

Course Syllabus

Applied Information Assurance 14-761

Instructors: Chris May (cjm@cert.org) and Richard Nolan (ran@cert.org)

Course Description:

This course focuses on practical applications of Information Assurance (IA) policies and technologies in enterprise network environments. The course will include lecture and demonstrations, but is designed around a virtual lab environment and scenario that provides for robust and realistic hands-on experiences in dealing with a range of information assurance topic areas. Students will be provided numerous practical opportunities to apply information security practices and technologies to solve real-world IA problems.

Virtual Lab Assignments:

The keystone components of this course are the virtual lab exercises. These labs are comprised of VMware virtual machines and a lab document that focus on various IA and Defense in Depth concepts. Students will configure, harden, install, and test various IA and Defense in Depth security tools and practices. Each student will be provided with an account that you will use to login to the CERT XNET environment. You **must** have java (<http://java.com>) and a Remote Desktop Client installed on your computer. Each lab is designed to take between 1 and 2 hours to complete. Two to three labs per week are **required** but there are optional labs that are also available; for a listing see table #3. Students should **avoid rushing** to complete these labs and take time to fully understand the practices and concepts being illustrated.

Group Projects:

By **week 3** of the course, students **must** organize themselves into teams comprised of about 4 students each. These teams will research, integrate, and document a cyber security/forensics technology best practice lab. This will include the configuration of VMware virtual machines and developing step-by-step procedures for completing the security or forensics technology best practice. These best practices will be subject to peer review and may be made available to future AIA classes and to the Internet community via CERT VTE and XNET. The goal of the project is to provide a meaningful instructional experience for future users. Teams must select their security/forensics/incident response lab topic and submit their own proposal (subject to instructor approval).

Teams must submit their **final Group Project proposal no later** than the start of class on **week 5** of the course. This proposal should briefly (Word document, no more than 2 pages) describe their IA best practice selection and lay out the planned components and technical objectives of their hands-on lab. Email your teams' proposal to the instructors and TA and make sure you identify your team number and all members in the document.

Teams will build out their projects using assigned CERT Lab servers. The T.A./instructors will demonstrate how this is done in class on week 5. The documentation of the lab manual must be written clearly and concisely and must also contain instructive, contextual information that describes **why** the specific steps are being completed and why they are important. At least 1 lab verification step must be included that attempts to clearly demonstrate what has been accomplished. **This document should be the original work of the team. Proper citation of all technical sources is required.**

To enhance the quality of the final products and to promote collaboration, group project peer reviews will be conducted. **On Week 14** of the course, teams will be assigned to test-drive another team's lab and make comments on their documentation and structure. These comments are to be compiled into one document (**Word document, no more than 5 pages**) and must be emailed to the owning team (cc the Instructors and TA) no later than **11:59 pm on Friday** of that week. This will give the owning team time to consider these comments and incorporate any suggestions/changes into their final lab submission. This will be a **graded activity** representing **5%** of the students' overall grade.

Group Project deliverables to the instructors will be:

- Step-by-Step Lab Manual no more than 50 pages—to include screenshots. (Use Weekly Lab Docs as THE template and as an example for organization)
- VMware virtual machines. These must be in a **final starting state** and contain **zero** snapshots. You should attempt to use Virtual Machines from the existing VM Library before you create your own.

All of the above deliverables **must be made available** for grading by the **start of class on week 15**. All required files are to be placed in the “Final Projects” folder on the lab environment file server.

Information Assurance Exercise:

The Information Assurance Exercise (IAX) will be a team-based, scenario-driven exercise. This is an entirely hands-on exercise where students must work together in groups (about 4 per team) to complete the IAX requirements. Each team will be presented with a remotely accessible virtual network and a scenario that describes a fictitious bankrupt company that has failed an IA audit. In this scenario, the teams will serve as consultants who’ve been hired to implement the bankruptcy court’s mandated IA get-well plan. The teams must work collaboratively to re-architect the company’s network, integrating interdependent security systems and IA practices. Each week, team members will rotate through the securing of the network and hardening of the 12 servers in the scenario. This network build process will occur during **weeks 6-9** and some class time will be dedicated to this effort. The rest of the weekly build is the responsibility of the team and must be accomplished before the start of class the following week. The instructors and TA will **audit and verify the IAX network** for compliance with the get-well plan every week. These weekly audits will be graded (**25 points x 4**) and will represent **10%** of each student’s final grade for AIA. A specific **grading rubric** will be posted on Blackboard so teams can ensure they fulfill IAX requirements prior to instructor grading.

On week 10, students must respond to live instructor injected attacks and network anomalies. They must correctly identify and attempt to mitigate these attacks. **To test students’ understanding of IAX objectives and appropriate response actions, a short quiz (50 points) will be administered in Blackboard during week 11.**

Incident Response Exercise:

The Incident Response Exercise (IRX) is another in-class, scenario-driven exercise designed to test and challenge the students’ practical knowledge of the live cyber forensics. To prepare students for the IRX, in-class instructor guided forensics lectures/demos will be conducted in weeks 11 and 13. Then during weeks 12 and 14, students must work together in their group project teams to complete the hands-on IRX requirements. Each team will be presented with a remotely accessible virtual network and 2 scenarios. The teams will need to self-organize, formulate a plan of response (in relation to the scenarios), investigate their networks, collect artifacts that support their conclusions, and suggest possible remediation steps. **A capstone in-class exercise during week 15 will conclude the IRX.**

Grading: 1000 points total

Course Requirement / Percent of Final Grade	
Mid-Term Exam	200 points / 20%
Final Exam	200 points / 20%
Information Assurance Exercise (IAX)	150 points / 15%
Incident Response Exercise (IRX)	150 points / 15%
Group Project	300 points / 30 % broken down as follows:
• Peer Reviews	50 points / 5%
• Lab documentation and Virtual Machines	250 points / 25%

Table 1

Reading Assignments:

The course has two handbooks that are assigned as supplemental readings. These are both free and can be downloaded in pdf format here: <http://www.sei.cmu.edu/publications/documents/06.reports/06hb003.html> and <http://www.sei.cmu.edu/publications/documents/05.reports/05hb001.html>. The high-level concepts from the Defense-in-Depth handbook will be testable on the Mid-Term Exam. The high-level concepts of the Forensics handbook will be testable on the Final exam.

Weekly Schedule

<p>Week 1 (Jan 17) Course Overview/Logistics & Principles of Information Assurance and Defense in Depth [CJM] Virtual Lab Environment Requirements / Procedures. Syllabus walkthrough. IA Defense-in-Depth Framework. Background and Applications of Confidentiality, Integrity and Availability (CIA), Authentication, Authorization..</p>	<p>Week 9 (Mar 20) Securing Network Infrastructure, [CJM] Routers / Switches / Network Authentication, Core Services, Wireless Security</p> <p style="color: blue;">***Continue IAX network build***</p>
<p>Week 2 (Jan 24) Security Threats/Vulnerabilities [CJM] Networking 101, Network monitoring. Mainstream Threats and Vulnerabilities as related to CIA and Defense-in-Depth.</p>	<p>Week 10 (Mar 27) In-Class Information Assurance Exercise (IAX) [CJM]</p>
<p>Week 3 (Jan 31) Securing Windows Systems [CJM] Windows Architecture, Security Templates, Group Policy, Windows Applications Security, Patching, etc.</p> <p style="color: red;">*** Group Project Teams Due****</p>	<p>Week 11 (Apr 3) Computer Forensics: Volatile Data [RAN] Introduction to Volatile Data Collection and Analysis, Creating Safe Tool Sets, etc. Introduction to Memory Collection and analysis</p>
<p>Week 4 (Feb 7) Securing Linux-Based Systems [RAN] Architecture, Updating/Patching, Security Policy – Bastille, SELinux Applications Security, Access Controls, etc.</p>	<p>Week 12 (Apr 10) In-Class Incident Response Exercise (IRX) Volatile Scenario [RAN]</p>
<p>Week 5 (Feb 14) Firewalls, Logging, and Time Synchronization [RAN] Packet filtering 101, NAT, Windows Firewalls, Linux IPTables, TCP Wrappers, etc. NTP Servers / Clients, Syslog / Syslog_ng, Swatch. Microsoft Log Parser, Splunk, Log Analysis, etc</p> <p style="color: red;">*** Group Project Proposals Due****</p>	<p>Week 13 (Apr 17) Computer Forensics: Persistent Data [RAN] Introduction to Persistent Data Collection and Analysis, Web Artifacts, Deleted Files, Autopsy / Sleuth Kit, PyFLAG, etc.</p>
<p>Week 6 (Feb 21) Intrusion Detection/Prevention [CJM] IDS Types, Snort, OSSEC, OSSIM, etc. Vulnerability Assessment with Nessus, NMap, OpenVAS</p> <p style="color: blue;">***Start IAX network build***</p>	<p>Week 14 (Apr 24) In-Class Incident Response Exercise (IRX) [RAN] Persistent</p> <p style="color: red;">Peer Reviews teams assigned. Group Project materials must be made available to Peer Review team.</p>
<p>Week 7 (Feb 28) Data Protection and Privacy; Secure Remote Access [CJM] Applied Data encryption 101, securing stored data and network and Internet communications.</p> <p style="color: blue;">***Continue IAX network build***</p>	<p>Week 15 (May 1) IRX Capstone [RAN] All Group Project deliverables due to instructors by start of class!</p>
<p>Week 8 (Mar 6) Mid-Term Exam ***Continue IAX network build***</p>	<p>Week 16 (May 8) Final Exam Questions for the final exam are not cumulative for the entire course—weeks 9-15 only</p>

Table 2

Lab Assignments

In addition to readings, each student must complete numerous virtual hands-on laboratory exercises. Step-by-step Lab instructions will be made available on the course blackboard website. You are to complete the required labs **PRIOR** to the week due (see table 3).

Lab Number	Lab Name	Week Due
1	Security Auditing and Attack Prevention	2
2	Introduction to Penetration Testing	2
3	Capture the flag for Penetration Testers	2
4	Securing Windows Server 2008 R2 as an Applications Server	3
5	Windows Domain Security	3
6	Client-Side Security in Windows 7	3
7	Linux Host System Hardening	4
8	Advanced Reconnaissance and Enumeration with Backtrack	4
9	Securing BIND with chroot	4
10	Centralized System Logging for Windows and Linux	5
11	Log File Analysis using Log Parser and Splunk	5
12	Windows Firewall Configuration	5
13	Using Snort on Windows	6
14	Intrusion Detection using Open Source Security (OSSEC)	6
15	Vulnerability Assessment with OpenVAS4	6
16	Building a Microsoft PKI	7
17	Encrypting Email	7
18	Identifying MAC and IP Address Spoofing attacks with ARPWatch (Very Good but Optional)	7
19	Heterogeneous Backup with Secure Archival (Very Good but Optional)	8
20	Hardening Exchange 2003 and Outlook Web Access (Very Good but Optional)	8
21	Transitioning to an IPv6 Network (Very Good but Optional)	8
22	Packet Sniffing with Wireshark and TCPDump	9
23	Securing a CISCO Routing Infrastructure	9
24	Vulnerability Scanning with MBSA and Nessus (Very Good but Optional)	9
25	Network Traffic Monitoring with Ntop	10
26	Web Application Vulnerability Testing	10
27	Multiplatform Network Traffic Encryption with IPSec (Very Good but Optional)	10
28	Preserving live digital evidence on Windows using Helix	11
29	Windows Incident Response with Sysinternals Tools	11
30	Forensic Collection and Analysis of Volatile data (Very Good but Optional)	11
31	Memory Resident Malware Analysis	12
32	Using Volatility Framework and PyFlag to perform Forensic Memory and Hard Drive Analysis	12
33	Malware Attacks, Analysis, and Defense	13
34	Network Forensic Analysis with Wireshark, Xplico, and Network Miner	13
35	Analysis of Persistent data with the Sleuthkit	14
36	Data carving and analysis with Scalpel/Foremost and DCFLdd	14

Table 3