agent:

Figure 16: Starting OSSEC

16. Click OK, then close the OSSEC Agent Manager and (if required) click 'Finish' on the OSSEC setup wizard.

Windows Security Configuration Wizard

1 Run the SCW

1. Click ‘Start’ -> ‘Administrative Tools’ -> ‘Security Configuration Wizard’
2. ’Click ‘Next’ on the ‘Welcome’ screen.
3. Click ‘Next’, to ‘Create a new Security Policy’.

Figure 1: Create a new security policy

4. Click ‘Next’**,** on the ‘Select Server’ dialog. We will not be importing a configuration from a different server.
5. Once the ‘Processing of the Security Configuration Database’ is complete click ‘Next’ to continue.
6. Click ‘Next’, on the ‘Role-Based Service Configuration’ dialog.
7. A list of currently installed roles will be presented. For ‘Hotel’, select only the following:
   - ‘ASP.NET State Service’.
   - ‘Web Server’
   - ‘Windows Process Activation Service’
8. Click **‘**Next’.
9. Uncheck ‘Microsoft Networking Client’. This is not needed as this server is not part of the domain. Click ‘Next’.

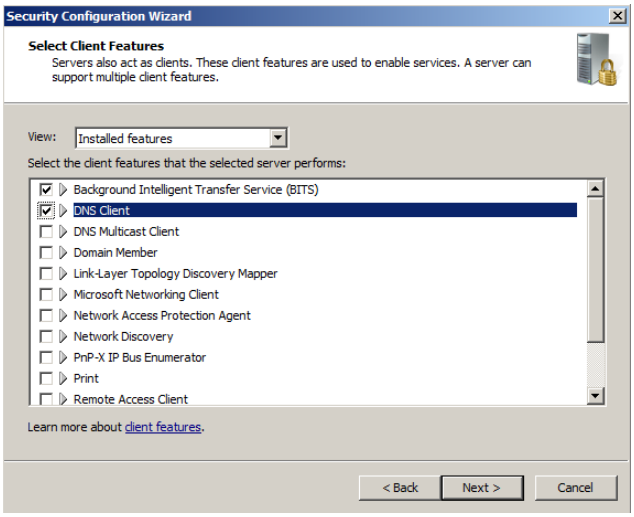


Figure 2: Client features settings

10. ‘Administration and Other Options’, select only:
    - ‘Application Experience Lookup Service’
    - ‘Browse Master’
    - ‘Error reporting’
    - ‘Local application installation’
    - ‘Performance Logs and Alerts’
    - ‘Remote Desktop’
    - ‘Windows User Mode Driver Framework’

    Click ‘Next’.
11. ‘Additional Services,’ select only:
    - ‘MSSQLSERVER’
    - ‘MSSQLServerADHelper’
    - ‘OSSEC Hids’

    Click ‘Next’.
12. Accept the default option of ‘Do not change the startup mode of the service’ for any unspecified services. Click ‘Next’.
13. Review the list of service changes before clicking ‘Next’.
14. Click ‘Next’ to begin the ‘Network Security Configuration’.
15. The SCW attempts to identify the necessary ports that the server will need open for your previous selections. However, we will minimize even further by disabling unnecessary rules. Uncheck the following:
    - Core Networking – Ipv6 (IPv6-In)
    - Core Networking – Ipv6 (IPv6-Out)
    - File and Printer Sharing (NB-Datagram-In)
    - File and Printer Sharing (NB-Datagran-Out)
    - File and Printer Sharing (NB-Name-In)
    - File and Printer Sharing (NB-Name-Out)
16. Click ‘Next’.
17. Click ‘Next’ to begin the ‘Registry Wizard’.
18. Click ‘Next’, to accept the default SMB security settings.
19. Click ‘Next’ to confirm the default Outbound Authentication Methods.
20. Uncheck both options under ‘Inbound Authentication Methods’ and click ‘Next’.

21. Click ‘Next’ to confirm the Registry Settings.

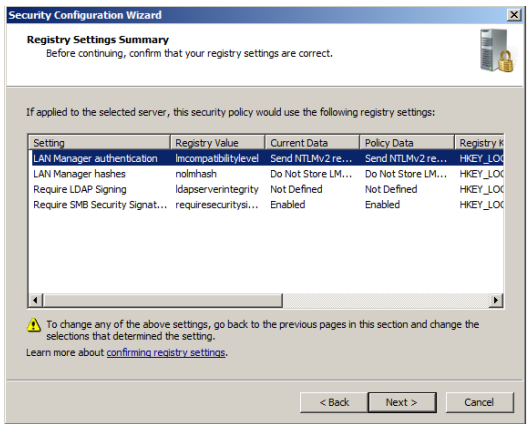


Figure 3: Review the registry settings

22. Check ‘Skip this section’ to bypass configuration of the Audit Policy as this is configured using Group Policy and click ‘Next’.

Figure 4: Ensure the box is checked

23. Click ‘Next’. Save the current configuration by appending the server name to the displayed path and click ‘Next’.

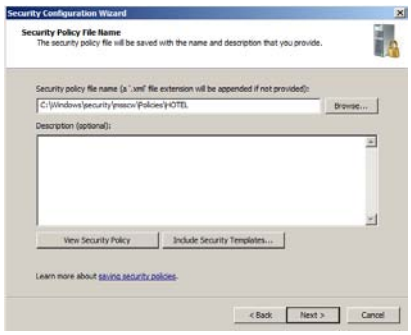


Figure 5: Append ‘HOTEL’ to the path

24. Select the option to ‘Apply Now’ and then click ‘Next’.
25. Once the wizard has completed the necessary changes, click ‘Next’, and then ‘Finish’.
26. From the ‘Start’ menu, select ‘Log off’ -> ’Restart’ to reboot the server. Select ‘Operating System: Reconfiguration (Planned)’ at the ‘Shut Down’ prompt.

2 Add Additional Firewall Rule

1. After the reboot, log in and go to ‘Start -> ‘Administrative Tools’ -> ‘Windows Firewall with Advanced Security’.
2. Click on ‘Inbound Rules’ in the left pane.
3. Click ‘New Rule…’ on the right.
4. Select ‘Custom’ and click ‘Next’.
5. Click ‘Next’.
6. Select ‘ICMPv4’ under ‘Protocol type’ and click ‘Next’.
7. Keep ‘Any IP address’ selected for local IP addresses and select ‘These IP addresses’ for remote IP addresses.
8. Click ‘Add…’ in the remote IP addresses section.
9. Enter Mike’s IP address, **10.0.3.2** into the ‘This IP address or subnet’ box and click ‘OK’.

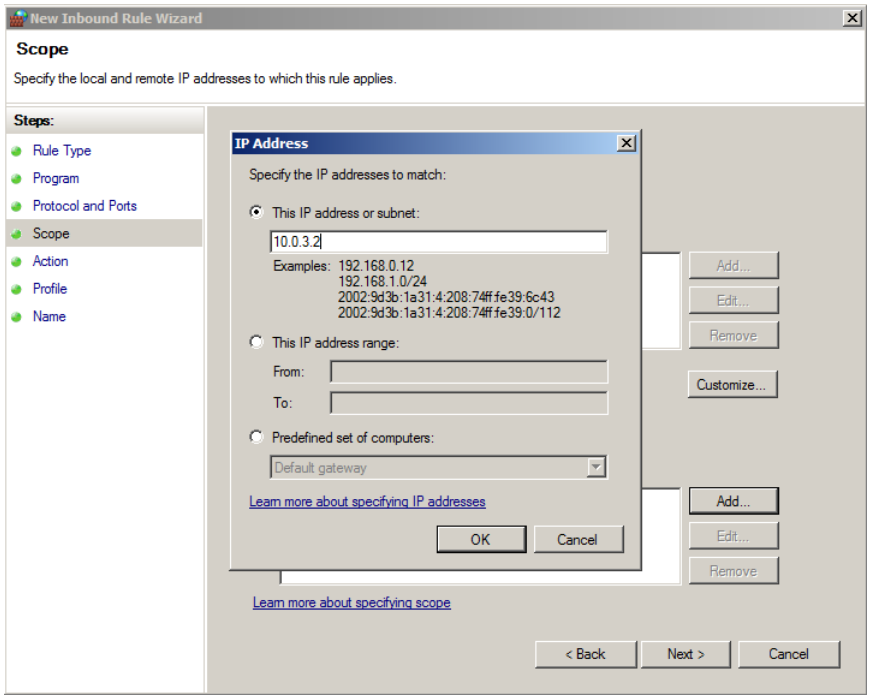


Figure 6: Specify the IP Address

10. Click ‘Next’.
11. Ensure ‘Allow the connection’ is selected and click ‘Next’.
12. Click ‘Next’.
13. Enter ‘Allow Ping from Mike-Nagios’ in the ‘Name’ field and click ‘Finish’.
14. Close the firewall window.

Juliet High Level Description

Juliet is a Domain Name System (DNS) server running BIND. This DNS server has been configured to implement split DNS, and as such, has no knowledge of the internal AIA.CLASS network, and only supports the systems in the DMZ network.

Following are descriptions of Juliet's specific hands-on tasks that students must complete:

Task 1. Linux Host System Hardening

Students will be minimizing non-essential services (e.g., xinetd, sendmail, portmap) as well as extraneous default users and groups. As a standalone DNS server, Juliet does not require these components and so students will follow security best practices for removing them. Also, students will create a non-privileged administrator account to provide an audit trail for all administrative access.

Task 2. Configuring Time Synchronization

Network Time Protocol (NTP) is used to synchronize the host computer's time to a local time server, in this deployment it is the Internet firewall (Quebec).

Alpha will synchronize to Quebec every ten minutes; the Linux hosts will synchronize with Quebec every ten minutes; and the Window hosts will synchronize with Alpha every forty-five minutes until three good synchronizations occur, then once every eight hours. With all the hosts' time across the network synchronized, the cross examination of multiple hosts' logs, or the logs at the syslog Server, become more meaningful and easier to examine.

Task 3. Securing BIND via chroot jail

The idea behind chroot is fairly simple. When you run BIND (or any other process) in a chroot jail, the process is simply unable to see any part of the file system outside the jail. We will configure BIND to run chrooted to the directory /chroot/named. With respect to BIND, the contents of this directory will appear to be /, the root directory. Nothing outside this directory will be accessible to it. This will limit the amount of access any malicious individual could gain by exploiting vulnerabilities in BIND. It is for the same reason that we also run BIND as a non-root user.

This should be considered as a supplement to the normal security precautions (running the latest version, using access control, etc.), certainly not as a replacement for them.

Task 4. Configure reverse proxy using Pound

Pound is a reverse proxy, load balancer, and HTTPS front-end for Web servers. The current network setup forwards SMTP traffic through the firewall directly to Bravo on the internal network. This creates a security risk by exposing Bravo to the Internet and bypassing the DMZ. We will be using Pound to pass Outlook Web Access requests from external hosts, through Juliet to Bravo. In this way, only Juliet, a DMZ server, is directly exposed to external threats and our internal network is protected.

Task 5. Configuring Bastille

The Bastille hardening system is a user-configurable script that attempts to lock down Linux/UNIX operating systems. The Bastille script embodies recommendations from every major reputable source on Linux/UNIX security. We will use pre-configured Bastille templates to lock down such weak system settings as maximum password age, user privileges, etc.

Task 6. Configuring IPTables

IPTables is a Linux firewall application which can be configured to do packet filtering on network firewalls or on host systems. IPTables will be configured on this host as a host-based firewall to allow only valid packets to and from this host. To do this, we will set up INPUT and OUTPUT rules to specifically allow known-good packets into and out of the host, and will create default LOG rules and DROP rules.

Task 7. Configuring OSSEC Agent

Students will install and configure OSSEC Agent, which will then send information about security events to the syslog/OSSEC server (Foxtrot).

Linux Host System Hardening

1 Remove Zeroconf Route

1. If you have not already done so, log on the console using:

   Username: **root** Password: **tartans@1**

2. Open a terminal window by going to ‘Applications’ -> ‘Accessories’ -> ‘Terminal’.

By default Linux adds a "zeroconf" route at boot time. This is a static route that designates the 169.254/16 prefix as local. This is unnecessary on our network, so we will remove the route:

3. Specify to not use zeroconf at boot time:

NOTE: In this and all subsequent Linux documents, the ‘#’ at the beginning of each line should *not* be typed in as part of the command. It is simply meant to represent a command prompt.

```
# echo "NOZEROCONF=yes" >> /etc/sysconfig/network
```

2 Linux Kernel Upgrade

One of the most essential hardening tasks for Linux systems is to ensure that the latest kernel version is being used. The kernel is the core of the operating system and every effort should be made to ensure the most current updated and/or patched version is in use. Most versions of Linux include some automated means for updating software, including the kernel. We will use a tool called YUM (Yellowdog Updater Modified) to download updates from an external web server hosting our YUM repository.

2.1 Apply latest updates to Kernel and other installed packages

1. Edit the yum config file using vi:

```
# vi /etc/yum.repos.d/CentOS-Base.repo
```

2. There are six sections of the file denoted by names in brackets. You will edit 3 of these sections and disable the other 3. Press `[Insert]` or `[i]` to edit the file and scroll down to the first section, ‘[base]’. Comment out the line beginning with ‘mirrorlist=’ by typing a # at the beginning of the line. Next, uncomment the line below it beginning with ‘baseurl=’ and edit the URL to point to our trusted yum repository at `http://192.168.30.14/centos/5.4/os/i386/`. The updated lines will be as follows:

```
[base]
name=CentOS-$releasever - Base
#mirrorlist=http://mirrorlist.centos.org/?release=$releasever&arch=$basearch&rep
o=os
baseurl=http://192.168.30.14/centos/5.4/os/i386/
gpgcheck=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-CentOS-5
```

Figure 1: Configuring YUM base repository

3. Repeat the above steps for the second section, '[updates]', pointing it to the URL `http://192.168.30.14/centos/5.4/updates/i386/`.

```
#released updates
[updates]
name=CentOS-$releasever - Updates
#mirrorlist=http://mirrorlist.centos.org/?release=$releasever&arch=$basearch&rep
o=updates
baseurl=http://192.168.30.14/centos/5.4/updates/i386/
gpgcheck=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-CentOS-5
```

Figure 2: Configuring YUM updates repository

4. Scroll down to the next section, '[addons]' and add `enabled=0` underneath the last line of the section to disable it. The updated lines will be as follows:

```
#packages used/produced in the build but not released
[addons]
name=CentOS-$releasever - Addons
mirrorlist=http://mirrorlist.centos.org/?release=$releasever&arch=$basearch&repo
=addons
#baseurl=http://mirror.centos.org/centos/$releasever/addons/$basearch/
gpgcheck=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-CentOS-5
enabled=0
```

Figure 3: Disabling YUM addons repository

5. Scroll down to the next section, '[extras]' and point it to the URL `http://192.168.30.14/centos/5.4/extras/i386/`.

```
#additional packages that may be useful
[extras]
name=CentOS-$releasever - Extras
#mirrorlist=http://mirrorlist.centos.org/?release=$releasever&arch=$basearch&rep
o=extras
baseurl=http://192.168.30.14/centos/5.4/extras/i386/
gpgcheck=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-CentOS-5
```

Figure 4: Configuring YUM extras repository

We will leave the remaining two sections at their default setting of disabled.

6. Press `[Esc]`, then type `:wq` and press `[Enter]` to save the changes and exit VI.
7. Add a variable to '/etc/yum.conf' so that all future updates use the HTTP proxy. Edit '/etc/yum.conf' with vi:

```
# vi /etc/yum.conf
```

8. To configure yum to use the web proxy server we need to add a line to the '/etc/yum.conf file'. Add the following line to the end of the '[main]' section of the file:

```
proxy=http://10.0.1.1:3128
```

```
[main]
cachedir=/var/cache/yum
keepcache=0
debuglevel=2
logfile=/var/log/yum.log
distroverpkg=redhat-release
tolerant=1
exactarch=1
obsoletes=1
gpgcheck=1
plugins=1
proxy=http://10.0.1.1:3128
```

Figure 5: Configuring YUM proxy server

Press `[Esc]` then type `:wq` and press `[Enter]` to save the changes and exit VI.

NOTE: In order to access the Internet, or even our trusted update server, routing will need to be enabled on Quebec and Romeo. Once the Access control lists are in place on these two router/firewall machines, very few devices will be able to access external networks directly. You may need to wait until these tasks are completed--check with your teammates on this.

9. Run yum in update mode:

```
# yum update
```

10. Type `y` then press `[Enter]` when prompted to download the updates.
11. Type `y` then press `[Enter]` when prompted to import the CentOS 5 GPG key.

    A number of packages will be downloaded and installed, including a newer kernel.

    This step may take several minutes to complete. Press `[Ctrl]` + `[Shift]` + `[T]` to open a new terminal tab if you want to move on to the next steps while the updates take place.

3 Service Minimization

3.1 Removing Unnecessary Services

By default Linux runs many services that a standalone server will not need. Extraneous services are dangerous because they provide possible attack vectors.

The services that will need to be removed from this system are:

- anacron
- apmd
- atd
- autofs
- cpuspeed
- cups
- gpm
- irqbalance
- mdmonitor
- mdmpd
- microcode_ctl
- netfs
- nfslock
- portmap
- rawdevices
- rpcgssd
- rpcsvcgssd
- rpcidmapd
- sendmail
- xinetd

1. Terminate the 'anacron' service properly by using the following command:

```
# service anacron stop
```

2. Remove the 'anacron' startup routine using the following command:

```
# chkconfig --del anacron
```

```
Stopping anacron:                                          [  OK  ]
```

Figure 6: Removing a service

3. Repeat steps #1 and #2 for each service listed above. (ADVANCED: see the 'Bash Script' ADDENDUM located on the last two pages of this section to automate these repetitive steps.)

   Note: On some systems, some of the services may not be started and may not return the 'OK' when stopped. If this is the case, it will be sufficient to simply delete the service.

4. To check that the appropriate services have been removed, use the following two commands from a terminal window:

```
# netstat –ntap | grep –i listen
```

```
tcp        0      0 10.0.1.3:53                 0.0.0.0:*                   LIST
EN      2468/named
tcp        0      0 127.0.0.1:953               0.0.0.0:*                   LIST
EN      2468/named
tcp        0      0 :::22                       :::*                        LIST
EN      3164/sshd
```

Figure 7: Confirming service removal

```
# chkconfig --list | grep on | sort
```

```
acpid           0:off   1:off   2:on    3:on    4:on    5:on    6:off
auditd          0:off   1:off   2:on    3:on    4:on    5:on    6:off
avahi-daemon    0:off   1:off   2:off   3:on    4:on    5:on    6:off
avahi-dnsconfd  0:off   1:off   2:off   3:off   4:off   5:off   6:off
conman          0:off   1:off   2:off   3:off   4:off   5:off   6:off
crond           0:off   1:off   2:on    3:on    4:on    5:on    6:off
firstboot       0:off   1:off   2:off   3:on    4:off   5:on    6:off
haldaemon       0:off   1:off   2:off   3:on    4:on    5:on    6:off
hidd            0:off   1:off   2:on    3:on    4:on    5:on    6:off
ip6tables       0:off   1:off   2:on    3:on    4:on    5:on    6:off
iptables        0:off   1:off   2:on    3:on    4:on    5:on    6:off
lvm2-monitor    0:off   1:on    2:on    3:on    4:on    5:on    6:off
mcstrans        0:off   1:off   2:on    3:on    4:on    5:on    6:off
messagebus      0:off   1:off   2:off   3:on    4:on    5:on    6:off
netconsole      0:off   1:off   2:off   3:off   4:off   5:off   6:off
network         0:off   1:off   2:on    3:on    4:on    5:on    6:off
pcscd           0:off   1:off   2:on    3:on    4:on    5:on    6:off
readahead_early 0:off   1:off   2:on    3:on    4:on    5:on    6:off
readahead_later 0:off   1:off   2:off   3:off   4:off   5:on    6:off
restorecond     0:off   1:off   2:on    3:on    4:on    5:on    6:off
sendmail        0:off   1:off   2:on    3:on    4:on    5:on    6:off
sshd            0:off   1:off   2:on    3:on    4:on    5:on    6:off
syslog          0:off   1:off   2:on    3:on    4:on    5:on    6:off
vmware-tools    0:off   1:off   2:on    3:on    4:off   5:on    6:off
wdaemon         0:off   1:off   2:off   3:off   4:off   5:off   6:off
xfs             0:off   1:off   2:on    3:on    4:on    5:on    6:off
```

Figure 8: Results of service removals

5. If your results are ***similar*** to the output shown above, the services have been removed successfully.

4 User / Group Account Minimization

It is important to disable all default vendor accounts that will be unused. Typically a default account, e.g., gopher or news, is created only when the respective service is also installed; however, many default accounts will exist even if you have not installed the related services on your system. In our case, we will not use many of the default accounts and so we will remove them. The more accounts you have, the easier it is for outsiders to access your system.

4.1 Remove Default User Accounts

The users we will need to remove are:

- adm
- apache
- ftp
- games
- gopher
- halt
- lp
- mail
- mailnull
- news
- nfsnobody
- nobody
- nscd
- operator
- rpcuser
- rpc
- shutdown
- smmsp
- uucp
- vcsa
- xfs

1. Remove the ‘adm’ user account using the following command:

```
# userdel adm
```

2. Repeat the previous step for each account listed above. Verify removal by executing the following command:

```
# cat /etc/passwd
```

```
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
distcache:x:94:94:Distcache:/:/sbin/nologin
webalizer:x:67:67:Webalizer:/var/www/usage:/sbin/nologin
dovecot:x:97:97:dovecot:/usr/libexec/dovecot:/sbin/nologin
squid:x:23:23::/var/spool/squid:/sbin/nologin
mysql:x:27:27:MySQL Server:/var/lib/mysql:/bin/bash
pcap:x:77:77::/var/arpwatch:/sbin/nologin
ntp:x:38:38::/etc/ntp:/sbin/nologin
dbus:x:81:81:System message bus:/:/sbin/nologin
avahi:x:70:70:Avahi daemon:/:/sbin/nologin
named:x:25:25:Named:/var/named:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
haldaemon:x:68:68:HAL daemon:/:/sbin/nologin
avahi-autoipd:x:100:102:avahi-autoipd:/var/lib/avahi-autoipd:/sbin/nologin
gdm:x:42:42::/var/gdm:/sbin/nologin
user:x:500:500:User:/home/user:/bin/bash
```

Figure 8 : Results of removing unnecessary default user accounts

3. If the default user accounts have been successfully removed, your /etc/passwd file will look ***similar*** to the output shown in the figure above.

4.2 Remove Default Groups

Now that we have removed all unnecessary accounts from the /etc/passwd file, we will clean up the /etc/groups file.

The groups that we will remove are:

- adm
- dip
- lock
- lp
- mail
- news
- uucp

Removing a group account is similar to the process of removing a user shown above.

1. Delete the ‘adm’ group using the following command:

```
# groupdel adm
```

2. Repeat the previous step for each group listed above.

3. Verify removal by executing the following command:

```
# cat /etc/group
```

```
root:x:0:root
bin:x:1:root,bin,daemon
daemon:x:2:root,bin,daemon
sys:x:3:root,bin
tty:x:5:
disk:x:6:root
mem:x:8:
kmem:x:9:
wheel:x:10:root
man:x:15:
users:x:100:
utmp:x:22:
utempter:x:35:
audio:x:63:gdm
distcache:x:94:
floppy:x:19:
webalizer:x:67:
dovecot:x:97:
squid:x:23:
mysql:x:27:
pcap:x:77:
slocate:x:21:
ntp:x:38:
ecryptfs:x:101:
dbus:x:81:
avahi:x:70:
named:x:25:
sshd:x:74:
haldaemon:x:68:
avahi-autoipd:x:102:
gdm:x:42:
user:x:500:
```

Figure 9: Results of removing unnecessary default groups

4. If the default groups have been successfully removed, the /etc/group file will look ***similar*** to the output shown in the figure above.

4.3 Create the 'Admin' User

The last account management task we will perform manually is to create an 'admin' user for daily administration tasks once the initial setup is complete.

1. Add the admin user using the following command:

```
# useradd admin
```

2. Set the password for the 'admin' account:

```
# passwd admin
```

3. When prompted for a password use the following: `steelers`

   The output will resemble that shown below:

```
Changing password for user admin.
New UNIX password:
BAD PASSWORD: it is based on a dictionary word
Retype new UNIX password:
passwd: all authentication tokens updated successfully.
```

Figure 10: Creating an Admin user

Note: In a real production environment you should always choose a strong password or passphrase that is sufficiently long and contains a combination of letters, numbers, and special characters. The above password is used for demonstration purposes only.

5 Installing ClamAV

1. Copy the ClamAV tarball from the course CD to the /root directory:

```
# cp /media/AISTS/Tools/Linux/ClamAV/clamav-0.96.1.tar.gz /root
```

2. Untar ClamAV:

```
# cd /root
# tar xvzf clamav-0.96.1.tar.gz
```

3. We need to install a few prerequisite packages before installing ClamAV. We will use our trusted yum repository that we set up earlier in this task to install zlib-devel. Additionally, in order to compile ClamAV and other tools in later tasks from source code we will need a compiler installed on the machine. This distribution of CentOS does not come with a compile pre-installed so we will install the gcc compiler ourselves.

   Make sure to remove this compiler when all of this machine's tasks have been completed as it can be leveraged by an attacker to compile malicious code if they were to gain access to the system.

```
# yum install gcc zlib-devel
```

4. Type `y` then press `[Enter]` when prompted to confirm the download.
5. Change into the clamav-0.96.1 directory and install ClamAV:

```
# cd clamav-0.96.1
# adduser clamav
# ./configure --sysconfdir=/etc
# make
# make install
```

6. Use the VI editor to open the clamav.conf file in order to configure ClamAV:

```
# vi /etc/clamd.conf
```

7. Press `[Insert]` to enter edit mode. Comment out the line near the beginning of the file containing 'Example':

```
# Comment or remove the line below.
#Example
```

Figure 11: Editing clamd.conf

8. Find and uncomment the following lines by removing the '#' in front of them:
   a. 'LogFile /tmp/clamd.log'
   b. 'LogTime yes'
   c. 'LogSyslog yes'
   d. 'LocalSocket /tmp/clamd.socket'

9. Save and exit the file. Press `[Esc]` and type `:wq` then press `[Enter]`.

10. The ClamAV updater (freshclam) needs to be pointed to our internal proxy (10.0.1.1) in order to be able to update virus definitions. Use the VI editor to open the freshclam.conf file:

```
# vi /etc/freshclam.conf
```

11. Comment out the line near the beginning of the file containing 'Example':

```
# Comment or remove the line below.
#Example
```

Figure 12: Editing freshclam.conf

12. Find the proxy settings. Uncomment and make the following changes to indicate the IP of the proxy server and the port number to use:

```
HTTPProxyServer 10.0.1.1
HTTPProxyPort 3128
```

Note: Although freshclam has been configured, it probably won't successfully run yet. The Squid Proxy server may still need to be set up.

13. Save and exit the file. Press `[Esc]` and type `:wq` then press `[Enter]`.

14. Enable the ClamAV daemon to start automatically as a service:

```
# cp /media/AISTS/Tools/Linux/ClamAV/clamd /etc/init.d/
# chkconfig --add clamd
# service clamd start
```

15. Setup cron jobs for Virus definition updates and nightly virus scans:

```
# crontab –u root -e
```

16. Add the following two lines to the file:

```
15 2 * * * /usr/local/bin/freshclam --quiet
15 3 * * * /usr/local/bin/clamdscan --quiet /
```

17. Save and exit the cron file. Press `[Esc]` and type `:wq` then press `[Enter]`.

18. Remove ClamAV installation files (they contain test signatures that will be found on every scan if we don't remove them) then reboot the server.

```
# cd /root
# rm -rf clamav-0.96*
# reboot
```

ADDENDUM Bash Script: 'for loop'

Create a file containing the list of items

1. If you would like to automate the task of removing the unwanted services, users and groups, you can write a Bash script to loop through the list of items and process them one by one. First, start by creating a text file containing the list of items that you want to process. Enter the following command to create the text file:

```
# cat > deletedSvcList
```

2. After you typed the previous command and hit the `[Enter]` key, notice that there is no prompt ('#') at the cursor. The file is now open and you can enter the list of items that you want to process. Enter each item on a separate line, hitting the `[Enter]` key to move to the next line.

3. When all of the items have been entered into the file, press `[Ctrl+d]` to save and close the file. Notice that the prompt ('#') has returned to the shell.

Write the 'for loop'

1. Now we will create a 'for loop' that will read the items in the deletedSvcList file one by one and stop each service. Enter the following script as it appears below to stop the unwanted services:

```
# for str in $(cat deletedSvcList); do service $str stop; done
```

   A simple modification makes sure that those services do not start on bootup:

```
# for str in $(cat deletedSvcList); do chkconfig --del $str; done
```

2. Notice that the script is in three sections, separated by semi-colons (';'). The first section of this script creates a variable, named 'str', and assigns to it the first item in the file. The second section inserts the value of the variable, 'str', into the shell command. The command is executed and then the process is repeated for each item in the file. When there are no more items in the file, the third section of the script ends the process and returns control back to the shell.

   As you go through the steps, you will have to create three separate files for services, users and groups. Then you must modify the file name in the first section of the script. Likewise, you will have to modify the command in the second section to perform the action that you want.

Here are the files and scripts that should be created to remove the following items:

Users:

```
# cat > deletedUserList
```

```
# for str in $(cat deletedUserList); do userdel $str; done
```

Groups:

```
# cat > deletedGrpList
```

```
# for str in $(cat deletedGrpList); do groupdel $str; done
```

Linux Network Time Protocol Daemon (ntpd) Client

1 Setup Linux ntpd Client Service

1.1 Installation

1. If you have not already done so, log on the console using:

   Username: **root** Password: **tartans@1**

2. Open a terminal window by going to 'Applications' -> 'Accessories' -> 'Terminal'.
3. The Network Time Protocol Daemon (ntpd) is installed with most Linux distributions. You will create a cron job that will cause the Linux ntpd to periodically query Quebec's ntp server and update the system time.

1.2 Configuration

1. Run the following command to see the current local system time. Hopefully, it is significantly different from the time server's system time as this will explicitly demonstrate when the client becomes synchronized with the server:

```
# date
```

2. If the date is not significantly different from the time server's system time, you can change the local client's system time manually by entering the following command (you can change the system date and time to whatever you want):

```
# date -s "Fri Sep 12 14:38:19 EDT 2003"
```

3. The ntp configuration file must be modified to tell it which time server to use to update the system time. This file is located in the '/etc' directory. To open the config file in the 'vi' text editor, enter:

```
# vi /etc/ntp.conf
```

4. In order to modify the file in the 'vi' editor, the `[Insert]` or `[i]` key must be pressed before trying to add or change text.

5. Scroll down to the section beginning with "# Use public servers" which is excerpted here:

```
# Use public servers from the pool.ntp.org project.
# Please consider joining the pool (http://www.pool.ntp.org/join.html).
server 0.centos.pool.ntp.org
server 1.centos.pool.ntp.org
server 2.centos.pool.ntp.org
```

Figure 1: Default NTP configuration file

Comment out the previous servers and add the following two lines at the end of this section:

```
restrict 10.0.1.1 mask 255.255.255.255 nomodify notrap noquery
server 10.0.1.1 prefer
```

Your section should look similar to the following:

```
# Use public servers from the pool.ntp.org project.
# Please consider joining the pool (http://www.pool.ntp.org/join.html).
#server 0.centos.pool.ntp.org
#server 1.centos.pool.ntp.org
#server 2.centos.pool.ntp.org
restrict 10.0.1.1 mask 255.255.255.255 nomodify notrap noquery
server 10.0.1.1 prefer
```

Figure 2: Edited NTP configuration file

6. Save and exit the file. Press `[Esc]` and type `:wq` then press `[Enter]`.

7. Now we need to cause ntpd to update to the ntp server time by modifying /etc/ntp/step-tickers to run ntpdate when ntpd is started. Do this by running these two commands:

```
# echo "10.0.1.1" > /etc/ntp/step-tickers
```

8. The 'step-tickers' file should now contain only the ntp server's IP address. The file contents can be viewed by entering this command:

```
# cat /etc/ntp/step-tickers
```

9. Enter the date command to see that the date is still incorrect.

10. If the ntpd service is not currently running, it must be started by entering the following command. If the service is currently running, replace 'start' with `restart`. NOTE: Once the service is running, always remember to 'restart' after making any changes to the ntp config file. Otherwise, the service will continue to run according to the previous config file settings until the service is restarted. Later, we will be creating a cron job to periodically restart the service. For now, enter this command:

```
# service ntpd start
```

11. You should see these two messages:

```
ntpd: Synchronizing with time server:                    [  OK  ]
Starting ntpd:                                           [  OK  ]
```

Figure 3: Starting the NTP service

12. Enter the date command again to see that the time has been synchronized.
    Note: This will only be successful after Quebec's time server has been configured properly. Check with your teammates for its status.

13. The service can be verified and the current pid identified by entering:

```
# service ntpd status
```

14. Now, we are going to make sure that ntpd updates the system time regularly. Skew the local system time again by entering the following command that you entered earlier (up arrow to find this command and press enter):

```
# date -s "Fri Sep 12 14:38:19 EDT 2003"
```

15. A cron job must be created to cause the ntpd service to periodically query the time server and update the local system time accordingly. Enter this command to create the cron job file:

```
# crontab –u root –e
```

16. This file should automatically open using the 'vi' text editor again, so you must press the `[Insert]` or `[i]` key before you can add or modify text.

17. Insert the following line at the top of the file to set up a cron job that will execute every 10 minutes. You can review the 'man 5 crontab' pages to understand the crontab fields in more depth after you are done with this task. After the ntpd is verified to be up and running correctly, the first set of numbers can be changed to a '0' to cause the cron job to run at the top of every hour (0th minute of every hour) instead.

    Make sure that there is a space after the 50 and between each '*' and the '/' character following them. There are no spaces between the initial set of numbers.

```
0,10,20,30,40,50 * * * * /etc/rc.d/init.d/ntpd restart
```

```
0,10,20,30,40,50 * * * * /etc/rc.d/init.d/ntpd restart
15 2 * * * /usr/local/bin/freshclam --quiet
15 3 * * * /usr/local/bin/clamdscan --quiet /
```

18. Now Save and exit the file. Press `[Esc]` and type `:wq` then press `[Enter]`.

19. Entering the following command will create init scripts at run levels 3-5 to start the ntpd service every time the system is started up.

```
# chkconfig --level 345 ntpd on
```

20. Use the following command to verify that the ntpd service is turned on at run levels 3, 4, and 5:

```
# chkconfig --list | grep ntpd
```

21. Make sure that it looks like this:

```
ntpd            0:off   1:off   2:off   3:on    4:on    5:on    6:off
```

Figure 4: NTP service startup run levels

22. Now, use the date command to see if the cron job has updated the system time. If not, wait a few more minutes and try again.

23. Once the remote centralized syslog server is installed and configured, we can review the logs that are generated from the Network Time Server process. There we will see each time that the client is updated and the offset amount by which it is updated.

Securing BIND via a 'chroot' jail

1 Check existing BIND

1.1 Verify existing BIND installation

1. If you have not already done so, open a terminal from Applications -> Accessories -> Terminal.

2. Check the existing BIND service is running by entering following command:

```
# ps –eaf | grep named
```

3. Check the run levels of the existing BIND installation:

```
# chkconfig --list | grep named
```

4. Verify the BIND service is properly configured using dig:

```
# dig @10.0.1.3 www.aia.class
```

The response should list '192.168.30.13' in the 'ANSWER' section.

```
[root@Juliet ~]# dig @10.0.1.3 www.aia.class

; <<>> DiG 9.3.6-P1-RedHat-9.3.6-4.P1.el5 <<>> @10.0.1.3 www.aia.class
; (1 server found)
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 41832
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 0

;; QUESTION SECTION:
;www.aia.class.                 IN      A

;; ANSWER SECTION:
www.aia.class.          38400   IN      A       192.168.30.13

;; AUTHORITY SECTION:
aia.class.              38400   IN      NS      ns.aia.class.

;; Query time: 8 msec
;; SERVER: 10.0.1.3#53(10.0.1.3)
;; WHEN: Wed Jun  2 16:07:26 2010
;; MSG SIZE  rcvd: 64
```

Figure 1: Named query

2 Prepare the jail

2.1 Shut down BIND

1. Terminate the BIND process by entering the following command:

```
# service named stop
```

```
[root@Juliet ~]# service named stop
Stopping named:                                            [  OK  ]
[root@Juliet ~]#
```

Figure 2: Stopping named

2.2 Install bind-chroot package

Once we install bind-chroot package for the CentOS 5 it will automatically create the following directory structure for our jail in /var directory.

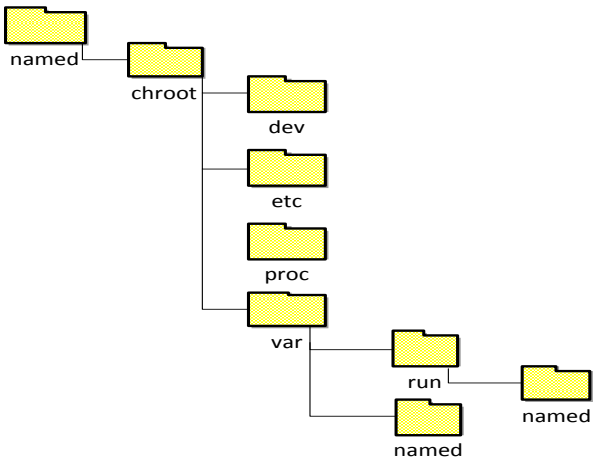


Figure 3: Chroot Directory Structure

1. Install bind-chroot package for jail:

```
# yum install bind-chroot
```

2. Type y and press `[Enter]` to download and install the package.
3. Check BIND is running from / named /chroot/ directory:

```
# cat /etc/sysconfig/named
```

```
# KEYTAB_FILE="/dir/file"    --  Specify named service keytab file (for GSS-TSIG)
ROOTDIR=/var/named/chroot
[root@Juliet named]#
```

Figure 4: Named Configuration File

4. Check all symbolic links and permission set correctly after bind-chroot package installation.

```
# cd /var/named
# ls -l
```

```
[root@Juliet named]# ls -l
total 20
lrwxrwxrwx 1 root  named   44 Jun  3 16:32 aia.class.hosts -> /var/named/chroot//var/named/aia.cl
ass.hosts
drwxr-x--- 6 root  named 4096 Jun  3 16:32 chroot
drwxrwx--- 2 named named 4096 Sep  3  2009 data
lrwxrwxrwx 1 root  named   43 Jun  3 16:32 localhost.zone -> /var/named/chroot//var/named/localho
st.zone
lrwxrwxrwx 1 root  named   37 Jun  3 16:32 named.ca -> /var/named/chroot//var/named/named.ca
lrwxrwxrwx 1 root  named   40 Jun  3 16:32 named.local -> /var/named/chroot//var/named/named.loca
l
drwxrwx--- 2 named named 4096 Sep  3  2009 slaves
[root@Juliet named]#
```

Figure 5: Named symbolic links

If you need to configure the jail manually, you have to create the directory structure shown in *Figure* 3 and restrict the permissions according to following steps. In our case it has been done automatically by bind-chroot package. **The following does NOT need to be done and is for reference only. Continue to Step 5 after reviewing this section.**

First we will restrict access to the /chroot directory

```
# cd /var/named/
# chown –R root:named /chroot
```

Remove world access

```
# chmod –R o-rwx /chroot
```

Remove group write from dev/ etc/ and var/

```
# chmod g-w dev etc
# chmod –R g-w var
```

Allow read only access to primary zone files

```
# chmod 750 /chroot/var/named
# chmod –R go-w /chroot/var/named
```

Allow named user to write pid files

```
# chmod 770 /chroot/var/run/named
```

Allow named to access the BIND configuration file

```
# chmod 750 /chroot/etc
# chmod 640 /chroot/etc/named.conf
```

Assigning corresponding rights to devices

```
# cd /chroot/dev
# chmod 666 null random
# chmod 640 log
# chgrp sys null random
```

5. Start named service:

```
# service named start
```

```
[root@Juliet named]# service named start
Starting named:                                            [  OK  ]
[root@Juliet named]#
```

Figure 6: Starting the Named service

6. Verify BIND service is working properly using dig and responding to the query as before in Step 3 of Task 1.2:

```
# dig @10.0.1.3 www.aia.class
```

2.3 Configure Logging

Since BIND will be unable to access syslog from inside its jail, we will create a socket inside the jail that allows BIND to communicate with syslog.

1. Use vi to edit the /etc/sysconfig/syslog file.

```
# vi /etc/sysconfig/syslog
```

Press the `[Insert]` key to change the line that reads:

```
SYSLOGD_OPTIONS="-m 0"
```

To:

```
SYSLOGD_OPTIONS="-m 0 –a /var/named/chroot/dev/log"
```

2. Save your changes and exit vi by pressing `[Esc]` and entering:

```
:wq
```

3. To put your changes into effect, use the following command to restart syslog:

```
# service syslog restart
```

```
[root@Juliet dev]# service syslog restart
Shutting down kernel logger:                               [  OK  ]
Shutting down system logger:                               [  OK  ]
Starting system logger:                                    [  OK  ]
Starting kernel logger:                                    [  OK  ]
```

Figure 7: Restart Syslog

4. To verify your changes, use the following command:

```
# ps –eaf | grep syslog
```

```
[root@Juliet dev]# ps -eaf | grep syslog
root      5384     1  0 16:50 ?        00:00:00 syslogd -m 0 -a /var/named/chroot/dev/log
root      5448  4553  0 16:52 pts/1    00:00:00 grep syslog
```

Figure 8: Syslog Process Info

If syslogd was successfully modified, the output of your system should match the output shown in Figure 8 above.

This page left intentionally blank for pagination purposes

Install and Configure Reverse Proxy Using Pound

Pound is a reverse proxy, load balancer, and HTTPS front-end for Web servers. The current network setup forwards SMTP traffic through the firewall directly to Bravo on the internal network. We will be using Pound to pass Outlook Web Access requests from external hosts, through Juliet to Bravo. In this way, only Juliet, a DMZ server, is directly exposed to external threats and our internal network is protected.

1 Install Pound

1. Install Pound by executing the following commands:

```
# cd /media/AISTS/Tools/Linux/Pound/
# useradd pound
# rpm –ivh pound-2.4.3-1.el5.rf.i386.rpm
```

2. We want to use SSL for external connections to Outlook Web Access. Create a certificate for this using the following commands:

```
# cd /usr/local/etc
# openssl req -new -newkey rsa:1024 -nodes -x509 -keyout
owa.aia.class.pem  -out owa.aia.class.pem
```

3. Answer the questions as shown in following screenshot:

```
[root@Juliet etc]# openssl req -new -newkey rsa:1024 -nodes -x509 -keyout owa.aia.class.pem  -out
 owa.aia.class.pem
Generating a 1024 bit RSA private key
................++++++
..++++++
writing new private key to 'owa.aia.class.pem'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [GB]:US
State or Province Name (full name) [Berkshire]:PA
Locality Name (eg, city) [Newbury]:Pittsburgh
Organization Name (eg, company) [My Company Ltd]:AIA
Organizational Unit Name (eg, section) []:Class
Common Name (eg, your name or your server's hostname) []:owa.aia.class
Email Address []:administrator@aia.class
[root@Juliet etc]#
```

Figure 1: SSL Certificate Creation

2 Configure Pound

1. Open the Pound configuration file in Vi editor:

```
# vi /etc/pound.cfg
```

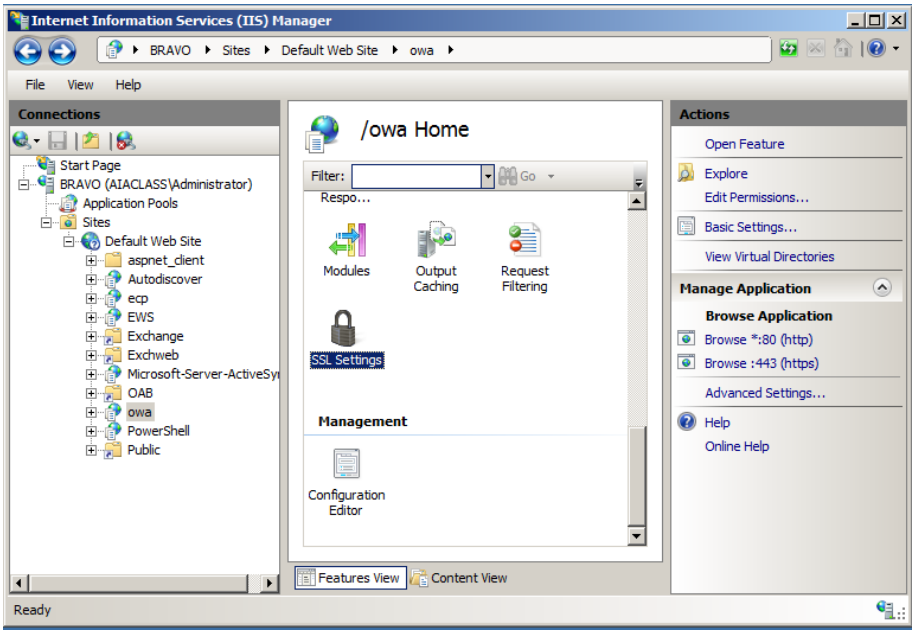
2. Delete the existing default configuration and type following configuration into the Pound configuration file:

```
User      “pound"
Group     "pound"
LogLevel    1
Alive      30
Daemon      1

ListenHTTPS
Address 10.0.1.3
AddHeader "Front-End-Https: on"
Port    443
Cert    "/usr/local/etc/owa.aia.class.pem"
End

Service
BackEnd
Address 10.0.2.3
Port    80
Priority 5
End
End
```

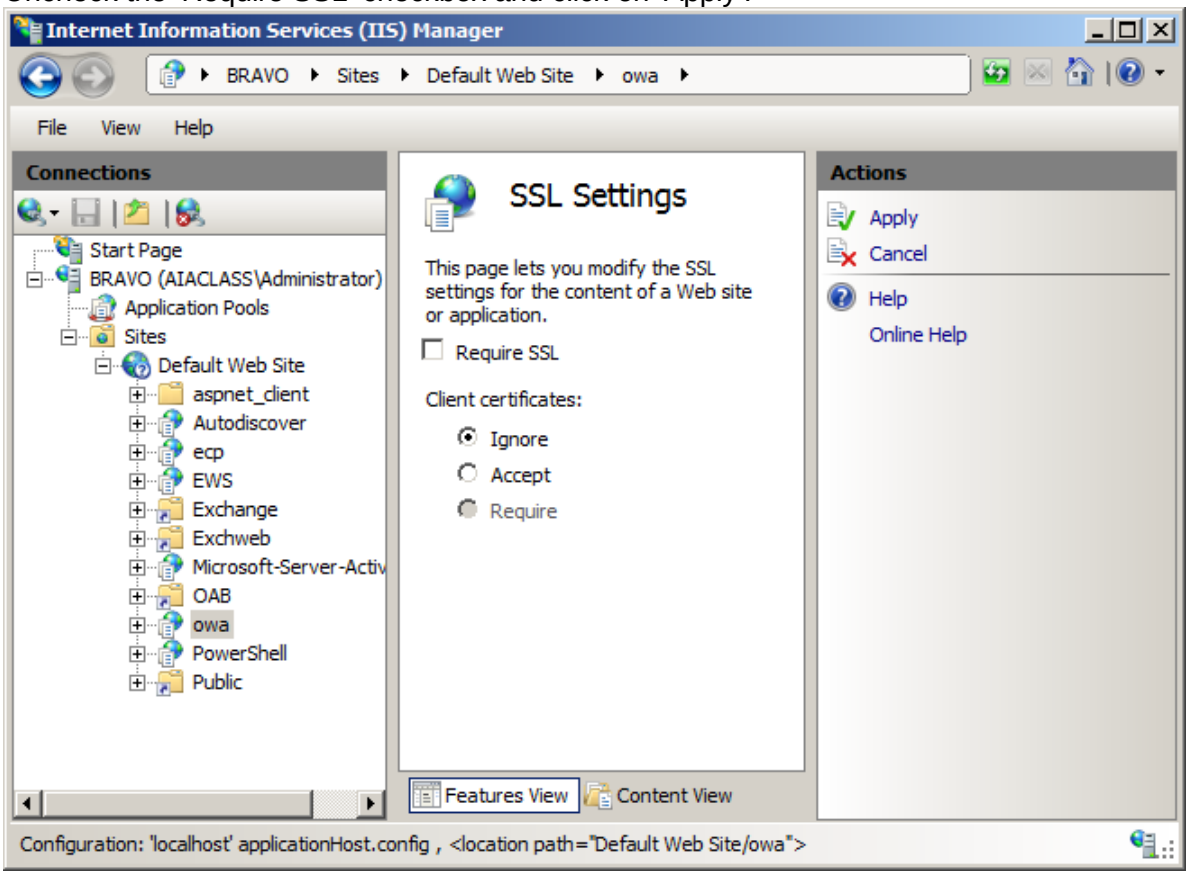
3 Configure Outlook Web Access

1. Log into Bravo and open ‘Start’ -> ‘Administrative Tools’ -> ‘Internet Information Services (IIS) Manager’.

2. Go into ‘BRAVO’ -> ‘Sites’ -> ‘Default Web site’ -> ‘owa’ and click on ‘SSL Settings’ from the central pane.



3. Uncheck the 'Require SSL' checkbox and click on 'Apply'.



Pound will now accept SSL connections from the Internet and forward them to Bravo using HTTP. Internal hosts can still connect to Bravo directly using SSL.

4 Start Pound

1. Go back into Juliet and start the Pound service by executing following command:

```
# service pound start
```

2. Set pound to start on boot with the following:

```
# chkconfig --level 345 pound on
```

External requests for Outlook Web Access will now be forwarded from the firewall and directed to Bravo through Pound without exposing the internal machine directly to the Internet.

This page left intentionally blank for pagination purposes

Installing and Configuring Bastille-Linux

We have already done preliminary hardening (by removing users, groups, etc) and now we will use Bastille-Linux to finish the task. Bastille allows us to easily modify many OS settings. In this task, we will apply a previously configured Bastille template file (analogous to the Security Configuration templates used on Windows) to our system.

1 Bastille Configuration

1.1 Install Bastille

1. If you have not already done so, log on to the machine using:

   Username: **root**
   Password: **tartans@1**

2. Open a terminal window by clicking on:
   'Applications' -> 'Accessories' -> 'Terminal'.

3. There are two modules that are required to implement Bastille:
   perl-Curses-1.12-1.2.el4.rf.i386.rpm
   Bastille-3.0.8-1.0.noarch.rpm

   Copy the required modules to the /root directory with this command:

```
# cp /media/AISTS/Tools/Linux/Bastille/* /root
```

4. Using the following commands, change to the /root directory and get a directory listing to confirm all of the Bastille files copied:

```
# cd /root
# ls –l
```

5. Install perl-Curses module:

```
# rpm –ivh perl-Curses-1.28-1.el5.rf.i386.rpm
```

6. Install Bastille module:

```
# rpm –ivh Bastille-3.0.9-1.0.noarch.rpm
```

1.2 Run Bastille

1. Copy Juliet's Bastille template to the Bastille configuration directory (this command should be typed as one continuous line with a space after 'cp' and after 'bastille-ids-config'):

```
# cp
/media/AISTS/Tools/Linux/Config_Files/Juliet_10.0.1.3/bast
ille-dns-config /etc/Bastille/config
```

2. Run Bastille in batch mode to apply the preconfigured template:

```
# bastille –b –n 2>/dev/null
```

Note: The template generates error messages about the CentOS version, but the settings will be applied successfully. These messages are not important, and so in this command, we divert all error messages to /dev/null (the trash).

```
NOTE:    Entering Critical Code Execution.
         Bastille has disabled keyboard interrupts.


NOTE:    Bastille is scanning the system configuration...

NOTE:    Bastille is now locking down your system in accordance with your
         answers in the "config" file.  Please be patient as some modules
         may take a number of minutes, depending on the speed of your
         machine.
NOTE:    Executing Firewall Specific Configuration
NOTE:    Executing File Permissions Specific Configuration
NOTE:    Executing Account Security Specific Configuration
NOTE:    Executing Boot Security Specific Configuration
NOTE:    Executing Inetd Specific Configuration
NOTE:    Executing PAM Specific Configuration
NOTE:    Executing Logging Specific Configuration
NOTE:    Executing Daemon Specific Configuration
NOTE:    Executing Sendmail Specific Configuration
NOTE:    Executing Apache Specific Configuration
NOTE:    Executing FTP Specific Configuration
NOTE:    Executing Temporary Directory Specific Configuration
```

Figure 1: Bastille Output

2 Bastille Configuration

1. The template we applied has been previously configured as follows.
   Enter the following command to view the new Bastille security settings:

```
# cat /etc/Bastille/config | less
```

2. Now you can scroll up and down to view the entire file. When you are finished reviewing the file, press the 'q' key to quit viewing the file and return to the shell prompt.

3. After reviewing the config file, *reboot* the system by typing `reboot`. You will now have to login with the admin account that was created in the Linux Host System Hardening task. *Make sure that the admin account was created before rebooting the system or you will not be able to login.*

   You may need to reset the screen resolution to 1024x768 the first time you log on to the admin account. You can do this by going to 'System' -> 'Preferences' -> 'Screen Resolution'.

   The remaining sections of this document detail the previously configured template that we applied. Note that you will *NOT* need to actually perform any tasks in the following sections; it is merely here for your edification. After reviewing, you can move on to the next task.

2.1 File Permissions

- Disallow non-root access to ping, usernetctl, mount/umount, and at
- Disable the r-tools (rsh, rlogin, etc) which are troublesome due to their use of weak authentication.

```
# Q:  Would you like to set more restrictive permissions on the administration u
tilities? [N]
FilePermissions.generalperms_1_1="Y"

# Q:  Would you like to disable SUID status for mount/umount?
FilePermissions.suidmount="Y"

# Q:  Would you like to disable SUID status for ping? [Y]
FilePermissions.suidping="Y"

# Q:  Would you like to disable SUID status for at? [Y]
FilePermissions.suidat="Y"

# Q:  Would you like to disable the r-tools? [Y]
FilePermissions.suidrtool="Y"

# Q:  Would you like to disable SUID status for usernetctl? [Y]
FilePermissions.suidusernetctl="Y"
```

Figure 2: File Permissions

2.2 Account Security Settings

- Enforce password aging
- Restrict cron (scheduler) to the root user
- Disallow root from direct login. After we apply this template all administrators must login using the 'admin' account and then su to root.
- Set permissions on all user-created files so that the file is only readable by the user who created it.

```
# Q:  Should Bastille disable clear-text r-protocols that use IP-based authentic
ation? [Y]
AccountSecurity.protectrhost="Y"

# Q:  Would you like to enforce password aging? [Y]
AccountSecurity.passwdage="Y"

# Q:  Do you want to set the default umask? [Y]
AccountSecurity.umaskyn="Y"

# Q:  What umask would you like to set for users on the system? [077]
AccountSecurity.umask="077"

# Q:  Should we disallow root login on tty's 1-6? [N]
AccountSecurity.rootttylogins="N"
```

Figure 3: Account Security Settings

2.3 Boot Security Settings

- Disable CTRL-ALT-DELETE rebooting so that a user must have a valid login and password to reboot the machine.
- Password protect single user mode to require the root password. Single user mode is equivalent to run level 1. You are granted root access, but networking is disabled.

```
# Q:  Would you like to password-protect the GRUB prompt? [N]
BootSecurity.protectgrub="N"

# Q:  Would you like to disable CTRL-ALT-DELETE rebooting? [N]
BootSecurity.secureinittab="Y"

# Q:  Would you like to password protect single-user mode? [Y]
BootSecurity.passsum="Y"
```

Figure 4: Boot Security Settings

2.4 Securing inetd and TCP Wrappers

- Disable telnet and ftp
- Create authorized use banners that will be displayed before the user can log in
- We do not set default deny on TCP wrappers in this configuration. Later on we will configure an IPtables firewall which will handle this for us.

```
# Q:  Would you like to set a default-deny on TCP Wrappers and xinetd? [N]
SecureInetd.tcpd_default_deny="N"

# Q:  Would you like to display "Authorized Use" messages at log-in time? [Y]
SecureInetd.banners="Y"

# Q:  Who is responsible for granting authorization to use this machine?
SecureInetd.owner="administrator@aia.class"
```

Figure 5: Securing inetd and TCP Wrappers

2.5 Configure PAM

- Set limits on resources. Users will only be allowed to start 150 concurrently running processes, and will be unable to open core system (kernel) files.
- Only allow root and admin to log in at the console

```
# Q:  Would you like to put limits on system resource usage? [N]
ConfigureMiscPAM.limitsconf="Y"

# Q:  Should we restrict console access to a small group of user accounts? [N]
ConfigureMiscPAM.consolelogin="Y"

# Q:  Which accounts should be able to login at console? [root]
ConfigureMiscPAM.consolelogin_accounts="root,admin"
```

Figure 6: PAM Settings

2.6 Logging Settings

- We will configure logging in a later module, therefore we will not configure logging through Bastille

```
# Q:  Would you like to set up process accounting? [N]
Logging.pacct="N"
```

Figure 7: Logging Settings

2.7 Sendmail Settings

- Prevent sendmail from running in daemon mode. This machine will not be a mail server, so sendmail need not listen for connections

```
# Q:  Do you want to stop sendmail from running in daemon mode? [Y]
Sendmail.sendmaildaemon="Y"
```

Figure 8: Sendmail Settings

2.8 DNS Settings

- We have configured and chrooted BIND in another module, so we will not configure it through Bastille

```
# Q: Would you like to chroot named and set it to run as a non-root user? [N]
DNS.chrootbind="N"

# Q:  Would you like to deactivate named, at least for now? [Y]
DNS.namedoff="N"
```

2.9 Miscellaneous Daemons

```
# Q:  Would you like to disable acpid and/or apmd? [Y]
MiscellaneousDaemons.apmd="Y"

# Q:  Would you like to disable GPM? [Y]
MiscellaneousDaemons.gpm="Y"

# Q:  Would you like to deactivate the HP OfficeJet (hpoj) script on this machin
e?
MiscellaneousDaemons.disable_hpoj="Y"

# Q:  Would you like to deactivate the ISDN script on this machine?
MiscellaneousDaemons.disable_isdn="Y"
```

Figure 9: Miscellaneous Deamons

2.10 Apache Web Server Settings

```
# Q:  Would you like to bind the Web server to listen only to the localhost? [N]
Apache.bindapachelocal="N"

# Q:  Would you like to bind the web server to a particular interface? [N]
Apache.bindapachenic="N"

# Q:  Would you like to deactivate the following of symbolic links? [Y]
Apache.symlink="N"
```

Figure 10: Apache Web Server Settings

2.11 Tempdir Scripts

- This system is not a multi-user system, and therefore we will not be very concerned with the temporary (shared) directories

```
# Q:  Would you like to install TMPDIR/TMP scripts? [N]
TMPDIR.tmpdir="N"
```

Figure 11: Tempdir Scripts

2.12 Packet Filtering Firewall

- We will configure a firewall in a later module, therefore we will not use Bastille's firewall configuration

```
# Q:  Would you like to run the packet filtering script? [N]
Firewall.ip_intro="N"
```

Figure 12: Packet Filtering Firewall

2.13 FTP Settings

```
# Q:  Would you like to disable anonymous download? [N]
FTP.anonftp="Y"

# Q:  Would you like to disable user privileges on the FTP daemon? [N]
FTP.userftp="Y"
```

Figure 13: FTP Settings

This page left intentionally blank for pagination purposes

Configuring IPTables as a Host Based Firewall on Linux Systems

The host based firewall for Linux, iptables, can be configured by accessing the console directly or via SSH from a management workstation. Iptables has six pre-defined "chains" that are available with the ability to create user defined chains as well. The default chains are:

- INPUT
- OUTPUT
- INPUT
- FORWARD
- PREROUTING
- POSTROUTING

The table below lists various options that can be used when configuring iptables rules. Additional information is available by typing `iptables --help` at the Linux command line or by reviewing the iptables man page (type: `man iptables`).

--table -t	Description
filter	Default table. This is used if not specified
nat	Network address translation
mangle	Used for Quality Of Service (QOS) and preferential treatment
raw	Enables optimization. i.e. Ignore firewall state matching for port 80 for enhanced speed due to less processing. Requires kernel patch

Command (Use one)	Description
-A --append	Append rule to chain
-D --delete	Delete rule from chain
-I --insert	Insert rule at beginning or at specified sequence number in chain.
-R --replace	Replace rule
-F --flush	Flush all rules
-Z --zero	Zero byte counters in all chains
-L --list	List all rules. Add option --line-numbers for rule number.
-N --new-chain	Create new chain
-X --delete-chain	Delete user defined chain
-P --policy	Set default policy for a chain
-E --rename-chain	Rename a chain

Command Option	Description
-s --source	Source address of packet
-d --destination	Destination address of packet
-i --in-interface	Interface packet is arriving from
-o --out-interface	Interface packet is going to
-p --protocol	Protocol: °tcp --sport port[:port] --dport port[:port] --syn °udp °icmp °mac ...
-j --jump	Target to send packet to
-f --fragment	Fragment matching
-c --set-counters	Set packet/byte counter
-m tcp --match tcp	°--source-port port[:port] (port # or range ##) °--destination-port port[:port] °--tcp-flags
-m state --match state	--state °ESTABLISHED °RELATED °NEW °INVALID (Push content, not expected to recieve this packet.)

Defined Policies	Description
ACCEPT	Let packet through
DROP	Deny packet with no reply
REJECT	Deny packet and notify sender
RETURN	Handled by default targets
MARK	Used for error response. Use with option --reject-with type
MASQUERADE	Used with nat table and DHCP.
LOG	Log to file and specify message: °--log-level # °--log-prefix "prefix" °--log-tcp-sequence °--log-tcp-options °--log-ip-options
ULOG	Log to file and specify userpace logging messages
SNAT	Valid in PREROUTING chain. Used by nat.
REDIRECT	Used with nat table. Output.
DNAT	Valid in POSTROUTING chain. Output.
QUEUE	Pass packet to userspace.

Figure 1: IPtables Options

1 Creating Inbound and Outbound Filtering Rules

The filtering rules for this server will be set up to allow the following traffic into and out of the system:

Source Address	Destination Address	Proto	Source Ports	Destination Port	Direction	Purpose
10.0.4.0/24	10.0.1.3/32	ANY	ANY	ANY	Inbound	Management
10.0.3.2/32	10.0.1.3/32	ANY	ANY	ANY	Inbound	Mike-Nagios
0.0.0.0/0	10.0.1.3/32	UDP	ANY	53	Inbound	DNS
0.0.0.0/0	10.0.1.3/32	TCP	ANY	443	Inbound	OWA
127.0.0.1/32	127.0.0.1/32	*	*	*	Inbound	Loopback
Log All Denied						
10.0.1.3/32	10.0.4.0/24	ANY	ANY	ANY	Outbound	Management
10.0.1.3/32	10.0.1.1/32	TCP	ANY	25	Outbound	SMTP
10.0.1.3/32	10.0.1.1/32	UDP	ANY	53	Outbound	DNS
10.0.1.3/32	10.0.2.3/32	TCP	ANY	80	Outbound	OWA
10.0.1.3/32	10.0.2.3/32	TCP	ANY	443	Outbound	OWA
10.0.1.3/32	10.0.1.1/32	UDP	123	123	Outbound	NTP
10.0.1.3/32	10.0.1.1/32	TCP	ANY	3128	Outbound	Squid Proxy
10.0.1.3/32	0.0.0.0/0	UDP	53	ANY	Outbound	DNS
127.0.0.1/32	127.0.0.1/32	*	*	*	Outbound	Loopback
Log All Denied						

1. If you have not already done so, log on to the machine using the newly enforced admin account:

   Username: **admin** Password: **steelers**

2. Open a terminal window by going to ‘Applications’ -> ‘Accessories’ -> ‘Terminal’.
3. Elevate to root level privileges by typing the following command and entering the root password **tartans@1**

```
# su -
```

4. Ensure iptables is stopped.

```
# service iptables stop
```

5. Clear all existing iptables rules.

```
# iptables --flush
```

6. Set the default policy for the FORWARD chain to DROP all packets.

```
# iptables –P FORWARD DROP
```

7. Create the iptables file that will be used to save firewall rules.

```
# iptables-save > /etc/sysconfig/iptables
# vi /etc/sysconfig/iptables
```

8. Remove the last two lines. Move the cursor to each line and press the [D] key twice. This will delete the current line in VI. The file should look like the following when completed:

```
# Generated by iptables-save v1.3.5 on Mon Jun 14 10:52:10 2010
*filter
:INPUT ACCEPT [5:420]
:FORWARD DROP [0:0]
:OUTPUT ACCEPT [5:420]
```

9. Add the remaining rules to the iptables file as listed below. Comments/remarks are identified with a '#' at the beginning of the line. These lines are used to identify what the rules beneath them are used for. Although they are not required, it is a good practice to describe the rules, their intent, who added the rule, and potentially the date on which the rule was added or modified. Use the cursor to go to the bottom of the file. Simultaneously press the [Shift] and [A] keys to append text to the end of the last line. Press [Enter] to add a new line. Enter the following lines:

```
# Allow all inbound traffic from the MGMT network
-A INPUT -s 10.0.4.0/24 -d 10.0.1.3/32 -i eth0 -j ACCEPT

# Allow all inbound traffic from Mike-Nagios
-A INPUT -s 10.0.3.2/32 -d 10.0.1.3/32 -i eth0 -j ACCEPT

# Allow inbound DNS queries from the Internet
-A INPUT -d 10.0.1.3/32 -i eth0 -p udp --dport 53 -j ACCEPT

# Allow inbound OWA requests from the Internet
-A INPUT -d 10.0.1.3/32 -i eth0 -p tcp --dport 443 -j ACCEPT

# Allow all established connections
-A INPUT -i eth0 -m state --state ESTABLISHED,RELATED -j ACCEPT

# Allow all inbound traffic on the loopback interface
-A INPUT -i lo -p all -j ACCEPT

# Enable logging on INPUT chain
-A INPUT -j LOG --log-level 6

# Set the default INPUT policy to Drop
-P INPUT DROP
```

Figure 2: IPtables Input Rules

```
# Allow outbound mail traffic to Quebec
-A OUTPUT -s 10.0.1.3/32 -d 10.0.1.1/32 -o eth0 -p tcp --dport 25 -j ACCEPT

# Allow outbound DNS queries to Quebec
-A OUTPUT -s 10.0.1.3/32 -d 10.0.1.1/32 -o eth0 -p udp --dport 53 -j ACCEPT

# Allow Pound to forward OWA requests to Bravo
-A OUTPUT -s 10.0.1.3/32 -o eth0 -p tcp --dport 80 -j ACCEPT
-A OUTPUT -s 10.0.1.3/32 -o eth0 -p tcp --dport 443 -j ACCEPT

# Allow outbound web proxy traffic to Quebec
-A OUTPUT -s 10.0.1.3/32 -d 10.0.1.1/32 -o eth0 -p tcp --dport 3128 -j ACCEPT

# Allow outbound NTP traffic to Quebec
-A OUTPUT -s 10.0.1.3/32 -d 10.0.1.1/32 -o eth0 -p udp --dport 123 -j ACCEPT

# Allow outbound DNS replies to the Internet
-A OUTPUT -s 10.0.1.3/32 -d 0.0.0.0/0 -o eth0 -p udp --sport 53 -j ACCEPT

# Allow all outbound traffic to the MGMT network
-A OUTPUT -s 10.0.1.3/32 -d 10.0.4.0/24 -o eth0 -p all -j ACCEPT

# Allow all established connections
-A OUTPUT -o eth0 -m state --state ESTABLISHED,RELATED -j ACCEPT

# Allow all outbound traffic on the loopback interface
-A OUTPUT -o lo -p all -j ACCEPT

# Enable logging on OUTPUT chain
-A OUTPUT -j LOG --log-level 6

# Set the default OUTPUT policy to Drop
-P OUTPUT DROP

# Enable rule set
COMMIT
```

Figure 3: IPtables Output Rules

10. Save and exit the file. Press `[Esc]` and type `:wq` then press `[Enter]`.

1.1 Applying the firewall rules

1. Enter the following command to start the iptables firewall:

```
# service iptables start
```

2. If the service started successfully, you should see the following:

```
Flushing firewall rules:                                   [  OK  ]
Setting chains to policy ACCEPT: filter                    [  OK  ]
Unloading iptables modules:                                [  OK  ]
Applying iptables firewall rules:                          [  OK  ]
Loading additional iptables modules: ip_conntrack_netbios_n[  OK  ]
```

Figure 4: IPtables Successful Startup

1.2 Making the iptables file immutable

1. Since we do not want the iptables file to change for ANY reason after the rules have been built without intervention from the administrator, we will make this file immutable. To do this, we will issue the following command.

```
# chattr +i /etc/sysconfig/iptables
```

2. Relinquish the elevated root privileges by typing the following command:

```
# exit
```

This page left intentionally blank for pagination purposes

OSSEC Agent

OSSEC agents will be installed on each Linux and Windows server and send events to the OSSEC server which is running on Foxtrot. The OSSEC server processes events and generate warnings and alerts sent by agents. Before installing the OSSEC agent make sure you have successfully deployed the OSSEC server in order to connect agents to the server running on Foxtrot.

1 OSSEC Agent setup

1.1 Installation

1. If you have not already done so, log on to the machine using the newly enforced admin account:

   Username: **admin** Password: **steelers**

2. Open a terminal window by going to 'Applications' -> 'Accessories' -> 'Terminal'.
3. Elevate to root level privileges by typing the following command and entering the root password **tartans@1**

```
# su -
```

4. Navigate to the Course CD by executing following command:

```
# cd /media/AISTS/Tools/Linux/OSSEC/
```

5. Copy OSSEC installation package:

```
# cp ossec-hids-2.4.1.tar.gz /root/
```

6. Extract installation package in root directory

```
# cd /root/
# tar -xzvf ossec-hids-2.4.1.tar.gz
```

7. Start installation using following command and accept default language by pressing `[Enter]`:

```
# cd ossec-hids-2.4.1
# ./install.sh
```

8. Read the information and press `[Enter]`:

```
OSSEC HIDS v2.4.1 Installation Script - http://www.ossec.net

You are about to start the installation process of the OSSEC HIDS.
You must have a C compiler pre-installed in your system.
If you have any questions or comments, please send an e-mail
to dcid@ossec.net (or daniel.cid@gmail.com).

 - System: Linux Juliet 2.6.18-164.el5
 - User: root
 - Host: Juliet


 -- Press ENTER to continue or Ctrl-C to abort. --
```

9. Answer the rest of the questions as shown in below and press `[Enter]` when you have finished:

```
1- What kind of installation do you want (server, agent, local or help)?
 agent

  - Agent(client) installation chosen.

2- Setting up the installation environment.

 - Choose where to install the OSSEC HIDS [/var/ossec]:

    - Installation will be made at  /var/ossec .

3- Configuring the OSSEC HIDS.

  3.1- What's the IP Address of the OSSEC HIDS server?: 10.0.4.2

   - Adding Server IP 10.0.4.2

  3.2- Do you want to run the integrity check daemon? (y/n) [y]: y

   - Running syscheck (integrity check daemon).

  3.3- Do you want to run the rootkit detection engine? (y/n) [y]: y
```

```
3.4 - Do you want to enable active response? (y/n) [y]: n

 - Active response disabled.

3.5- Setting the configuration to analyze the following logs:
  -- /var/log/messages
  -- /var/log/secure
  -- /var/log/maillog

- If you want to monitor any other file, just change
  the ossec.conf and add a new localfile entry.
  Any questions about the configuration can be answered
  by visiting us online at http://www.ossec.net .


  --- Press ENTER to continue ---
```

10. When the installation has completed you should see following screen and press `[Enter]`:

```
- System is Redhat Linux.
- Init script modified to start OSSEC HIDS during boot.

- Configuration finished properly.

- To start OSSEC HIDS:
               /var/ossec/bin/ossec-control start

- To stop OSSEC HIDS:
               /var/ossec/bin/ossec-control stop

- The configuration can be viewed or modified at /var/ossec/etc/ossec.c
onf


   Thanks for using the OSSEC HIDS.
   If you have any question, suggestion or if you find any bug,
   contact us at contact@ossec.net or using our public maillist at
   ossec-list@ossec.net
   ( http://www.ossec.net/main/support/ ).

   More information can be found at http://www.ossec.net

   ---  Press ENTER to finish (maybe more information below). ---
```

1.2 Configuration

1. Now we are going to setup a shared key between the OSSEC agent and the OSSEC server. In order to get a shared key from the OSSEC server, login to Foxtrot through SSH:

```
# ssh root@10.0.4.2
```

Accept SSH connectivity by typing `yes` and type the password `tartans@1` and you will be connected to Foxtrot.

```
[root@Juliet ~]# ssh root@10.0.4.2
The authenticity of host '10.0.4.2 (10.0.4.2)' can't be established.
RSA key fingerprint is f5:b7:79:02:ff:f8:7d:af:a2:3f:87:db:e0:ee:c0:5e.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.0.4.2' (RSA) to the list of known hosts.
root@10.0.4.2's password:
Last login: Wed Jun 16 12:03:50 2010 from 10.0.2.10
[root@Foxtrot ~]#
```

2. Start the OSSEC agent manager:

```
# /var/ossec/bin/manage-agents
```

```
[root@Foxtrot ~]# /var/ossec/bin/manage_agents


****************************************
* OSSEC HIDS v2.4.1 Agent manager.     *
* The following options are available: *
****************************************
   (A)dd an agent (A).
   (E)xtract key for an agent (E).
   (L)ist already added agents (L).
   (R)emove an agent (R).
   (Q)uit.
Choose your action: A,E,L,R or Q:
```

3. Now add Juliet's OSSEC agent to the OSSEC server by entering `A`. Type `y` and press `[Enter]` when you have finished entering the information about Juliet as shown below:

```
 - Adding a new agent (use '\q' to return to the main menu).
   Please provide the following:
    * A name for the new agent: Juliet
    * The IP Address of the new agent: 10.0.1.3
    * An ID for the new agent[002]: 002
 Agent information:
    ID:002
    Name:Juliet
    IP Address:10.0.1.3

 Confirm adding it?(y/n): y
 Agent added.
```

4. Now type `E` and press `[Enter]` to extract the shared key for Juliet, and enter `002` when the OSSEC agent manager asks for an agent ID. Please note that key will not be same as shown in following screenshot, because shared keys are generated randomly each time an OSSEC agent is added:

```
****************************************
* OSSEC HIDS v2.4.1 Agent manager.     *
* The following options are available: *
****************************************
   (A)dd an agent (A).
   (E)xtract key for an agent (E).
   (L)ist already added agents (L).
   (R)emove an agent (R).
   (Q)uit.
Choose your action: A,E,L,R or Q: E

Available agents:
   ID: 001, Name: Hotel, IP: 10.0.1.5
   ID: 002, Name: Juliet, IP: 10.0.1.3
Provide the ID of the agent to extract the key (or '\q' to quit): 002

Agent key information for '002' is:
MDAyIEp1bGlldCAxMC4wLjEuMyBjNzM0YTkyOTQxNjQ3Yzc3YWYwNDNmZjdiYzIwYjQzN2Nk
Dg5NWExNzE2YzA2

** Press ENTER to return to the main menu.
```

5. Copy the shared key to your clipboard by highlighting it, right-clicking and choosing ‘Copy’.

6. Type `Q` and press `[Enter]` to quit from the OSSEC agent manager, and type `exit` and press `[Enter]` to end the SSH session:

```
****************************************
* OSSEC HIDS v2.4.1 Agent manager.     *
* The following options are available: *
****************************************
   (A)dd an agent (A).
   (E)xtract key for an agent (E).
   (L)ist already added agents (L).
   (R)emove an agent (R).
   (Q)uit.
Choose your action: A,E,L,R or Q: Q
```

7. Now you should be back in the shell of Juliet. Execute the following command to import the copied key.

```
# /var/ossec/bin/manage_agents
```

8. Type `I` then press `[Enter]`.

9. Paste the copied key by right-clicking and choosing ‘Paste’ to import the key and accept confirmation by typing `y` then pressing `[Enter]` as shown below:

```
****************************************
* OSSEC HIDS v2.4.1 Agent manager.     *
* The following options are available: *
****************************************
   (I)mport key from the server (I).
   (Q)uit.
Choose your action: I or Q: I

* Provide the Key generated by the server.
* The best approach is to cut and paste it.
*** OBS: Do not include spaces or new lines.

Paste it here (or '\q' to quit): MDAyIEp1bGlldCAxMC4wLjEuMyBjNzM0YTkyOTQ
xNjQ3Yzc3YWYwNDNmZjdiYzIwYjQzN2NkNTU2MTFlNDM0OGExYmU3MTA2MDg5NWExNzE2YzA
2

Agent information:
   ID:002
   Name:Juliet
   IP Address:10.0.1.3

Confirm adding it?(y/n):
```

10. Exit from OSSEC manager by typing `Q` then pressing `[Enter]`:

```
Confirm adding it?(y/n): y
Added.
** Press ENTER to return to the main menu.



****************************************
* OSSEC HIDS v2.4.1 Agent manager.     *
* The following options are available: *
****************************************
   (I)mport key from the server (I).
   (Q)uit.
Choose your action: I or Q: Q

** You must restart the server for your changes to have effect.

manage_agents: Exiting ..
```

11. Start the OSSEC agent by executing following command:

```
# /var/ossec/bin/ossec-control start
```

```
[root@Juliet ~]# /var/ossec/bin/ossec-control start
Starting OSSEC HIDS v2.4.1 (by Trend Micro Inc.)...
Started ossec-execd...
Started ossec-agentd...
Started ossec-logcollector...
Started ossec-syscheckd...
Completed.
```

12. If you are not performing any more administrative tasks on this machine, relinquish the elevated root privileges by typing the following command:

```
# exit
```

Lima High Level Description

Lima is a Linux system operating in the services network. The main purpose of Lima is to operate the Snort sensor. Once configured, it will alert administrators to any unusual or malicious activity by monitoring network traffic and hosts and sending alerts to the alert collection database.

Snort is a free IDS that can make use of other multiple tools—such as MySQL and BASE—in order to monitor network activity. Snort can record logs in a variety of different formats/databases.

Following are descriptions of the hands-on tasks you must complete on Lima's:

Task 1. Linux Host System Hardening

You will be minimizing non-essential services (e.g., xinetd, portmap) as well as extraneous default users and groups. As a standalone system running Snort, Lima does not require these components; as a result, you will follow security best practices by removing them. Also,you will create a non-privileged administrator account to provide an audit trail for all administrative access.

Task 2. Configuring Time Synchronization

Network Time Protocol (NTP) is used to synchronize the host computer's time to a local time server—in this deployment the local time server is the Internet firewall (Quebec).

Alpha will synchronize to Quebec every ten minutes; the Linux hosts will synchronize with Quebec every ten minutes; and the Window hosts will synchronize with Alpha every forty-five minutes until three good synchronizations occur, then once every eight hours. With all the hosts' time synchronized across the network, cross examining multiple hosts' logs or logs at the syslog server is easier to perform and is more meaningful.

Task 3. Configuring Bastille

The Bastille hardening system is a user-configurable script that attempts to lock down Linux/UNIX operating systems. The Bastille script embodies recommendations from every major reputable source on Linux/UNIX security. You will use pre-configured Bastille templates to lock down weak system settings such as maximum password age, user privileges, etc.

Task 4. Configuring IPTables

IPTables is a Linux firewall application that can be configured to perform packet filtering on network firewalls or host systems. IPTables will be configured on this host as a host-based firewall to allow only valid packets to and from this host. To do this, you will set up INPUT and OUTPUT rules to specifically allow known-good packets into and out of the host, and will create default LOG rules and DROP rules.

Task 5. Installing and Configuring Snort

Snort will be configured to fit this network's particular needs. You will be led through the steps to enable/disable rules and setup up the Snort configuration file.

Task 6. Configuring OSSEC Agent

You will install and configure OSSEC Agent, which will then send information about security events to the syslog/OSSEC server (Foxtrot).

Task 7. Wireshark Network Protocol Analyser

You will install and configure Wireshark in order to perform packet analysis.

Linux Host System Hardening

1 Remove Zeroconf Route

1. If you have not already done so, log on to the machine using:

   Username: **root** Password: **tartans@1**

2. Open a terminal window by going to ‘Applications’ -> ‘Accessories’ -> ‘Terminal’.

By default Linux adds a "zeroconf" route at boot time. This is a static route that designates the 169.254/16 prefix as local. This is unnecessary on our network, so you will remove the route:

3. Specify to not use zeroconf at boot time:

NOTE: In this and all subsequent Linux documents, the ‘#’ at the beginning of each line should *not* be typed in as part of the command. It is simply meant to represent a command prompt.

```
# echo "NOZEROCONF=yes" >> /etc/sysconfig/network
```

2 Linux Kernel Upgrade

One of the most essential hardening tasks for Linux systems is to ensure that the latest kernel version is being used. The kernel is the core of the operating system and every effort should be made to ensure that the most current version is in use. Most versions of Linux include some automated means for updating software, including the kernel. You will use a tool called YUM (Yellowdog Updater Modified) to download updates from an external web server that is hosting the YUM repository.

2.1 Apply latest updates to the kernel and other installed packages

1. Edit the yum config file using vi:

```
# vi /etc/yum.repos.d/CentOS-Base.repo
```

2. There are six sections of the file denoted by names in brackets. You will edit 3 of these sections and disable the other 3. Press `[Insert]` or `[i]` to edit the file and scroll down to the first section, ‘[base]’. Comment out the line beginning with ‘mirrorlist=’ by typing a # at the beginning of the line. Next, uncomment the line below it beginning with ‘baseurl=’ and edit the URL to point to the trusted yum repository at `http://192.168.30.14/centos/5.4/os/i386/`

   The updated lines will be as follows:

```
[base]
name=CentOS-$releasever - Base
#mirrorlist=http://mirrorlist.centos.org/?release=$releasever&arch=$basearch&rep
o=os
baseurl=http://192.168.30.14/centos/5.4/os/i386/
gpgcheck=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-CentOS-5
```

Figure 1: Configuring YUM base repository

3. Repeat the above steps for the second section, '[updates]', pointing it to the URL `http://192.168.30.14/centos/5.4/updates/i386/`

```
#released updates
[updates]
name=CentOS-$releasever - Updates
#mirrorlist=http://mirrorlist.centos.org/?release=$releasever&arch=$basearch&rep
o=updates
baseurl=http://192.168.30.14/centos/5.4/updates/i386/
gpgcheck=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-CentOS-5
```

Figure 2: Configuring YUM updates repository

4. Scroll down to the next section, '[addons]' and add `enabled=0` underneath the last line of the section to disable it. The updated lines will be as follows:

```
#packages used/produced in the build but not released
[addons]
name=CentOS-$releasever - Addons
mirrorlist=http://mirrorlist.centos.org/?release=$releasever&arch=$basearch&repo
=addons
#baseurl=http://mirror.centos.org/centos/$releasever/addons/$basearch/
gpgcheck=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-CentOS-5
enabled=0
```

Figure 3: Disabling YUM addons repository

5. Scroll down to the next section '[extras]', comment out the 'mirrorlist', and point 'baseurl' to the URL `http://192.168.30.14/centos/5.4/extras/i386/`

```
#additional packages that may be useful
[extras]
name=CentOS-$releasever - Extras
#mirrorlist=http://mirrorlist.centos.org/?release=$releasever&arch=$basearch&rep
o=extras
baseurl=http://192.168.30.14/centos/5.4/extras/i386/
gpgcheck=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-CentOS-5
```

Figure 4: Configuring YUM extras repository

You will leave the remaining two sections at their default setting of disabled.

6. Press `[Esc]`, then type `:wq` and press `[Enter]` to save the changes and exit VI.
7. Add a variable to '/etc/yum.conf' so that all future updates use the HTTP proxy. Edit '/etc/yum.conf' with vi:

```
# vi /etc/yum.conf
```

8. To configure yum to use the web proxy server, you need to add a line to the '/etc/yum.conf file'. Add the following line to the end of the '[main]' section of the file:

```
proxy=http://10.0.2.1:3128
```

```
[main]
cachedir=/var/cache/yum
keepcache=0
debuglevel=2
logfile=/var/log/yum.log
distroverpkg=redhat-release
tolerant=1
exactarch=1
obsoletes=1
gpgcheck=1
plugins=1
proxy=http://10.0.2.1:3128
```

Figure 5: Configuring YUM proxy server

Press `[Esc]` then type `:wq` and press `[Enter]` to save the changes and exit VI.

NOTE: In order to access the Internet or even the trusted update server, routing needs to be enabled on Quebec and Romeo. Once the access control lists are in place on these two router/firewall machines, only a few devices will be able to directly access external networks. You may need to wait until these tasks are completed—check with your teammates on this.

9. Run yum in update mode:

```
# yum update
```

10. Type `y` then press `[Enter]` when prompted to download the updates.
11. Type `y` then press `[Enter]` when prompted to import the CentOS 5 GPG key.

A number of packages will be downloaded and installed, including a newer kernel.

This step may take several minutes to complete. Press `[Ctrl]` + `[Shift]` + `[T]` to open a new terminal tab if you want to move on to the next steps while the updates take place.

3 Service Minimization

3.1 Removing Unnecessary Services

By default Linux runs many services that a standalone server will not need. Extraneous services are dangerous because they provide possible attack vectors.

The services that need to be removed from this system are:

- anacron
- apmd
- atd
- autofs
- cpuspeed
- cups
- gpm
- irqbalance
- mdmonitor
- mdmpd
- microcode_ctl
- netfs
- nfslock
- portmap
- rawdevices
- rpcgssd
- rpcsvcgssd
- rpcidmapd
- sendmail
- xinetd

1. Terminate the 'anacron' service properly by using the following command:

```
# service anacron stop
```

2. Remove the 'anacron' startup routine using the following command:

```
# chkconfig --del anacron
```

Figure 6: Removing a service

3. Repeat steps #1 and #2 for each service listed above. (ADVANCED: see the 'Bash Script' ADDENDUM located on the last two pages of this section to automate these repetitive steps.)

   Note: On some systems, some of the services may not be started and may not return the 'OK' when stopped. If this is the case, it is sufficient to simply delete the service.

4. To check that the appropriate services have been removed, use the following two commands from a terminal window:

```
# netstat –ntap | grep –i listen
```

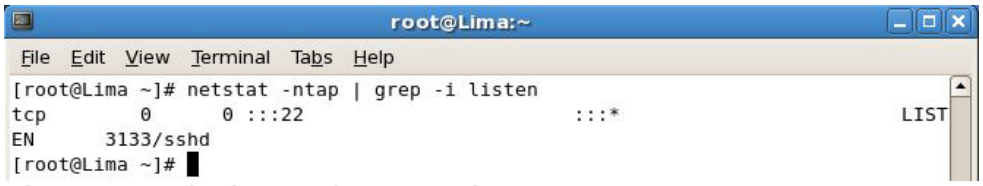
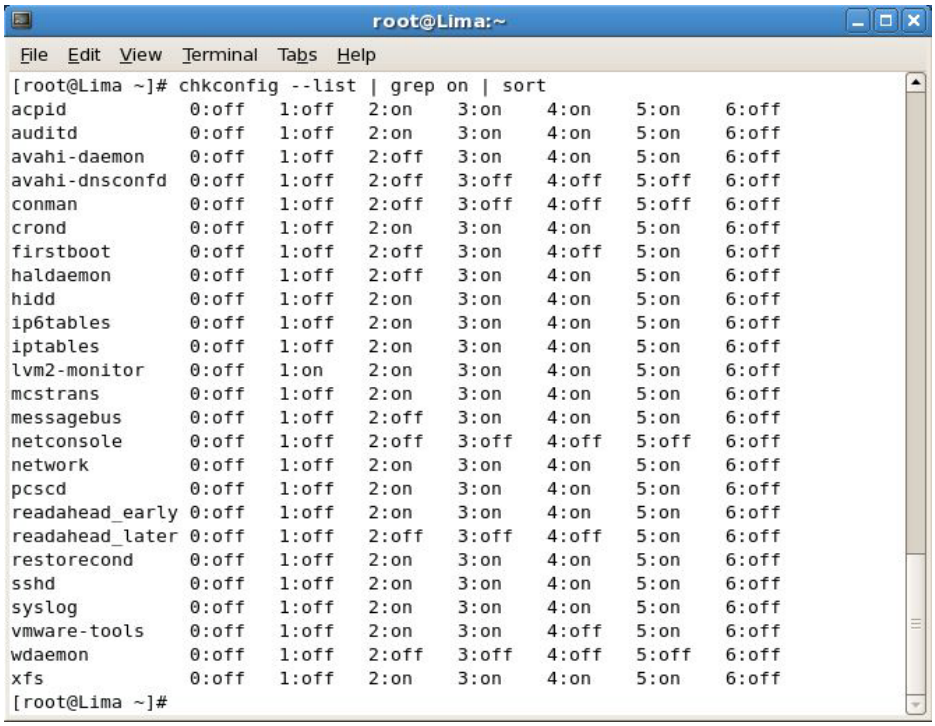


Figure 7: Confirming service removal

```
# chkconfig --list | grep on | sort
```



```
[root@Lima ~]# chkconfig --list | grep on | sort
acpid           0:off   1:off   2:on    3:on    4:on    5:on    6:off
auditd          0:off   1:off   2:on    3:on    4:on    5:on    6:off
avahi-daemon    0:off   1:off   2:off   3:on    4:on    5:on    6:off
avahi-dnsconfd  0:off   1:off   2:off   3:off   4:off   5:off   6:off
conman          0:off   1:off   2:off   3:off   4:off   5:off   6:off
crond           0:off   1:off   2:on    3:on    4:on    5:on    6:off
firstboot       0:off   1:off   2:off   3:on    4:off   5:on    6:off
haldaemon       0:off   1:off   2:off   3:on    4:on    5:on    6:off
hidd            0:off   1:off   2:on    3:on    4:on    5:on    6:off
ip6tables       0:off   1:off   2:on    3:on    4:on    5:on    6:off
iptables        0:off   1:off   2:on    3:on    4:on    5:on    6:off
lvm2-monitor    0:off   1:on    2:on    3:on    4:on    5:on    6:off
mcstrans        0:off   1:off   2:on    3:on    4:on    5:on    6:off
messagebus      0:off   1:off   2:off   3:on    4:on    5:on    6:off
netconsole      0:off   1:off   2:off   3:off   4:off   5:off   6:off
network         0:off   1:off   2:on    3:on    4:on    5:on    6:off
pcscd           0:off   1:off   2:on    3:on    4:on    5:on    6:off
readahead_early 0:off   1:off   2:on    3:on    4:on    5:on    6:off
readahead_later 0:off   1:off   2:off   3:off   4:off   5:on    6:off
restorecond     0:off   1:off   2:on    3:on    4:on    5:on    6:off
sshd            0:off   1:off   2:on    3:on    4:on    5:on    6:off
syslog          0:off   1:off   2:on    3:on    4:on    5:on    6:off
vmware-tools    0:off   1:off   2:on    3:on    4:off   5:on    6:off
wdaemon         0:off   1:off   2:off   3:off   4:off   5:off   6:off
xfs             0:off   1:off   2:on    3:on    4:on    5:on    6:off
[root@Lima ~]#
```

Figure 8: Results of service removals

5. If your results are *similar* to the output shown above, the services have been removed successfully.

4 User / Group Account Minimization

It is important to disable all default vendor accounts that will be unused. Typically, a default account (e.g., gopher or news) is created only when the respective service is also installed; however, many default accounts exist even if you have not installed the related services on your system. In this case, you will not use many of the default accounts and so you will remove them. The more accounts you have, the easier it is for outsiders to access your system.

4.1 Remove Default User Accounts

The users you will need to remove are:

- adm
- apache
- ftp
- games
- gopher
- halt
- lp
- mail
- mailnull
- news
- nfsnobody
- nobody
- nscd
- operator
- rpcuser
- rpc
- shutdown
- smmsp
- uucp
- vcsa
- xfs

1. Remove the ‘adm’ user account using the following command:

```
# userdel adm
```

2. Repeat the previous step for each account listed above. Verify removal by executing the following command:

```
# cat /etc/passwd
```

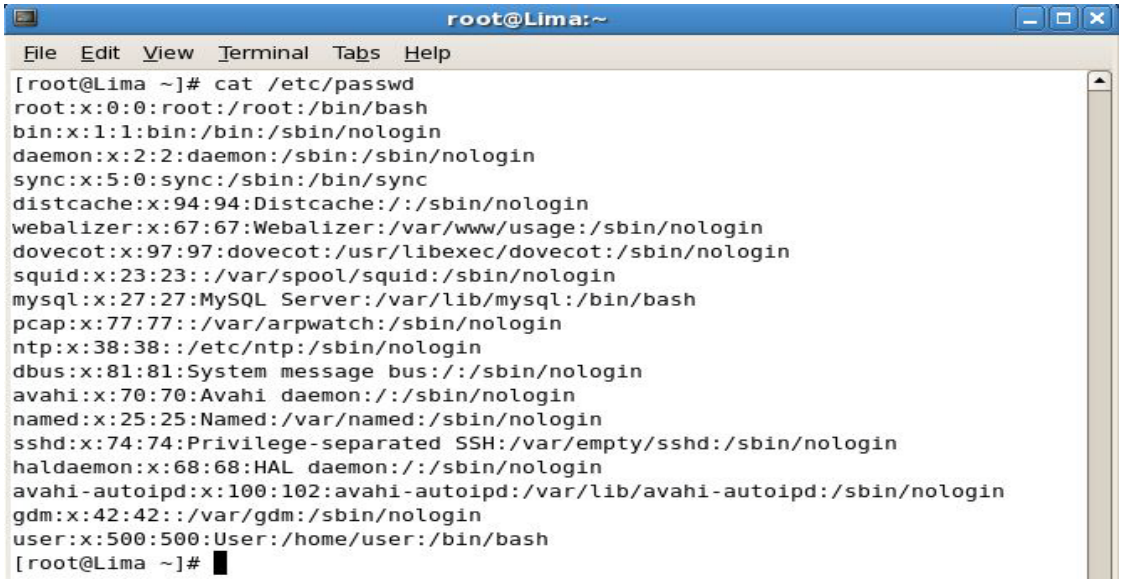


Figure 9: Results of removing unnecessary default user accounts

3. If the default user accounts have been successfully removed, your /etc/passwd file will look *similar* to the output shown in the figure above.

4.2 Remove Default Groups

Now that you have removed all unnecessary accounts from the /etc/passwd file, you will clean up the /etc/groups file.

The groups that you will remove are:

- adm
- dip
- lock
- lp
- mail
- news
- uucp

Removing a group account is similar to the process of removing a user shown above.

1. Delete the ‘adm’ group using the following command:

```
# groupdel adm
```

2. Repeat the previous step for each group listed above.

3. Verify removal by executing the following command:

```
# cat /etc/group
```

```
[root@Lima ~]# cat /etc/group
root:x:0:root
bin:x:1:root,bin,daemon
daemon:x:2:root,bin,daemon
sys:x:3:root,bin
tty:x:5:
disk:x:6:root
mem:x:8:
kmem:x:9:
wheel:x:10:root
man:x:15:
users:x:100:
utmp:x:22:
utempter:x:35:
audio:x:63:gdm
distcache:x:94:
floppy:x:19:
webalizer:x:67:
dovecot:x:97:
squid:x:23:
mysql:x:27:
pcap:x:77:
slocate:x:21:
ntp:x:38:
ecryptfs:x:101:
dbus:x:81:
avahi:x:70:
```

Figure 10: Results of removing unnecessary default groups

4. If the default groups have been successfully removed, the /etc/group file will look similar to the output shown in the figure above.

4.3 Create the 'Admin' User

The last account management task you will perform manually is to create an 'admin' user for daily administration tasks.

1. Add the admin user using the following command:

```
# useradd admin
```

2. Set the password for the 'admin' account:

```
# passwd admin
```

3. When prompted for a password use the following: `steelers`

   The output will resemble that shown below:

```
[root@Lima ~]# useradd admin
Group 'mail' not found. Creating the user mailbox file with 0600 mode.
[root@Lima ~]# passwd admin
Changing password for user admin.
New UNIX password:
BAD PASSWORD: it is based on a dictionary word
Retype new UNIX password:
passwd: all authentication tokens updated successfully.
[root@Lima ~]#
```

Figure 11: Creating an Admin user

Note: In a real production environment you should always choose a strong password or passphrase that is sufficiently long and contains a combination of letters, numbers, and special characters. The above password is used for demonstration purposes only.

5 Installing ClamAV

1. Copy the ClamAV tarball from the course CD to the /root directory:

```
# cp /media/AISTS/Tools/Linux/ClamAV/clamav-0.96.1.tar.gz /root
```

2. Untar ClamAV:

```
# cd /root
# tar xvzf clamav-0.96.1.tar.gz
```

3. You will need to install a few prerequisite packages before installing ClamAV. You will use the trusted yum repository that you set up earlier in this task to install zlib-devel. Additionally, in order to compile ClamAV and other tools in later tasks from source code you will need to install a compiler on the machine because this distribution of CentOS does not come with a compiler pre-installed.

   Make sure to remove the installed compiler when all of this machine's tasks have been completed;.it could be used to compile malicious code if an attacker gained access to the system.

```
# yum install gcc zlib-devel
```

4. Type `y` then press `[Enter]` when prompted to confirm the download.
5. Change into the clamav-0.96.1 directory and install ClamAV:

```
# cd clamav-0.96.1
# adduser clamav
# ./configure --sysconfdir=/etc
# make
# make install
```

6. Use the VI editor to open the clamav.conf file in order to configure ClamAV:

```
# vi /etc/clamd.conf
```

7. Press `[Insert]` to enter edit mode. Comment out the line near the beginning of the file containing 'Example':

```
# Comment or remove the line below.
#Example
```

Figure 12: Editing clamd.conf

8. Find and uncomment the following lines by removing the '#' in front of them:
   a. 'LogFile /tmp/clamd.log'
   b. 'LogTime yes'
   c. 'LogSyslog yes'
   d. 'LocalSocket /tmp/clamd.socket'

9. Save and exit the file. Press `[Esc]` and type `:wq` then press `[Enter]`.

10. The ClamAV updater (freshclam) needs to be pointed to the internal proxy (10.0.2.1) in order to update virus definitions. Use the VI editor to open the freshclam.conf file:

```
# vi /etc/freshclam.conf
```

11. Comment out the line near the beginning of the file containing 'Example':

```
# Comment or remove the line below.
#Example
```

Figure 13: Editing freshclam.conf

12. Find the proxy settings. Uncomment them and make the following changes to indicate the IP address of the proxy server and the port number to use:

```
HTTPProxyServer 10.0.2.1
HTTPProxyPort 3128
```

Note: Although freshclam has been configured, it probably will not successfully run yet. The Squid Proxy server may still need to be set up.

13. Save and exit the file. Press `[Esc]` and type `:wq` then press `[Enter]`.

14. Enable the ClamAV daemon to start it automatically as a service:

```
# cp /media/AISTS/Tools/Linux/ClamAV/clamd /etc/init.d/
# chkconfig --add clamd
# service clamd start
```

15. Setup cron jobs for Virus definition updates and nightly virus scans:

```
# crontab –u root -e
```

16. Add the following two lines to the file:

```
15 2 * * * /usr/local/bin/freshclam --quiet
15 3 * * * /usr/local/bin/clamdscan --quiet /
```

17. Save and exit the cron file. Press `[Esc]` and type `:wq` then press `[Enter]`.

18. Remove the ClamAV installation files (they contain test signatures that will be found on every scan if you do not remove them) then reboot the server.

```
# cd /root
# rm -rf clamav-0.96*
# reboot
```

ADDENDUM Bash Script: 'for loop'

Create a file containing the list of items

1. If you would like to automate the task of removing the unwanted services, users, and groups you can write a Bash script to loop through the list of items and process them one by one. First, start by creating a text file containing the list of items that you want to process. Enter the following command to create the text file:

```
# cat > deletedSvcList
```

2. After you typed the previous command and hit the `[Enter]` key, notice that there is no prompt ('#') at the cursor. The file is now open and you can enter the list of items that you want to process. Enter each item on a separate line, hitting the `[Enter]` key to move to the next line.

3. When all of the items have been entered into the file, press `[Ctrl+d]` to save and close the file. Notice that the prompt ('#') has returned to the shell.

Write the 'for loop'

1. Now you will create a 'for loop' that will read the items in the deletedSvcList file one by one and stop each service. Enter the following script as it appears below to stop the unwanted services:

```
# for str in $(cat deletedSvcList); do service $str stop; done
```

   A simple modification makes sure that those services do not start on boot up:

```
# for str in $(cat deletedSvcList); do chkconfig --del $str; done
```

2. Notice that the script is in three sections, separated by semi-colons (';'). The first section of this script creates a variable, named 'str', and assigns it to the first item in the file. The second section inserts the value of the variable, 'str', into the shell command. The command is executed and then the process is repeated for each item in the file. When there are no more items in the file, the third section of the script ends the process and returns control back to the shell.

   As you go through the steps, you will have to create three separate files for services, users, and groups. Then you must modify the file name in the first section of the script. Likewise, you will have to modify the command in the second section to perform the action that you want.

Here are the files and scripts that should be created to remove the following items:

Users:

```
# cat > deletedUserList
```

```
# for str in $(cat deletedUserList); do userdel $str; done
```

Groups:

```
# cat > deletedGrpList
```

```
# for str in $(cat deletedGrpList); do groupdel $str; done
```

This page left intentionally blank for pagination purposes

Linux Network Time Protocol Daemon (ntpd) Client

1 Setup Linux ntpd Client Service

1.1 Installation

1. If you have not already done so, log on the console using:

   Username: **root** Password: **tartans@1**

2. Open a terminal window by going to 'Applications' -> 'Accessories' -> 'Terminal'.
3. The Network Time Protocol Daemon (ntpd) is installed with most Linux distributions. You will create a cron job that will cause the Linux ntpd to periodically query Quebec's ntp server and update the system time.

1.2 Configuration

1. Run the following command to see the current local system time. Hopefully, it is significantly different from the time server's system time as this will explicitly demonstrate when the client becomes synchronized with the server:

```
# date
```

2. If the date is not significantly different from the time server's system time, you can change the local client's system time manually by entering the following command (you can change the system date and time to whatever you want):

```
# date -s "Fri Sep 12 14:38:19 EDT 2003"
```

3. The ntp configuration file must be modified to tell it which time server to use to update the system time. This file is located in the '/etc' directory. To open the config file in the 'vi' text editor, enter:

```
# vi /etc/ntp.conf
```

4. In order to modify the file in the 'vi' editor, the `[Insert]` or `[i]` key must be pressed before trying to add or change text.

5. Scroll down to the section beginning with "# Use public servers" which is excerpted here:

```
# Use public servers from the pool.ntp.org project.
# Please consider joining the pool (http://www.pool.ntp.org/join.html).
#server 0.centos.pool.ntp.org
#server 1.centos.pool.ntp.org
#server 2.centos.pool.ntp.org
restrict 10.0.2.1 mask 255.255.255.255 nodmodify notrap noquery
server 10.0.2.1 prefer
```

Figure 1: Default NTP configuration file

Comment out the previous servers and add the following two lines at the end of this section:

```
restrict 10.0.2.1 mask 255.255.255.255 nomodify notrap noquery
server 10.0.2.1 prefer
```

Your section should look similar to the following:

```
# Use public servers from the pool.ntp.org project.
# Please consider joining the pool (http://www.pool.ntp.org/join.html).
#server 0.centos.pool.ntp.org
#server 1.centos.pool.ntp.org
#server 2.centos.pool.ntp.org
restrict 10.0.2.1 mask 255.255.255.255 nomodify notrap noquery server 10.0.2.1 p
refer
```

Figure 2: Edited NTP configuration file

6. Save and exit the file. Press `[Esc]` and type `:wq` then press `[Enter]`.

7. Now we need to cause ntpd to update to the ntp server time by modifying /etc/ntp/step-tickers to run ntpdate when ntpd is started. Do this by running these two commands:

```
# echo "10.0.2.1" > /etc/ntp/step-tickers
```

8. The 'step-tickers' file should now contain only the ntp server's IP address. The file contents can be viewed by entering this command:

```
# cat /etc/ntp/step-tickers
```

9. Enter the date command to see that the date is still incorrect.

10. If the ntpd service is not currently running, it must be started by entering the following command. If the service is currently running, replace 'start' with `restart`. NOTE: Once the service is running, always remember to 'restart' after making any changes to the ntp config file. Otherwise, the service will continue to run according to the previous config file settings until the service is restarted. Later, we will be creating a cron job to periodically restart the service. For now, enter this command:

```
# service ntpd start
```

11. You should see these two messages:

```
ntpd: Synchronizing with time server:                      [  OK  ]
Starting ntpd:                                             [  OK  ]
```

Figure 3: Starting the NTP service

12. Enter the date command again to see that the time has been synchronized.
    Note: This will only be successful after Quebec's time server has been configured properly. Check with your teammates for its status.

13. The service can be verified and the current pid identified by entering:

```
# service ntpd status
```

14. Now, we are going to make sure that ntpd updates the system time regularly. Skew the local system time again by entering the following command that you entered earlier (up arrow to find this command and press enter):

```
# date -s "Fri Sep 12 14:38:19 EDT 2003"
```

15. A cron job must be created to cause the ntpd service to periodically query the time server and update the local system time accordingly. Enter this command to create the cron job file:

```
# crontab –u root –e
```

16. This file should automatically open using the 'vi' text editor again, so you must press the `[Insert]` key before you can add or modify text.

17. Insert the following line at the top of the file to set up a cron job that will execute every 10 minutes. You can review the 'man 5 crontab' pages to understand the crontab fields in more depth after you are done with this task. After the ntpd is verified to be up and running correctly, the first set of numbers can be changed to a '0' to cause the cron job to run at the top of every hour (0th minute of every hour) instead.

    Make sure that there is a space after the 50 and between each '*' and the '/' character following them. There are no spaces between the initial set of numbers.

```
0,10,20,30,40,50 * * * * /etc/rc.d/init.d/ntpd restart
```

```
0,10,20,30,40,50 * * * * /etc/rc.d/init.d/ntpd restart
15 2 * * * /usr/local/bin/freshclam --quiet
15 3 * * * /usr/local/bin/clamdscan --quiet /
```

18. Now Save and exit the file. Press `[Esc]` and type `:wq` then press `[Enter]`.

19. Entering the following command will create init scripts at run levels 3-5 to start the ntpd service every time the system is started up.

```
# chkconfig --level 345 ntpd on
```

20. Use the following command to verify that the ntpd service is turned on at run levels 3, 4, and 5:

```
# chkconfig --list | grep ntpd
```

21. Make sure that it looks like this:

```
ntpd            0:off   1:off   2:off   3:on    4:on    5:on    6:off
```

Figure 4: NTP service startup run levels

22. Now, use the date command to see if the cron job has updated the system time. If not, wait a few more minutes and try again.

23. Once the remote centralized syslog server is installed and configured, we can review the logs that are generated from the Network Time Server process. There we will see each time that the client is updated and the offset amount by which it is updated.

Installing and Configuring Bastille-Linux

You have already completed preliminary hardening (by removing users, groups, etc) and now will use Bastille-Linux to finish the task. Bastille allows you to easily modify many OS settings. In this task, you will apply a previously configured Bastille template file (analogous to the Security Configuration templates used on Windows) to the system.

1 Bastille Configuration

1.1 Install Bastille

1. If you have not already done so, log on to the machine using:

   Username: **root**
   Password: **tartans@1**

2. Open a terminal window by clicking on:
   'Applications' -> 'Accessories' -> 'Terminal'.

3. There are two modules that are required to implement Bastille:
   perl-Curses-1.12-1.2.el4.rf.i386.rpm
   Bastille-3.0.8-1.0.noarch.rpm

   Copy the required modules to the /root directory with this command:

```
# cp /media/AISTS/Tools/Linux/Bastille/* /root
```

4. Using the following commands, change to the /root directory and get a directory listing to confirm that all the Bastille files copied:

```
# cd /root
# ls –l
```

5. Install perl-Curses module:

```
# rpm –ivh perl-Curses-1.28-1.el5.rf.i386.rpm
```

6. Install Bastille module:

```
# rpm –ivh Bastille-3.0.9-1.0.noarch.rpm
```

1.2 Run Bastille

1. Copy Lima's Bastille template to the Bastille configuration directory (this command should be typed as one continuous line with a space after 'cp' and after 'bastille-ids-config'):

```
# cp /media/AISTS/Tools/Linux/Config_Files/Lima_10.0.2.5/bast
ille-ids-config /etc/Bastille/config
```

2. Run Bastille in batch mode to apply the preconfigured template:

```
# bastille –b –n 2>/dev/null
```

Note: The template generates error messages about the CentOS version but the settings will be applied successfully. These messages are not important and so in this command, you divert all error messages to /dev/null (the trash).

```
NOTE:    Entering Critical Code Execution.
         Bastille has disabled keyboard interrupts.


NOTE:    Bastille is scanning the system configuration...

NOTE:    Bastille is now locking down your system in accordance with your
         answers in the "config" file.  Please be patient as some modules
         may take a number of minutes, depending on the speed of your
         machine.
NOTE:    Executing Firewall Specific Configuration
NOTE:    Executing File Permissions Specific Configuration
NOTE:    Executing Account Security Specific Configuration
NOTE:    Executing Boot Security Specific Configuration
NOTE:    Executing Inetd Specific Configuration
NOTE:    Executing PAM Specific Configuration
NOTE:    Executing Logging Specific Configuration
NOTE:    Executing Daemon Specific Configuration
NOTE:    Executing Sendmail Specific Configuration
NOTE:    Executing Apache Specific Configuration
NOTE:    Executing FTP Specific Configuration
NOTE:    Executing Temporary Directory Specific Configuration
```

Figure 1: Bastille Output

2 Bastille Configuration

1. The template you applied has been previously configured as follows.
   Enter the following command to view the new Bastille security settings:

```
# cat /etc/Bastille/config | less
```

2. You can scroll up and down to view the entire file. When you are finished reviewing the file, press the 'q' key to quit and return to the shell prompt.

3. After reviewing the config file, *reboot* the system by typing `reboot`. You will now have to login with the admin account that was created in the Linux Host System Hardening task. *Make sure that the admin account was created before rebooting the system or you will not be able to login.*

   You may need to reset the screen resolution to 1024x768 the first time you log on to the admin account. You can do this by going to 'System' -> 'Preferences' -> 'Screen Resolution'.

   The remaining sections of this document detail the previously configured template that you applied. Note that you will *NOT* need to actually perform any tasks in the following sections; it is merely here for your edification. After reviewing, you can move on to the next task.

2.1 File Permissions

- Disallow non-root access to ping, usernetctl, mount/umount, and at
- Disable the r-tools (rsh, rlogin, etc) which are troublesome due to their use of weak authentication.

```
# Q:  Would you like to set more restrictive permissions on the administration u
tilities? [N]
FilePermissions.generalperms_1_1="Y"

# Q:  Would you like to disable SUID status for mount/umount?
FilePermissions.suidmount="Y"

# Q:  Would you like to disable SUID status for ping? [Y]
FilePermissions.suidping="Y"

# Q:  Would you like to disable SUID status for at? [Y]
FilePermissions.suidat="Y"

# Q:  Would you like to disable the r-tools? [Y]
FilePermissions.suidrtool="Y"

# Q:  Would you like to disable SUID status for usernetctl? [Y]
FilePermissions.suidusernetctl="Y"
```

Figure 2: File Permissions

2.2 Account Security Settings

- Enforce password aging
- Restrict cron (scheduler) to the root user
- Disallow root from direct login. After you apply this template all administrators must login using the 'admin' account and then su to root.
- Set permissions on all user-created files so that the file is only readable by the user who created it.

```
# Q:  Should Bastille disable clear-text r-protocols that use IP-based authentic
ation? [Y]
AccountSecurity.protectrhost="Y"

# Q:  Would you like to enforce password aging? [Y]
AccountSecurity.passwdage="Y"

# Q:  Do you want to set the default umask? [Y]
AccountSecurity.umaskyn="Y"

# Q:  What umask would you like to set for users on the system? [077]
AccountSecurity.umask="077"

# Q:  Should we disallow root login on tty's 1-6? [N]
AccountSecurity.roottylogins="Y"
```

Figure 3: Account Security Settings

2.3 Boot Security Settings

- Disable CTRL-ALT-DELETE rebooting so that a user must have a valid login and password to reboot the machine.
- Password protect single user mode to require the root password. Single user mode is equivalent to run level 1. You are granted root access, but networking is disabled.

```
# Q:  Would you like to password-protect the GRUB prompt? [N]
BootSecurity.protectgrub="N"

# Q:  Would you like to disable CTRL-ALT-DELETE rebooting? [N]
BootSecurity.secureinittab="Y"

# Q:  Would you like to password protect single-user mode? [Y]
BootSecurity.passsum="Y"
```

Figure 4: Boot Security Settings

2.4 Securing inetd and TCP Wrappers

- Disable telnet and ftp
- Create authorized use banners that will be displayed before the user can log in
- You do not set default deny on TCP wrappers in this configuration. Later on you will configure an IPtables firewall which will handle this.

```
# Q:  Would you like to set a default-deny on TCP Wrappers and xinetd? [N]
SecureInetd.tcpd_default_deny="N"

# Q:  Would you like to display "Authorized Use" messages at log-in time? [Y]
SecureInetd.banners="Y"

# Q:  Who is responsible for granting authorization to use this machine?
SecureInetd.owner="administrator@aia.class"
```

Figure 5: Securing inetd and TCP Wrappers

2.5 Configure PAM

- Set limits on resources. Users will only be allowed to start 150 concurrently running processes, and will be unable to open core system (kernel) files.
- Only allow admin to log in at the console

```
# Q:  Would you like to put limits on system resource usage? [N]
ConfigureMiscPAM.limitsconf="Y"

# Q:  Should we restrict console access to a small group of user accounts? [N]
ConfigureMiscPAM.consolelogin="Y"

# Q:  Which accounts should be able to login at console? [root]
ConfigureMiscPAM.consolelogin_accounts="admin"
```

Figure 6: PAM Settings

2.6 Logging Settings

- You will configure logging in a later module, therefore you will not configure logging through Bastille

```
# Q:  Would you like to set up process accounting? [N]
Logging.pacct="N"
```

Figure 7: Logging Settings

2.7 Sendmail Settings

- Prevent sendmail from running in daemon mode. This machine will not be a mail server, so sendmail need not listen for connections

```
# Q:  Do you want to stop sendmail from running in daemon mode? [Y]
Sendmail.sendmaildaemon="Y"
```

Figure 8: Sendmail Settings

2.8 Miscellaneous Daemons

```
# Q:  Would you like to disable acpid and/or apmd? [Y]
MiscellaneousDaemons.apmd="Y"

# Q:  Would you like to disable GPM? [Y]
MiscellaneousDaemons.gpm="Y"

# Q:  Would you like to deactivate the HP OfficeJet (hpoj) script on this machin
e?
MiscellaneousDaemons.disable_hpoj="Y"

# Q:  Would you like to deactivate the ISDN script on this machine?
MiscellaneousDaemons.disable_isdn="Y"
```

Figure 9: Miscellaneous Deamons

2.9 Apache Web Server Settings

```
# Q:  Would you like to bind the Web server to listen only to the localhost? [N]
Apache.bindapachelocal="N"

# Q:  Would you like to bind the web server to a particular interface? [N]
Apache.bindapachenic="N"

# Q:  Would you like to deactivate the following of symbolic links? [Y]
Apache.symlink="N"
```

Figure 10: Apache Web Server Settings

2.10 Tempdir Scripts

- This system is not a multi-user system, and therefore you will not be very concerned with the temporary (shared) directories

```
# Q:  Would you like to install TMPDIR/TMP scripts? [N]
TMPDIR.tmpdir="N"
```

Figure 11: Tempdir Scripts

2.11 Packet Filtering Firewall

- You will configure a firewall in a later module, therefore you will not use Bastille's firewall configuration

```
# Q:  Would you like to run the packet filtering script? [N]
Firewall.ip_intro="N"
```

Figure 12: Packet Filtering Firewall

2.12 FTP Settings

```
# Q:  Would you like to disable anonymous download? [N]
FTP.anonftp="Y"

# Q:  Would you like to disable user privileges on the FTP daemon? [N]
FTP.userftp="Y"
```

Figure 13: FTP Settings

Configuring IPTables as a Host Based Firewall on Linux Systems

The host based firewall for Linux, iptables, can be configured by accessing the console directly or via SSH from a management workstation. Iptables has six pre-defined "chains" that are available with the ability to create user defined chains as well. The default chains are:

- INPUT
- OUTPUT
- INPUT
- FORWARD
- PREROUTING
- POSTROUTING

The table below lists various options that can be used when configuring iptables rules. Additional information is available by typing `iptables --help` at the Linux command line or by reviewing the iptables man page (type: `man iptables`).

--table -t	Description
filter	Default table. This is used if not specified
nat	Network address translation
mangle	Used for Quality Of Service (QOS) and preferential treatment
raw	Enables optimization. i.e. Ignore firewall state matching for port 80 for enhanced speed due to less processing. Requires kernel patch

Command (Use one)	Description
-A --append	Append rule to chain
-D --delete	Delete rule from chain
-I --insert	Insert rule at beginning or at specified sequence number in chain.
-R --replace	Replace rule
-F --flush	Flush all rules
-Z --zero	Zero byte counters in all chains
-L --list	List all rules. Add option --line-numbers for rule number.
-N --new-chain	Create new chain
-X --delete-chain	Delete user defined chain
-P --policy	Set default policy for a chain
-E --rename-chain	Rename a chain

Command Option	Description
-s --source	Source address of packet
-d --destination	Destination address of packet
-i --in-interface	Interface packet is arriving from
-o --out-interface	Interface packet is going to
-p --protocol	Protocol: °tcp --sport port[:port] --dport port[:port] --syn °udp °icmp °mac ...
-j --jump	Target to send packet to
-f --fragment	Fragment matching
-c --set-counters	Set packet/byte counter
-m tcp --match tcp	°--source-port port[:port] (port # or range ##) °--destination-port port[:port] °--tcp-flags
-m state --match state	--state °ESTABLISHED °RELATED °NEW °INVALID (Push content, not expected to recieve this packet.)

Defined Policies	Description
ACCEPT	Let packet through
DROP	Deny packet with no reply
REJECT	Deny packet and notify sender
RETURN	Handled by default targets
MARK	Used for error response. Use with option --reject-with type
MASQUERADE	Used with nat table and DHCP.
LOG	Log to file and specify message: °--log-level # °--log-prefix "prefix" °--log-tcp-sequence °--log-tcp-options °--log-ip-options
ULOG	Log to file and specify userpace logging messages
SNAT	Valid in PREROUTING chain. Used by nat.
REDIRECT	Used with nat table. Output.
DNAT	Valid in POSTROUTING chain. Output.
QUEUE	Pass packet to userspace.

Figure 1: IPtables Options

1 Creating Inbound and Outbound Filtering Rules

The filtering rules for this server will be set up to allow the following traffic into and out of the system:

Source Address	Destination Address	Proto	Source Ports	Destination Port	Direction	Purpose
10.0.4.0/24	10.0.2.5/32	ANY	ANY	ANY	Inbound	Management
10.0.3.2/32	10.0.2.5/32	ANY	ANY	ANY	Inbound	Mike-Nagios
127.0.0.1/32	127.0.0.1/32	*	*	*	Inbound	Loopback
Log All Denied						
10.0.2.5/32	10.0.4.0/24	ANY	ANY	ANY	Outbound	Management
10.0.2.5/32	10.0.3.2/32	ANY	ANY	ANY	Outbound	Mike-Nagios
10.0.2.5/32	10.0.2.3/32	TCP	ANY	25	Outbound	SMTP
10.0.2.5/32	10.0.2.4/32	UDP	ANY	53	Outbound	DNS
10.0.2.5/32	10.0.2.1/32	UDP	123	123	Outbound	NTP
10.0.2.5/32	10.0.2.1/32	TCP	ANY	3128	Outbound	Squid Proxy
127.0.0.1/32	127.0.0.1/32	*	*	*	Outbound	Loopback
Log All Denied						

1. If you have not already done so, log on to the machine using the newly enforced admin account:

   Username: **admin** Password: **steelers**

2. Open a terminal window by going to ‘Applications’ -> ‘Accessories’ -> ‘Terminal’.
3. Elevate to root level privileges by typing the following command and entering the root password **tartans@1**

```
# su -
```

4. Ensure iptables is stopped.

```
# service iptables stop
```

5. Clear all existing iptables rules.

```
# iptables --flush
```

6. Set the default policy for the FORWARD chain to DROP all packets.

```
# iptables –P FORWARD DROP
```

7. Create the iptables file that will be used to save firewall rules.

```
# iptables-save > /etc/sysconfig/iptables
# vi /etc/sysconfig/iptables
```

8. Remove the last two lines. Move the cursor to each line and press the [D] key twice. This will delete the current line in VI. The file should look like the following when completed:

```
# Generated by iptables-save v1.3.5 on Mon Jun 14 10:52:10 2010
*filter
:INPUT ACCEPT [5:420]
:FORWARD DROP [0:0]
:OUTPUT ACCEPT [5:420]
```

9. Add the remaining rules to the iptables file as listed below. Comments/remarks are identified with a '#' at the beginning of the line. These lines are used to identify what the rules beneath them are used for. Although they are not required, it is a good practice to describe the rules, their intent, who added the rule, and potentially the date on which the rule was added or modified. Use the cursor to go to the bottom of the file. Simultaneously press the [Shift] and [A] keys to append text to the end of the last line. Press [Enter] to add a new line. Enter the following lines:

```
# Allow all inbound traffic from the MGMT network
-A INPUT -s 10.0.4.0/24 -d 10.0.2.5/32 -i eth0 -j ACCEPT

# Allow all inbound traffic from Mike-Nagios
-A INPUT -s 10.0.3.2/32 -d 10.0.2.5/32 -i eth0 -j ACCEPT

# Allow all established connections
-A INPUT -i eth0 -m state --state ESTABLISHED,RELATED -j ACCEPT

# Allow all inbound traffic on the loopback interface
-A INPUT -i lo -p all -j ACCEPT

# Enable logging on INPUT chain
-A INPUT -j LOG --log-level 6

# Set the default INPUT policy to Drop
-P INPUT DROP
```

Figure 2: IPtables Input Rules

```
# Allow outbound mail traffic to Bravo
-A OUTPUT -d 10.0.2.3/32 -o eth0 -p tcp --dport 25 -j ACCEPT

# Allow outbound DNS traffic to Alpha
-A OUTPUT -d 10.0.2.4/32 -o eth0 -p udp --dport 53 -j ACCEPT

# Allow all outbound traffic to Mike-Nagios
-A OUTPUT -d 10.0.3.2/32 -o eth0 -p all -j ACCEPT

# Allow outbound web proxy traffic to Quebec
-A OUTPUT -d 10.0.2.1/32 -o eth0 -p tcp --dport 3128 -j ACCEPT

# Allow outbound NTP traffic to Quebec
-A OUTPUT -d 10.0.2.1/32 -o eth0 -p udp --dport 123 -j ACCEPT

# Allow all outbound traffic to the MGMT network
-A OUTPUT -d 10.0.4.0/24 -o eth0 -p all -j ACCEPT

# Allow all outbound traffic on the loopback interface
-A OUTPUT -o lo -p all -j ACCEPT

# Enable logging on OUTPUT chain
-A OUTPUT -j LOG --log-level 6

# Set the default OUTPUT policy to Drop
-P OUTPUT DROP

# Enable rule set
COMMIT
```

Figure 3: IPtables Output Rules

10. Save and exit the file. Press `[Esc]` and type `:wq` then press `[Enter]`.

1.1 Applying the firewall rules

1. Enter the following command to start the iptables firewall:

```
# service iptables start
```

2. If the service started successfully, you should see the following:

```
Flushing firewall rules:                                   [  OK  ]
Setting chains to policy ACCEPT: filter                    [  OK  ]
Unloading iptables modules:                                [  OK  ]
Applying iptables firewall rules:                          [  OK  ]
Loading additional iptables modules: ip_conntrack_netbios_n[  OK  ]
```

Figure 4: IPtables Successful Startup

1.2 Making the iptables file immutable

1. Since we do not want the iptables file to change for ANY reason after the rules have been built without intervention from the administrator, we will make this file immutable. To do this, we will issue the following command.

```
# chattr +i /etc/sysconfig/iptables
```

2. Relinquish the elevated root privileges by typing the following command:

```
# exit
```

This page left intentionally blank for pagination purposes

Installing and Configuring Snort

1 Snort Installation and Configuration

The Snort Intrusion Detection System can be a powerful tool to help in protecting a network. We will be installing Snort, along with other modules that Snort requires.

1.1 Installation

Snort can log in a variety of different formats, including a few different database formats and flat text. We will be installing Snort to log to a MySQL database.

There are several prerequisites that must be installed for Snort to run. Snort uses libpcap to capture packets from the ethernet interface. There are also a number of other packages we need to install in order to configure Snort to send our alerts to the central MySQL console.

1. If you have not already done so, log on to the machine using the newly enforced admin account:

   Username: **admin** Password: **steelers**

2. Open a terminal window by going to 'Applications' -> 'Accessories' -> 'Terminal'.
3. Elevate to root level privileges by typing the following command and entering the root password **tartans@1**

```
# su -
```

4. Download and install the prerequisites from the trusted repository that was set up in the Linux Host System Hardening step by executing the following command:

```
# yum install mysql-server mysql-bench mysql-devel libpcap
libpcap-devel pcre-devel
```

5. Type **`y [Enter]`** when prompted to download the packages.
6. There are several files that we will need to implement Snort:

   snort-2.8.6.tar.gz
   snortd
   snortrules-aists.tar.gz

Copy the required files to the /root directory with this command:

```
# cp /media/AISTS/Tools/Linux/Snort/* /root
```

7. Setup folders that we will use for Snort:

```
# mkdir /var/log/snort
# mkdir /etc/snort
```

8. Untar the Snort installation file and cd into the new directory:

```
# tar xvzf snort-2.8.6.tar.gz
# cd snort-2.8.6
```

9. Configure the installation to have Snort be compatible with MySQL, compile the code, then install the files to their final location:

```
# ./configure –-with-mysql –-enable-zlib
# make
# make install
```

10. Install the rules and configuration files:

```
# cd /root
# cp ./snortrules-aists.tar.gz /etc/snort
# cd /etc/snort
# tar xvzf snortrules-aists.tar.gz
# rm –f snortrules-aists.tar.gz
# cp etc/* .
# rm –rf etc
```

11. Copy the Snort startup script into the /etc/rc.d/init.d directory:

```
# cp /root/snortd /etc/rc.d/init.d
```

12. Configure Snort to start when the machine is booted:

```
# cd /etc/rc.d/init.d
# chmod 755 snortd
# chkconfig –-level 2345 snortd on
```

13. Use chkconfig to ensure that snort is configured to start at the correct run levels (2,3,4,5):

```
# chkconfig –-list | grep snortd
```

```
snortd          0:off   1:off   2:on    3:on    4:on    5:on    6:off
```

Figure 1: Chkconfig output for Snort

14. The snortd file needs to be edited to ensure that snort starts after MySQL has started on bootup. Use VI to edit the snortd file:

```
# vi /etc/rc.d/init.d/snortd
```

15. During the boot, MySQL is started first, but does not complete before Snort is started, so Snort fails to start. We need to make sure that Snort is set to wait extra time before it runs. Verify that the following line has been added to the snortd file right below the line labeled “start)”:

```
sleep 3
```

This causes the Snort startup script to wait 3 seconds before continuing to run the script. It should look like the figure below:

```
# Source function library.
. /etc/rc.d/init.d/functions

# Specify your network interface here
INTERFACE=eth0

# See how we were called.
case "$1" in
  start)
        sleep 3
        echo -n "Starting snort: "
        daemon /usr/local/bin/snort -d -D \
                -c /etc/snort/snort.conf
        touch /var/lock/subsys/snort
        echo
        ;;
  stop)
        echo -n "Stopping snort: "
        killproc snort
        rm -f /var/lock/subsys/snort
        echo
        ;;
  restart)
```

Figure 2: Have Snort pause 3 seconds

16. To save and exit the VI editor, press `[Esc]` then type `:wq` and press `[Enter]`.

1.2 Configuration

1. Edit the snort configuration file

```
# vi /etc/snort/snort.conf
```

2. Scroll down to the section titled ‘Step #1: Set the network variables’. This is where we will tell Snort the layout of our network and the location of the rules that we just installed. Press `[Insert]` to edit the file. Change the following lines, making sure to include the brackets “[“ and “]” where shown when entering the info:

   var HOME_NET [10.0.2.0/24,10.0.3.0/24,10.0.4.0/24]
   var EXTERNAL_NET !$HOME_NET
   var DNS_SERVERS [10.0.2.4/32]
   var SMTP_SERVERS [10.0.2.3/32]
   var HTTP_SERVERS [10.0.1.5/32,10.0.2.3/32,10.0.2.6/32]
   var SQL_SERVERS [10.0.2.10/32]
   portvar HTTP_Ports 80
   portvar SHELLCODE_PORTS !$HTTP_PORTS
   var RULE_PATH /etc/snort/rules
   var SO_RULE_PATH /etc/snort/so_rules
   var PREPROC_RULE_PATH /etc/snort/preproc_rules

Note: When entering in the IP addresses, be sure not to include any spaces or carriage returns.

3. Scroll down to the section titled 'Step #5: Configure preprocessors'. We are going remove the small_segments directive in the Snort stream5_tcp preprocessor because it can cause a large number of false positive alerts. Find the line beginning with 'preprocessor stream5_tcp:' and remove the 'small_segments 3 bytes 150,' text from the line. The result should look like the following:

```
preprocessor stream5_tcp: policy windows, detect_anomalies, require_3whs 180, \
   overlap_limit 10, timeout 180, \
    ports client 21 22 23 25 42 53 79 109 110 111 113 119 135 136 137 139 143 \
        161 445 513 514 587 593 691 1433 1521 2100 3306 6665 6666 6667 6668 6669
 \
```

Figure 3: Edit Snort preprocessor

4. Next find the 'Portscan detection' heading in this section and enable portscan detection by removing the '#' in front of the line beginning with 'preprocessor sfportscan' and set the 'sense_level' to `medium`.

5. Add a new 'ignore_scanners' directive to not alert us of portscan traffic coming from hosts on our network that are known to cause false positives of such alerts:

```
# Portscan detection.  For more information, see README.sfportscan
 preprocessor sfportscan: proto  { all } memcap { 10000000 } sense_level { mediu
m } \
 ignore_scanners { 10.0.2.1/32,10.0.2.3/32,10.0.2.4/32,10.0.2.6/32,10.0.3.2/32 }
```

6. Scroll down to the section titled 'Step #6: Configure output plugins'. We will be configuring Snort to log to our MySQL database. Find the section beginning with '# database' and edit the first 'output database' line to look like the following:

```
# database
output database: alert, mysql, user=snort password=snortpw dbname=snort host=10.
0.4.4 port=3306 sensor_name=lima
# output database: log, <db_type>, user=<username> password=<password> test dbna
me=<name> host=<hostname>
```

Figure 4: Configure Snort output database

1.3 Rules

There are many rules that are enabled by default when Snort is initially installed. Many of these may or may not be necessary depending on your particular network configuration. We will be disabling some unnecessary rules. The reason that we do this is that the more rules that are active, the more Snort has to parse for each packet that is scanned.

1. We do not need all of the rule sets since the User network does not have many of the services that Snort is looking for exploits for. For example, there is no Oracle database and telnet should be disabled on all hosts. Scroll down to the 'Step #7: Customize your rule set' section of the config file. Disable all rule sets by placing '#' at the beginning of each rule line, except for the following rules which we will leave enabled:

   include $RULE_PATH/chat.rules
   include $RULE_PATH/exploit.rules
   include $RULE_PATH/icmp.rules
   include $RULE_PATH/policy.rules
   include $RULE_PATH/sql.rules
   include $RULE_PATH/web-iis.rules
   include $RULE_PATH/web-misc.rules

   Scroll down to the 'Step #9: Customize your Shared Object Snort Rules' section of the config file. Enable the following rule sets by removing the '#' at the beginning of each of the following rule lines:

   include $SO_RULE_PATH/chat.rules
   include $SO_RULE_PATH/exploit.rules
   include $SO_RULE_PATH/icmp.rules
   include $SO_RULE_PATH/sql.rules
   include $SO_RULE_PATH/web-iis.rules
   include $SO_RULE_PATH/web-misc.rules

2. Save and exit the file. Press `[Esc]` type `:wq` then press `[Enter]`.
3. Install pre-compiled shared object rules:

```
# mkdir /usr/local/lib/snort_dynamicrules

# cp /etc/snort/so_rules/precompiled/Centos-5-
4/i386/2.8.6.0/* /usr/local/lib/snort_dynamicrules/

# snort -c /etc/snort/snort.conf --dump-dynamic-
rules=/etc/snort/so_rules
```

```
  Finished Loading all dynamic preprocessor libs from /usr/local/lib/snort_dynam
icpreprocessor/
Dumping dynamic rules...
Dumping dynamic rules for Library icmp 1.0.1
Dumping dynamic rules for Library misc 1.0.1
Dumping dynamic rules for Library imap 1.0.1
Dumping dynamic rules for Library web-activex 1.0.1
Dumping dynamic rules for Library exploit 1.0.1
Dumping dynamic rules for Library chat 1.0.1
Dumping dynamic rules for Library bad-traffic 1.0.1
Dumping dynamic rules for Library multimedia 1.0.1
Dumping dynamic rules for Library smtp 1.0.1
Dumping dynamic rules for Library nntp 1.0.1
Dumping dynamic rules for Library web-misc 1.0.1
Dumping dynamic rules for Library web-client 1.0.1
Dumping dynamic rules for Library netbios 1.0.1
Dumping dynamic rules for Library dos 1.0.1
Dumping dynamic rules for Library web-iis 1.0.1
Dumping dynamic rules for Library sql 1.0.1
Dumping dynamic rules for Library p2p 1.0.1
  Finished dumping dynamic rules.
Snort exiting
```

Figure 5: Install Snort dynamic rules

4. Start the snort service:

```
# service snortd start
```

5. Make sure that Snort has started successfully:

```
# ps –ef | grep snort
```

If the output of the above command looks similar to the following, Snort has successful started:

```
root     29737     1  0 09:53 ?        00:00:00 /usr/local/bin/snort -d -D -c /e
tc/snort/snort.conf
root     29740  4259  0 09:54 pts/1    00:00:00 grep snort
```

Figure 6: Snort process running

6. If Snort did not start successfully, look at the syslog messages file to search for Snort entries:

```
# tail -100 /var/log/messages | grep snort
```

7. If you are not performing any more administrative tasks on this machine, relinquish the elevated root privileges by typing the following command:

```
# exit
```

OSSEC Agent

OSSEC agents will be installed on each Linux and Windows server and will send events to the OSSEC server, which is running on Foxtrot. The OSSEC server processes events and generate warnings and alerts sent by agents. Before installing the OSSEC agent make sure you have successfully deployed the OSSEC server in order to connect agents to the server running on Foxtrot.

1 OSSEC Agent setup

1.1 Installation

1. If you have not already done so, log on to the machine using the newly enforced admin account:

   Username: **admin** Password: **steelers**

2. Open a terminal window by going to ‘Applications’ -> ‘Accessories’ -> ‘Terminal’.
3. Elevate to root level privileges by typing the following command and entering the root password **tartans@1**

```
# su -
```

4. Navigate to the Course CD by executing following command:

```
# cd /media/AISTS/Tools/Linux/OSSEC/
```

5. Copy OSSEC installation package:

```
# cp ossec-hids-2.4.1.tar.gz /root/
```

6. Extract installation package in root directory

```
# cd /root/
# tar -xzvf ossec-hids-2.4.1.tar.gz
```

7. Start installation using following command and accept default language by pressing `[Enter]`:

```
# cd ossec-hids-2.4.1
# ./install.sh
```

8. Read the introduction and press [Enter]:

```
OSSEC HIDS v2.4.1 Installation Script - http://www.ossec.net

You are about to start the installation process of the OSSEC HIDS.
You must have a C compiler pre-installed in your system.
If you have any questions or comments, please send an e-mail
to dcid@ossec.net (or daniel.cid@gmail.com).

 - System: Linux Lima 2.6.18-164.15.1.el5
 - User: root
 - Host: Lima


 -- Press ENTER to continue or Ctrl-C to abort. --
```

9. Answer the rest of the questions as shown below and press [Enter] when you have finished:

```
1- What kind of installation do you want (server, agent, local or help)?
 agent

  - Agent(client) installation chosen.

2- Setting up the installation environment.

 - Choose where to install the OSSEC HIDS [/var/ossec]:

    - Installation will be made at  /var/ossec .

3- Configuring the OSSEC HIDS.

  3.1- What's the IP Address of the OSSEC HIDS server?: 10.0.4.2

   - Adding Server IP 10.0.4.2

  3.2- Do you want to run the integrity check daemon? (y/n) [y]: y

   - Running syscheck (integrity check daemon).

  3.3- Do you want to run the rootkit detection engine? (y/n) [y]: y
```

```
3.4 - Do you want to enable active response? (y/n) [y]: n

 - Active response disabled.

3.5- Setting the configuration to analyze the following logs:
  -- /var/log/messages
  -- /var/log/secure
  -- /var/log/maillog

- If you want to monitor any other file, just change
  the ossec.conf and add a new localfile entry.
  Any questions about the configuration can be answered
  by visiting us online at http://www.ossec.net .


  --- Press ENTER to continue ---
```

10. When the installation has finished you should see following screen and press `[Enter]`:

```
- System is Redhat Linux.
- Init script modified to start OSSEC HIDS during boot.

- Configuration finished properly.

- To start OSSEC HIDS:
              /var/ossec/bin/ossec-control start

- To stop OSSEC HIDS:
              /var/ossec/bin/ossec-control stop

 - The configuration can be viewed or modified at /var/ossec/etc/ossec.c
onf


   Thanks for using the OSSEC HIDS.
   If you have any question, suggestion or if you find any bug,
   contact us at contact@ossec.net or using our public maillist at
   ossec-list@ossec.net
   ( http://www.ossec.net/main/support/ ).

   More information can be found at http://www.ossec.net

   ---  Press ENTER to finish (maybe more information below). ---
```

1.2 Configuration

1. Now you are going to setup a shared key between the OSSEC agent and the OSSEC server. In order to get a shared key from the OSSEC server, login to Foxtrot through SSH:

```
# ssh root@10.0.4.2
```

Accept SSH connectivity by typing `yes` and type the password `tartans@1` and you will be connected to Foxtrot.

```
[root@Lima ~]# ssh root@10.0.4.2
The authenticity of host '10.0.4.2 (10.0.4.2)' can't be established.
RSA key fingerprint is f5:b7:79:02:ff:f8:7d:af:a2:3f:87:db:e0:ee:c0:5e.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.0.4.2' (RSA) to the list of known hosts.
root@10.0.4.2's password:
Last login: Wed Jun 16 12:03:50 2010 from 10.0.2.10
[root@Foxtrot ~]#
```

2. Start the OSSEC agent manager:

```
# /var/ossec/bin/manage_agents
```

```
[root@Foxtrot ~]# /var/ossec/bin/manage_agents


****************************************
* OSSEC HIDS v2.4.1 Agent manager.     *
* The following options are available: *
****************************************
   (A)dd an agent (A).
   (E)xtract key for an agent (E).
   (L)ist already added agents (L).
   (R)emove an agent (R).
   (Q)uit.
Choose your action: A,E,L,R or Q:
```

3. Now add Lima's OSSEC agent to the OSSEC server by entering `A`. Type `y` and press `[Enter]` when you have finished entering the information about Lima as shown below:

```
 - Adding a new agent (use '\q' to return to the main menu).
   Please provide the following:
    * A name for the new agent: Lima
    * The IP Address of the new agent: 10.0.2.5
    * An ID for the new agent[005]: 005
 Agent information:
    ID:005
    Name:Lima
    IP Address:10.0.2.5

 Confirm adding it?(y/n): y
 Agent added.
```

4. Now type `E` and press `[Enter]` to extract the shared key for Lima, and enter `005` when the OSSEC agent manager asks for an agent ID. Please note that key will not be the same as shown in following screenshot because the shared key is generated randomly each time an OSSEC agent is added.

```
* OSSEC HIDS v2.4.1 Agent manager.     *
* The following options are available: *
****************************************
   (A)dd an agent (A).
   (E)xtract key for an agent (E).
   (L)ist already added agents (L).
   (R)emove an agent (R).
   (Q)uit.
Choose your action: A,E,L,R or Q: E

Available agents:
   ID: 001, Name: Hotel, IP: 10.0.1.5
   ID: 002, Name: Juliet, IP: 10.0.1.3
   ID: 003, Name: Bravo, IP: 10.0.2.3
   ID: 004, Name: Alpha, IP: 10.0.2.4
   ID: 005, Name: Lima, IP: 10.0.2.5
Provide the ID of the agent to extract the key (or '\q' to quit): 005

Agent key information for '005' is:
MDA1IExpbWEgMTAuMC4yLjUgODIwZDkzN2YwYWMwNjNhMmY3MzYxMDcyMzI5MDMxNDNiZG
IxZDhlZjdiN2QxMGIwZmJjNDA3YjUyNzc4ZDdmYg==

** Press ENTER to return to the main menu.
```

5. Copy the shared key to your clipboard by highlighting it, right-clicking and choosing ‘Copy’.

6. Type `Q` and press `[Enter]` to quit from the OSSEC agent manager, and type `exit` and press `[Enter]` to end the SSH session:

```
****************************************
* OSSEC HIDS v2.4.1 Agent manager.     *
* The following options are available: *
****************************************
   (A)dd an agent (A).
   (E)xtract key for an agent (E).
   (L)ist already added agents (L).
   (R)emove an agent (R).
   (Q)uit.
Choose your action: A,E,L,R or Q: Q
```

7. Now you should be back in the shell of Lima. Execute following command to import the copied key.

```
# /var/ossec/bin/manage_agents
```

8. Type `I` then press `[Enter]`.

9. Paste the copied key by right-clicking and choosing ‘Paste’ to import the key and accept confirmation by typing `y` then pressing `[Enter]` as shown below:

```
****************************************
* OSSEC HIDS v2.4.1 Agent manager.     *
* The following options are available: *
****************************************
   (I)mport key from the server (I).
   (Q)uit.
Choose your action: I or Q: I

* Provide the Key generated by the server.
* The best approach is to cut and paste it.
*** OBS: Do not include spaces or new lines.

Paste it here (or '\q' to quit): MDA1IExpbWEgMTAuMC4yLjUgODIwZDkzN2YwY
WMwNjNhMmY3MzYxMDcyMzI5MDMxNDNiZGIxZDhlZjdiN2QxMGIwZmJjNDA3YjUyNzc4ZDd
mYg==

Agent information:
   ID:005
   Name:Lima
   IP Address:10.0.2.5

Confirm adding it?(y/n): y
```

10. Exit from OSSEC manager by typing `Q` then pressing `[Enter]`:

```
   Confirm adding it?(y/n): y
   Added.
   ** Press ENTER to return to the main menu.



   ****************************************
   * OSSEC HIDS v2.4.1 Agent manager.     *
   * The following options are available: *
   ****************************************
      (I)mport key from the server (I).
      (Q)uit.
   Choose your action: I or Q: Q

   ** You must restart the server for your changes to have effect.

   manage_agents: Exiting ..
```

11. Start Lima's OSSEC agent by executing following command:

```
# /var/ossec/bin/ossec-control start
```

```
[root@Lima ossec-hids-2.4.1]# /var/ossec/bin/ossec-control start
Starting OSSEC HIDS v2.4.1 (by Trend Micro Inc.)...
Started ossec-execd...
Started ossec-agentd...
Started ossec-logcollector...
Started ossec-syscheckd...
Completed.
```

12. If you are not performing any more administrative tasks on this machine, relinquish the elevated root privileges by typing the following command:

```
# exit
```

This page left intentionally blank for pagination purposes

Wireshark Network Protocol Analyzer

1 Install Wireshark

1. If you have not already done so, log on to the machine using the newly enforced admin account:

   Username: **admin** Password: **steelers**

2. Open a terminal window by going to ‘Applications’ -> ‘Accessories’ -> ‘Terminal’.
3. Elevate to root level privileges by typing the following command and entering the root password **tartans@1**

```
# su -
```

4. Use the trusted yum repository to install arpwatch:

```
# yum install wireshark-gnome
```

5. Type `y` and press `[Enter]` if asked to confirm the download or import the GPG key.

```
================================================================================
 Package                Arch        Version                   Repository   Size
================================================================================
Installing:
 wireshark-gnome        i386        1.0.8-1.el5_3.1           base        671 k
Installing for dependencies:
 libsmi                 i386        0.4.5-2.el5               base        2.4 M
 wireshark              i386        1.0.8-1.el5_3.1           base         11 M

Transaction Summary
================================================================================
Install      3 Package(s)
Update       0 Package(s)
Remove       0 Package(s)

Total download size: 14 M
Is this ok [y/N]: y
```

Figure 1: Installing Wireshark

2 Running Wireshark

1. Start Wireshark with the following command:

```
# wireshark &
```

2. A warning message may appear cautioning against running as root. Place a check in the 'Do not show this message again' box and click 'OK'. The message may appear behind the main Wireshark window. If so, you will have to drag the Wireshark window to the side in order to handle the warning before the program will respond.

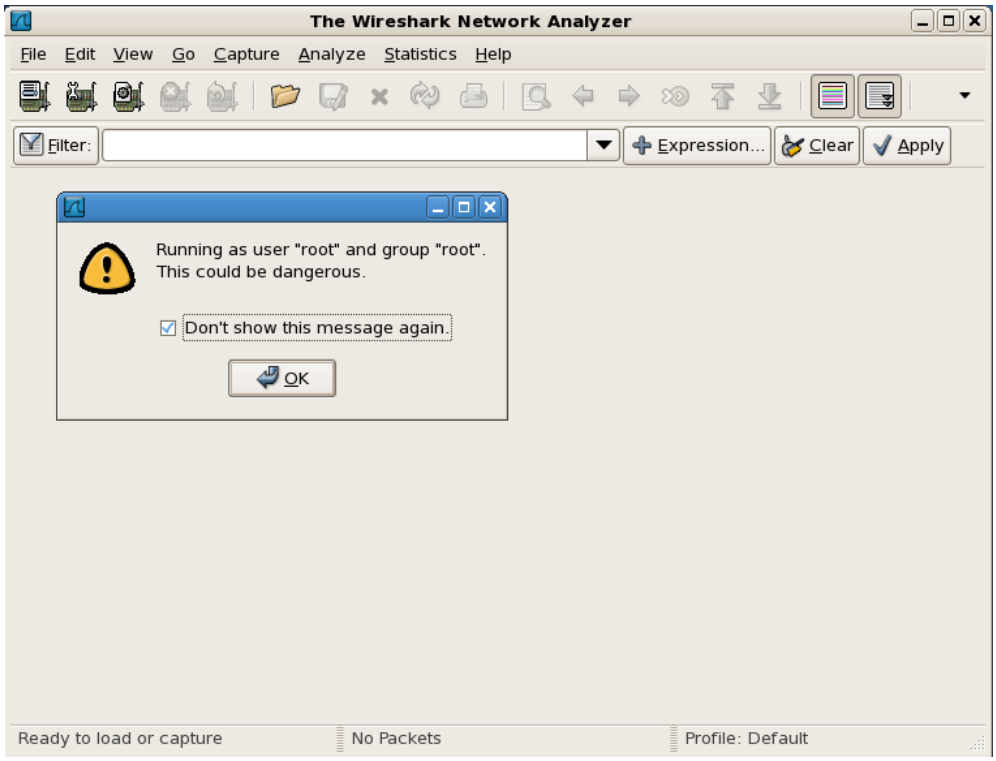


Figure 2: Running Wireshark

3. You can experiment with the settings and options of the program to familiarize yourself with it. Knowledge of packet analysis will be important in the upcoming exercise.
4. When you have finished, close Wireshark by clicking on the 'x' in the top right corner of the window.
5. If you are not performing any more administrative tasks on this machine, relinquish the elevated root privileges by typing the following command:

```
# exit
```

Mike High Level Description

Mike is a Linux System running three different services: ArpWatch, TCPDump, and Snort.

ArpWatch is a security application that will track the IP Address/MAC Address pairings on the User Network and report any changes via email and/or syslog to the Management Network. TCPDump is a network packet sniffer that will be configured to specially look for DHCP offer packets (excluding the DHCP server) and report this information via email to the Management Network. The purpose of these services is to prevent MAC/IP Spoofing and Man-in-the-Middle Attacks.

Following are descriptions of Mike's specific hands-on tasks that students must complete:

Task 1. Linux Host System Hardening

Students will be minimizing non-essential services (e.g., xinetd, portmap) as well as extraneous default users and groups. As a standalone system running TCPDump and ArpWatch, Mike does not require these components and so students will follow security best practices in removing them. Also, students will create a non-privileged administrator account to provide an audit trail for all administrative access.

Task 2. Configuring Time Synchronization

Network Time Protocol (NTP) is used to synchronize the host computer's time to a local time server, in this deployment it is the Internet firewall (Quebec).

Alpha will synchronize to Quebec every ten minutes; the Linux hosts will synchronize with Quebec every ten minutes; and the Window hosts will synchronize with Alpha every forty-five minutes until three good synchronizations occur, then once every eight hours. With all the hosts' time across the network synchronized, the cross examination of multiple hosts' logs, or the logs at the Syslog Server, become more meaningful and easier to examine.

Task 3. Configuring Bastille

The Bastille hardening system is a user-configurable script that attempts to lock down Linux/UNIX operating systems. The Bastille script embodies recommendations from every major reputable source on Linux/UNIX security. We will use pre-configured Bastille templates to lock down such weak system settings as maximum password age, user privileges, etc.

Task 4. Configuring IPTables

IPTables is a Linux firewall application, which can be configured to do packet filtering on network firewalls or on host systems. IPTables will be configured on this host as a host-based firewall to allow only valid packets to and from this host. To do this, we will set up INPUT and OUTPUT rules to specifically allow known-good packets into and out of the host, and we'll create default LOG rules and DROP rules.

Task 5. Hardening Apache

Nagios requires a web server for its monitoring interface. We will use the Apache web server. Like any other widely distributed software, Apache is vulnerable to attacks. The student will be stepped through the process of protecting Apache by configuring it to be more resistant to common attacks.

Task 6. Configuring ArpWatch

ArpWatch is a Linux/Unix based security application that tracks and monitors MAC/IP pairing for systems on the subnet, which it is deployed. ArpWatch has the capability to send reports either via email or Syslog.

Task 7. DHCP Packet Filter for TCPDump

TCPDump is a lightweight packet sniffer. In this deployment, TCPDump will be configured to filter on DHCP offer packets (excluding the recognized network DHCP Server) and report any captured DHCP offer packets via email to an administrator account (Eventwatch@AIA.Class)

Task 8. Installing and Configuring Snort

Snort will be configured to fit this network's particular needs. Students will be led through the steps to enable/disable rules and setup up the Snort configuration file.

Task 9. Nagios Network Monitoring

Nagios is a powerful free tool for network monitoring. Nagios itself is simply a monitoring framework; the actual monitoring is done by plug-ins. A wide variety of Nagios plug-ins are freely available and an active user base continues to contribute more. Nagios provides a web interface for checking host and service availability and it can also send notification emails proactively.

Task 10. Configuring OSSEC Agent

Students will install and configure the OSSEC Agent, which will then send information about security events to the syslog/OSSEC server (Foxtrot).

Task 11. Wireshark Network Protocol Analyzer

Students will install and configure Wireshark in order to do packet analysis.

Linux Host System Hardening

1 Remove Zeroconf Route

1. If you have not already done so, log on to the machine using:

   Username: **root** Password: **tartans@1**

2. Open a terminal window by going to ‘Applications’ -> ‘Accessories’ -> ‘Terminal’.

By default Linux adds a "zeroconf" route at boot time. This is a static route that designates the 169.254/16 prefix as local. This is unnecessary on our network, so we will remove the route:

3. Specify to not use zeroconf at boot time:

NOTE: In this and all subsequent Linux documents, the ‘#’ at the beginning of each line should *not* be typed in as part of the command. It is simply meant to represent a command prompt.

```
# echo "NOZEROCONF=yes" >> /etc/sysconfig/network
```

2 Linux Kernel Upgrade

One of the most essential hardening tasks for Linux systems is to ensure that the latest kernel version is being used. The kernel is the core of the operating system and every effort should be made to ensure the most current updated and/or patched version is in use. Most versions of Linux include some automated means for updating software, including the kernel. We will use a tool called YUM (Yellowdog Updater Modified) to download updates from an external web server hosting our YUM repository.

2.1 Apply latest updates to Kernel and other installed packages

1. Edit the yum config file using vi:

```
# vi /etc/yum.repos.d/CentOS-Base.repo
```

2. There are six sections of the file denoted by names in brackets. You will edit 3 of these sections and disable the other 3. Press `[Insert]` or `[i]` to edit the file and scroll down to the first section, ‘[base]’. Comment out the line beginning with ‘mirrorlist=’ by typing a # at the beginning of the line. Next, uncomment the line below it beginning with ‘baseurl=’ and edit the URL to point to our trusted yum repository at `http://192.168.30.14/centos/5.4/os/i386/`. The updated lines will be as follows:

```
[base]
name=CentOS-$releasever - Base
#mirrorlist=http://mirrorlist.centos.org/?release=$releasever&arch=$basearch&rep
o=os
baseurl=http://192.168.30.14/centos/5.4/os/i386/
gpgcheck=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-CentOS-5
```

Figure 1: Configuring YUM base repository

3. Repeat the above steps for the second section, '[updates]', pointing it to the URL `http://192.168.30.14/centos/5.4/updates/i386/`.

```
#released updates
[updates]
name=CentOS-$releasever - Updates
#mirrorlist=http://mirrorlist.centos.org/?release=$releasever&arch=$basearch&rep
o=updates
baseurl=http://192.168.30.14/centos/5.4/updates/i386/
gpgcheck=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-CentOS-5
```

Figure 2: Configuring YUM updates repository

4. Scroll down to the next section, '[addons]' and add `enabled=0` underneath the last line of the section to disable it. The updated lines will be as follows:

```
#packages used/produced in the build but not released
[addons]
name=CentOS-$releasever - Addons
mirrorlist=http://mirrorlist.centos.org/?release=$releasever&arch=$basearch&repo
=addons
#baseurl=http://mirror.centos.org/centos/$releasever/addons/$basearch/
gpgcheck=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-CentOS-5
enabled=0
```

Figure 3: Disabling YUM addons repository

5. Scroll down to the next section, '[extras]' and point it to the URL `http://192.168.30.14/centos/5.4/extras/i386/`.

```
#additional packages that may be useful
[extras]
name=CentOS-$releasever - Extras
#mirrorlist=http://mirrorlist.centos.org/?release=$releasever&arch=$basearch&rep
o=extras
baseurl=http://192.168.30.14/centos/5.4/extras/i386/
gpgcheck=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-CentOS-5
```

Figure 4: Configuring YUM extras repository

We will leave the remaining two sections at their default setting of disabled.

6. Press `[Esc]`, then type `:wq` and press `[Enter]` to save the changes and exit VI.
7. Add a variable to '/etc/yum.conf' so that all future updates use the HTTP proxy. Edit '/etc/yum.conf' with vi:

```
# vi /etc/yum.conf
```

8. To configure yum to use the web proxy server we need to add a line to the '/etc/yum.conf file'. Add the following line to the end of the '[main]' section of the file:

```
proxy=http://10.0.2.1:3128
```

```
[main]
cachedir=/var/cache/yum
keepcache=0
debuglevel=2
logfile=/var/log/yum.log
distroverpkg=redhat-release
tolerant=1
exactarch=1
obsoletes=1
gpgcheck=1
plugins=1
proxy=http://10.0.2.1:3128
```

Figure 5: Configuring YUM proxy server

Press `[Esc]` then type `:wq` and press `[Enter]` to save the changes and exit VI.

NOTE: In order to access the Internet, or even our trusted update server, routing will need to be enabled on Quebec and Romeo. Once the Access control lists are in place on these two router/firewall machines, very few devices will be able to access external networks directly. You may need to wait until these tasks are completed--check with your teammates on this.

9. Run yum in update mode:

```
# yum update
```

10. Type `y` then press `[Enter]` when prompted to download the updates.
11. Type `y` then press `[Enter]` when prompted to import the CentOS 5 GPG key.

A number of packages will be downloaded and installed, including a newer kernel.

This step may take several minutes to complete. Press `[Ctrl]` + `[Shift]` + `[T]` to open a new terminal tab if you want to move on to the next steps while the updates take place.

3 Service Minimization

3.1 Removing Unnecessary Services

By default Linux runs many services that a standalone server will not need. Extraneous services are dangerous because they provide possible attack vectors.

The services that will need to be removed from this system are:

- anacron
- apmd
- atd
- autofs
- cpuspeed
- cups
- gpm
- irqbalance
- mdmonitor
- mdmpd
- microcode_ctl
- netfs
- nfslock
- portmap
- rawdevices
- rpcgssd
- rpcsvcgssd
- rpcidmapd
- xinetd

1. Terminate the 'anacron' service properly by using the following command:

```
# service anacron stop
```

2. Remove the 'anacron' startup routine using the following command:

```
# chkconfig --del anacron
```

```
Stopping anacron:                                          [  OK  ]
```

Figure 6: Removing a service

3. Repeat steps #1 and #2 for each service listed above. (ADVANCED: see the 'Bash Script' ADDENDUM located on the last two pages of this section to automate these repetitive steps.)

   Note: On some systems, some of the services may not be started and may not return the 'OK' when stopped. If this is the case, it will be sufficient to simply delete the service.

4. To check that the appropriate services have been removed, use the following two commands from a terminal window:

```
# netstat –ntap | grep –i listen
```

```
tcp        0      0 127.0.0.1:25                0.0.0.0:*                   LIST
EN      3163/sendmail: acce
tcp        0      0 :::22                       :::*                        LIST
EN      3131/sshd
```

Figure 7: Confirming service removal

```
# chkconfig --list | grep on | sort
```

```
acpid           0:off   1:off   2:on    3:on    4:on    5:on    6:off
auditd          0:off   1:off   2:on    3:on    4:on    5:on    6:off
avahi-daemon    0:off   1:off   2:off   3:on    4:on    5:on    6:off
avahi-dnsconfd  0:off   1:off   2:off   3:off   4:off   5:off   6:off
conman          0:off   1:off   2:off   3:off   4:off   5:off   6:off
crond           0:off   1:off   2:on    3:on    4:on    5:on    6:off
firstboot       0:off   1:off   2:off   3:on    4:off   5:on    6:off
haldaemon       0:off   1:off   2:off   3:on    4:on    5:on    6:off
hidd            0:off   1:off   2:on    3:on    4:on    5:on    6:off
ip6tables       0:off   1:off   2:on    3:on    4:on    5:on    6:off
iptables        0:off   1:off   2:on    3:on    4:on    5:on    6:off
lvm2-monitor    0:off   1:on    2:on    3:on    4:on    5:on    6:off
mcstrans        0:off   1:off   2:on    3:on    4:on    5:on    6:off
messagebus      0:off   1:off   2:off   3:on    4:on    5:on    6:off
netconsole      0:off   1:off   2:off   3:off   4:off   5:off   6:off
network         0:off   1:off   2:on    3:on    4:on    5:on    6:off
pcscd           0:off   1:off   2:on    3:on    4:on    5:on    6:off
readahead_early 0:off   1:off   2:on    3:on    4:on    5:on    6:off
readahead_later 0:off   1:off   2:off   3:off   4:off   5:on    6:off
restorecond     0:off   1:off   2:on    3:on    4:on    5:on    6:off
sendmail        0:off   1:off   2:on    3:on    4:on    5:on    6:off
sshd            0:off   1:off   2:on    3:on    4:on    5:on    6:off
syslog          0:off   1:off   2:on    3:on    4:on    5:on    6:off
vmware-tools    0:off   1:off   2:on    3:on    4:off   5:on    6:off
wdaemon         0:off   1:off   2:off   3:off   4:off   5:off   6:off
xfs             0:off   1:off   2:on    3:on    4:on    5:on    6:off
```

Figure 8: Results of service removals

5. If your results are *similar* to the output shown above, the services have been removed successfully.

4 User / Group Account Minimization

It is important to disable all default vendor accounts that will be unused. Typically a default account, e.g., gopher or news, is created only when the respective service is also installed; however, many default accounts will exist even if you have not installed the related services on your system. In our case, we will not use many of the default accounts and so we will remove them. The more accounts you have, the easier it is for outsiders to access your system.

4.1 Remove Default User Accounts

The users we will need to remove are:

- adm
- ftp
- games
- gopher
- halt
- lp
- mail
- mailnull
- news
- nfsnobody
- nobody
- nscd
- operator
- rpcuser
- rpc
- shutdown
- uucp
- vcsa
- xfs

1. Remove the ‘adm’ user account using the following command:

```
# userdel adm
```

2. Repeat the previous step for each account listed above. Verify removal by executing the following command:

```
# cat /etc/passwd
```

```
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
distcache:x:94:94:Distcache:/:/sbin/nologin
webalizer:x:67:67:Webalizer:/var/www/usage:/sbin/nologin
dovecot:x:97:97:dovecot:/usr/libexec/dovecot:/sbin/nologin
squid:x:23:23::/var/spool/squid:/sbin/nologin
mysql:x:27:27:MySQL Server:/var/lib/mysql:/bin/bash
pcap:x:77:77::/var/arpwatch:/sbin/nologin
ntp:x:38:38::/etc/ntp:/sbin/nologin
dbus:x:81:81:System message bus:/:/sbin/nologin
avahi:x:70:70:Avahi daemon:/:/sbin/nologin
named:x:25:25:Named:/var/named:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
haldaemon:x:68:68:HAL daemon:/:/sbin/nologin
avahi-autoipd:x:100:102:avahi-autoipd:/var/lib/avahi-autoipd:/sbin/nologin
gdm:x:42:42::/var/gdm:/sbin/nologin
user:x:500:500:User:/home/user:/bin/bash
```

Figure 8 : Results of removing unnecessary default user accounts

3. If the default user accounts have been successfully removed, your /etc/passwd file will look *similar* to the output shown in the figure above.

4.2 Remove Default Groups

Now that we have removed all unnecessary accounts from the /etc/passwd file, we will clean up the /etc/groups file.

The groups that we will remove are:

- adm
- dip
- lock
- lp
- mail
- news
- uucp

Removing a group account is similar to the process of removing a user shown above.

1. Delete the ‘adm’ group using the following command:

```
# groupdel adm
```

2. Repeat the previous step for each group listed above.

3. Verify removal by executing the following command:

```
# cat /etc/group
```

```
root:x:0:root
bin:x:1:root,bin,daemon
daemon:x:2:root,bin,daemon
sys:x:3:root,bin
tty:x:5:
disk:x:6:root
mem:x:8:
kmem:x:9:
wheel:x:10:root
man:x:15:
users:x:100:
utmp:x:22:
utempter:x:35:
audio:x:63:gdm
distcache:x:94:
floppy:x:19:
webalizer:x:67:
dovecot:x:97:
squid:x:23:
mysql:x:27:
pcap:x:77:
slocate:x:21:
ntp:x:38:
ecryptfs:x:101:
dbus:x:81:
avahi:x:70:
named:x:25:
sshd:x:74:
haldaemon:x:68:
avahi-autoipd:x:102:
gdm:x:42:
user:x:500:
```

Figure 9: Results of removing unnecessary default groups

4. If the default groups have been successfully removed, the /etc/group file will look similar to the output shown in the figure above.

4.3 Create the 'Admin' User

The last account management task we will perform manually is to create an 'admin' user for daily administration tasks once the initial setup is complete.

1. Add the admin user using the following command:

```
# useradd admin
```

2. Set the password for the 'admin' account:

```
# passwd admin
```

3. When prompted for a password use the following: `steelers`

   The output will resemble that shown below:

```
Changing password for user admin.
New UNIX password:
BAD PASSWORD: it is based on a dictionary word
Retype new UNIX password:
passwd: all authentication tokens updated successfully.
```

Figure 10: Creating an Admin user

Note: In a real production environment you should always choose a strong password or passphrase that is sufficiently long and contains a combination of letters, numbers, and special characters. The above password is used for demonstration purposes only.

5 Installing ClamAV

1. Copy the ClamAV tarball from the course CD to the /root directory:

```
# cp /media/AISTS/Tools/Linux/ClamAV/clamav-0.96.1.tar.gz /root
```

2. Untar ClamAV:

```
# cd /root
# tar xvzf clamav-0.96.1.tar.gz
```

3. We need to install a few prerequisite packages before installing ClamAV. We will use our trusted yum repository that we set up earlier in this task to install zlib-devel. Additionally, in order to compile ClamAV and other tools in later tasks from source code we will need a compiler installed on the machine. This distribution of CentOS does not come with a compiler pre-installed so we will install the gcc compiler ourselves.

   Make sure to remove this compiler when all of this machine's tasks have been completed as it can be leveraged by an attacker to compile malicious code if they were to gain access to the system.

```
# yum install gcc zlib-devel
```

4. Type `y` then press `[Enter]` when prompted to confirm the download.
5. Change into the clamav-0.96.1 directory and install ClamAV:

```
# cd clamav-0.96.1
# adduser clamav
# ./configure --sysconfdir=/etc
# make
# make install
```

6. Use the VI editor to open the clamav.conf file in order to configure ClamAV:

```
# vi /etc/clamd.conf
```

7. Press `[Insert]` to enter edit mode. Comment out the line near the beginning of the file containing 'Example':

```
# Comment or remove the line below.
#Example
```

Figure 11: Editing clamd.conf

8. Find and uncomment the following lines by removing the '#' in front of them:
   a. 'LogFile /tmp/clamd.log'
   b. 'LogTime yes'
   c. 'LogSyslog yes'
   d. 'LocalSocket /tmp/clamd.socket'

9. Save and exit the file. Press `[Esc]` and type `:wq` then press `[Enter]`.

10. The ClamAV updater (freshclam) needs to be pointed to our internal proxy (10.0.2.1) in order to be able to update virus definitions. Use the VI editor to open the freshclam.conf file:

```
# vi /etc/freshclam.conf
```

11. Comment out the line near the beginning of the file containing 'Example':

```
# Comment or remove the line below.
#Example
```

Figure 12: Editing freshclam.conf

12. Find the proxy settings. Uncomment and make the following changes to indicate the IP of the proxy server and the port number to use:

```
HTTPProxyServer 10.0.2.1
HTTPProxyPort 3128
```

Note: Although freshclam has been configured, it probably won't successfully run yet. The Squid Proxy server may still need to be set up.

13. Save and exit the file. Press `[Esc]` and type `:wq` then press `[Enter]`.

14. Enable the ClamAV daemon to start automatically as a service:

```
# cp /media/AISTS/Tools/Linux/ClamAV/clamd /etc/init.d/
# chkconfig --add clamd
# service clamd start
```

15. Setup cron jobs for Virus definition updates and nightly virus scans:

```
# crontab –u root -e
```

16. Add the following two lines to the file:

```
15 2 * * * /usr/local/bin/freshclam --quiet
15 3 * * * /usr/local/bin/clamdscan --quiet /
```

17. Save and exit the cron file. Press `[Esc]` and type `:wq` then press `[Enter]`.

18. Remove ClamAV installation files (they contain test signatures that will be found on every scan if we don't remove them) then reboot the server.

```
# cd /root
# rm -rf clamav-0.96*
# reboot
```

ADDENDUM Bash Script: 'for loop'

Create a file containing the list of items

1. If you would like to automate the task of removing the unwanted services, users and groups, you can write a Bash script to loop through the list of items and process them one by one. First, start by creating a text file containing the list of items that you want to process. Enter the following command to create the text file:

```
# cat > deletedSvcList
```

2. After you typed the previous command and hit the `[Enter]` key, notice that there is no prompt ('#') at the cursor. The file is now open and you can enter the list of items that you want to process. Enter each item on a separate line, hitting the `[Enter]` key to move to the next line.

3. When all of the items have been entered into the file, press `[Ctrl+d]` to save and close the file. Notice that the prompt ('#') has returned to the shell.

Write the 'for loop'

1. Now we will create a 'for loop' that will read the items in the deletedSvcList file one by one and stop each service. Enter the following script as it appears below to stop the unwanted services:

```
# for str in $(cat deletedSvcList); do service $str stop; done
```

   A simple modification makes sure that those services do not start on bootup:

```
# for str in $(cat deletedSvcList); do chkconfig --del $str; done
```

2. Notice that the script is in three sections, separated by semi-colons (';'). The first section of this script creates a variable, named 'str', and assigns to it the first item in the file. The second section inserts the value of the variable, 'str', into the shell command. The command is executed and then the process is repeated for each item in the file. When there are no more items in the file, the third section of the script ends the process and returns control back to the shell.

   As you go through the steps, you will have to create three separate files for services, users and groups. Then you must modify the file name in the first section of the script. Likewise, you will have to modify the command in the second section to perform the action that you want.

Here are the files and scripts that should be created to remove the following items:

Users:

```
# cat > deletedUserList
```

```
# for str in $(cat deletedUserList); do userdel $str; done
```

Groups:

```
# cat > deletedGrpList
```

```
# for str in $(cat deletedGrpList); do groupdel $str; done
```

This page left intentionally blank for pagination purposes

Linux Network Time Protocol Daemon (ntpd) Client

1 Setup Linux ntpd Client Service

1.1 Installation

1. If you have not already done so, log on the console using:

   Username: **root** Password: **tartans@1**

2. Open a terminal window by going to 'Applications' -> 'Accessories' -> 'Terminal'.
3. The Network Time Protocol Daemon (ntpd) is installed with most Linux distributions. You will create a cron job that will cause the Linux ntpd to periodically query Quebec's ntp server and update the system time.

1.2 Configuration

1. Run the following command to see the current local system time. Hopefully, it is significantly different from the time server's system time as this will explicitly demonstrate when the client becomes synchronized with the server:

```
# date
```

2. If the date is not significantly different from the time server's system time, you can change the local client's system time manually by entering the following command (you can change the system date and time to whatever you want):

```
# date -s "Fri Sep 12 14:38:19 EDT 2003"
```

3. The ntp configuration file must be modified to tell it which time server to use to update the system time. This file is located in the '/etc' directory. To open the config file in the 'vi' text editor, enter:

```
# vi /etc/ntp.conf
```

4. In order to modify the file in the 'vi' editor, the `[Insert]` or `[i]` key must be pressed before trying to add or change text.

5. Scroll down to the section beginning with "# Use public servers" which is excerpted here:

```
# Use public servers from the pool.ntp.org project.
# Please consider joining the pool (http://www.pool.ntp.org/join.html).
server 0.centos.pool.ntp.org
server 1.centos.pool.ntp.org
server 2.centos.pool.ntp.org
```

Figure 1: Default NTP configuration file

Comment out the previous servers and add the following two lines at the end of this section:

```
restrict 10.0.2.1 mask 255.255.255.255 nomodify notrap noquery
server 10.0.2.1 prefer
```

Your section should look similar to the following:

```
# Use public servers from the pool.ntp.org project.
# Please consider joining the pool (http://www.pool.ntp.org/join.html).
#server 0.centos.pool.ntp.org
#server 1.centos.pool.ntp.org
#server 2.centos.pool.ntp.org
restrict 10.0.2.1 mask 255.255.255.255 nomodify notrap noquery
server 10.0.2.1 prefer
```

Figure 2: Edited NTP configuration file

6. Save and exit the file. Press `[Esc]` and type `:wq` then press `[Enter]`.

7. Now we need to cause ntpd to update to the ntp server time by modifying /etc/ntp/step-tickers to run ntpdate when ntpd is started. Do this by running these two commands:

```
# echo "10.0.2.1" > /etc/ntp/step-tickers
```

8. The 'step-tickers' file should now contain only the ntp server's IP address. The file contents can be viewed by entering this command:

```
# cat /etc/ntp/step-tickers
```

9. Enter the date command to see that the date is still incorrect.

10. If the ntpd service is not currently running, it must be started by entering the following command. If the service is currently running, replace 'start' with `restart`. NOTE: Once the service is running, always remember to 'restart' after making any changes to the ntp config file. Otherwise, the service will continue to run according to the previous config file settings until the service is restarted. Later, we will be creating a cron job to periodically restart the service. For now, enter this command:

```
# service ntpd start
```

11. You should see these two messages:

```
ntpd: Synchronizing with time server:                      [  OK  ]
Starting ntpd:                                             [  OK  ]
```

Figure 3: Starting the NTP service

12. Enter the date command again to see that the time has been synchronized.
    Note: This will only be successful after Quebec's time server has been configured properly. Check with your teammates for its status.

13. The service can be verified and the current pid identified by entering:

```
# service ntpd status
```

14. Now, we are going to make sure that ntpd updates the system time regularly. Skew the local system time again by entering the following command that you entered earlier (up arrow to find this command and press enter):

```
# date -s "Fri Sep 12 14:38:19 EDT 2003"
```

15. A cron job must be created to cause the ntpd service to periodically query the time server and update the local system time accordingly. Enter this command to create the cron job file:

```
# crontab –u root –e
```

16. This file should automatically open using the 'vi' text editor again, so you must press the `[Insert]` or `[i]` key before you can add or modify text.

17. Insert the following line at the top of the file to set up a cron job that will execute every 10 minutes. You can review the 'man 5 crontab' pages to understand the crontab fields in more depth after you are done with this task. After the ntpd is verified to be up and running correctly, the first set of numbers can be changed to a '0' to cause the cron job to run at the top of every hour (0th minute of every hour) instead.

    Make sure that there is a space after the 50 and between each '*' and the '/' character following them. There are no spaces between the initial set of numbers.

```
0,10,20,30,40,50 * * * * /etc/rc.d/init.d/ntpd restart
```

```
0,10,20,30,40,50 * * * * /etc/rc.d/init.d/ntpd restart
15 2 * * * /usr/local/bin/freshclam --quiet
15 3 * * * /usr/local/bin/clamdscan --quiet /
```

18. Now Save and exit the file. Press `[Esc]` and type `:wq` then press `[Enter]`.

19. Entering the following command will create init scripts at run levels 3-5 to start the ntpd service every time the system is started up.

```
# chkconfig --level 345 ntpd on
```

20. Use the following command to verify that the ntpd service is turned on at run levels 3, 4, and 5:

```
# chkconfig --list | grep ntpd
```

21. Make sure that it looks like this:

```
ntpd            0:off   1:off   2:off   3:on    4:on    5:on    6:off
```

Figure 4: NTP service startup run levels

22. Now, use the date command to see if the cron job has updated the system time. If not, wait a few more minutes and try again.

23. Once the remote centralized syslog server is installed and configured, we can review the logs that are generated from the Network Time Server process. There we will see each time that the client is updated and the offset amount by which it is updated.

Installing and Configuring Bastille-Linux

We have already done preliminary hardening (by removing users, groups, etc) and now we will use Bastille-Linux to finish the task. Bastille allows us to easily modify many OS settings. In this task, we will apply a previously configured Bastille template file (analogous to the NSA templates used on Windows) to our system.

1 Bastille Configuration

1.1 Install Bastille

1. If you have not already done so, log on to the machine using:

   Username: **root**
   Password: **tartans@1**

2. Open a terminal window by clicking on:
   'Applications' -> 'Accessories' -> 'Terminal'.

3. There are two modules that are required to implement Bastille:
   perl-Curses-1.12-1.2.el4.rf.i386.rpm
   Bastille-3.0.8-1.0.noarch.rpm

   Copy the required modules to the /root directory with this command:

```
# cp /media/AISTS/Tools/Linux/Bastille/* /root
```

4. Using the following commands, change to the /root directory and get a directory listing to confirm all of the Bastille files copied:

```
# cd /root
# ls –l
```

5. Install perl-Curses module:

```
# rpm –ivh perl-Curses-1.28-1.el5.rf.i386.rpm
```

6. Install Bastille module:

```
# rpm –ivh Bastille-3.0.9-1.0.noarch.rpm
```

1.2 Run Bastille

1. Copy Mike's Bastille template to the Bastille configuration directory (this command should be typed as one continuous line with a space after 'cp' and after 'bastille-sniffer-config'):

```
# cp /media/AISTS/Tools/Linux/Config_Files/Mike_10.0.3.2/bast
ille-sniffer-config /etc/Bastille/config
```

2. Run Bastille in batch mode to apply the preconfigured template:

```
# bastille –b –n 2>/dev/null
```

Note: The template generates error messages about the CentOS version, but the settings will be applied successfully. These messages are not important, and so in this command, we divert all error messages to /dev/null (the trash).

```
NOTE:    Entering Critical Code Execution.
         Bastille has disabled keyboard interrupts.


NOTE:    Bastille is scanning the system configuration...

NOTE:    Bastille is now locking down your system in accordance with your
         answers in the "config" file.  Please be patient as some modules
         may take a number of minutes, depending on the speed of your
         machine.
NOTE:    Executing Firewall Specific Configuration
NOTE:    Executing File Permissions Specific Configuration
NOTE:    Executing Account Security Specific Configuration
NOTE:    Executing Boot Security Specific Configuration
NOTE:    Executing Inetd Specific Configuration
NOTE:    Executing PAM Specific Configuration
NOTE:    Executing Logging Specific Configuration
NOTE:    Executing Daemon Specific Configuration
NOTE:    Executing Sendmail Specific Configuration
NOTE:    Executing Apache Specific Configuration
NOTE:    Executing FTP Specific Configuration
NOTE:    Executing Temporary Directory Specific Configuration
```

Figure 1: Bastille Output

2 Bastille Configuration

1. The template we applied has been previously configured as follows.
   Enter the following command to view the new Bastille security settings:

```
# cat /etc/Bastille/config | less
```

2. Now you can scroll up and down to view the entire file. When you are finished reviewing the file, press the 'q' key to quit viewing the file and return to the shell prompt.

3. After reviewing the config file, *reboot* the system by typing `reboot`. You will now have to login with the admin account that was created in the Linux Host System Hardening task. *Make sure that the admin account was created before rebooting the system or you will not be able to login.*

   You may need to reset the screen resolution to 1024x768 the first time you log on to the admin account. You can do this by going to 'System' -> 'Preferences' -> 'Screen Resolution'.

   The remaining sections of this document detail the previously configured template that we applied. **Note that you will *NOT* need to actually perform any tasks in the following sections; it is merely here for your edification**. After reviewing, you can move on to the next task.

2.1 File Permissions

- Disallow non-root access to ping, usernetctl, mount/umount, and at
- Disable the r-tools (rsh, rlogin, etc) which are troublesome due to their use of weak authentication.

```
# Q:  Would you like to set more restrictive permissions on the administration u
tilities? [N]
FilePermissions.generalperms_1_1="Y"

# Q:  Would you like to disable SUID status for mount/umount?
FilePermissions.suidmount="Y"

# Q:  Would you like to disable SUID status for ping? [Y]
FilePermissions.suidping="Y"

# Q:  Would you like to disable SUID status for at? [Y]
FilePermissions.suidat="Y"

# Q:  Would you like to disable the r-tools? [Y]
FilePermissions.suidrtool="Y"

# Q:  Would you like to disable SUID status for usernetctl? [Y]
FilePermissions.suidusernetctl="Y"
```

Figure 2: File Permissions

2.2 Account Security Settings

- Enforce password aging
- Restrict cron (scheduler) to the root user
- Disallow root from direct login. After we apply this template all administrators must login using the 'admin' account and then su to root.
- Set permissions on all user-created files so that the file is only readable by the user who created it.

```
# Q:  Should Bastille disable clear-text r-protocols that use IP-based authentic
ation? [Y]
AccountSecurity.protectrhost="Y"

# Q:  Would you like to enforce password aging? [Y]
AccountSecurity.passwdage="Y"

# Q:  Do you want to set the default umask? [Y]
AccountSecurity.umaskyn="Y"

# Q:  What umask would you like to set for users on the system? [077]
AccountSecurity.umask="077"

# Q:  Should we disallow root login on tty's 1-6? [N]
AccountSecurity.rootttylogins="Y"
```

Figure 3: Account Security Settings

2.3 Boot Security Settings

- Disable CTRL-ALT-DELETE rebooting so that a user must have a valid login and password to reboot the machine.
- Password protect single user mode to require the root password. Single user mode is equivalent to run level 1. You are granted root access, but networking is disabled.

```
# Q:  Would you like to password-protect the GRUB prompt? [N]
BootSecurity.protectgrub="N"

# Q:  Would you like to disable CTRL-ALT-DELETE rebooting? [N]
BootSecurity.secureinittab="Y"

# Q:  Would you like to password protect single-user mode? [Y]
BootSecurity.passsum="Y"
```

Figure 4: Boot Security Settings

2.4 Securing inetd and TCP Wrappers

- Disable telnet and ftp
- Create authorized use banners that will be displayed before the user can log in
- We do not set default deny on TCP wrappers in this configuration. Later on we will configure an IPtables firewall which will handle this for us.

```
# Q:  Would you like to set a default-deny on TCP Wrappers and xinetd? [N]
SecureInetd.tcpd_default_deny="N"

# Q:  Would you like to display "Authorized Use" messages at log-in time? [Y]
SecureInetd.banners="Y"

# Q:  Who is responsible for granting authorization to use this machine?
SecureInetd.owner="administrator@aia.class"
```

Figure 5: Securing inetd and TCP Wrappers

2.5 Configure PAM

- Set limits on resources. Users will only be allowed to start 150 concurrently running processes, and will be unable to open core system (kernel) files.
- Only allow admin to log in at the console

```
# Q:  Would you like to put limits on system resource usage? [N]
ConfigureMiscPAM.limitsconf="Y"

# Q:  Should we restrict console access to a small group of user accounts? [N]
ConfigureMiscPAM.consolelogin="Y"

# Q:  Which accounts should be able to login at console? [root]
ConfigureMiscPAM.consolelogin_accounts="admin"
```

Figure 6: PAM Settings

2.6 Logging Settings

- We will configure logging in a later module, therefore we will not configure logging through Bastille

```
# Q:  Would you like to set up process accounting? [N]
Logging.pacct="N"
```

Figure 7: Logging Settings

2.7 Sendmail Settings

- Sendmail will be used by arpwatch to send mail alerts so we will keep it enabled

```
# Q:  Do you want to stop sendmail from running in daemon mode? [Y]
Sendmail.sendmaildaemon="N"
```

Figure 8: Sendmail Settings

2.8 Miscellaneous Daemons

```
# Q:  Would you like to disable acpid and/or apmd? [Y]
MiscellaneousDaemons.apmd="Y"

# Q:  Would you like to disable GPM? [Y]
MiscellaneousDaemons.gpm="Y"

# Q:  Would you like to deactivate the HP OfficeJet (hpoj) script on this machin
e?
MiscellaneousDaemons.disable_hpoj="Y"

# Q:  Would you like to deactivate the ISDN script on this machine?
MiscellaneousDaemons.disable_isdn="Y"
```

Figure 9: Miscellaneous Deamons

2.9 Apache Web Server Settings

```
# Q:  Would you like to bind the Web server to listen only to the localhost? [N]
Apache.bindapachelocal="N"

# Q:  Would you like to bind the web server to a particular interface? [N]
Apache.bindapachenic="N"

# Q:  Would you like to deactivate the following of symbolic links? [Y]
Apache.symlink="N"
```

Figure 10: Apache Web Server Settings

2.10 Tempdir Scripts

- This system is not a multi-user system, and therefore we will not be very concerned with the temporary (shared) directories

```
# Q:  Would you like to install TMPDIR/TMP scripts? [N]
TMPDIR.tmpdir="N"
```

Figure 11: Tempdir Scripts

2.11 Packet Filtering Firewall

- We will configure a firewall in a later module, therefore we will not use Bastille's firewall configuration

```
# Q:  Would you like to run the packet filtering script? [N]
Firewall.ip_intro="N"
```

Figure 12: Packet Filtering Firewall

2.12 FTP Settings

```
# Q:  Would you like to disable anonymous download? [N]
FTP.anonftp="Y"

# Q:  Would you like to disable user privileges on the FTP daemon? [N]
FTP.userftp="Y"
```

Figure 13: FTP Settings

Configuring IPTables as a Host Based Firewall on Linux Systems

The host based firewall for Linux, iptables, can be configured by accessing the console directly or via SSH from a management workstation. Iptables has six pre-defined "chains" that are available with the ability to create user defined chains as well. The default chains are:

- INPUT
- OUTPUT
- INPUT
- FORWARD
- PREROUTING
- POSTROUTING

The table below lists various options that can be used when configuring iptables rules. Additional information is available by typing `iptables --help` at the Linux command line or by reviewing the iptables man page (type: `man iptables`).

--table -t	Description
filter	Default table. This is used if not specified
nat	Network address translation
mangle	Used for Quality Of Service (QOS) and preferential treatment
raw	Enables optimization. i.e. Ignore firewall state matching for port 80 for enhanced speed due to less processing. Requires kernel patch

Command (Use one)	Description
-A --append	Append rule to chain
-D --delete	Delete rule from chain
-I --insert	Insert rule at beginning or at specified sequence number in chain.
-R --replace	Replace rule
-F --flush	Flush all rules
-Z --zero	Zero byte counters in all chains
-L --list	List all rules. Add option --line-numbers for rule number.
-N --new-chain	Create new chain
-X --delete-chain	Delete user defined chain
-P --policy	Set default policy for a chain
-E --rename-chain	Rename a chain

Command Option	Description
-s --source	Source address of packet
-d --destination	Destination address of packet
-i --in-interface	Interface packet is arriving from
-o --out-interface	Interface packet is going to
-p --protocol	Protocol: °tcp --sport port[:port] --dport port[:port] --syn °udp °icmp °mac ...
-j --jump	Target to send packet to
-f --fragment	Fragment matching
-c --set-counters	Set packet/byte counter
-m tcp --match tcp	°--source-port port[:port] (port # or range ##) °--destination-port port[:port] °--tcp-flags
-m state --match state	--state °ESTABLISHED °RELATED °NEW °INVALID (Push content, not expected to recieve this packet.)

Defined Policies	Description
ACCEPT	Let packet through
DROP	Deny packet with no reply
REJECT	Deny packet and notify sender
RETURN	Handled by default targets
MARK	Used for error response. Use with option --reject-with type
MASQUERADE	Used with nat table and DHCP.
LOG	Log to file and specify message: °--log-level # °--log-prefix "prefix" °--log-tcp-sequence °--log-tcp-options °--log-ip-options
ULOG	Log to file and specify userpace logging messages
SNAT	Valid in PREROUTING chain. Used by nat.
REDIRECT	Used with nat table. Output.
DNAT	Valid in POSTROUTING chain. Output.
QUEUE	Pass packet to userspace.

Figure 1: IPtables Options

1 Creating Inbound and Outbound Filtering Rules

The filtering rules for this server will be set up to allow the following traffic into and out of the system:

Source Address	Destination Address	Proto	Source Ports	Destination Port	Direction	Purpose
10.0.4.0/24	10.0.3.2/32	ANY	ANY	ANY	Inbound	Management
127.0.0.1/32	127.0.0.1/32	*	*	*	Inbound	Loopback
Log All Denied						
10.0.3.2/32	10.0.1.0/24	ANY	ANY	ANY	Outbound	DMZ
10.0.3.2/32	10.0.2.0/24	ANY	ANY	ANY	Outbound	LAN
10.0.3.2/32	10.0.4.0/24	ANY	ANY	ANY	Outbound	Management
10.0.3.2/32	10.0.2.1/32	TCP	ANY	3128	Outbound	Squid Proxy
10.0.3.2/32	10.0.2.1/32	UDP	ANY	123	Outbound	NTP
10.0.3.2/32	192.168.30.13/32	ICMP	ANY	ANY	Outbound	ICMP-Quebec
10.0.3.2/32	10.0.3.1/32	ICMP	ANY	ANY	Outbound	ICMP-Romeo
127.0.0.1/32	127.0.0.1/32	*	*	*	Outbound	Loopback
Log All Denied						

1. If you have not already done so, log on to the machine using the newly enforced admin account:

   Username: **admin** Password: **steelers**

2. Open a terminal window by going to ‘Applications’ -> ‘Accessories’ -> ‘Terminal’.
3. Elevate to root level privileges by typing the following command and entering the root password **tartans@1**

```
# su -
```

4. Ensure iptables is stopped.

```
# service iptables stop
```

5. Clear all existing iptables rules.

```
# iptables --flush
```

6. Set the default policy for the FORWARD chain to DROP all packets.

```
# iptables –P FORWARD DROP
```

7. Create the iptables file that will be used to save firewall rules.

```
# iptables-save > /etc/sysconfig/iptables
# vi /etc/sysconfig/iptables
```

8. Remove the last two lines. Move the cursor to each line and press the [D] key twice. This will delete the current line in VI. The file should look like the following when completed:

```
# Generated by iptables-save v1.3.5 on Mon Jun 14 10:52:10 2010
*filter
:INPUT ACCEPT [5:420]
:FORWARD DROP [0:0]
:OUTPUT ACCEPT [5:420]
```

9. Add the remaining rules to the iptables file as listed below. Comments/remarks are identified with a '#' at the beginning of the line. These lines are used to identify what the rules beneath them are used for. Although they are not required, it is a good practice to describe the rules, their intent, who added the rule, and potentially the date on which the rule was added or modified. Use the cursor to go to the bottom of the file. Simultaneously press the [Shift] and [A] keys to append text to the end of the last line. Press [Enter] to add a new line. Enter the following lines:

```
# Allow all inbound traffic from the MGMT network
-A INPUT -s 10.0.4.0/24 -d 10.0.3.2/32 -i eth0 -j ACCEPT

# Allow all established connections
-A INPUT -i eth0 -m state --state ESTABLISHED,RELATED -j ACCEPT

# Allow all inbound traffic on the loopback interface
-A INPUT -i lo -p all -j ACCEPT

# Enable logging on INPUT chain
-A INPUT -j LOG --log-level 6

# Set the default INPUT policy to Drop
-P INPUT DROP
```

Figure 2: IPtables Input Rules

```
# Allow all outbound traffic to the DMZ network
-A OUTPUT -d 10.0.1.0/24 -o eth0 -p all -j ACCEPT

# Allow all outbound traffic to the Services network
-A OUTPUT -d 10.0.2.0/24 -o eth0 -p all -j ACCEPT

# Allow outbound web proxy traffic to Quebec
-A OUTPUT -d 10.0.2.1/32 -o eth0 -p tcp --dport 3128 -j ACCEPT

# Allow outbound NTP traffic to Quebec
-A OUTPUT -d 10.0.2.1/32 -o eth0 -p udp --dport 123 -j ACCEPT

# Allow all outbound traffic to the MGMT network
-A OUTPUT -d 10.0.4.0/24 -o eth0 -p all -j ACCEPT

# Allow outbound ICMP to Quebec eth2
-A OUTPUT -d 192.168.30.13 -o eth0 -p icmp -j ACCEPT

# Allow outbound ICMP to Romeo eth1
-A OUTPUT -d 10.0.3.1 -o eth0 -p icmp -j ACCEPT

# Allow all outbound traffic on the loopback interface
-A OUTPUT -o lo -p all -j ACCEPT

# Enable logging on OUTPUT chain
-A OUTPUT -j LOG --log-level 6

# Set the default OUTPUT policy to Drop
-P OUTPUT DROP

# Enable rule set
COMMIT
```

Figure 3: IPtables Output Rules

10. Save and exit the file. Press `[Esc]` and type `:wq` then press `[Enter]`.

1.1 Applying the firewall rules

1. Enter the following command to start the iptables firewall:

```
# service iptables start
```

2. If the service started successfully, you should see the following:

```
Flushing firewall rules:                                   [  OK  ]
Setting chains to policy ACCEPT: filter                    [  OK  ]
Unloading iptables modules:                                [  OK  ]
Applying iptables firewall rules:                          [  OK  ]
Loading additional iptables modules: ip_conntrack_netbios_n[  OK  ]
```

Figure 4: IPtables Successful Startup

1.2 Making the iptables file immutable

1. Since we do not want the iptables file to change for ANY reason after the rules have been built without intervention from the administrator, we will make this file immutable. To do this, we will issue the following command.

```
# chattr +i /etc/sysconfig/iptables
```

2. Relinquish the elevated root privileges by typing the following command:

```
# exit
```

This page left intentionally blank for pagination purposes

Installing and Hardening the Apache Web Server

1 Setup the Apache Web Server

1.1 Configure Apache

1. Entering the following command will create init scripts at run levels 2-5 to start the httpd (Apache) service every time the system is started up.

```
# chkconfig –-level 2345 httpd on
```

2. Use chkconfig to ensure that httpd is configured to be running on the correct run levels (2,3,4,5):

```
# chkconfig –-list | grep httpd
```

```
httpd           0:off   1:off   2:on    3:off   4:on    5:on    6:off
```

3. To help apache start, ensure that the server has an entry in its' host file. This will speed up the start process and allow httpd to start even if the configured DNS server is unavailable.

```
# vi /etc/hosts
```

4. Add the following host entry at the bottom of the file:

```
10.0.3.2        mike
```

5. Press [Esc] to exit edit mode and save and exit the file:

```
:wq
```

6. Open the Apache configuration file for editing:

```
# vi /etc/httpd/conf/httpd.conf
```

7. Change the 'ServerName' variable to 'ServerName mike.aia.class':

```
#
# ServerName gives the name and port that the server uses to identify itself.
# This can often be determined automatically, but we recommend you specify
# it explicitly to prevent problems during startup.
#
# If this is not set to valid DNS name for your host, server-generated
# redirections will not work.  See also the UseCanonicalName directive.
#
# If your host doesn't have a registered DNS name, enter its IP address here.
# You will have to access it by its address anyway, and this will make
# redirections work in a sensible way.
#
ServerName mike.aia.class
```

8. Press [Esc] to exit edit mode and save and exit the file:

```
:wq
```

9. Start the web server:

```
# service httpd start
```

10. Make sure that Apache is running:

```
# ps –eaf | grep httpd
```

If the output from the above command is similar to the output in the following screenshot, then Apache is up and running.

```
root     24946     1  0 11:59 ?        00:00:00 /usr/sbin/httpd
apache   24948 24946  0 11:59 ?        00:00:00 /usr/sbin/httpd
apache   24949 24946  0 11:59 ?        00:00:00 /usr/sbin/httpd
apache   24950 24946  0 11:59 ?        00:00:00 /usr/sbin/httpd
apache   24951 24946  0 11:59 ?        00:00:00 /usr/sbin/httpd
apache   24952 24946  0 11:59 ?        00:00:00 /usr/sbin/httpd
apache   24953 24946  0 11:59 ?        00:00:00 /usr/sbin/httpd
apache   24954 24946  0 11:59 ?        00:00:00 /usr/sbin/httpd
apache   24955 24946  0 11:59 ?        00:00:00 /usr/sbin/httpd
root     24982 24653  0 12:00 pts/1    00:00:00 grep httpd
```

2 Securing the Apache Web Server

Apache, like any other largely distributed software, is vulnerable to attack. In order to lessen the probability of an attack succeeding against Apache, we will harden the configuration of Apache.

2.1 Securing Apache with SSL

1. The first thing that needs to be done is to create our own SSL certificate with information pertaining to our network. Issue the following command:

```
# cd /root
# openssl req –new –out server.csr
```

When prompted, enter the passphrase **pirates**. Verify the passphrase by reentering it when asked. You will be asked to enter in information about your organization. We will leave most of these blank. In order to do this, a period must be entered to avoid having the default value filled in. Enter a period and press `[Enter]` for the following fields:

Country Name (2 letter code)
State or Province Name (full name)
Locality Name (ed, city)
Organizational Name (eg, company)
Organizational Unit Name (eg, section)

2. For the Common Name, enter in the IP address of Mike (10.0.3.2) and press `[Enter]`.
3. For the Email Address, enter `apache@MIKE` and press `[Enter]`.
4. Ignore the prompts for a ‘challenge password’ and ‘optional company name’ and just press `[Enter]` twice to pass through these.

```
Country Name (2 letter code) [GB]:.
State or Province Name (full name) [Berkshire]:.
Locality Name (eg, city) [Newbury]:.
Organization Name (eg, company) [My Company Ltd]:.
Organizational Unit Name (eg, section) []:.
Common Name (eg, your name or your server's hostname) []:10.0.3.2
Email Address []:apache@MIKE

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
[root@Mike ~]#
```

5. Next issue the following command to create a key:

```
# openssl rsa –in privkey.pem –out server.key
```

Enter the passphrase that was entered for the certificate creation (**pirates**) and press `[Enter]`.

```
[root@Mike ~]# openssl rsa -in privkey.pem -out server.key
Enter pass phrase for privkey.pem:
writing RSA key
[root@Mike ~]#
```

6. Now, generate the certificate by entering the following command:

```
# openssl x509 –in server.csr –out server.crt –req –signkey server.key –days 365
```

This creates the certificate that has been signed and is good for 365 days. Note that this certificate has been signed by MIKE, which is enough for an internal network. However, if this was going to be used as a public web server, then we would want to get the certificate signed by a valid certificate authority such as Verisign.

```
[root@Mike ~]# openssl x509 -in server.csr -out server.crt -req -signkey server.
key -days 365
Signature ok
subject=/CN=10.0.3.2/emailAddress=apache@MIKE
Getting Private key
[root@Mike ~]#
```

7. Copy the generated files so that Apache knows where they are:

```
# mkdir /etc/httpd/conf/ssl.csr/
# mkdir /etc/httpd/conf/ssl.key/
# mkdir /etc/httpd/conf/ssl.crt/
# mv –f server.csr /etc/httpd/conf/ssl.csr/
# mv –f server.key /etc/httpd/conf/ssl.key/
# mv –f server.crt /etc/httpd/conf/ssl.crt/
```

8. Restart the web server:

```
# service httpd restart
```

2.2 Verifying Correct Configuration

1. On a management workstation, open Internet Explorer, and connect to the default Apache web page by typing the following URL: `https://10.0.3.2`
2. If the following message appears, click 'Yes'.

Figure 1: Security Alert

3. After clicking 'Yes' you should be at the default Apache web page – with 'https://10.0.3.2' in the browser Address window.

2.3 Change permissions of root directory and configuration files

1. Return to the MIKE system command line interface.
2. Change the ownership/permissions of the HTML document root to be owned by the apache user and group and use the ls –l command to ensure that the changes were successful. We want the entire directory structure to have rwx (7) permissions for the apache user and group and rx (5) permissions for everyone else:

```
# chown –R apache.apache /var/www/html
# chmod –R 775 /var/www/html
# ls –l /var/www/ | grep html
```

```
[root@Mike ~]# chown -R apache.apache /var/www/html
[root@Mike ~]# chmod -R 775 /var/www/html
[root@Mike ~]# ls -l /var/www/ | grep html
drwxrwxr-x  2 apache    apache 4096 Mar 27 13:56 html
[root@Mike ~]#
```

3. Change the ownership/permissions of the Apache configuration directory to be owned by the *root* user and *apache* group and use the ls –l command to ensure that the changes were successful. We want the entire directory structure to have rwx (7) permissions for the root user and the apache group, but no permissions at all for anyone else:

```
# chown –R root.apache /etc/httpd
# chmod –R 770 /etc/httpd
# ls –l /etc | grep httpd
```

```
[root@Mike ~]# chown -R root.apache /etc/httpd
[root@Mike ~]# chmod -R 770 /etc/httpd
[root@Mike ~]# ls -l /etc | grep httpd
drwxrwx---  4 root apache   4096 Jun 11 10:52 httpd
[root@Mike ~]#
```

Configuring Arpwatch

1 Install Arpwatch

1. If you have not already done so, log on to the machine using the newly enforced admin account:

   Username: **admin** Password: **steelers**

2. Open a terminal window by going to ‘Applications’ -> ‘Accessories’ -> ‘Terminal’.
3. Elevate to root level privileges by typing the following command and entering the root password **tartans@1**

```
# su -
```

4. Use the trusted yum repository to install arpwatch:

```
# yum install arpwatch
```

5. Type `y` and press `[Enter]` if asked to confirm the download or import the GPG key.

```
Installing:
 arpwatch          i386          14:2.1a13-21.el5           base          209 k

Transaction Summary
================================================================================
Install      1 Package(s)
Update       0 Package(s)
Remove       0 Package(s)

Total download size: 209 k
Is this ok [y/N]: y
Downloading Packages:
arpwatch-2.1a13-21.el5.i386.rpm                          | 209 kB     00:00
Running rpm_check_debug
Running Transaction Test
Finished Transaction Test
Transaction Test Succeeded
Running Transaction
  Installing     : arpwatch                                                 1/1

Installed:
  arpwatch.i386 14:2.1a13-21.el5

Complete!
```

Figure 1: Installing Arpwatch

2 Configuring and Running Arpwatch

2.1 Configuring Arpwatch

1. Edit the configuration file for Arpwatch with the VI editor. To do this, enter the following command:

```
# vi /etc/sysconfig/arpwatch
```

When the arpwatch command is entered, the configuration settings from this file will be used to start the application. The user needs to change to root and since the mail from arpwatch needs to go to the eventwatch@aia.class mailbox, it also needs to be set up in this configuration file as well.

2. Press the [Insert] key and edit the user after the –u tag and address after the –e tag on the OPTIONS line to be root and eventwatch@aia.class, respectively and leave the remainder of the settings the same in the /etc/sysconfig/arpwatch file. See Figure 2.

```
# -u <username> : defines with what user id arpwatch should run
# -e <email>    : the <email> where to send the reports
# -s <from>     : the <from>-address
OPTIONS="-u root -e eventwatch@aia.class -s 'root (Arpwatch)'"
```

Figure 2: Arpwatch configuration file

3. Save this file and exit. Press [Esc] and enter:

```
# :wq
```

4. To ensure that the arpwatch daemon will be started when the system is booted, the chkconfig for arpwatch needs to be on at the right levels (run level 3). To do this, enter the following command:

```
#  chkconfig –-level 2345 arpwatch on
```

5. To ensure that arpwatch will start when the system is booted, enter the following command and make sure levels 2, 3, 4, and 5 are set to on:

```
# chkconfig --list | grep arpwatch
```

The output of the commands should like similar to this:

```
[root@Mike ~]# chkconfig --list | grep arpwatch
arpwatch        0:off   1:off   2:on    3:on    4:on    5:on    6:off
```

Figure 3: Checking Arpwatch at run level 3

2.2 Running Arpwatch

1. To start the Arpwatch daemon, simply type the following command:

```
# arpwatch
```

2. To ensure that the arpwatch daemon is running, enter the following command:

```
# ps –eaf | grep arpwatch
```

The output should look similar this:

```
[root@Mike ~]# arpwatch
[root@Mike ~]# ps -eaf | grep arpwatch
root     18469     1  0 15:51 ?        00:00:00 arpwatch
root     18471 18273  0 15:52 pts/1    00:00:00 grep arpwatch
```

Figure 4: Checking the arpwatch process

3. Restart Arpwatch

```
# service arpwatch restart
```

As new stations are brought into the network, mail will be sent from arpwatch to eventwatch@aia.class - and should arrive at that mailbox within minutes of arpwatch being started.

4. If you are not performing any more administrative tasks on this machine, relinquish the elevated root privileges by typing the following command:

```
# exit
```

This page left intentionally blank for pagination purposes

Creating the DHCP Offer Packet Filter for tcpdump

1 Creating the tcpdump filter

1.1 Writing the tcpdump filter command

1. If you have not already done so, log on to the machine using the newly enforced admin account:

   Username: **admin** Password: **steelers**

2. Open a terminal window by going to 'Applications' -> 'Accessories' -> 'Terminal'.
3. Elevate to root level privileges by typing the following command and entering the root password **tartans@1**

```
# su -
```

4. The command for tcpdump needs to use the following switches and filters:
   a. x – print each packet in hexadecimal
   b. l – make standard out buffered (to increase readability)
   c. n – don't convert hostnames via DNS
   d. s – set the length of packet capture (default is 68 bytes) – we want to use 1500 to capture the entire Ethernet frame
   e. i – listen on specified interface (eth0 in this case)
   f. udp src 67 – to filter and display only packets which have a UDP source port of 67
   g. not src 10.0.3.1 – this filters out packets from 10.0.3.1 (the real DHCP server) and shows only DHCP offer and DHCP ACK packets from other hosts
   h. >> filename.file – redirects the output to a file named filename.file (we'll use /root/dhcprogue.list)

5. To put the complete command together, enter the following to get tcpdump running with all the above switches and filters each time your system boots. (**NOTE**: each of the following commands should be entered as single continuous lines in your terminal window. They appear as multiple lines in the text boxes due to space limitations.):

```
# echo "tcpdump –xlns 1500 –i eth0 udp src port 67 and not src
10.0.3.1 >> /root/dhcprogue.list&" >> /etc/rc.d/rc.local
```

6. To start tcpdump immediately, enter the command again without the echo and without everything after the closing quotes (").

```
# tcpdump –xlns 1500 –i eth0 udp src port 67 and not src
10.0.3.1 >> /root/dhcprogue.list&
```

7. To check to ensure that tcpdump is running enter the following command:

```
# ps –eaf | grep tcpdump
```

The output should look similar to this:

```
[root@Mike ~]# ps -eaf | grep tcpdump
pcap     18586 18273  0 15:55 pts/1    00:00:00 tcpdump -xlns 1500 -i eth0 udp s
rc port 67 and not src 10.0.3.1
root     18601 18273  0 15:55 pts/1    00:00:00 grep tcpdump
```

Figure 1: Verifying that tcpdump is running

2 Creating a cron job to review the contents of /root/dhcprogue.list

2.1 Writing a perl script to check the size of the /root/dhcprogue.list file

We will now copy a perl script from the course CD which will review the number of lines in a specified file (/root/dhcprogue.list in this case) and will send mail if the file is not 0 lines long.

1. Copy perl script to the root directory:

```
# cp
/media/AISTS/Tools/Linux/Config_Files/Mike_10.0.3.2/checkit.pl
/root
```

2. The perl script will check the contents of the /root/dhcprogue.list and can be reviewed below.

```
$count = `wc -l < /root/dhcprogue.list`;
die "wc failed: $?" if $?;
chomp($count);

if ($count != 0) {
print ($count);
open(SENDMAIL, "|/usr/sbin/sendmail -oi -t")
                or die "can't fork for sendmail: $!\n";
print SENDMAIL <<"EOF";
From: DHCP Offer Filter <root\@Mike.aia.class>
To: Event Watch <eventwatch\@aia.class>
Subject: DHCP Offer Filter Alert!

The /root/dhcprogue.list file is not 0 bytes - better check it
out!
EOF
close(SENDMAIL)         or warn "sendmail didn't close
nicely";
}
```

3. Change to the /root directory:

```
# cd /root
```

4. Test this script by running it with the following command:

```
# perl /root/checkit.pl
```

There should be no output from the file – and no mail should be sent.

5. Further test the script by entering some text into the /root/dhcprogue.list file by entering the following command:

```
# echo 1111 >> /root/dhcprogue.list
```

6. Run the perl script again (same command as from step 4 above)

7. The output from the script should be a 1 near the command line and a mail sent to eventwatch@aia.class - check that mailbox to ensure sendmail sent the message correctly

8. Remove the contents of the /root/dhcprogue.list file by entering the following commands:

```
# rm –f /root/dhcprogue.list
# touch /root/dhcprogue.list
```

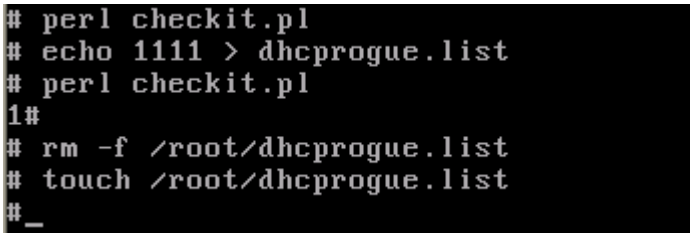


Figure 2: Testing the perl script

2.2 Creating a cron job

The cron job we will create will check the contents of the /root/dhcprogue.list file and alert the administrator if the file has any data.

1. First, we want to eliminate the mail messages which cron will create each time the cron job is run. To do this, open the /etc/crontab file with an editor. Enter the following command:

```
# vi /etc/crontab
```

2. Press the `[Insert]` key and change ‘MAILTO=root’ to ‘MAILTO=/dev/null’

3. Save and exit the vi session (`[ESC] :wq [Enter]`)

4. Enter this command to modify the existing scheduled jobs for the root user:

```
# crontab –u root –e
```

1. This file should automatically open using the ‘vi’ text editor again.
   Enter the following command at the bottom of the file to set up a cron job that will execute every 15 minutes:

```
0,15,30,45 * * * * perl /root/checkit.pl
```

2. Press the `[Enter]` key at the end of the line to make sure that there is a blank line at the bottom of the file.

3. Now to save and close the file, press the `[Esc]` key and the following command:

```
:wq
```

4. If you are not performing any more administrative tasks on this machine, relinquish the elevated root privileges by typing the following command:

```
# exit
```

Installing and Configuring Snort

1 Snort Installation and Configuration

The Snort Intrusion Detection System can be a powerful tool to help in protecting a network. We will be installing Snort, along with other modules that Snort requires.

1.1 Installation

Snort can log in a variety of different formats, including a few different database formats and flat text. We will be installing Snort to log to a MySQL database.

There are several prerequisites that must be installed for Snort to run. Snort uses libpcap to capture packets from the ethernet interface. There are also a number of other packages we need to install in order to configure Snort to send our alerts to the central MySQL console.

Additionally, in order to compile Snort from its source code we will need a compiler installed on the machine. This distribution of CentOS does not come with a compiler pre-installed so we will install the gcc compiler ourselves. We will make sure to remove this compiler when we are done with it as it can be leveraged by an attacker to compile malicious code if they were to gain access to the system.

1. If you have not already done so, log on to the machine using the newly enforced admin account:

   Username: **admin** Password: **steelers**

2. Open a terminal window by going to 'Applications' -> 'Accessories' -> 'Terminal'.
3. Elevate to root level privileges by typing the following command and entering the root password **tartans@1**

```
# su -
```

4. Download and install these prerequisites from the trusted repository that was set up in the Linux Host System Hardening step by executing the following command:

```
# yum install mysql-server mysql-bench mysql-devel libpcap
libpcap-devel pcre-devel
```

5. Type y [Enter] if prompted to download the packages.
6. Type y [Enter] if prompted to import the GPG key.
7. There are several files that we will need to implement Snort:

   snort-2.8.6.tar.gz
   snortd
   snortrules-aists.tar.gz

Copy the required files to the /root directory with this command:

```
# cp /media/AISTS/Tools/Linux/Snort/* /root
```

8. Setup folders that we will use for Snort:

```
# mkdir /var/log/snort
# mkdir /etc/snort
```

9. Untar the Snort installation file and cd into the new directory:

```
# tar xvzf snort-2.8.6.tar.gz
# cd snort-2.8.6
```

10. Configure the installation to have Snort be compatible with MySQL, compile the code, then install the files to their final location:

```
# ./configure --with-mysql --enable-zlib
# make
# make install
```

11. Install the rules and configuration files:

```
# cd /root
# cp ./snortrules-aists.tar.gz /etc/snort
# cd /etc/snort
# tar xvzf snortrules-aists.tar.gz
# rm -f snortrules-aists.tar.gz
# cp etc/* .
# rm -rf etc
```

12. Copy the Snort startup script into the '/etc/rc.d/init.d' directory:

```
# cp /root/snortd /etc/rc.d/init.d
```

13. Configure Snort to start when the machine is booted:

```
# cd /etc/rc.d/init.d
# chmod 755 snortd
# chkconfig --level 2345 snortd on
```

14. Use chkconfig to ensure that snort is configured to start at the correct run levels (2,3,4,5):

```
# chkconfig --list | grep snortd
```

```
[root@Mike init.d]# chmod 755 snortd
[root@Mike init.d]# chkconfig --level 2345 snortd on
[root@Mike init.d]# chkconfig --list | grep snortd
snortd          0:off   1:off   2:on    3:on    4:on    5:on    6:off
```

15. The snortd file needs to be edited to ensure that snort starts after MySQL has started on bootup. Use VI to edit the snortd file:

```
# vi /etc/rc.d/init.d/snortd
```

16. During the boot, MySQL is started first, but does not complete before Snort is started, so Snort fails to start. We need to make sure that Snort is set to wait extra time before it runs. Verify that the following line has been added to the snortd file right below the line labeled “start)”:

```
sleep 3
```

This causes the Snort startup script to wait 3 seconds before continuing to run the script. It should look like the figure below:

```
# Source function library.
. /etc/rc.d/init.d/functions

# Specify your network interface here
INTERFACE=eth0

# See how we were called.
case "$1" in
  start)
        sleep 3
        echo -n "Starting snort: "
        daemon /usr/local/bin/snort -d -D \
                -c /etc/snort/snort.conf
        touch /var/lock/subsys/snort
        echo
        ;;
  stop)
        echo -n "Stopping snort: "
        killproc snort
        rm -f /var/lock/subsys/snort
        echo
        ;;
  restart)
```

17. To save and exit the VI editor, press `[ESC] :wq [Enter]`

1.2 Configuration

1. Edit the snort configuration file

```
# vi /etc/snort/snort.conf
```

2. Scroll down to the section titled ‘Step #1: Set the network variables’. This is where we will tell Snort the layout of our network and the location of the rules that we just installed. Change the following lines, making sure to include the brackets ‘[‘ and ‘]’ where shown when entering the info:

   var HOME_NET [10.0.3.0/24]
   var EXTERNAL_NET !$HOME_NET
   var DNS_SERVERS [10.0.2.4/32]
   var SMTP_SERVERS [10.0.2.3/32]
   var HTTP_SERVERS [10.0.1.5/32,10.0.2.3/32,10.0.2.6/32]
   var SQL_SERVERS [10.0.2.10/32]
   portvar HTTP_PORTS [80]
   portvar SHELLCODE_PORTS !$HTTP_PORTS
   var RULE_PATH /etc/snort/rules
   var SO_RULE_PATH /etc/snort/so_rules
   var PREPROC_RULE_PATH /etc/snort/preproc_rules

   Note: When entering in the IP addresses, be sure <u>not</u> to include any spaces or carriage returns.

3. Scroll down to the section titled 'Step #5: Configure preprocessors'. We are going remove the small_segments directive in the Snort stream5_tcp preprocessor because it causes a large number of false positive alerts when new sensors are turned on. Find the line beginning with 'preprocessor stream5_tcp:' and remove the 'small_sements 3 bytes 150,' text from the line. The result should look like the following:

```
preprocessor stream5_tcp: policy windows, detect_anomalies, require_3whs 180, \
   overlap_limit 10, timeout 180, \
    ports client 21 22 23 25 42 53 79 109 110 111 113 119 135 136 137 139 143 \
        161 445 513 514 587 593 691 1433 1521 2100 3306 6665 6666 6667 6668 6669
 \
```

4. Next find the 'Portscan detection' heading in this section and enable portscan detection by removing the '#' in front of the line beginning with 'preprocessor sfportscan' and set the 'sense_level' to `medium`.

5. Add a new 'ignore_scanners' directive to not alert us of portscan traffic coming from hosts on our network that are known to cause false positives of such alerts:

```
# Portscan detection.  For more information, see README.sfportscan
preprocessor sfportscan: proto  { all } memcap { 10000000 } sense_level { medium
 } \
ignore_scanners { 10.0.3.2/32 }
```

6. Scroll down to the section titled 'Step #6: Configure output plugins'. We will be configuring Snort to log to our MySQL database. Find the section beginning with '#database' and edit the first 'output database' line to look like the following:

```
# database
output database: alert, mysql, user=snort password=snortpw dbname=snort host=10.
0.4.4 port=3306 sensor_name=mike
# output database: log, <db_type>, user=<username> password=<password> test dbna
me=<name> host=<hostname>
```

1.3 Rules

There are many rules that are enabled by default when Snort is initially installed. Many of these may or may not be necessary depending on your particular network configuration. We will be disabling some unnecessary rules. The reason that we do this is that the more rules that are active, the more that Snort has to parse for each packet that is scanned.

1. We do not need all of the rule sets since the User network does not have many of the services that Snort is looking for exploits for. For example, there is no Oracle database, and telnet should be disabled on all hosts. Scroll down to the 'Step #7: Customize your rule set' section of the config file. Disable all rule sets by placing '#' at the beginning of each rule line, except for the following rules which we will leave enabled:

```
include $RULE_PATH/chat.rules
include $RULE_PATH/exploit.rules
include $RULE_PATH/icmp.rules
include $RULE_PATH/policy.rules
```

Scroll down to the 'Step #9: Customize your Shared Object Snort Rules' section of the config file. Enable the following rule sets by removing the '#' at the beginning of each of the following rule lines:

```
include $SO_RULE_PATH/chat.rules
include $SO_RULE_PATH/exploit.rules
include $SO_RULE_PATH/icmp.rules
```

2. Press `[Esc]` to stop editing and then save and exit the file:

```
:wq
```

3. Install pre-compiled shared object rules:

```
# mkdir /usr/local/lib/snort_dynamicrules
# cp /etc/snort/so_rules/precompiled/Centos-5-4/i386/2.8.6.0/* /usr/local/lib/snort_dynamicrules/
# snort -c /etc/snort/snort.conf --dump-dynamic-rules=/etc/snort/so_rules
```

```
  Finished Loading all dynamic preprocessor libs from /usr/local/lib/snort_dynam
icpreprocessor/
Dumping dynamic rules...
Dumping dynamic rules for Library icmp 1.0.1
Dumping dynamic rules for Library misc 1.0.1
Dumping dynamic rules for Library imap 1.0.1
Dumping dynamic rules for Library web-activex 1.0.1
Dumping dynamic rules for Library exploit 1.0.1
Dumping dynamic rules for Library chat 1.0.1
Dumping dynamic rules for Library bad-traffic 1.0.1
Dumping dynamic rules for Library multimedia 1.0.1
Dumping dynamic rules for Library smtp 1.0.1
Dumping dynamic rules for Library nntp 1.0.1
Dumping dynamic rules for Library web-misc 1.0.1
Dumping dynamic rules for Library web-client 1.0.1
Dumping dynamic rules for Library netbios 1.0.1
Dumping dynamic rules for Library dos 1.0.1
Dumping dynamic rules for Library web-iis 1.0.1
Dumping dynamic rules for Library sql 1.0.1
Dumping dynamic rules for Library p2p 1.0.1
  Finished dumping dynamic rules.
Snort exiting
```

4. Start the snort service:

```
# service snortd start
```

5. Make sure that Snort has started successfully:

```
# ps -ef | grep snort
```

If the output of the above command looks similar to the following, Snort has successful started:

```
root     29737     1  0 09:53 ?        00:00:00 /usr/local/bin/snort -d -D -c /e
tc/snort/snort.conf
root     29740  4259  0 09:54 pts/1    00:00:00 grep snort
```

6. If Snort did not start successfully, look at the syslog messages file to search for Snort entries:

```
# tail -100 /var/log/messages | grep snort
```

7. If you are not performing any more administrative tasks on this machine, relinquish the elevated root privileges by typing the following command:

```
# exit
```

Nagios Network Monitoring

1 Installing Nagios

Nagios is a network monitoring framework. All monitoring functionality is left to plug-ins, which are separate from the main Nagios installation. Fortunately, a set of default plug-ins is available from the Nagios website, and these have all the monitoring functionality we will need.

1. If you have not already done so, log on to the machine using the newly enforced admin account:

   Username: **admin** Password: **steelers**

2. Open a terminal window by going to 'Applications' -> 'Accessories' -> 'Terminal'.
3. Elevate to root level privileges by typing the following command and entering the root password **tartans@1**

```
# su -
```

4. The following files are required:

   nagios-3.0.tar.gz

   nagios-plugins-1.4.11.tar.gz

   Copy the required modules to the root directory with the command:

```
# cp /media/AISTS/Tools/Linux/Nagios/* /root
```

5. Get a directory listing of the /root directory to ensure all of the files were copied there with the following command:

```
# ls –l /root
```

6. Switch into the root directory (if you are not already there):

```
# cd /root
```

7. Create a user for Nagios to run as:

```
# useradd nagios
```

8. Create the nagcmd group to support external commands through the web interface:

```
# groupadd nagcmd
# usermod –G nagcmd nagios
# usermod –G nagcmd apache
```

9. Install Nagios with the following series of commands (tar unpackages and then unzips the zipped tarball – which is a set of files packaged together). Install the main program, CGIs, and HTML files::

```
# tar zxvf nagios-3.2.1.tar.gz
# cd nagios-3.2.1
# ./configure --with-command-group=nagcmd
# make all
# make install
```

10. Install the init script in /etc/rc.d/inid.d:

```
# make install-init
```

11. Install the sample configuration files:

```
# make install-config
```

12. Copy over the pre-configured Nagios configuration files. Appendix – Configuring Nagios details the steps taken to update these files. To speed the installation process the finished configurations are provided on the Tools CD. Type the following command on a single line:

```
# cp –R
/media/AISTS/Tools/Linux/Config_Files/Mike_10.0.3.2/Nagios/etc/*
/usr/local/nagios/etc/
```

Confirm any requests to overwrite the current files by pressing `y` and then `[Enter]`.

13. Give the Nagios user access privileges to the nagios directories.

```
# make install-commandmode
```

14. Enable Nagios to run at boot-time:

```
# chkconfig --add nagios
```

15. Install the Nagios plug-ins with the following series of commands:

```
# cd /root
# tar zxvf nagios-plugins-1.4.14.tar.gz
# cd nagios-plugins-1.4.14
# ./configure --with-nagios-user=nagios --with-nagios-
group=nagios –disable-redhat-pthread-workaround
# make all
# make install
```

16. Give the Nagios user access privileges to ping and ntpdate (Bastille has limited access to these programs so only root can use them. Note: we are only giving Nagios access--all other users besides root are still prevented from running these programs). Next verify the settings are correct:

```
# chgrp nagios /bin/ping
# chmod u+s /bin/ping
# chgrp nagios /usr/sbin/ntpdate
# ls -l /bin/ping /usr/sbin/ntpdate
```

The output should be similar to the following:

```
[root@Mike nagios-plugins-1.4.14]# ls -l /bin/ping /usr/sbin/ntpdate
-rwsr-xr-x 1 root nagios 35832 Sep 26  2009 /bin/ping
-rwxr-xr-x 1 root nagios 63436 Dec 18 19:58 /usr/sbin/ntpdate
```

2 Configuring Apache

Nagios uses a web interface to report monitoring information, and therefore requires a web server to be configured. Nagios requires two virtual directories on the web server—one for CGI programs and one for static content. We will require basic authentication on each of these directories.

1. Edit the httpd.conf file with VI to add the virtual directories:

```
# vi /etc/httpd/conf/httpd.conf
```

2. Press [Esc] and then [Shift]+[G] to move to the end of the file.

3. Press [O] to add a new line and enter insert mode. Add the following lines to the file to create a scripts virtual directory:

```
ScriptAlias /nagios/cgi-bin /usr/local/nagios/sbin/
<Directory "/usr/local/nagios/sbin/">
 Options ExecCGI
 AuthName "Nagios Access"
 AuthType "Basic"
 AuthUserFile /usr/local/nagios/etc/htpasswd.users
 require valid-user
 Satisfy all
 allow from 10.0.4.0/24
 allow from 10.0.3.2/32
 deny from all
 order deny,allow
 ServerSignature Off
</Directory>
```

4. Press [Esc] to return to command mode. Press . to repeat the last command. The same lines will be added again. Now change the text marked in bold to add the static content virtual directory. The original pasted text:

```
ScriptAlias /nagios/cgi-bin /usr/local/nagios/sbin/
<Directory "/usr/local/nagios/sbin/">
 Options ExecCGI
```

Must be changed to the following:

```
Alias /nagios /usr/local/nagios/share/
<Directory "/usr/local/nagios/share/">
 Options None
```

5. Because this web server will not serve any content aside from Nagios, add a directive to redirect requests for the root virtual directory to the Nagios virtual directory. Press `[Esc]` and then `[Shift]+[G]` to move to the end of the file, then press `[O]` to enter insert mode on a new line, and type the following:

```
RedirectMatch ^/$ https://10.0.3.2/nagios/
```

6. Press [Esc] to stop editing and then save and exit the file:

```
:wq
```

7. Move to the Nagios etc directory:

```
# cd /usr/local/nagios/etc
```

8. Create a password file for Apache authentication:

```
# htpasswd –c htpasswd.users nagios
```

9. You will be prompted for a password twice; enter `tartans@1` each time.
10. Make sure Apache can access this file by giving it ownership:

```
# chown apache.apache htpasswd.users
# chmod 700 htpasswd.users
```

11. Restart the Apache service:

```
# service httpd restart
```

If you see the following, Apache is running correctly:

```
[root@Mike etc]# service httpd restart
Stopping httpd:                                            [  OK  ]
Starting httpd:                                            [  OK  ]
```

3 Test and Start Nagios

1. Run the Nagios configuration verification. Make sure ‘Total Warnings’ and ‘Total Errors’ are both zero:

```
# chown nagios.nagios /usr/local/nagios/etc/objects/aia.cfg
# cd /usr/local/nagios/etc
# ../bin/nagios –v nagios.cfg | less
```

2. Start Nagios

```
# service nagios start
```

If you see the following message, Nagios is running correctly:

```
[root@Mike etc]# service nagios start
Starting nagios: done.
```

3. If you are not performing any more administrative tasks on this machine, relinquish the elevated root privileges by typing the following command:

```
# exit
```

4 Using Nagios

1. Go to a system on the management network (10.0.4.0/24).
2. Open a web browser, and log into Nagios by typing as the URL: `https://10.0.3.2/nagios`
3. Click on 'Continue to this website' and login with the following credentials:

   Username: **nagios**

   Password: **tartans@1**

   (Note: it is recommended to not allow Internet Explorer to remember passwords in this exercise)
4. Explore the Nagios interface. Note that some of the features are not enabled by default. Of most interest are these items under "Monitoring":

   - Tactical Overview
   - Hosts
   - Services

   Note that if Nagios has been started recently, many services and hosts may be listed as "Pending" since Nagios hasn't polled them yet.

This page left intentionally blank for pagination purposes

OSSEC Agent

OSSEC agents will be installed on each Linux and Windows server and send events to the OSSEC server which is running on Foxtrot. The OSSEC server processes events and generate warnings and alerts sent by agents. Before installing the OSSEC agent make sure you have successfully deployed the OSSEC server in order to connect agents to the server running on Foxtrot.

1 OSSEC Agent setup

1.1 Installation

1. If you have not already done so, log on to the machine using the newly enforced admin account:

   Username: **admin** Password: **steelers**
2. Open a terminal window by going to 'Applications' -> 'Accessories' -> 'Terminal'.
3. Elevate to root level privileges by typing the following command and entering the root password **tartans@1**

```
# su -
```

4. Navigate to the Course CD by executing the following command:

```
# cd /media/AISTS/Tools/Linux/OSSEC/
```

5. Copy OSSEC installation package:

```
# cp ossec-hids-2.4.1.tar.gz /root/
```

6. Extract installation package in root directory

```
# cd /root/
# tar -xzvf ossec-hids-2.4.1.tar.gz
```

7. Start installation using following command and accept default language by pressing `[Enter]`:

```
# cd ossec-hids-2.4.1
# ./install.sh
```

8. Read the information and press `[Enter]`:

```
OSSEC HIDS v2.4.1 Installation Script - http://www.ossec.net

You are about to start the installation process of the OSSEC HIDS.
You must have a C compiler pre-installed in your system.
If you have any questions or comments, please send an e-mail
to dcid@ossec.net (or daniel.cid@gmail.com).

 - System: Linux Mike 2.6.18-164.el5
 - User: root
 - Host: Mike


 -- Press ENTER to continue or Ctrl-C to abort. --
```

9. Answer the rest of the questions as shown below and press `[Enter]` when you have finished:

```
1- What kind of installation do you want (server, agent, local or help)?
 agent

  - Agent(client) installation chosen.

2- Setting up the installation environment.

 - Choose where to install the OSSEC HIDS [/var/ossec]:

    - Installation will be made at  /var/ossec .

3- Configuring the OSSEC HIDS.

  3.1- What's the IP Address of the OSSEC HIDS server?: 10.0.4.2

   - Adding Server IP 10.0.4.2

  3.2- Do you want to run the integrity check daemon? (y/n) [y]: y

   - Running syscheck (integrity check daemon).

  3.3- Do you want to run the rootkit detection engine? (y/n) [y]: y
```

```
3.4 - Do you want to enable active response? (y/n) [y]: n

 - Active response disabled.

3.5- Setting the configuration to analyze the following logs:
  -- /var/log/messages
  -- /var/log/secure
  -- /var/log/maillog
  -- /var/log/httpd/error_log (apache log)
  -- /var/log/httpd/access_log (apache log)

 - If you want to monitor any other file, just change
  the ossec.conf and add a new localfile entry.
  Any questions about the configuration can be answered
  by visiting us online at http://www.ossec.net .


  --- Press ENTER to continue ---
```

10. When the installation has finished you should see following screen and press [Enter]:

```
- System is Redhat Linux.
- Init script modified to start OSSEC HIDS during boot.

- Configuration finished properly.

- To start OSSEC HIDS:
               /var/ossec/bin/ossec-control start

- To stop OSSEC HIDS:
               /var/ossec/bin/ossec-control stop

 - The configuration can be viewed or modified at /var/ossec/etc/ossec.c
onf


   Thanks for using the OSSEC HIDS.
   If you have any question, suggestion or if you find any bug,
   contact us at contact@ossec.net or using our public maillist at
   ossec-list@ossec.net
   ( http://www.ossec.net/main/support/ ).

   More information can be found at http://www.ossec.net

   ---  Press ENTER to finish (maybe more information below). ---
```

1.2 Configuration

1. Now we are going to setup a shared key between the OSSEC agent and the OSSEC server. In order to get a shared key from the OSSEC server, login to Foxtrot through SSH:

```
# ssh root@10.0.4.2
```

Accept SSH connectivity by typing `yes` and type the password **tartans@1** and you will be connected to Foxtrot.

```
[root@Mike ~]# ssh root@10.0.4.2
The authenticity of host '10.0.4.2 (10.0.4.2)' can't be established.
RSA key fingerprint is f5:b7:79:02:ff:f8:7d:af:a2:3f:87:db:e0:ee:c0:5e.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.0.4.2' (RSA) to the list of known hosts.
root@10.0.4.2's password:
Last login: Wed Jun 16 15:58:08 2010 from 10.0.1.5
[root@Foxtrot ~]#
```

2. Start the OSSEC agent manager:

```
# /var/ossec/bin/manage_agents
```

```
[root@Foxtrot ~]# /var/ossec/bin/manage_agents


****************************************
* OSSEC HIDS v2.4.1 Agent manager.     *
* The following options are available: *
****************************************
   (A)dd an agent (A).
   (E)xtract key for an agent (E).
   (L)ist already added agents (L).
   (R)emove an agent (R).
   (Q)uit.
Choose your action: A,E,L,R or Q:
```

3. Now add Mike's OSSEC agent to the OSSEC server by entering `A`. Type `y` and press `[Enter]` when you have finished entering the information about Mike as shown below:

```
- Adding a new agent (use '\q' to return to the main menu).
  Please provide the following:
   * A name for the new agent: Mike
   * The IP Address of the new agent: 10.0.3.2
   * An ID for the new agent[009]: 009
Agent information:
   ID:009
   Name:Mike
   IP Address:10.0.3.2

Confirm adding it?(y/n): y
Agent added.
```

4. Now type `E` and press `[Enter]` to extract the shared key for Mike, and enter `009` when the OSSEC agent manager asks for an agent ID. Please note that the key will not be the same as shown in the following screenshot, because the shared key is generated randomly each time an OSSEC agent is added.

```
****************************************
* OSSEC HIDS v2.4.1 Agent manager.     *
* The following options are available: *
****************************************
   (A)dd an agent (A).
   (E)xtract key for an agent (E).
   (L)ist already added agents (L).
   (R)emove an agent (R).
   (Q)uit.
Choose your action: A,E,L,R or Q: E

Available agents:
   ID: 001, Name: Hotel, IP: 10.0.1.5
   ID: 002, Name: Juliet, IP: 10.0.1.3
   ID: 003, Name: Bravo, IP: 10.0.2.3
   ID: 004, Name: Alpha, IP: 10.0.2.4
   ID: 005, Name: Lima, IP: 10.0.2.5
   ID: 006, Name: Charlie, IP: 10.0.2.6
   ID: 007, Name: Echo, IP: 10.0.2.10
   ID: 008, Name: Golf, IP: 10.0.4.4
   ID: 009, Name: Mike, IP: 10.0.3.2
Provide the ID of the agent to extract the key (or '\q' to quit): 009

Agent key information for '009' is:
MDA5IE1pa2UgMTAuMC4zLjIgMjA5OWNlM2FiMjgwMTIwZTQ2ZDc1YmVmYzgzMDRhNjg2ZTYx
YzJjZmExOThkODliMjcxMTAzNjcxYmUxY2U0OA==

** Press ENTER to return to the main menu.
```

5. Copy the shared key to your clipboard by highlighting it, right-clicking and choosing 'Copy'.

6. Type `Q` and press `[Enter]` to quit from the OSSEC agent manager, and type `exit` and press `[Enter]` to end the SSH session.

```
****************************************
* OSSEC HIDS v2.4.1 Agent manager.     *
* The following options are available: *
****************************************
   (A)dd an agent (A).
   (E)xtract key for an agent (E).
   (L)ist already added agents (L).
   (R)emove an agent (R).
   (Q)uit.
Choose your action: A,E,L,R or Q: Q
```

7. Now you should be back in shell of Mike. Execute the following command to import the copied key.

```
# /var/ossec/bin/manage_agents
```

8. Type `I` then press `[Enter]`.

9. Paste the copied key by right-clicking and choosing 'Paste' to import the key and accept confirmation by typing `y` then pressing `[Enter]` as shown below:

```
****************************************
* OSSEC HIDS v2.4.1 Agent manager.     *
* The following options are available: *
****************************************
   (I)mport key from the server (I).
   (Q)uit.
Choose your action: I or Q: I

* Provide the Key generated by the server.
* The best approach is to cut and paste it.
*** OBS: Do not include spaces or new lines.

Paste it here (or '\q' to quit): MDA5IE1pa2UgMTAuMC4zLjIgMjA5OWNlM2FiMjg
wMTIwZTQ2ZDc1YmVmYzgzMDRhNjg2ZTYxYzJjZmExOThkODliMjcxMTAzNjcxYmUxY2U0OA=
=

Agent information:
   ID:009
   Name:Mike
   IP Address:10.0.3.2

Confirm adding it?(y/n): y
```

10. Exit from OSSEC manager by typing `Q` then pressing `[Enter]`:

```
Confirm adding it?(y/n): y
Added.
** Press ENTER to return to the main menu.



****************************************
* OSSEC HIDS v2.4.1 Agent manager.     *
* The following options are available: *
****************************************
   (I)mport key from the server (I).
   (Q)uit.
Choose your action: I or Q: Q

** You must restart the server for your changes to have effect.

manage_agents: Exiting ..
```

11. Start Mike's OSSEC agent by executing the following command:

```
# /var/ossec/bin/ossec-control start
```

```
[root@Mike ~]# /var/ossec/bin/ossec-control start
Starting OSSEC HIDS v2.4.1 (by Trend Micro Inc.)...
Started ossec-execd...
Started ossec-agentd...
Started ossec-logcollector...
Started ossec-syscheckd...
Completed.
```

12. If you are not performing any more administrative tasks on this machine, relinquish the elevated root privileges by typing the following command:

```
# exit
```

This page left intentionally blank for pagination purposes

Wireshark Network Protocol Analyzer

1 Install Wireshark

1. If you have not already done so, log on to the machine using the newly enforced admin account:

   Username: **admin** Password: **steelers**

2. Open a terminal window by going to ‘Applications’ -> ‘Accessories’ -> ‘Terminal’.
3. Elevate to root level privileges by typing the following command and entering the root password **tartans@1**

```
# su -
```

4. Use the trusted yum repository to install arpwatch:

```
# yum install wireshark-gnome
```

5. Type y and press [Enter] if asked to confirm the download or import the GPG key.

```
================================================================================
 Package                Arch        Version                   Repository   Size
================================================================================
Installing:
 wireshark-gnome        i386        1.0.8-1.el5_3.1           base        671 k
Installing for dependencies:
 libsmi                 i386        0.4.5-2.el5               base        2.4 M
 wireshark              i386        1.0.8-1.el5_3.1           base         11 M

Transaction Summary
================================================================================
Install      3 Package(s)
Update       0 Package(s)
Remove       0 Package(s)

Total download size: 14 M
Is this ok [y/N]: y
```

Figure 1: Installing Wireshark

2 Running Wireshark

1. Start Wireshark with the following command:

```
# wireshark &
```

2. A warning message may appear cautioning against running as root. Place a check in the 'Do not show this message again' box and click 'OK'. The message may appear behind the main Wireshark window. If so, you will have to drag the Wireshark window to the side in order to handle the warning before the program will respond.

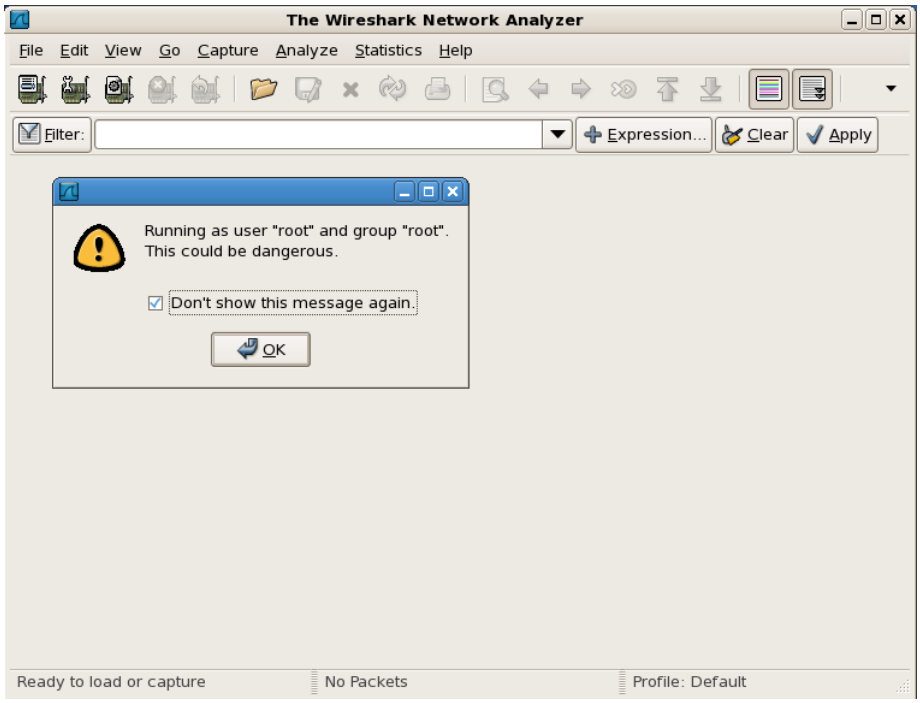


Figure 2: Running Wireshark

3. You can experiment with the settings and options of the program to familiarize yourself with it. Knowledge of packet analysis will be important in the upcoming exercise.
4. When you have finished, close Wireshark by clicking on the 'x' in the top right corner of the window.
5. If you are not performing any more administrative tasks on this machine, relinquish the elevated root privileges by typing the following command:

```
# exit
```

Appendix – Configuring Nagios

To speed up the installation process for this class, the following steps have been performed and the finished configurations have been saved to the tools CD.

1 Edit cgi.cfg

By default many of the Nagios features are inaccessible by *any* user. You need to explicitly allow access to use these features.

1. Edit cgi.cfg with VI. This file controls settings for the Nagios web interface CGI programs.

```
# vi /usr/local/nagios/etc/cgi.cfg
```

2. Use the VI find command ('/') to find the system information access setting:

```
/system_information
```

3. Press '0' (zero) to move to the beginning of the line. Press 'x' to remove the "#". Press <shift>+'A' to enter insert mode at the end of the line. Press <backspace> until the finished line looks as follows:

```
authorized_for_system_information=nagios
```

4. Press [Esc] to return to command mode. Use the VI search command ('/') to find the host access setting:

```
/all_hosts
```

5. Use the technique above to change the line as follows:

```
authorized_for_all_hosts=nagios
```

6. Press [Esc] to return to command mode. Use the VI search command ('/') to find the host access setting:

```
/enable_splunk_integration
```

7. Use the technique above to change the line as follows (remove the '#'):

```
enable_splunk_integration=1
```

8. Un-comment the Splunk URL line and change the address to the syslog server:

```
splunk_url=http://10.0.4.2:8000/
```

9. Press [Esc] to return to command mode, then save and exit:

```
:wq
```


2 Edit resource.cfg

1. This file contains definitions of *macros* used in other configuration files. It is particularly useful for storing sensitive information such as user names and passwords. The CGI programs do not directly access this file, so you can set restrictive permissions on it to protect its contents.

```
# vi /usr/local/nagios/etc/resource.cfg
```

2. There is already a section for users and passwords. Move the cursor to the line "#$USER$=someuser" (hint: '3}jj').:

3. Press '0' (zero) to move to the beginning of the line. Press 'x' to remove the "#". Move the cursor forward to the "s" of "someuser". Change "someuser" to "nagios" (hint: <shift>+'C'). The line should look as follows:

```
$USER3$=nagios
```

4. Press [Esc] to return to command mode. Do the same thing for the next line except set it to "administrator":

```
$USER4$=administrator
```

5. Now enter insert mode on a new line by typing 'o' and type the following:

```
$USER5$=base
$USER6$=tartans
```

6. Be sure you're in command mode ([Esc]), then save and exit:

```
:wq
```

7. Make sure this file is only accessible by Nagios and root:

```
# chmod 660 resource.cfg
```

3 Edit nagios.cfg

1. We will be creating a new object to monitor the network services. We need to tell nagios to use this new custom aia.cfg file:

```
# vi /usr/local/nagios/etc/nagios.cfg
```

2. Use the VI find command ('/') to find the system information access setting:

```
/templates.cfg
```

3. Press <shift>+'A' to enter insert mode at the end of the line. Press <Enter> to begin a new line:

```
cfg_file=/usr/local/nagios/etc/objects/aia.cfg
```

4. In command mode (Press [Esc] if unsure), save and exit the file:

```
:wq
```

4 Edit the commands file

1. Edit commands.cfg with VI. This file defines the commands that Nagios will use to monitor services. In addition to the defaults we will create several new commands to validate our services:

```
# vi /usr/local/nagios/etc/objects/commands.cfg
```

2. Many of the commands we will need are predefined. However, we need to create a few custom commands. Keep all the existing commands by pressing [Shift]+'G' to skip to the end of the file.

   Note that many commands use *macros* in the command line. Some of the macros Nagios uses are:

   - $HOSTADDRESS$ - the address of the host for which the command is run
   - $USER1$ - the full path to the Nagios plug-ins directory
   - $USER*N*$ - custom macros defined in resource.cfg
   - $ARG*N*$ - parameters supplied in the service definition

3. Add a command definition for checking Nagios itself. This command will verify that the correct Nagios process is running and the Nagios log file is updated frequently. Press 'o' to add a new line and enter edit mode, and press 'Enter' to add a blank line. Now add the following lines (note: 'command_line' must all appear on one line, even though it spans multiple lines in this document):

```
define command{
        command_name  check_nagios
        command_line  $USER1$/check_nagios –F
/usr/local/nagios/var/status.log –e 5 –C
/usr/local/nagios/bin/nagios
        }
```

4. Press ‘Enter’ to ensure there is a blank line after the ‘}’. Now add the following commands. First yank the command definition you just created (hint: ‘{’, ‘y}’), then put it eight times (hint: ‘8’<shift>+‘P’). Now press ‘i’ to enter insert mode and use the keyboard arrows to scroll down to the pasted command definitions and edit them per the table below:

Command_name	**command_line**
check_squid	$USER1$/check_http -H $HOSTADDRESS$ -p 3128 -u $ARG1$
check_ntp	$USER1$/check_ntp -H $HOSTADDRESS$
check_http_nagios	$USER1$/check_http -H $HOSTADDRESS$ --ssl –u /nagios/ -a $USER3$:$USER6$
check_http_splunk	$USER1$/check_http -H $HOSTADDRESS$ -p 8000 -u / -a $USER4$:$USER6$
check_http_base	$USER1$/check_http -H $HOSTADDRESS$ -u /base/ -a $USER5$:$USER6$
check_internal_dns	$USER1$/check_dns -H www.aia.class -s $HOSTADDRESS$
check_dmz_dns	$USER1$/check_dns -H www.aia.class -s $HOSTADDRESS$

5. In command mode (Press [Esc] if unsure), save and exit the file:

```
:wq
```

5 Edit the templates file

1. Edit commands.cfg with VI. This file defines the commands that Nagios will use to monitor services. In addition to the defaults we will create several new commands to validate our services:

```
# vi /usr/local/nagios/etc/objects/templates.cfg
```

2. Use the VI find command (‘/’) to find the system information access setting:

```
/generic_service
```

3. In the generic_service definition, change the contact_group from ‘admins’ to ‘aia-adimns’:

4. In command mode (Press [Esc] if unsure), save and exit the file:

```
:wq
```

6 Create a customized configuration

We will create a custom file for our environment to identify the various services, hosts, and host groups we will need to monitor. The localhost.cfg file has numerous examples that can be used for reference.

1. Create the aia.cfg with VI.

```
# vi /usr/local/nagios/etc/objects/aia.cfg
```

2. For every host we will define a “ping” service, just to verify that the machine is reachable. Press ‘o’ to add a new line and enter insert mode then press ‘Enter’ to add a blank line. Now add the following lines:

```
define service{
        use                     generic-service
        host_name               *
        service_description     PING
        check_command           check_ping!100.0,20%!500.0,60%
        }
```

3. Press ‘Enter’ to ensure there is a blank line after the ‘}’. Now we will add definitions for the specific services running on the hosts. The following is a list of all the services we will monitor. Press ‘Esc’ to return to command mode. First yank the service definition you just created (hint: ‘{’, ‘y}’), then put it 14 times (hint: ‘14’<shift>+‘P’). Now press ‘i’ to enter insert mode and use the keyboard arrows to scroll down to the pasted service definitions and edit them per the table below: (note: all settings must be written on a single line and “use” will always be “generic-service”):

Host_name	**service_description**	**check_command**
Mike	Nagios HTTP	check_http_nagios
Mike	Nagios	check_nagios
Quebec_eth0, Bravo	SMTP	check_smtp
Alpha	DNS	check_internal_dns
Juliet	DMZ DNS	check_dmz_dns
Hotel Golf	HTTP	check_http
Quebec	NTP	check_ntp
Echo	File/Print	check_tcp!445
Quebec_eth0	Squid Proxy	check_squid!http://www.aia.class
Foxtrot	Syslog	check_udp!514
Quebec_eth0, Romeo_eth0, Juliet, Lima, Mike	SSH	check_ssh

4. Add a host definition for Miker to the end of the file. The definition will specify which template to use, the host’s name, an alias, and the IP address. All other settings are taken from the template. Press ‘o’ to add a new line and enter insert mode, press ‘Enter’ to add a blank line and then add the following lines:

```
define host{
        use         generic-host
        host_name   Mike
        alias       mike
        address     10.0.3.2
        }
```

5. Press ‘Enter’ to ensure there is a blank line after the ‘}’. The remaining host definitions will be very similar to this one, so we will copy and paste this definition (or “yank” and “put” in VI jargon). Press ‘Esc’ to leave insert mode and then use ‘{’ to move to the line before “define host{”. Now type ‘y}’. This yanks to the next blank line. We will add nineteen more hosts, so use the command ‘16’<shift>+‘P’ to put the yanked text nineteen times before the cursor.

6. Now we need to edit the new hosts. The following is the host data:

host_name	**Address**
Quebec_eth2	192.168.30.13
Quebec_eth1	10.0.1.1
Juliet	10.0.1.3
Hotel	10.0.1.4
Quebec_eth0	10.0.2.1
Romeo_eth2	10.0.2.2
Bravo	10.0.2.3
Alpha	10.0.2.4
Lima	10.0.2.5
Charlie	10.0.2.6
Echo	10.0.2.10
Romeo_eth1	10.0.3.1
Mike	10.0.3.2
Romeo_eth0	10.0.4.1
Foxtrot	10.0.4.2
Golf	10.0.4.4

7. Here are some hints for speeding up these edits.
   a. Use ‘/’ to search for the string “Mike”
   b. Press <shift>+‘C’ to change the host_name
   c. Press [Esc] to stop editing
   d. Press ‘n’ to find the next “Mike”
   e. Press ‘.’ to repeat the previous “change” command, so the alias is changed to the new host name
   f. Press ‘n’ to find the next “Mike”
   g. repeat from step (b.) for all hosts
   h. Use ‘/’ to search for “10.0.3.2”. Note, the ‘/’ command uses regular expressions, so you must enter the command as follows: ‘/10\.0\.3\.2’ (the ‘\’ removes the wildcard meaning of ‘.’)
   i. Use ‘n’ and/or <shift>+N to move to the next address to change
   j. Press <shift>+‘C’ to change the address
   k. Press [Esc] to stop editing
   l. repeat from step (i.) for all hosts

8. Add a hostgroup definition for the DMZ hosts. Press ‘o’ to add a new line and enter edit mode, and add the following lines (note: ‘members’ must all appear on one line):

```
define hostgroup{
        hostgroup_name  DMZ-hosts
        alias           DMZ-hosts
        contact_groups  aia-admins
        members         Quebec_eth2, Juliet, Hotel
        }
```

9. Press ‘Enter’ to ensure there is a blank line after the ‘}’. Now add the following hostgroups. Use the same techniques from the hosts section to speed up the edits. Press ‘Esc’ to exit insert mode. First yank the initial hostgroup definition (hint: ‘{’, ‘y}’), then put it four times (hint: ‘4’<shift>+‘P’). Then search for “DMZ-hosts” (hint: ‘/’) and change that text to the appropriate hostgroup name and alias (hint: <shift>+‘C’). Finally, search for “Quebec_eth2”, and set the correct members for each hostgroup.

hostgroup_name	**Members**
Services-hosts	Quebec_eth0, Romeo_eth2, Bravo, Alpha, Lima, Charlie, Echo
User-hosts	Romeo_eth1, Mike
Mgmt-hosts	Romeo_eth0, Foxtrot, Golf
External	Quebec_eth2

10. Press [Esc] to stop editing and then save and exit the file:

```
:wq
```

This page left intentionally blank for pagination purposes

Quebec High Level Description

Quebec is an Endian firewall appliance built on Linux and Netfilter technology. This system will act as the border router and firewall for the aia.class domain. It will be configured to provide static routing and packet filtering between the networks it connects (10.0.1.0/24, 10.0.2.0/24, 10.0.3.0/24, and 10.0.4.0/24). It will perform port forwarding (Destination NAT) on inbound packets destined for the web and DNS servers in the DMZ. Additionally, the Endian firewall will provide the following services:

- Network Time Server: All Linux boxes and the Windows Domain controller (Alpha) will synchronize with Quebec.
- Traffic Monitoring Server: NTOP will be enabled to allow administrators the ability to view important network statistics.
- Intrusion Detection Services: Minimal Intrusion Prevention services will be enabled on the DMZ and LAN interfaces. Additional packet filtering rules will be configured on the firewall.
- Mail Gateway Server: Incoming e-mail must pass through the anti-virus and anti-spam services provided by Quebec before being forwarded to the internal Microsoft Exchange Server (Bravo).
- Web Proxy Server: Most servers and all User network machines will be required to use the Squid Web Proxy service on Quebec. There will also be filtering rules enabled to enforce web-browsing policies.

Following are descriptions of Quebec's specific hands-on tasks that students must complete:

Task 1. Endian Firewall Configuration

Routing and Network Access rules will be configured to support network connectivity from all networks and initialize administrative passwords. Routes must be added for the User and Management networks and additional network access permissions must be enabled to recognize those segments as trusted internal networks. Additional configuration tasks will include, configuring Syslog, NTP, IDS, NTOP, Squid, SMTP proxy, and firewall rules.

This page left intentionally blank for pagination purposes

Endian Firewall Configuration

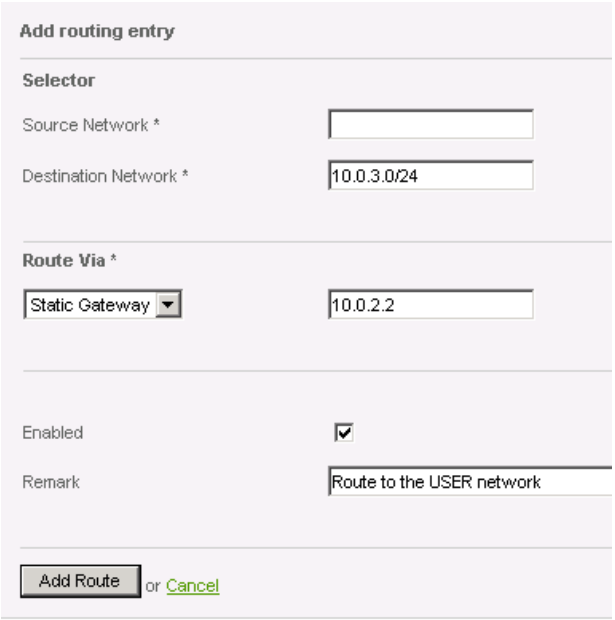
1 Firewall Login

You will need to login using the url `https://10.0.2.1:10443`. This will have to be from one of the LAN servers on the 10.0.2.0/24 network until we configure the necessary access permissions to allow access from the MGMT network.

1. If required, log in to the server 'Echo' with username: **Administrator** and password: **tartans@1**. This is our SQL server and does not have any immediate dependencies within our class network build.
2. Open Internet Explorer
3. In the address bar enter https://10.0.2.1:10443 and press [Enter].
4. Click 'Ask me later' if presented with the Internet Explorer 8 Welcome Screen.
5. Click 'OK' if presented with the IE Enhanced Security Configuration Alert.
6. Click 'OK' on the Security Alert informing you of the change to a secure web site.
7. Click 'Continue to this website' to accept the current SSL certificate provided by the Endian firewall.
8. Enter the username: 'admin' and the password 'tartans@1' (without the quotes).
9. Click 'Add' twice and then 'Close' to add the site to your trusted zone.

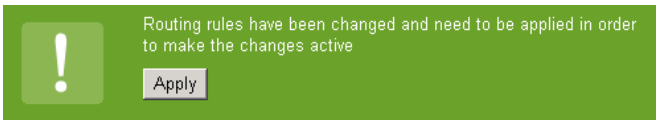
2 Enable Routing

In order for Quebec and it's directly connected networks to know how to reach the USER and MGMT networks we need to add two routing statements to the configuration.

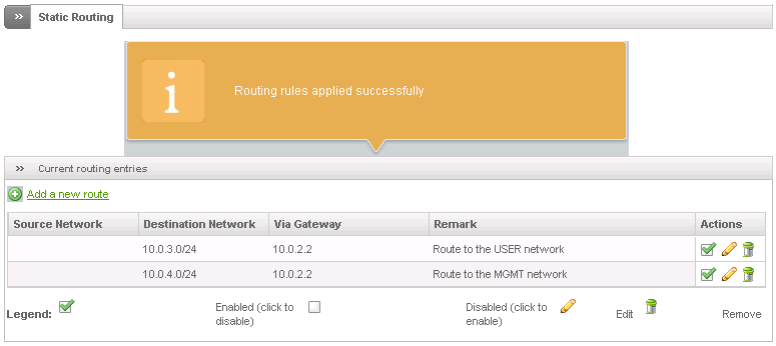


1. Click the 'Network' tab
2. Select the 'Routing' option from the menu on the left.
3. Select the 'Add a new route' link.
4. Set the Destination Network option: `10.0.3.0/24`.
5. Set the Static Gateway field: `10.0.2.2`.
6. Identify the purpose of the route in the remark field: `Route to the USER network`.
7. Click the 'Add Route' button.
8. Select the 'Add a new route' link.
9. Set the Destination Network option: `10.0.4.0/24`.
10. Set the Static Gateway field: `10.0.2.2`.
11. Identify the purpose of the route in the remark field: `Route to the MGMT network`.

12. Click the ‘Add Route’ button.
13. Click the ‘Apply’ button to activate your changes.



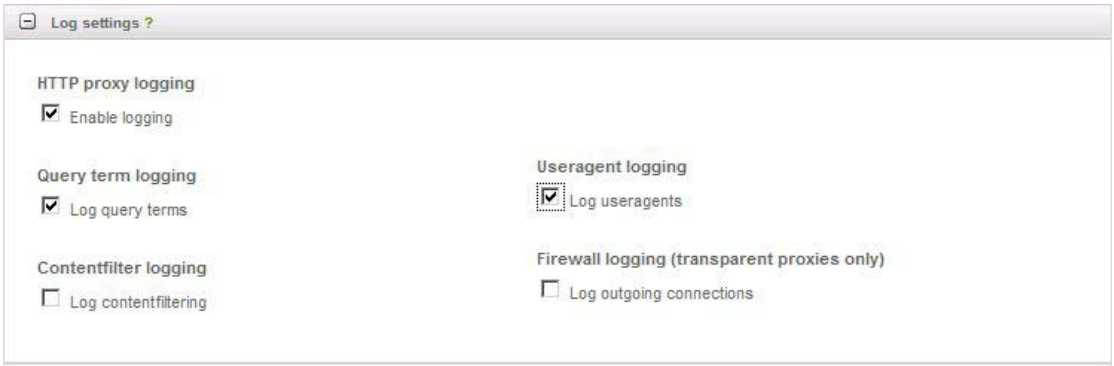
14. The finished rules should be similar to below:



3 Configure HTTP Proxy

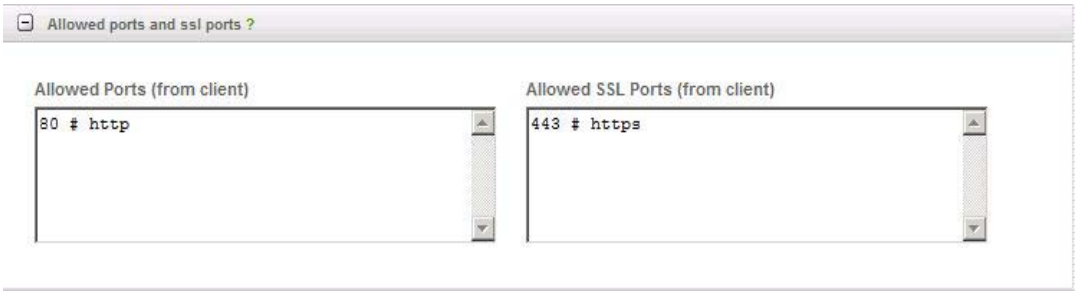
Squid is a widely deployed HTTP proxy server that will be enabled on port 3128 and required for outbound Internet access for DMZ/Services/User network machines (10.0.1.0/24, 10.0.2.0/24, 10.0.3.0/24). Web Content Filtering for Squid will be provided by the Dan’s Guardian service, which is also included with Endian. It is a powerful open source plug-in for Squid. It will be configured to allow all requests except those for pornographic sites.

1. Click the ‘Proxy’ tab.
2. Select the ‘HTTP’ option from the menu on the left.
3. Click the  button to enable Squid. The button should now be green to indicate that the service is running. 
4. Set the Proxy Port: `3128`.
5. Enter the Cache administrator email: `eventwatch@aia.class`.
6. Expand the ‘Log Settings’ section.
7. Enable HTTP proxy logging by selecting the ‘Enable logging’ box.
8. Check ‘Log query terms’ and ‘Log useragents’ as well.

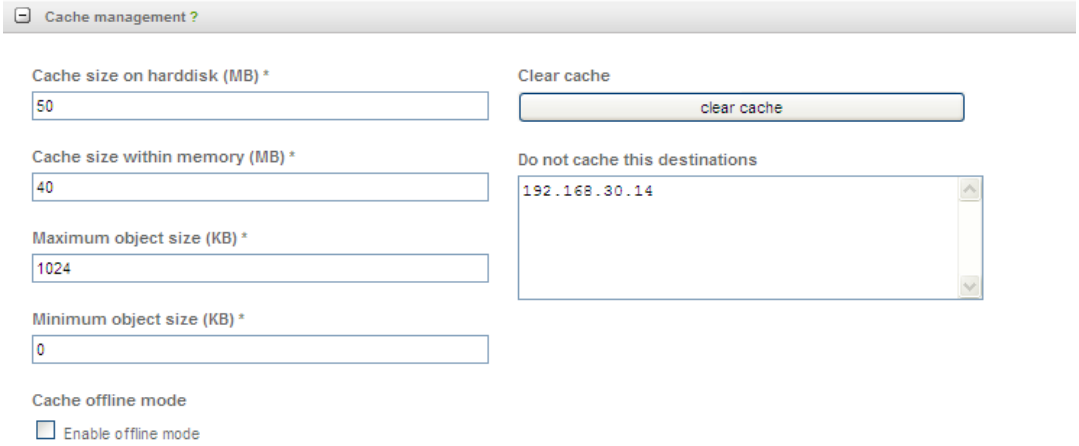


9. Expand the ‘Allowed Ports and SSL Ports’ section.

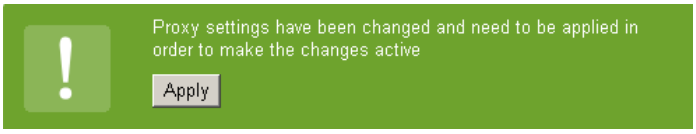
10. Remove all ports from the Ports list box except ‘80 # http’.
11. Remove all ports from the SSL ports list box except ‘443 # https’.



12. Expand the ‘Cache Management’ section.
13. Change the ‘Cache size on harddisk (MB)’ to `50`.
14. Add `192.168.30.14` to the ‘Do not cache this destinations’ box.

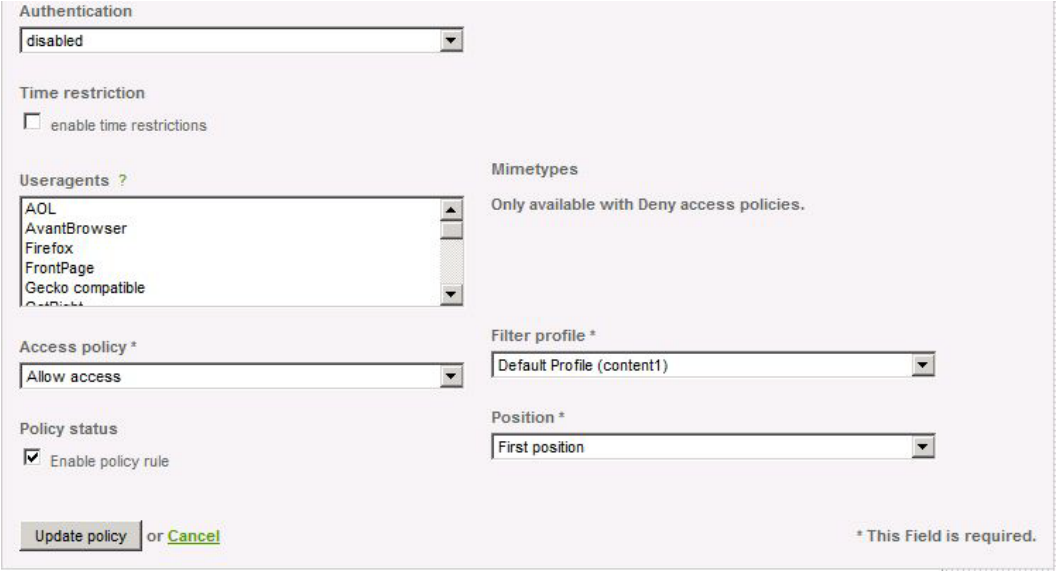


15. Click ‘Save’, and then ‘Apply’ the changes.

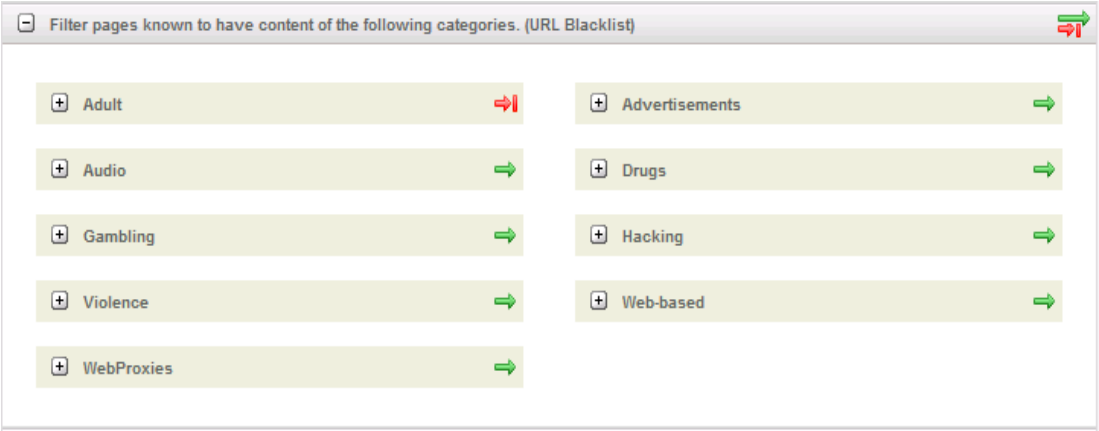


16. Go to the ‘Access Policy’ section.
17. We will edit the existing rule and enable the content filter in addition to scanning for viruses. Click on the pencil icon to edit the default rule.

18. From the ‘Filter profile’ drop down menu, select ‘Default Profile (content1)’ as shown below:



19. Click the ‘Update policy’ button, and then ‘Apply’ the changes.
20. In the ‘Proxy’ -> ‘HTTP’ -> ‘Content Filter’ section, click the pencil to edit the default profile.
21. Endian has the ability to not only block sites in specific categories, but can also filter content by evaluating words and phrases which exist on web pages or that were used in various search engines. Expand ‘Content Filtering’ and ‘URL Blacklist’ by clicking the plus sign next to each of them. Select the green arrow next to the ‘Adult’ category for both. This will toggle that category to being blocked as displayed by the now red icon . Click ‘Update profile’ and then ‘Apply’.



This is the only category being filtered for our training environment. The decision to block or allow certain categories should be made with management input and take into consideration existing acceptable use policies.

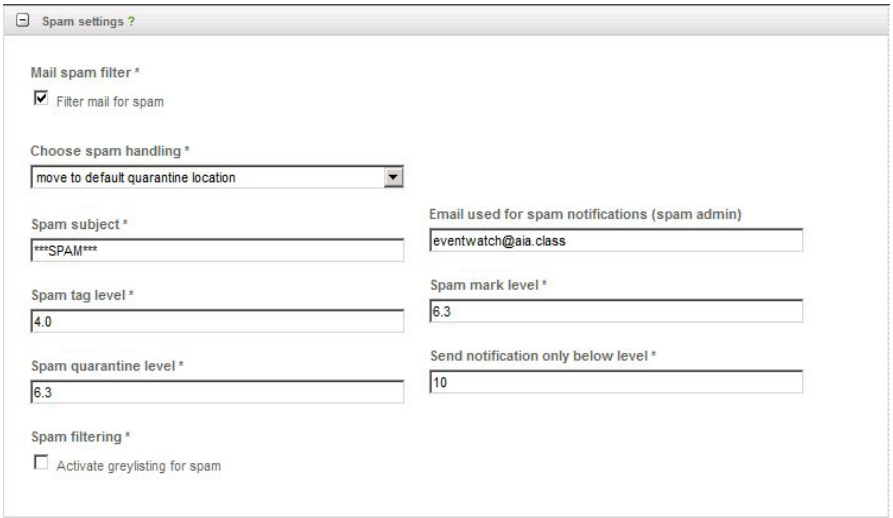
4 Configure SMTP Proxy

Anti-spam, Anti-Virus, and mail forwarding services will be configured to inspect incoming e-mail for this domain. Once scanned, it will be forwarded to the internal Exchange server for delivery to users.

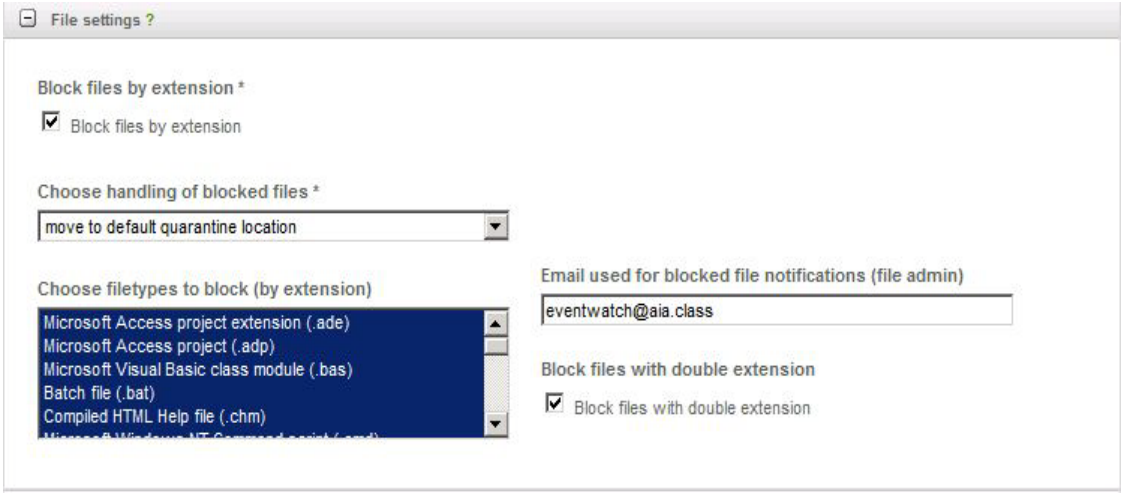
1. Click the 'Proxy' tab.
2. Select the 'SMTP' option from the menu on the left.
3. Click the  button to enable SMTP Proxy. The button should now be green to indicate that the service is running. 
4. Set the 'RED' interface to active to enable external hosts to send mail to the network.
5. Click the '+' next to 'Virus Settings' to expand the antivirus options.
6. Check 'Scan mail for virus' to enable virus scanning of Email.
7. Enter the Email address used for virus notifications: `eventwatch@aia.class`.

8. Click the '+' next to 'Spam settings' to expand the spam options.
9. Check 'Filter mail for spam' to enable spam filtering of Email.

10. Enter the Email address used for spam notifications: `eventwatch@aia.class`.



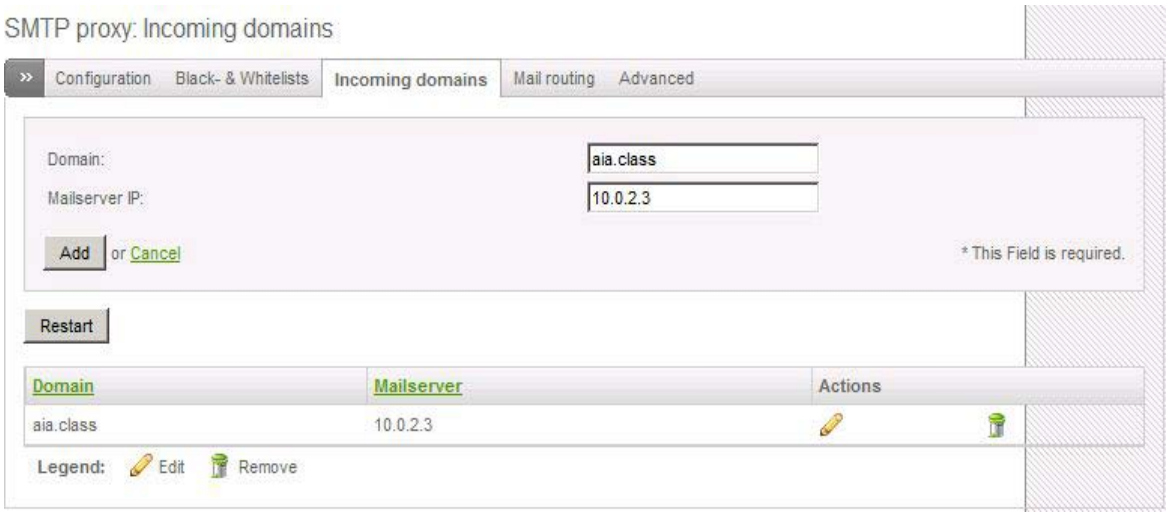
11. Click the '+' next to 'File settings' to expand the file extension options.
12. Check 'Block files by extension' to enable file extension blocking.
13. Check 'Block files with double extension'.
14. Enter the Email address used for banned file notifications: `eventwatch@aia.class`.
15. Highlight all of the file types in the 'Choose filetypes' to block box by clicking on the first item and then clicking on the last item while holding down `[Shift]`.



16. Click 'Save'.
17. Click on 'Black- & Whitelists' at the top of the SMTP proxy configuration screen.
18. Click the '+' next to 'Realtime Blacklist (RBL)'.

19. Enable all RBLs by clicking on the red arrows and changing them to green arrows as shown below:

20. Click 'Save'. As mail reaches the SMTP proxy server, the Real-time Black Lists (RBL) will be queried for the sending mail server and domain names. If present, the message will be tagged as SPAM. Additional settings allow an administrator to override the RBLs with specifically approved (whitelist) or denied (blacklist) settings.
21. In the 'Proxy' -> 'SMTP' -> 'Incoming Domains' section, click 'Add a domain' and enter the Domain: `aia.class` and the Internal mailserver: `10.0.2.3` as shown below and click 'Add'.

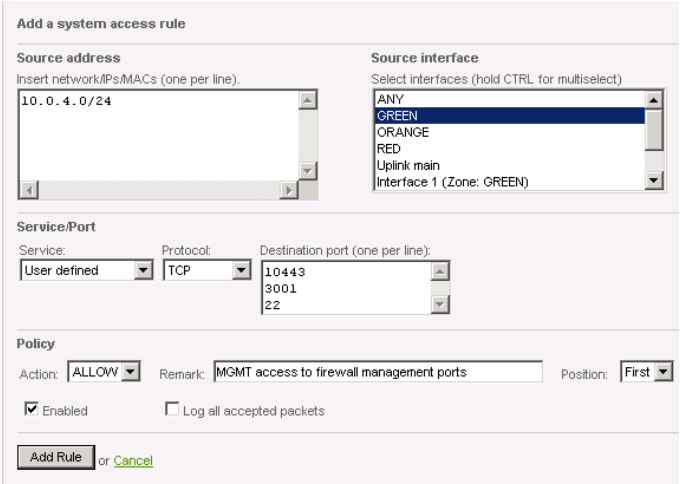


22. It is this Domains section where we are enabling the Endian firewall to receive mail for a designated domain and forward it to an Internal mail server. If necessary, multiple domain names could be enabled. Click 'Restart'.
23. Click on the 'Advanced' tab of the SMTP proxy section.
24. Expand the 'Mail server settings' section and set the 'Choose maximal email contentsize' option to 5 MB.
25. Click 'Save'.

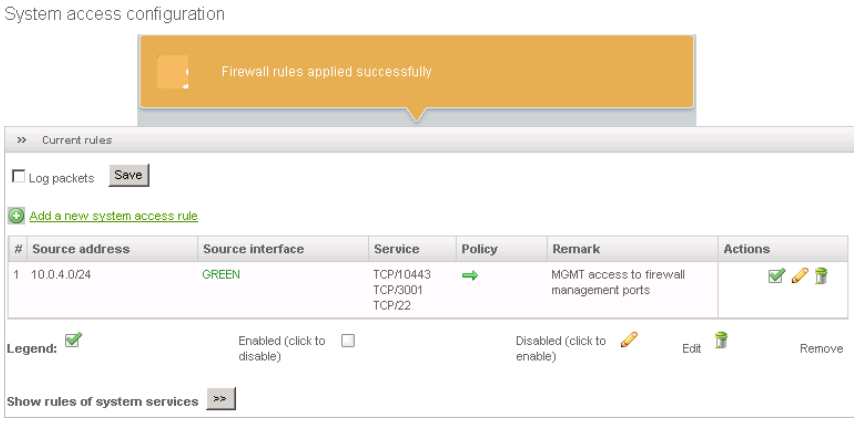
5 Configure System Access

Now that we can reach Quebec from the MGMT network we need to configure the System Access options to allow us to administer the firewall from that network segment.

1. Click the 'Firewall' tab.
2. Select 'System access' from the menu on the left.
3. Click the link to 'Add a new system access rule'.
4. Set the Source Address: `10.0.4.0/24`.
5. Set the Source Interface: 'Green'.
6. Set the Protocol: 'TCP'.
7. Set the Destination Ports to: `10443, 3001, 22` (one each line).
8. Set the Action to 'Allow'.



9. Identify the purpose of the rule in the remark field: `MGMT access to firewall management ports`.
10. Click the 'Add Rule' button to save. The finished rule should be similar to below:



11. Click 'Apply' to apply the changes.

At this point you can continue working from your current desktop or access Quebec from any of the Management network workstations.

6 Configure NTP

Quebec will synchronize network time with trusted North America NTP pool servers provided by NTP.org. Quebec will then act as the authoritative time server for all servers on the network. Alpha will synchronize to Quebec every ten minutes and so will the Linux hosts. Windows domain computers will synchronize with Alpha upon login and at regular intervals using the integrated Windows Time service.

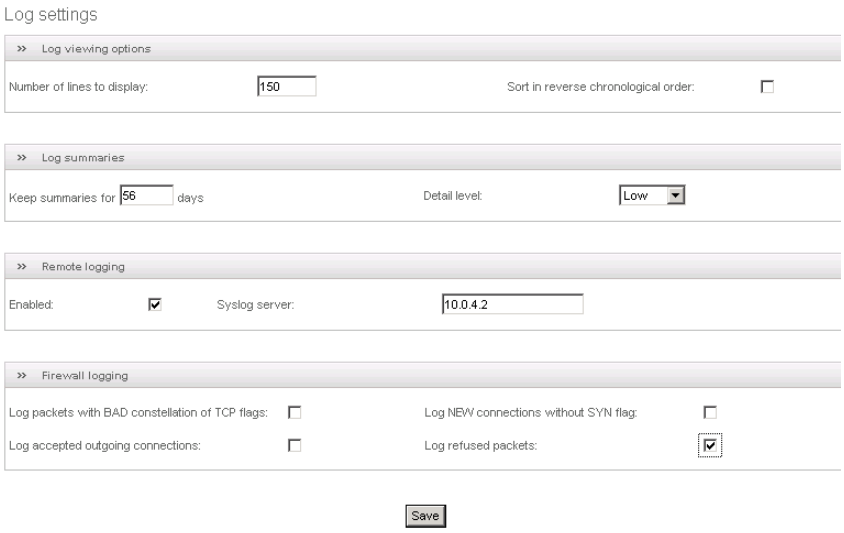
1. Click the 'Services' tab.

2. Select ‘Time server’ from the menu on the left.
3. Select the option to ‘Override default NTP Servers’, and then type `0.north-america.pool.ntp.org` in the list box that appears.
4. Choose your Timezone from the drop down list.
5. Click the ‘Save’ button.
6. Because Internet connectivity may not be currently available there may be a delay while the server attempts to reach the NTP server. Upon this failure, you can set the current date/time in the ‘Adjust manually’ dialogue--use 24-hour notation in the Hours box (i.e. 13 instead of 1). Click the ‘Set time’ button.

7 Configure Syslog

Now that all hosts will have their time settings synchronized, the cross examination of multiple hosts’ logs on the centralized Syslog server becomes more meaningful and easier. We now need to enable remote logging on Quebec.

1. Click the ‘Logs’ tab.
2. Select ‘Settings’ from the menu on the left.
3. Check the box to enable remote logging.
4. Enter the Syslog server in the appropriate field: `10.0.4.2`.
5. In the ‘Firewall logging’ area select the box to ‘Log refused packets’ as seen below:

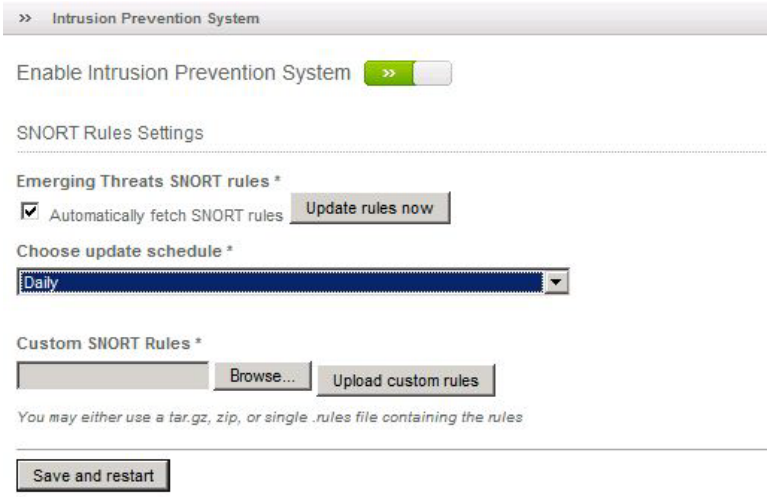


6. Click ‘Save’.

8 Enable IDS

Enabling IDS on the Green and Orange interfaces will allow us to use the Snort functionality built into Endian. Since we will be deploying Snort sensors on other servers and consolidating alerts to a central console, this task is used just to highlight the availability of this function on Endian.

1. Click the 'Services' tab.
2. Select 'Intrusion prevention' from the menu on the left.
3. Click the  button to enable Snort. The button should now be green to indicate that the service is running. 
4. After starting Snort, the option to enable automatic checking for updates will appear. Check the box to 'Automatically fetch SNORT rules', and set the update schedule to Daily.



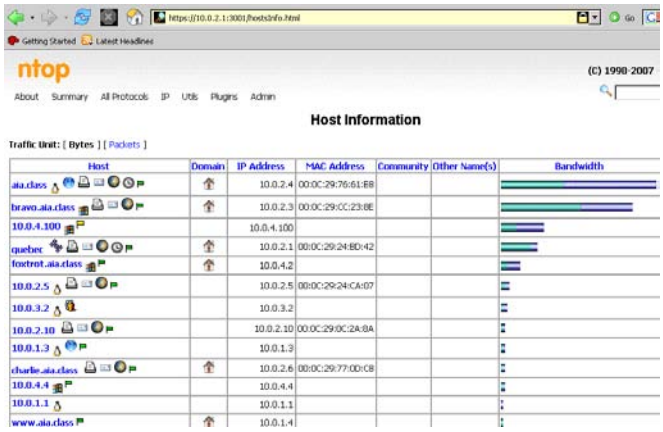
5. Click the 'Save and restart' button.

9 Enable NTOP

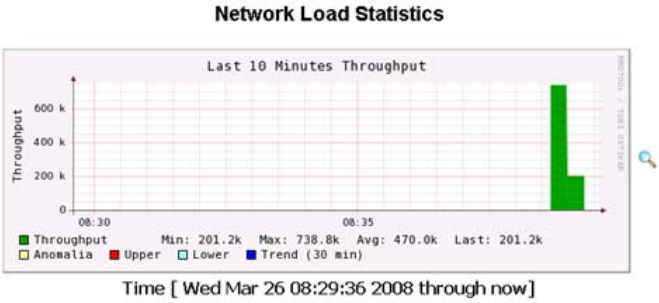
NTop is a network traffic probe that shows network utilization information. NTOP is included with Endian but the Traffic Monitoring service must be enabled. Once configured, a separate built in web server is used to display information about network traffic. Administrators can use a browser to navigate through a variety of different network statistics.

1. Click the 'Services' tab.
2. Select the 'Traffic Monitoring' option from the menu the left.
3. Click the  button to enable NTOP. The button should now be green to indicate that the service is running. 
4. Type `[Ctrl-N]` to open a new browser window and access NTop by entering the following URL: `https://10.0.2.1:3001`.

5. Click ‘Continue to this website’ to accept the security certificate and ‘OK’ to accept the secure connection.
6. NTop provides many options to observe network traffic flow information from the services network. Click on the ‘Summary’ link at the top of the page. This brings up a sub-menu on the line below it. Click on the ‘Hosts’ link in the sub-menu. This screen, ‘Host Information’, gives information about the traffic that has been seen from different hosts as it passes the NTop sniffing interface. This screen has a lot of important information that could be used to identify problem hosts in the network.



7. Click on the ‘Network Load’ link in the Summary sub-menu. This provides a MRTG like graph of the network throughput that is seen by NTop.
8. Close the NTop browser Window(s) to exit.



10 Configure Access Control Lists

Access controls will be configured on the firewall to allow only valid packets to/from each of the networks.

10.1 Configure Port Forwarding / NAT

Port forwarding steps have already been taken to enable external access to Web and DNS services in the DMZ. Port forwarding allows us to redirect any incoming packets that reach the Internet IP address of the firewall (on the RED interface) to an appropriate server in the DMZ. In this manner, our network can securely provide multiple services, on multiple servers, while using only one Internet IP address. However, it is not good practice to forward ports from external connections directly into the internal network. We will edit the existing rule forwarding external outlook web access requests to Bravo by instead directing them to Juliet in the DMZ which will then be directed to Bravo using the Pound reverse proxy that will be set up in Juliet’s tasks.

1. Click the ‘Firewall’ tab at the top of the page.
2. Select the ‘Port forwarding / NAT’ option from the menu on the left.

3. Click the pencil icon next to the bottom rule with the remark 'Support Internet Outlook Web Access' to edit it.
4. Change the line 'Insert IP' to `10.0.1.3`.
5. Click 'Update Rule'.
6. Click 'Apply', the finished rules should look similar to the figure below:

#	Incoming IP	Service	Policy	Translate to	Remark	Actions
1	192.168.30.13 (Uplink main)	UDP/53		10.0.1.3 : 53	Support Internet DNS queries	
	ALLOW with IPS from:			<ANY>		
2	192.168.30.13 (Uplink main)	TCP/80		10.0.1.5 : 80	Support Internet WWW server	
	ALLOW with IPS from:			<ANY>		
3	192.168.30.13 (Uplink main)	TCP/443		10.0.1.3 : 443	Support Internet Outlook Web Access	
	ALLOW with IPS from:			<ANY>		

10.2 Configure Outgoing Firewall

The Outgoing firewall allows us to control outbound network traffic. By explicitly allowing a minimum set of rules, we can even prevent the spread of unknown attacks or malware. For example, if we only allow our corporate mail server to send mail out on tcp/25, unauthorized mail servers or malware would not be able to send mail and/or circumvent filtering options or abuse our Internet bandwidth.

1. Go to the 'Firewall' tab.
2. Select the 'Outgoing traffic' option from the menu on the left.
3. Remove all existing rules by selecting the remove icon for each.
4. Click the 'Apply' button.
5. Using the 'Add a new firewall rule' link, create four separate outbound firewall rules. Ensure that you select 'Allow' as the action and not 'Allow with IPS' because we will be deploying our own Snort IPS sensors in the network. These rules will allow our trusted MGMT workstations and servers Internet access, our Exchange server to send e-mail, our Domain Controller/DNS Server to forward DNS name lookups, and Ping/Traceroute access from all of our networks to the Internet. Create the rules to match the list below:

#	Source	Destination	Service	Policy	Remark	Actions
1	10.0.4.0/24	RED	<ANY>	→	Allow MGMT Internet access.	
2	10.0.2.4	RED	TCP+UDP/53	→	Allow Alpha to forward DNS queries	
3	10.0.2.3	RED	TCP/25	→	Allow outbound mail from the Exchange Server	
4	10.0.1.0/24 10.0.2.0/24 10.0.3.0/24	RED	ICMP/8 ICMP/30	→	Allow Ping traffic	

6. After creating the four rules, click 'Apply' at the top of the page to enable the new firewall rules.

10.3 Zone firewall

The Zone firewall is designed to assign access controls which regulate network traffic that passes between each network segment attached to the firewall. Users have limited access to the DMZ whereas the MGMT network has full access to everything. We also need to poke “pinholes” from the DMZ to specific servers to support Syslog and Web-to-Database traffic.

1. Select the ‘Inter-Zone traffic’ option from the menu on the left.

   Take a look at the existing rules that were put in place to allow the network services to function. These rules are not restrictive enough and allow many ports to be open between zones that are not needed. Especially egregious is the top rule, allowing traffic between the DMZ and the services network. While this does accomplish the goal of allowing these two networks to talk, notably for connectivity between the web site on Hotel and the SQL database on Echo, it also completely defeats the purpose of the DMZ. We will tighten these rules so that only the minimum necessary connections are allowed between zones, reducing the attack surface of our network and the exposure of the internal machines from external threats.

#	Source	Destination	Service	Policy	Remark	Actions
1	ORANGE	GREEN	<ANY>		Allow DMZ to talk to Services	
2	GREEN	GREEN	<ANY>			
3	GREEN	BLUE	<ANY>			
4	GREEN	ORANGE	<ANY>			
5	BLUE	BLUE	<ANY>			
6	ORANGE	ORANGE	<ANY>			

2. Remove all existing rules by selecting the remove icon for each.
3. Click the ‘Apply’ button.
4. Using the ‘Add a new inter-zone firewall rule’ link, create eight separate zone firewall rules to match the final rule set listed below. Ensure that you select ‘Allow’ as the action and not ‘Allow with IPS’ because we will be deploying our own Snort sensors in the network.

#	Source	Destination	Service	Policy	Remark	Actions
1	10.0.1.3 10.0.1.5	10.0.4.2	UDP/1514		OSSEC to Foxtrot	
2	10.0.1.5	10.0.2.10	TCP/1433		MS-SQL from Web to DB Server	
3	10.0.3.0/24	10.0.1.5	TCP/80		Allow USER direct access to Hotel WWW	
4	10.0.4.0/24	<ANY>	<ANY>		Allow trusted MGMT access to all	
5	10.0.3.2	<ANY>	<ANY>		Allow Mike access to anywhere	
6	10.0.1.5 10.0.1.3	10.0.2.3	TCP/25		Allow DMZ servers to send e-mail using Bravo	
7	10.0.1.3	10.0.2.3	TCP/80		Allow Pound to access OWA on Bravo	
8	10.0.1.3 10.0.1.5	10.0.4.2	TCP/22		Allow SSH to Foxtrot: FOR INITIAL SETUP ONLY	

Note: The last rule that we created is for the initial setup of OSSEC on the DMZ servers to allow the keys to be transferred between Hotel/Juliet and Foxtrot without the need for the user to type out the entire keys by hand. Allowing SSH access from the DMZ to the internal network is a dangerous practice and this rule *MUST BE DISABLED* as soon as the OSSEC installation tasks are completed on Hotel and Juliet.

5. Ensure the rules are applied by clicking the ‘Apply’ button.

10.4 SSH access

Endian firewall allows remote SSH access. By default this is disabled, only allowing web and console access. You will enable this to allow administrators remote logon capabilities.

1. Click on the ‘System’ tab.
2. Select the ‘SSH access’ option from the menu on the left.
3. Click the  button to enable Secure Shell Access. The button should now be green to indicate that the service is running. 

Romeo High Level Description

Romeo is a system that will act as the interior router/firewall for the aia.class domain. It will be configured to perform static routing and packet filtering between the networks it connects (10.0.2.0/24, 10.0.3.0/24, and 10.0.4.0/24). It will also provide DHCP services to the 10.0.3.0/24 network.

Below are descriptions of the hands-on tasks that you must complete on Romeo:

Task 1. Securing the Cisco router platform

Cisco routers have virtually no security enabled in their default configuration. It is the engineer's responsibility (and yours for this exercise) to enhance security, including:

- Creating user accounts (because it is exponentially easier to guess a password alone than it is to guess a username/password pair)
- Encrypting stored passwords (so that an unauthorized person who somehow gains access to the router, a backup of its configuration, or a printout of its configuration will not be able to read the password in plaintext.)
- Requiring passwords for system access (to control access to the router appliance to only users that are both authenticated and authorized)
- Setting controls on system access connections (to limit access to the router appliance from only authorized sources; e.g., only from the management subnet and not from the user subnets or from the Internet. This means that even if an attacker compromises a username/password, they cannot use it to attack from unauthorized source networks).
- Requiring encrypted remote system access (this will safeguard against capturing username/password combinations while in transmission between the source terminal and the router).
- Eliminating unnecessary services (this has the same effect as eliminating unnecessary services on any other computer—it reduces the exposed 'footprint' of the router and makes the router less vulnerable to attack).
- Synchronizing the system clock using NTP service (the major function of synchronized Network Time Protocol services is to ensure all devices have the same relative timestamps, which allows for log file correlation between devices and accurate reporting of the true time of an event. Additionally, it assists in the correct operation of security certificates; all certificates have effective date windows included in the certificate and the certificate is invalid when system time does not align with the certificate validity period).
- Logging using Syslog (Cisco logging is limited due to a lack of storage space, so a syslog server is required. Additionally, security best practices dictate that logging for any given system should be stored outside of that system so that a compromise of the system does not also give the attacker the ability to modify its logs).
- Creating login banner notifications (these warnings caution unauthorized personnel to not enter the router, while also removing any excuse that someone 'didn't know' that what they were doing was an unapproved act.).

This page left intentionally blank for pagination purposes

Configuring the Cisco internal router as a Network Firewall – Internal Firewall

1 Using the router to secure the network infrastructure

To build the internal firewall, you will be using Access Control Lists (ACLs) on the internal Cisco router to control traffic between subnets via the Cisco IOS Command Line Interface (CLI). At the end, you will review the rules through the

`show running-config` command to ensure the rules are accurate and make sense.

1.1 Creating Filtering Rules

For Romeo to function as designed, it is necessary to understand the theory behind Cisco ACLs. ACLs obey the following rules:

- ACLs can be written as standard ACLs (which only identify the traffic source by IP) or extended ACLs (which can identify traffic by its source and destination, using its IP, its ICMP type, its TCP or UDP ports, or other parameters).
- ACLs, once written, are inactive until applied to a network interface. ACLs can be applied to any given interface:
    - INBOUND (checking traffic proceeding into that particular router interface from the network beyond the interface), or
    - OUTBOUND (checking traffic which has already entered the router and is now attempting to leave the router through an interface to flow out to a network beyond the interface).

(Put another way: if IN and OUT are judged from a position at the center of the router, any traffic coming toward the router through a given interface is tagged as INBOUND; any traffic leaving the router through a given interface is seen as OUTBOUND.)

*Only one ACL can be applied per direction per interface, for a maximum of two ACLs per interface (one IN and one OUT). The ACL itself can have as many access control entries in the ACL as are necessary to control the traffic, but only one ACL can be referenced per interface per direction.)

The general syntax for a standard access-list is as follows:

```
access-list [1-99] [permit|deny] a.b.c.d[address]
w.x.y.z[wildcard mask]
```

A sample access-list line would be

```
access-list 1 permit 10.0.4.0 0.0.0.255
```

NOTE: the mask used above is not a subnet mask; rather, it is called a wildcard mask. Skipping a long explanation, a wildcard mask is generally the binary opposite of a subnet mask. So, if a subnet mask of 255.255.255.0 in binary would look like

11111111 11111111 11111111 00000000,

then the binary of a wildcard mask for the same expression would be

00000000 00000000 00000000 11111111, or 0.0.0.255

Wildcard masks use a binary 0 to represent a significant bit which must match to be true, while a binary 1 represents an insignificant bit that does not have to match. In the example above, the wildcard mask is indicating that the first 3 octets (10.0.4) must

match, while the 4th octet (.0) can be anything (thus identifying any host in the 10.0.4.0 network).

The general syntax for an extended access-list is as follows:

```
access-list [100-199] [permit|deny] [protocol] a.b.c.d[source address] w.x.y.z[mask] a.b.c.d[destination address] w.x.y.z[mask] [protocol modifier (such as TCP port#, etc.)]
```

A sample extended access-list that permits HTTP traffic originating in the 10.0.2.0 network destined for the 10.0.4.0 network would look like this:

```
access-list 101 permit tcp 10.0.2.0 0.0.0.255 10.0.4.0 0.0.0.255 eq 80
```

SPECIAL RULES FOR INDIVIDUAL HOSTS OR THE DEFAULT NETWORK

Normally, any access-list uses the syntax **a.b.c.d w.x.y.z** to identify a network followed by its wildcard mask. There are two special cases where you can use alternative syntax, (1) on an individual host or (2) on the default network. An individual host can be identified by 10.0.4.2 0.0.0.0 (one address, with a mask identifying all 32 bits as significant). However, that same single address can also be identified by the syntax **`host 10.0.4.2`**. You can specify the address using either syntax but the router will store it using the host syntax.

Similarly, the default network (usually used to identify all Internet addresses), can be identified as **`0.0.0.0 255.255.255.255`** (signifying the wildcard network, with no network bits identified as significant). However, the same effect can be accomplished by using the single word **`any`** instead of the longer syntax (which is the way the router will always store it).

Let's take the example extended access-list above and create a new list. In this new list, we will allow any Internet address to access the web server at address 10.0.4.9. In this case, using the rules above, the access-list could be written as:

```
access-list 101 permit tcp any host 10.0.4.9 eq 80
```

ACCESS-LIST ENTRIES, ORDER OF EXECUTION, AND THE IMPLICIT DENY

The final aspect that must be understood is that an access-list may be a series of access-list line entries. In access-lists, line entries are processed one line at a time in sequence. This means that if you want to let any host on the 10.0.3.0 network except 10.0.3.3 to be able to access the Internet, you first have to deny 10.0.3.3, and then permit 10.0.3.0/24. If you reversed the order and permit 10.0.3.0/24 as the first line, the address 10.0.3.3 will be permitted by line 1 and would not be denied by line 2.

One last rule, all access-lists ends with a default rule: **`deny any any`**. This rule does not have to be written; however, some people do write it to remind them of its existence. It means that any traffic not explicitly permitted will be implicitly denied. This is a default behavior of access-lists in Cisco: the deny any any rule will always block traffic not specifically permitted. This means that one sanity check for validating an access-list is that it must have at least one permit statement to be valid; otherwise, all traffic will be blocked.

It also means that if you want to have the default rule to permit traffic—as you might want if you desire to deny one host and permit everything else—then your last line in the access-list will be **`permit any any.`**

For this exercise, you will be told exactly what to type. The information above is to assist you in understanding the effects of the lines you will type.

ACCESS-GROUP and ACCESS-CLASS commands

Access-lists can be written, but they do not take effect until they are applied. The act of applying an access-list is to tell it where on the router you want the list to take its action, which usually means selecting an interface like Ethernet 0. To apply an access-list to traffic through an interface, you apply the access-list to an interface using the **`access-group`** command. If you want an access-list to safeguard a service like Telnet, you apply the access-list using the **`access-class`** command to the 5 default virtual terminal lines (vty 0 4).

When applying an access-list, you also have to decide whether the list is being applied IN or OUT (as previously discussed). The access-list must be written with the traffic direction in mind—with the actual direction being applied at the access-class or access-group command. In this exercise, you will be instructed what to type to make the lists operate correctly.

1.2 Identifying the traffic controls that need to be implemented

For this course, the Cisco router will use ACLs to control traffic between subnets internally. The three subnets managed by the router are:

- The services subnet (10.0.2.0/24)
- The user subnet (10.0.3.0/24)
- The management subnet (10.0.4.0/24)

The security philosophy here is to explicitly permit traffic that is authorized and expected and deny all other traffic. The implementation does take some shortcuts for the sake of brevity, but executes the essential elements of that philosophy. (Note that in the syntax below, the ‘deny any any’ default ACL behavior will cut off all traffic not explicitly permitted.)

In the LHS scenario network, the traffic to be permitted includes:

- User access to the web proxy server (Quebec) (to permit web access while blocking direct Internet access)
- Unlimited user access to the Windows Domain Controller and DNS server (Alpha)
- IMAP mail client access to the Exchange mail server (Bravo)
- Direct HTTP access to the WSUS server for windows updates (Charlie)
- Unlimited access to all nets/hosts for the user subnet security host (Mike)
- Unlimited management network access to all subnets
- Ping requests and responses will be allowed between networks to support connectivity diagnostics

These rules need to be translated into IP addresses and protocol ports.

This means:

- Network 10.0.3.0 should have HTTP access to the web proxy (10.0.2.1 on proxy port 3128) and only WSUS (10.0.2.6).

- Network 10.0.3.0 should have unlimited access to the Windows DC/DNS server (10.0.2.4)
- Network 10.0.3.0 should have IMAP4 mail client access (TCP 143) to the mail server (10.0.2.3)
- Host 10.0.3.2 should have unlimited access to all subnets
- Network 10.0.4.0 should have unlimited access to all subnets
- All networks should be able to communicate using ICMP echo-request and echo-reply messages to support Ping diagnostics

1.3 Converting security rules to access-lists

Using the access-list rules of section 1.2, the effective access-lists should filter traffic in the following manner:

Ethernet 1/0 inbound:

- Network 10.0.4.0 and host 10.0.3.2 are permitted to ssh to the router
- Network 10.0.3.0 should permit all traffic to 10.0.2.4
- Network 10.0.3.0 should allow DHCP requests
- Network 10.0.3.0 should permit IMAP traffic (tcp 143) to 10.0.2.3
- Network 10.0.3.0 should permit HTTP traffic (tcp 80) to 10.0.2.3
- Network 10.0.3.0 should permit SMTP traffic (tcp 25) to 10.0.2.3
- Network 10.0.3.0 should permit Windows File and Print Sharing (udp 137, udp 138, tcp 139, tcp 445) to 10.0.2.6.
- Network 10.0.3.0 should permit squid proxy traffic (tcp 3128) to 10.0.2.1 and deny all other traffic to 10.0.2.1
- Network 10.0.3.0 should permit traffic from 10.0.3.2 to all nets
- All networks should allow ICMP echo-request and ICMP echo-reply messages to/from each segment
- Network 10.0.3.0 should deny all other traffic to network 10.0.4.0

1.4 Entering and applying access-lists

Note: In this document, all tasks that require your input (typing) will be displayed in white text on a black background (just how the router display looks.) Anything else is for your information only.

What if I make a mistake?

If you make a mistake in a router configuration, there are two main methods to fix the mistake. If you need to change something like a hostname, simply enter the hostname line again and the router will overwrite the wrong answer with the right answer. If you need to undo or reverse something you have already done, almost any command can be removed by going to the same config area in the router and repeating the command with the word **no** in front of it. You have already done that by turning off the default behavior of automatically resolving any text string to DNS when you typed the command ***no*** **`ip domain-lookup`** *(italics for emphasis only).*

Return to the router and type the following commands as shown below:

```
ROMEO>
ROMEO>enable
ROMEO#config t
ROMEO(config)#access-list 1 permit 10.0.3.2
ROMEO(config)#access-list 1 permit 10.0.4.0 0.0.0.255
ROMEO(config)#access-list 101 permit udp any eq 68 any eq 67
ROMEO(config)#access-list 101 permit icmp any any echo
ROMEO(config)#access-list 101 permit icmp any any echo-reply
ROMEO(config)#access-list 101 permit ip 10.0.3.0 0.0.0.255 host
10.0.2.4
ROMEO(config)#access-list 101 permit tcp 10.0.3.0 0.0.0.255 host
10.0.2.3 eq 25
ROMEO(config)#access-list 101 permit tcp 10.0.3.0 0.0.0.255 host
10.0.2.3 eq 80
ROMEO(config)#access-list 101 permit tcp 10.0.3.0 0.0.0.255 host
10.0.2.3 eq 143
ROMEO(config)#access-list 101 permit udp 10.0.3.0 0.0.0.255 host
10.0.2.6 eq 137
ROMEO(config)#access-list 101 permit udp 10.0.3.0 0.0.0.255 host
10.0.2.6 eq 138
ROMEO(config)#access-list 101 permit tcp 10.0.3.0 0.0.0.255 host
10.0.2.6 eq 139
ROMEO(config)#access-list 101 permit tcp 10.0.3.0 0.0.0.255 host
10.0.2.6 eq 445
ROMEO(config)#access-list 101 permit tcp 10.0.3.0 0.0.0.255 host
10.0.2.1 eq 3128
ROMEO(config)#access-list 101 permit ip host 10.0.3.2 any
ROMEO(config)#access-list 101 deny   ip any 10.0.4.0 0.0.0.255
ROMEO(config)# interface FastEthernet 1/0
ROMEO(config-if)#ip access-group 101 in
ROMEO(config-if)#exit
ROMEO(config)#line vty 0 4
ROMEO(config-line)#access-class 1 in
ROMEO(config-line)#exit
ROMEO(config)#exit
ROMEO#copy run start
```

2 Securing the Cisco router platform

It is important to shut down all unneeded TCP/UDP services on the router. Services that are not running can not cause problems or be used as the basis for attacks. Also, you will be freeing up memory and processing cycles by minimizing services.

You may require some TCP/IP services (like TFTP or SNMP) as part of your network management and administrative tasks. Use these services with caution—they can open the door to intruders if they are not tightly controlled. There are many features in Cisco IOS that are enabled by default (for legacy reasons); however, they present security risks and should be disabled (see below).

The **show processes** command can help to show active information about the servers on the router.

Type the following commands to disable the following servers: TCP/UDP small servers (echo, discard, daytime, chargen), bootps, finger, http, and snmp.

```
ROMEO#config t
ROMEO(config)# no service tcp-small-servers
ROMEO(config)# no service udp-small-servers
ROMEO(config)# no ip bootp server
ROMEO(config)# no service finger
ROMEO(config)# no snmp-server community public
ROMEO(config)# no snmp-server community private
```

Type the following commands to disable these unneeded services: Cisco Discovery Protocol (CDP), remote configuration downloading, and source routing.

```
ROMEO(config)# no cdp run
ROMEO(config)# no service config
ROMEO(config)# no ip source-route
```

Type the following commands to disable web services on the router:

```
ROMEO(config)#no ip http server
ROMEO(config)#no ip http secure-server
```

Type the following commands to enable router logging and send the results to the syslog server:

```
ROMEO(config)#logging buffered 16000 debugging
ROMEO(config)#logging console critical
ROMEO(config)#logging facility local1
ROMEO(config)#logging 10.0.4.2
```

Type the following commands to set correct time for the router so digital certificates will be valid:

```
ROMEO(config)#ntp server 10.0.2.1
ROMEO(config)#clock timezone EST -5
ROMEO(config)#clock summer-time EDT recurring 2 SUN MAR 02:00 1 SUN
NOV 02:00
```

Type the following commands to restrict remote terminal access to SSH by creating a digital certificate on the router and denying telnet access to the vty (virtual terminal) ports:

```
ROMEO(config)#ip domain-name aia.class
ROMEO(config)#crypto key generate rsa
   (Some output omitted)
How many bits in the modulus [512]: 1024
Generating 1024 bit RSA keys, keys will be non-exportable…[OK]
ROMEO(config)#line vty 0 4
ROMEO(config-line)#transport input ssh
```

Type the following commands to enable the SSH server using the new digital certificate:

```
ROMEO(config-line)#ip ssh source-interface FastEthernet0/0
ROMEO(config)#ip ssh rsa keypair-name ROMEO.aia.class
ROMEO(config-line)#exit
```

Type the following commands to create and enable a secret [MD5 encrypted] password, create username/password pairs on all service connections, encrypt all system passwords, and enable timeouts on all service connections

```
ROMEO#config t
ROMEO(config)#enable secret tartans@1
ROMEO(config)#username admin password tartans@1
ROMEO(config)#service password-encryption
ROMEO(config)#line con 0
ROMEO(config-line)#exec-timeout 5 0
ROMEO(config-line)#login local
ROMEO(config-line)#line vty 0 4
ROMEO(config-line)#exec-timeout 5 0
ROMEO(config-line)#login local
ROMEO(config-line)#exit
```

The router can also display security messages through its ‘banner’ service. You will use the message-of-the-day banner (**`banner motd`**) to display a security message to anyone attempting to connect to the router.

The command sequence for banners uses a ‘delimiter character’ to mark the beginning and end of the message. In the syntax, you will use the % symbol as the delimiter. Type the following to complete this security banner task:

```
ROMEO(config)#banner motd %
Enter TEXT message.  End with character ‘%’.
WARNING:  AUTHORIZED ACCESS ONLY.  VIOLATORS MAY BE PROSECUTED
%
ROMEO(config)#exit
```

FOR THE FINAL STEP, inspect the running configuration (sh run) then save it (copy run start)