Network Situational Awareness

Group Project Report

Fall 2009

Chanon Sinitskul, Napat Ratanasirintrawoot, Will Zickefoose

Table of Contents

Executive Summary 3

Network Profile 5

General information and assumption 5

Network summary 5

Network Component summary 8

Network incident analysis summary 8

Common port and protocol inspection 10

TCP 10

HTTP/HTTPS 11

SMTP 14

FTP 17

UDP 20

DNS 21

ICMP 23

Network incident inspection 25

Suggestion for improvement 34

Recent Event Case and its Impact on our Network 36

Appendix

A - Commands used and results 42

B - Vulnerabilities associated with specific ports 66

C – References 68

Executive Summary

In order to make an architecture improvement to the class B network block of 173.94.00/16, a one-day traffic flows data has been analyzed to profile the network. The dataset used for the analysis was captured from a trans-Pacific transit point from March 30, 2009 3pm to March 31, 2009 3pm.

The profiling shows that the network traffic mainly comprises of TCP traffic, especially HTTP traffic which contributes 77% of the traffic. Other significant TCP traffic includes HTTPS, SMTP, RTPS, and FTP traffic. While the UDP traffic and ICMP traffic contributes 14.61% and 0.49% of the traffic, respectively. Major network components were identified as follows.

Web Server
The host IP of 173.94.202.147 is the main web server in the network. It accounts for 69% of inbound web traffic and 84% of outbound web traffic. It is also the top bandwidth consumer with 45.23% bandwidth usage.

SMTP Server
The host IP of 173.94.164.194 is the main SMPT server with the inbound and outbound SMTP traffic volume of 91% and 67% of all traffic, respectively. Another host (173.94.167.7) was identified as secondary SMTP server. This host has inbound and outbound SMTP traffic volume of 8.5% and 33% respectively.

There are 4 external SMTP servers identified as main SMTP servers that our network has connection to. These 4 external SMTP servers account for 84% of inbound SMTP traffic and 76.5% of outbound SMTP traffic.

FTP Server
The host IP 173.94.202.153 is the main FTP server in the network with 99.9% of all FTP traffic, both inbound and outbound.

The external host IP of 192.216.84.155 is identified as the external FTP server that our network relies upon. It accounts for 25% of inbound FTP traffic and 68% of outbound FTP traffic.

DNS Server
The host IP 173.94.167.24 is the main DNS server in the network which accounts for 97% of inbound DNS traffic and 99% of outbound DNS traffic.

Based on the general profile of the network, the following architectural improvements are recommended for the network.

- Redundant servers are recommended for the identified choke points and single point of failure, which are web server, DNS server, and FTP server.
- Proper load balancing should be established for SMTP servers since the secondary SMTP server has much lower traffic volume than the main SMTP server.
- Alternative routes for dependency external SMTP servers and FTP server should be established to increase survivability of the network.

Apart from general profile of the network, further analysis has been conducted on the traffic flows data to identify possible security-related traffic. The result yields two types of scan traffic on the dataset. The first scan traffic was generated from 8 external hosts to the entire network range on the commonly known vulnerable ports. These ports are TCP port 1433 which is used by Microsoft SQL

Server database management system Server, TCP port 2967 which is used by Symantec Antivirus Corporate Edition, TCP port 3389 which is used by Windows Based Terminal (Remote Desktop Protocol), and TCP port 8080 which is an alternate port for web server. Most of the requests generated by the scan traffic were either dropped or responded back with TCP RESET; however, there were three hosts that replied the scan request with TCP SYN/ACK. These three hosts are 173.94.202.192 on port 3389, 173.94.202.162 on port 8080, and 173.94.202.169 on port 8080. As a result, the scanning host would know that there are services running on these ports on these three hosts and might try to exploit the vulnerability on these hosts.

The other scan traffic was in the form of SYN scan on TCP port 3128, 3127, and 3124. These ports are normally used by squid web proxy and CoDeeN proxy. The scan was performed mainly on three hosts (173.94.202.222, 173.94.202223, and 173.94.202.208) throughout the day, but with relatively low traffic volume.

The last security-related incident found on the dataset was backscatter traffic which indicates DDoS attack or other forms of IP spoofed traffic in internal and external network. These backscatter traffic volume was very low and is considered to be normal in any network traffic.

Based on these incident analyses, the following actions are recommended to improve the network's security.

- The administrator who looks after the host 173.94.202.192, 173.94.202.162, and 173.94.202.169 should be notified about possible attacks on these hosts in order to perform necessary inspection.
- Inspection should be performed on host 173.94.202.208, 173.94.202.222, and 173.94.202.223 to find possible relation with the suspicious scan traffic found in the analysis.
- Ensure that the network firewall is configured properly to drop illegitimate or malicious traffic.
- Ensure that the latest patches are applied for the Operating Systems and services run on the network's hosts, especially for the services associated with the ports identified in the analysis.

Network Profile

General information and assumptions on the chosen network

We pick 173.94.0.0/16 network to perform an thorough network analysis. The traffic associated with this network is accounted approximately for 4% of the overall traffic volume by bytes. The analysis was conducted on the MAWI sample point F dataset with an appropriate anonymization scheme already applied to the dataset before the analysis.

For some client-server connection (request-response), there is a chance that either request or response traffic went through the MAWI sample point F while the matching request or response traffic traversed to the destination using different path(not crossing MAWI sample point F). For our analysis, we will assume that every packet on the same connection will traverse using the same path. Moreover, many traffic associated with our chosen network might not traverse through the MAWI sample point F. Thus, an unknown amount of traffic associated with our network wasn't captured by the MAWI sample point F dataset. Therefore, it is important to note that our analysis might not reflected the complete picture of the traffic and might be slightly distorted.

Network summary

Network address: 173.94.x.x/16

Traffic Trace Info

Start time	March 30 15:00:00 2009
End time	March 31 15:00:00 2009
Total time	86400 seconds
Number of packets	272794639 (225561584988 Bytes)
Average Rate	20.89 Mbps

IP flow (unique src/dst pair) Information

Number of flows 11715564 (avg. 23.28 pkts/flow)

Top 10 big flow size (bytes/total in %):

0.80% 0.71% 0.58% 0.53% 0.47% 0.47% 0.39% 0.38% 0.37% 0.36%

IP address Information

Top 10 bandwidth usage (bytes/total in %) – Internal host:

sIP	%_of_total
173.94.202.147	45.23%
173.94.210.209	4.91%
173.94.36.236	3.45%
173.94.17.222	3.36%
173.94.202.157	2.00%
173.94.202.208	1.66%
173.94.202.220	1.55%
173.94.202.223	1.21%

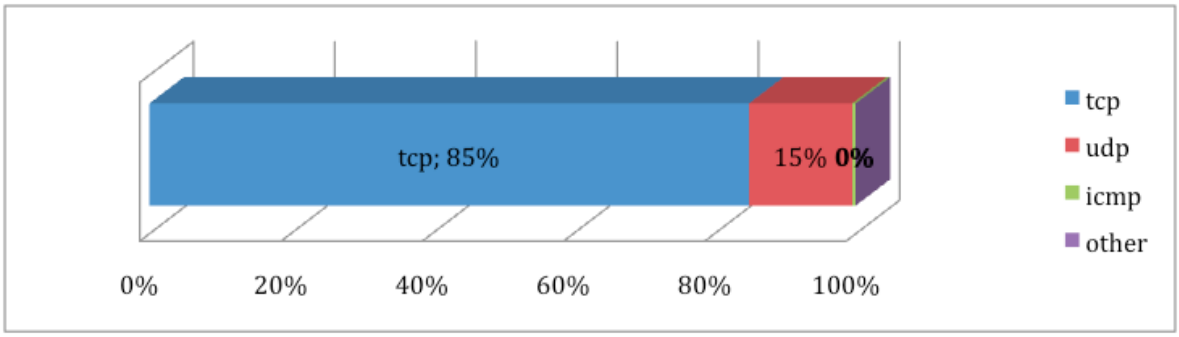
173.94.202.222	1.19%
173.94.89.99	1.69%

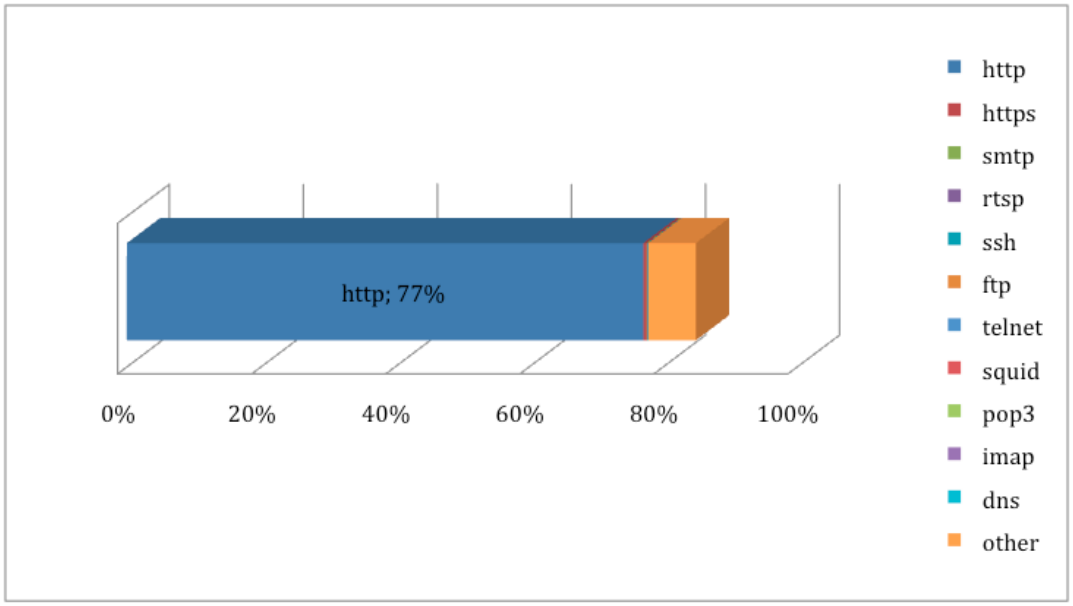
Top 10 bandwidth usage (bytes/total in %) – External host:

dIP	%_of_total
11.78.21.28	5.11%
8.87.199.65	3.29%
5.174.1.134	0.31%
6.87.64.225	0.21%
36.87.65.27	0.17%
96.110.14.23	0.13%
53.59.99.197	0.11%
36.87.68.213	0.11%
200.35.5.149	0.10%
45.174.1.75	0.09%

Protocol Breakdown

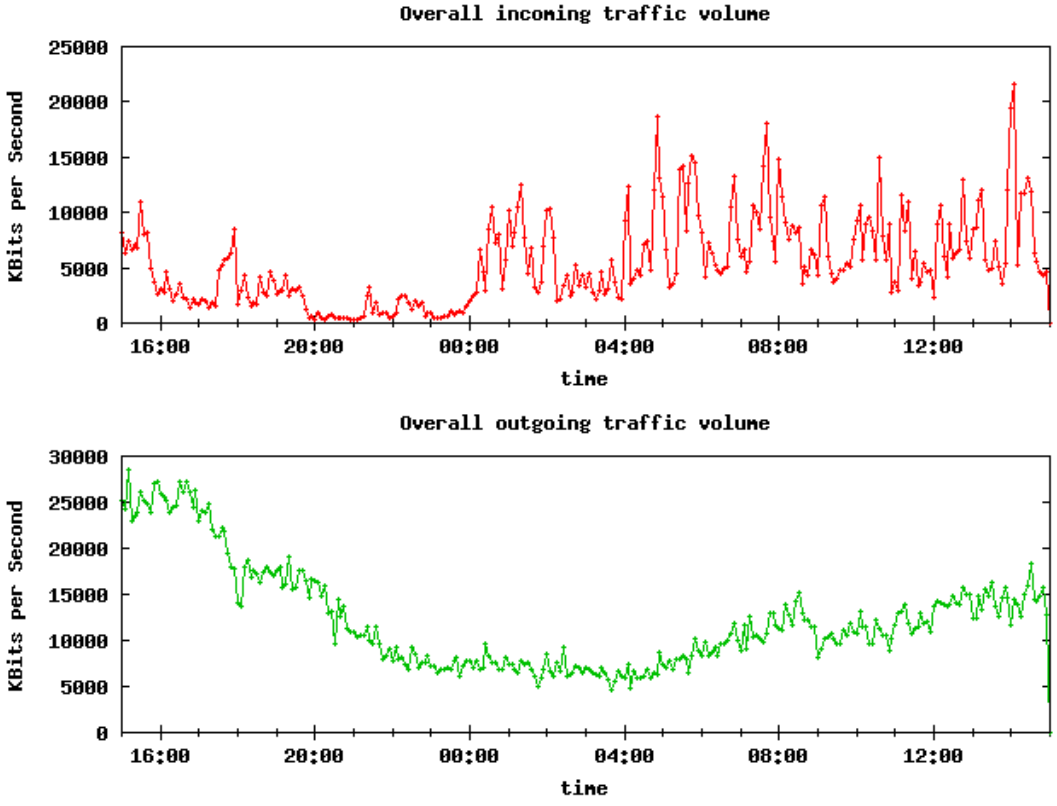
The right-hand protocol and application list are sort in order of the amount of the traffic by bytes.





Protocol	Packets		Bytes		bytes/pckt
total	272794639	100%	225561584988	100%	826.8549
tcp	212692956	78%	191517619060	85%	900.44176
http	181648252	67%	173816747403	77%	956.88643

https	1985492	1%	1101652440	0%	554.85111
smtp	906783	0%	339305329	0%	374.18581
rtsp	90005	0%	122555848	0%	1361.656
ssh	336047	0%	66735825	0%	198.59075
ftp	668582	0%	51355587	0%	76.812698
telnet	127978	0%	35851122	0%	280.13504
squid	7211	0%	6150972	0%	852.99847
pop3	35243	0%	3570296	0%	101.30511
imap	24030	0%	2553601	0%	106.26721
dns	3067	0%	147958	0%	48.24193
other	26860266	10%	15970992679	7%	594.59548
udp	54736874	20%	32948674014	15%	601.94658
dns	3210306	1%	432841088	0%	134.82861
cuseeme	3096	0%	1865608	0%	602.58656
quake	491	0%	67504	0%	137.48269
other	51522981	19%	32513899814	14%	631.05626
icmp	5364548	2%	1095280898	0%	204.17021
other	261	0%	11016	0%	42.206897



Overall traffic volume(used as an reference to compare the trend between data)

Network component summary

Web server

- 173.94.202.147

Account for 69% of inbound web traffic and 84% of outbound web traffic. It is also the top bandwidth user with 45.23% bandwidth usage.

SMTP server

- 173.94.164.194

  Account for 91% of inbound SMTP traffic and 67% of outbound SMTP traffic

- 173.94.167.7

  Account for 8.5% of inbound SMTP traffic and 33% of outbound SMTP traffic

External SMTP server (dependency)

- 213.137.161.91
- 213.137.161.6
- 45.188.42.135
- 192.50.217.134

Account for 84% of inbound SMTP traffic and 76.5% of outbound SMTP traffic

FTP server

- 173.94.202.153

  Account for 99.9% of inbound and outbound FTP traffic

- 192.216.84.155

  Account for 25% of inbound and 68% of outbound FTP traffic

- 36.87.65.27 and 192.100.211.64

  might use ftp accelerator to download large file from the internal FTP server

DNS server

- 173.94.167.24

  Account for 97% of inbound and 99% of outbound DNS traffic ICMP

- A lot of outgoing echo request (67%) and incoming echo reply (41%)
- A lot of incoming time exceeded message (40%)
- A lot of outbound destination unreachable message (30%) -> scan attempt

Network incident analysis summary

1. There're 8 hosts performing a SYN-scanning on the commonly known vulnerable port on the entire network range. Each host perform the scanning once over a very brief period in that day. These ports are,

   1433 - used for remote connection to the SQL server database

   2967 - used by Symantec anti-virus software known to have a severe vulnerability associated with this port.

   3389 - used for remote desktop connection to the window platform server.

Most of the scanning packets were dropped either by ACL-devices or because the host being scanned isn't exist in the network. The rest of the packets for 192 hosts that got into the network were mostly responded by the RST packet. Only 3 host which is,

173.94.202.192 / Port 3389

173.94.202.162,169/ Port 8080

These hosts did responded back to the SYN scanning with SYN/ACK. This means that these ports on these hosts are opened. The scanning host will realize this fact and potentially try to exploit the vulnerability on those ports on each host.

The scanning host used port 6000 to perform a scan. This suggests that the scanning hosts might use same automated tool to perform a SYN-sweep scan on our network, or those scanning hosts might be infected by malicious code performing the scanning on our network under control by those codes.

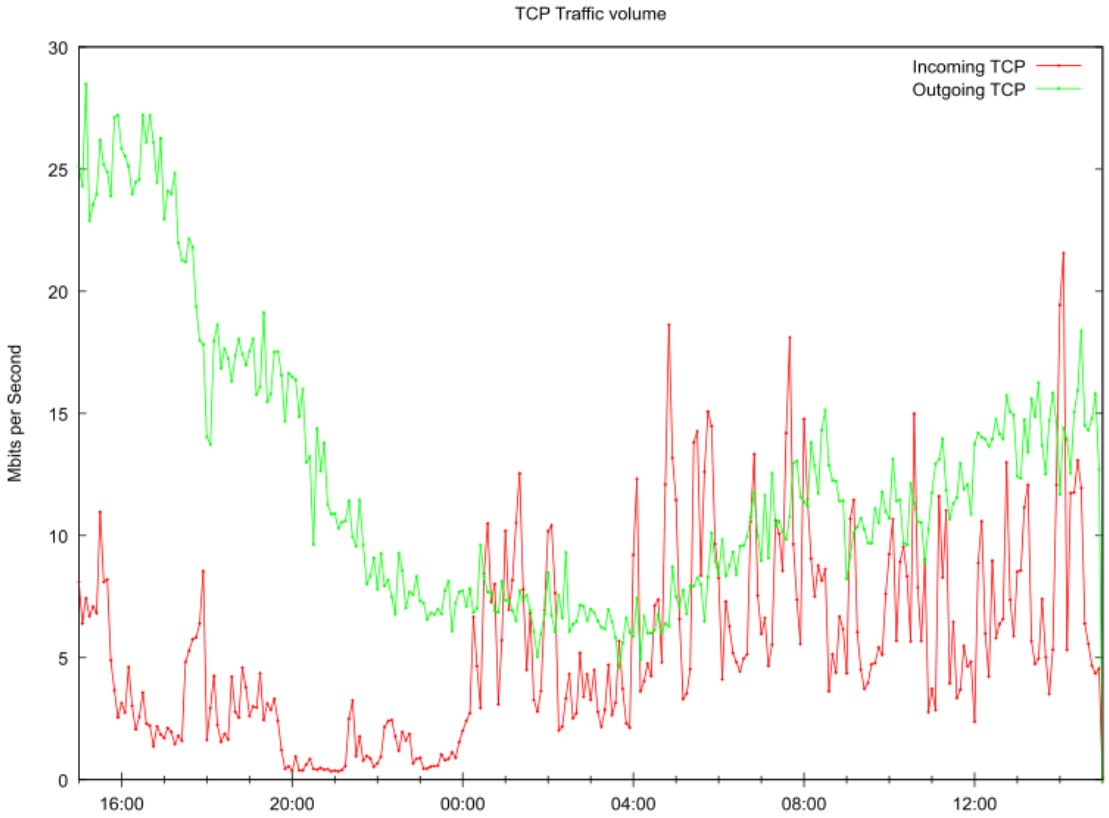
2. There are up to thousand hosts performing a SYN-scan on port 3128, 3127, 3124 (3127 is known for squid web proxy, 3128 = squid's control port, 3124 is also a proxy). These scans were performed consistently throughout the day with a very low traffic volume(less than 3 kb/sec accumulatively). The hosts being scanned using this method are 173.94.202.222, 223 and 173.94.202.208. This could be either malicious traffic or just keep-alive traffic with the server listening on these ports.

3. In our analysis, we found a small amount of backscattering associated with our network in which the attacker spoofed the message using our network address as a spoofed ip address. Also, we found a miniscule amount of backscattering when our network is the target thus the attacker sent the spoofed ip address packet into our network, and, as a result, our network reply this packet back to the spoofed-ip host. These backscattering indicates either the DDOS attack upon external network or the DDOS attack on our network. However, the volume is not significant to create such damages.

Common protocol and port inspection

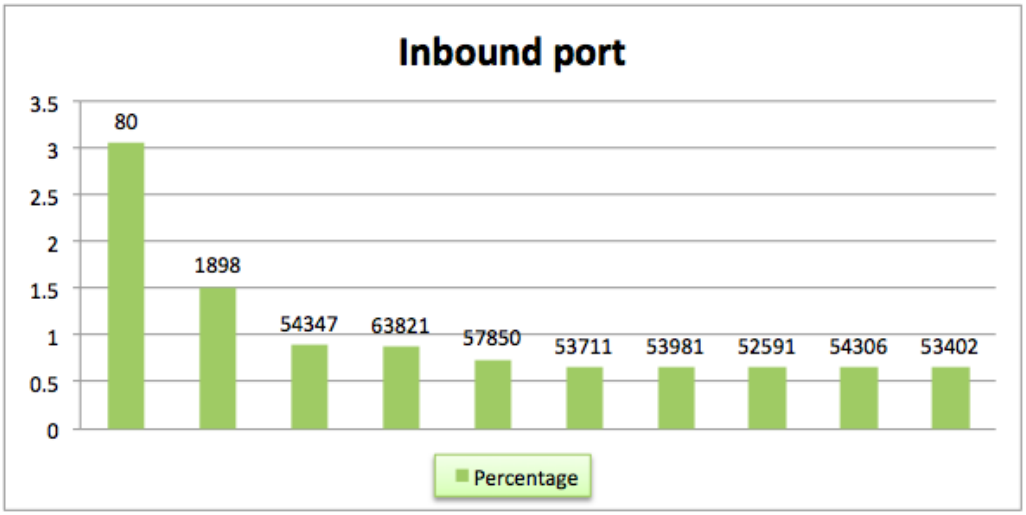
TCP and TCP port

TCP traffic accounted for 78% of the overall traffic. Outbound and inbound TCP traffic volume is approximately running around 13-14 Mbps and 4-5 Mbps respectively. The TCP traffic volume graph, as shown below, doesn't show any suspicious pattern/activity of the traffic. The graph follows the normal behavior of regular network usage. That is, higher volume of traffic for the working period 07:00 - 20:00 and lower volume of traffic for 20:00-07:00. More specific



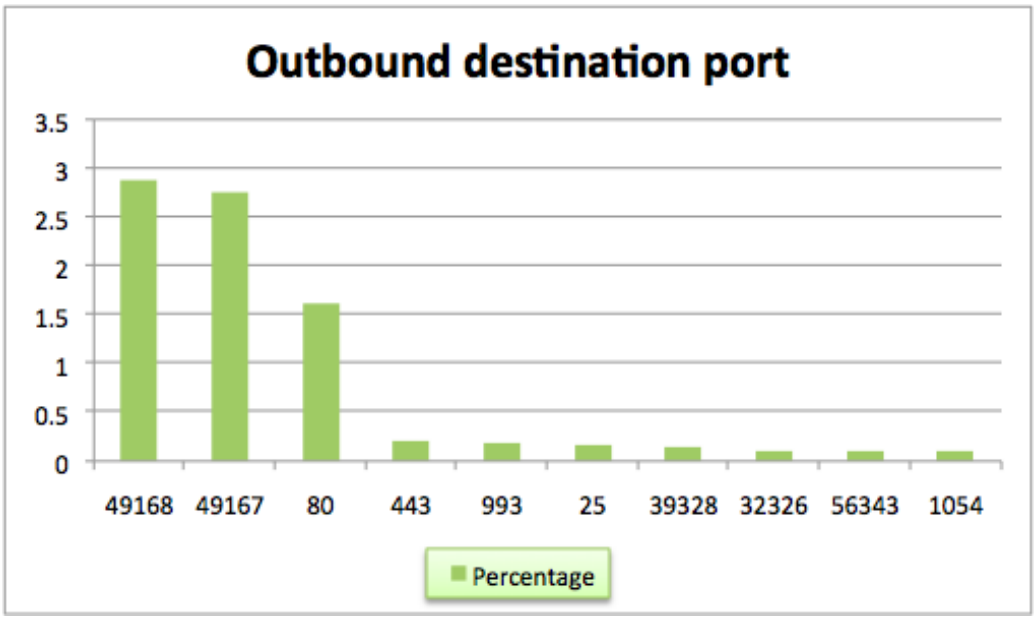
inspection is required in order to find activity pattern for specific application.

When we look into the proportion of the tcp port, we will see that port 80 accounts for the most internal port inside the network being connected to(inbound traffic). This suggests that there are web server resides in our network offering web page (HTTP) service. Note that the other ports in our network being connected to, which is rank 2-10 in term of traffic volume are high-number port which might indicate the port for web-browser application or any other application that connects to the external network. Thus, the traffic volume on these ports might be web-data (html) or other application data responded back from external network to our network.



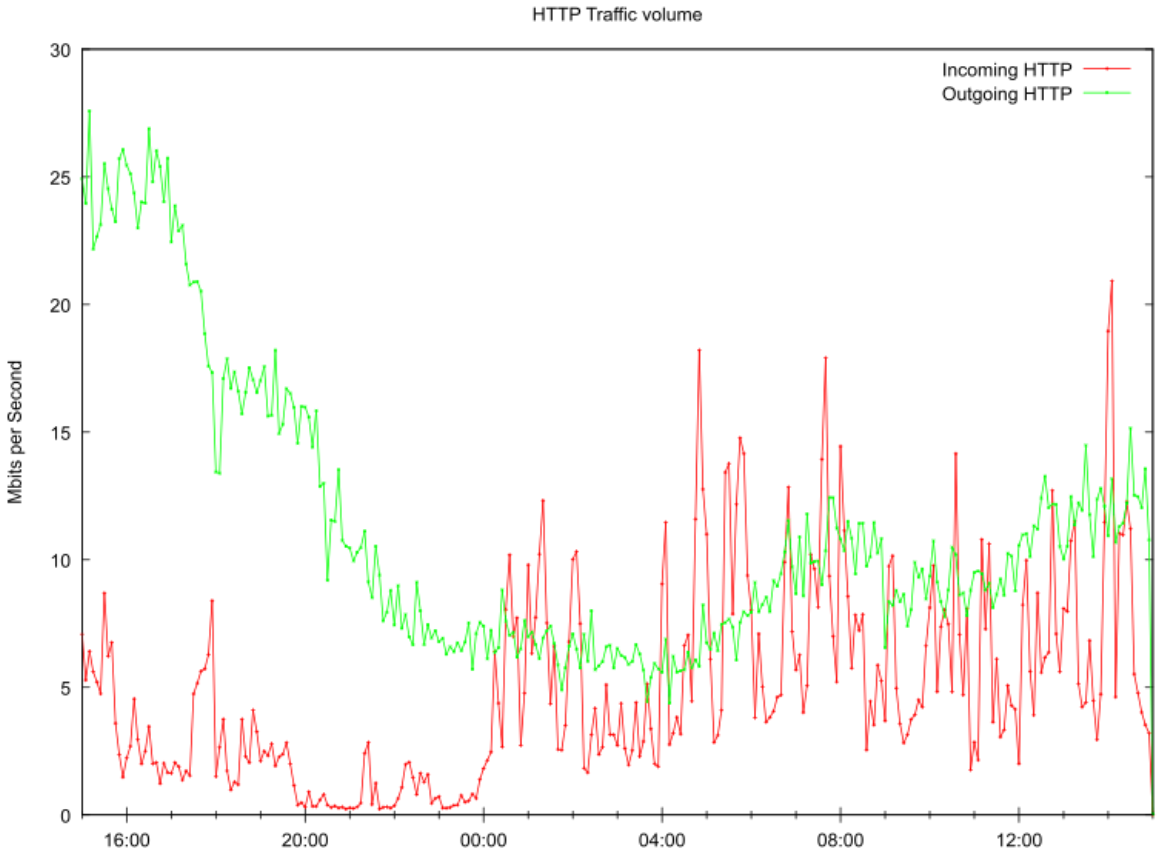
For the outbound traffic, we can see that our network used the service offered by other networks on common ports 80(HTTP), 443(HTTPs), 25(SMTP) in order by traffic volume. Note that high port outgoing traffic on destination port 49168, 49167 and other high-number port account for the first,second and high-rank place in term of the outbound traffic volume respectively.

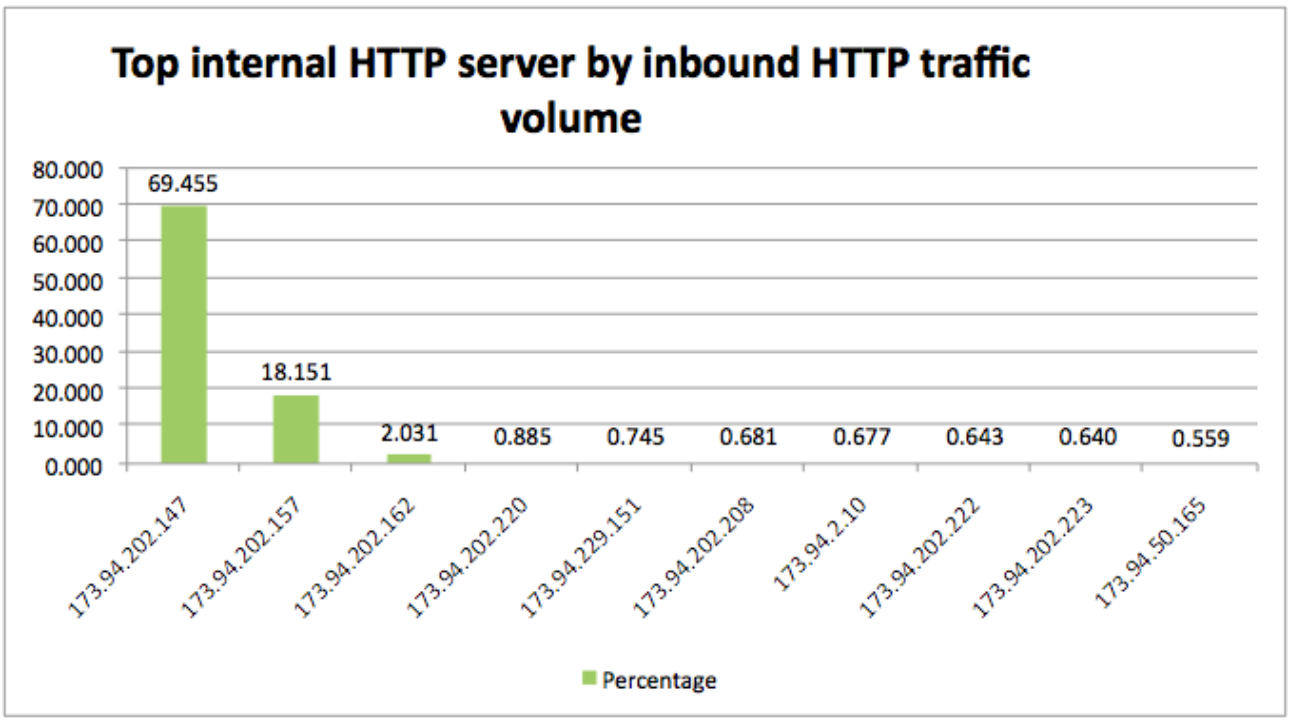
We inspected further on port 49168 and 49167 and found out that the traffic on these port mostly (>90%) are HTTP responses from the web server inside our network (173.94.36.236) to 18.87.199.65(>98% of the response, in term of bytes, went to this address). This indicates large proportion of http traffic which is a http connection between 173.94.36.236 and 18.87.199.65 traversed pass our collection point. Therefore, this might indicate the high dependency (in term of http connection) between those two hosts. Other high-number destination ports (39328m 32326 and beyond) also communicated with the internal port 80 on many internal web servers.

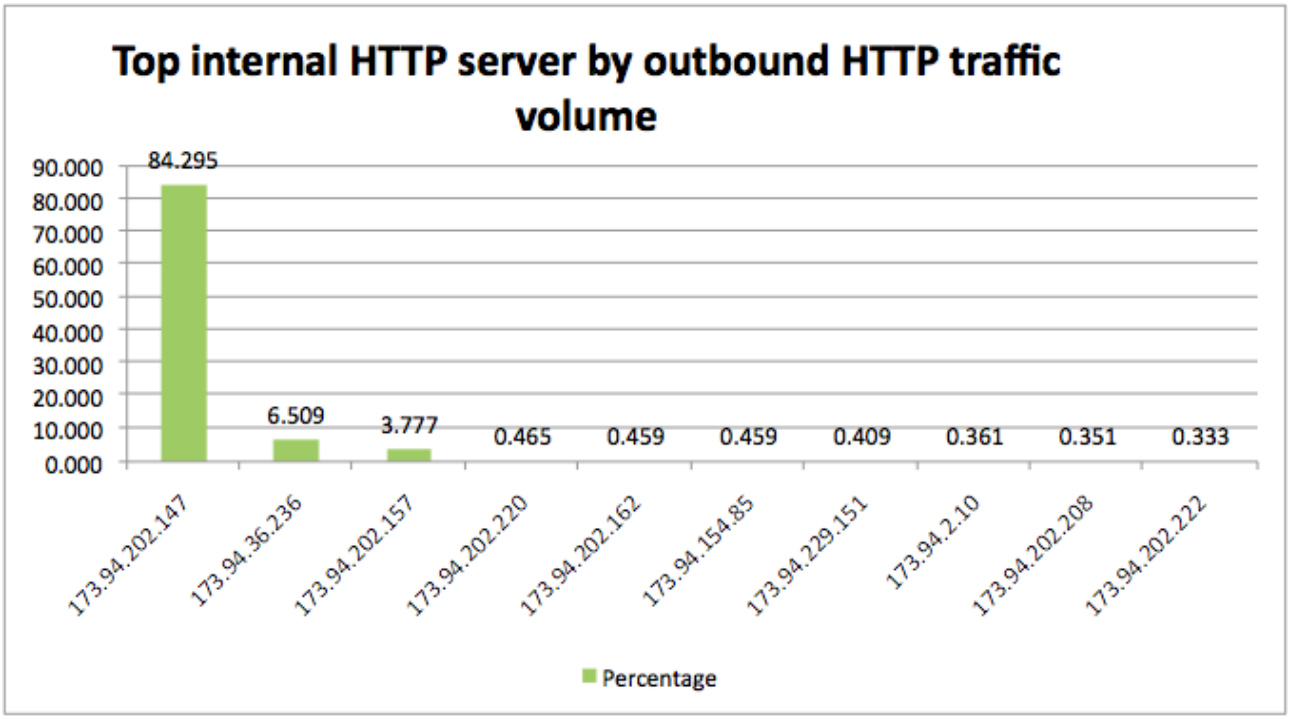


HTTP/HTTPS

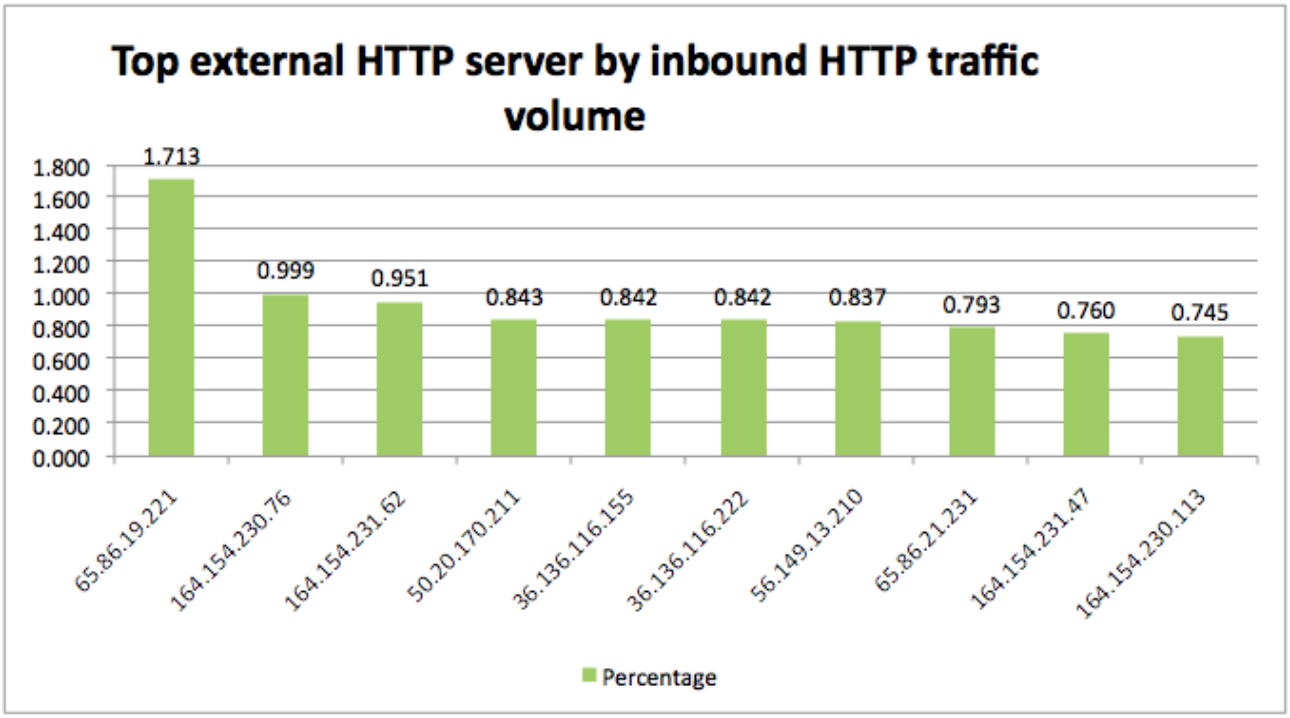
HTTP and HTTPS traffic also followed the TCP traffic trend since both accumulatively are accounted up to 68% of TCP traffic. the large proportion of http/https traffic plus the fact that the incoming HTTP traffic volume was larger than outgoing HTTP traffic volume, indicates that our network mainly serves web traffic to other networks.

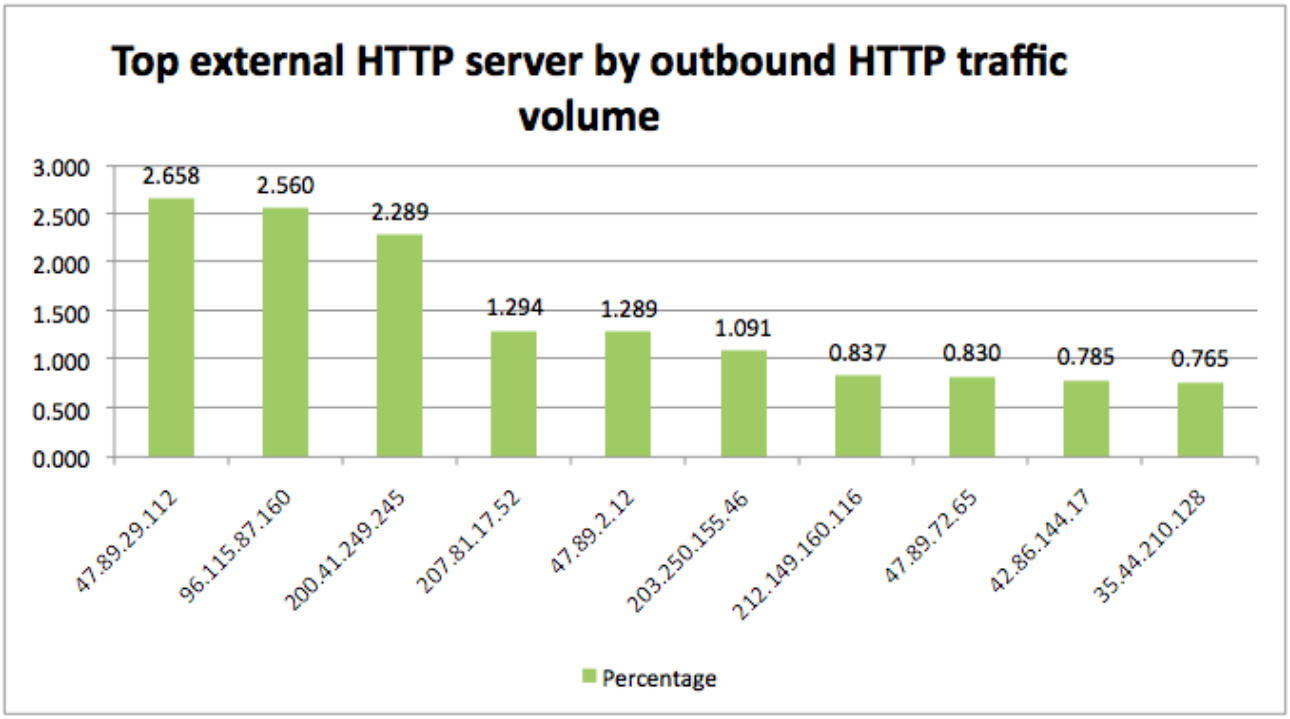

HTTP Traffic volume
Incoming HTTP
Outgoing HTTP
Mbits per Second
30
25
20
15
10
5
0
16:00
20:00
00:00
04:00
08:00
12:00


Top internal HTTP server by inbound HTTP traffic volume
80.000
70.000
60.000
50.000
40.000
30.000
20.000
10.000
0.000
69.455
18.151
2.031
0.885
0.745
0.681
0.677
0.643
0.640
0.559
173.94.202.147
173.94.202.157
173.94.202.162
173.94.202.220
173.94.229.151
173.94.202.208
173.94.2.10
173.94.202.222
173.94.202.223
173.94.50.165
Percentage



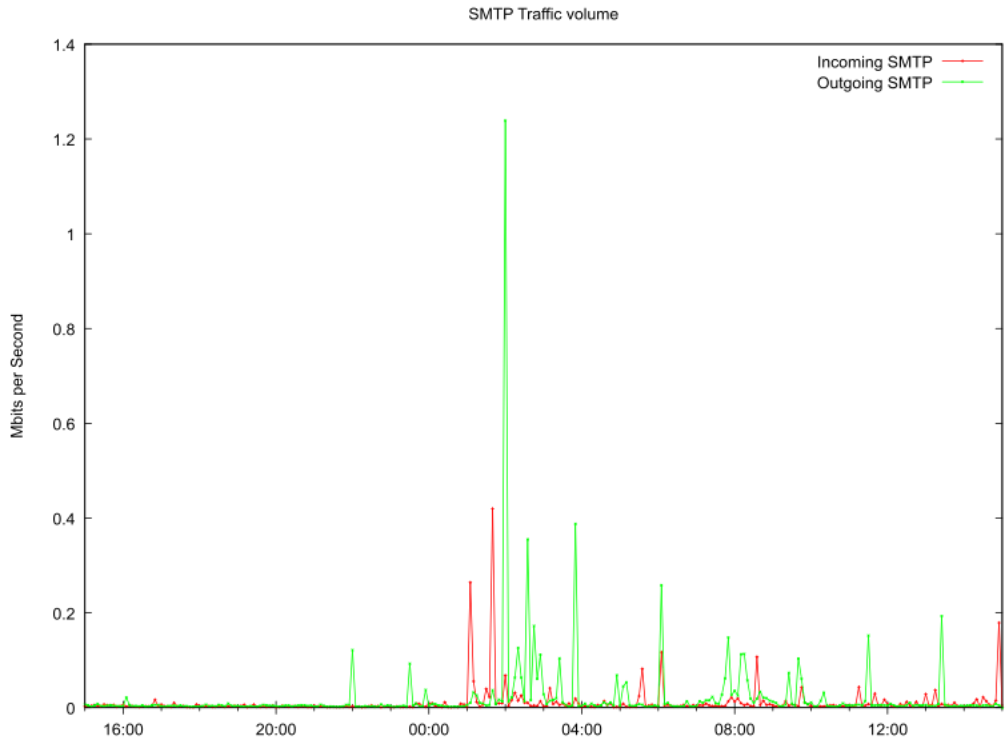
From above data we will see that most of the port 80 traffic are from/to 173.94.202.147 (69% and 84% respectively). 173.94.36.236 and 173.94.202.157 were the second place and third place respectively. Other internal web server traffic volume is insignificant comparing to the majority of the traffic on those three hosts.





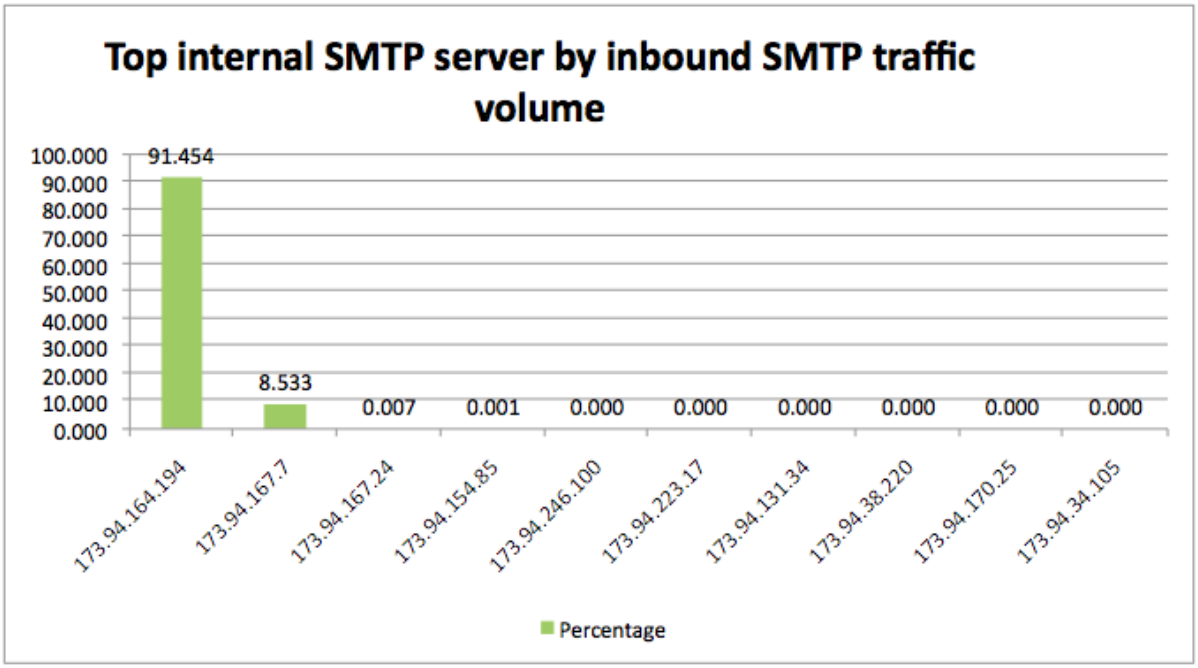
The traffic to/from external web server, however, distributed evenly across the entire range and showed no prominence other than there's a certain amount of HTTP requests from our network to many external networks.

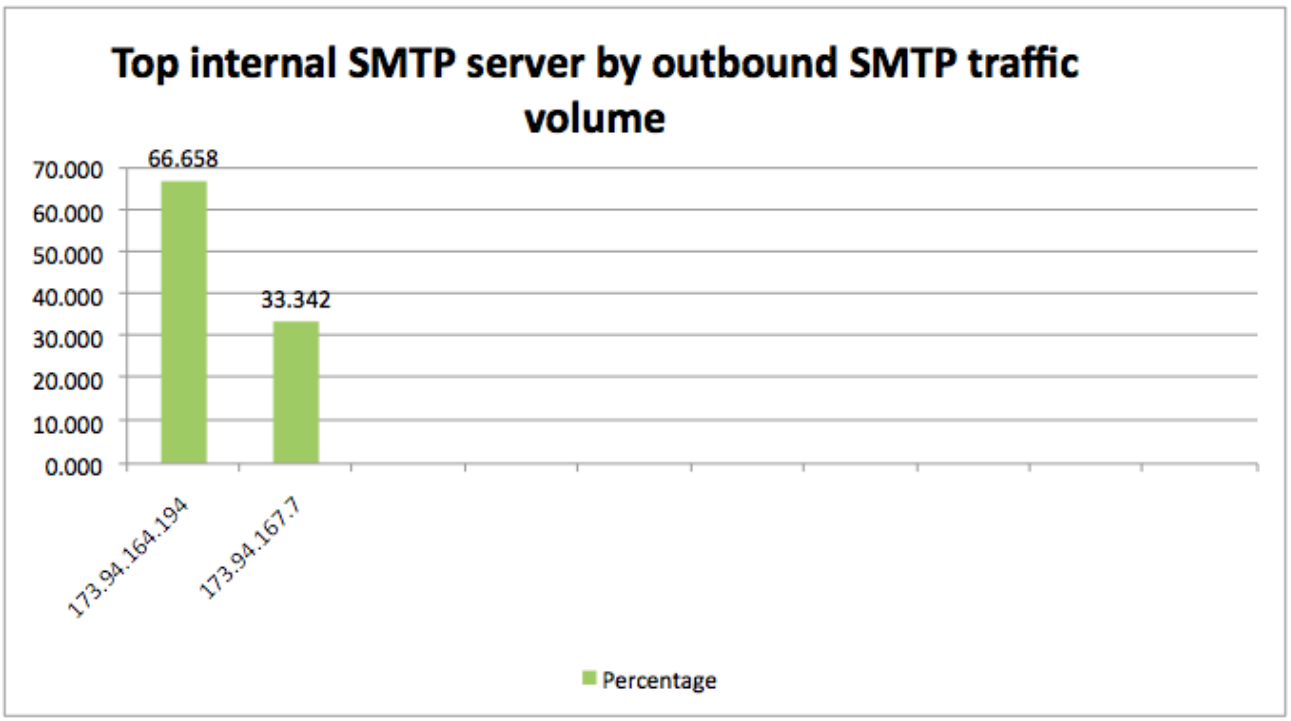
SMTP



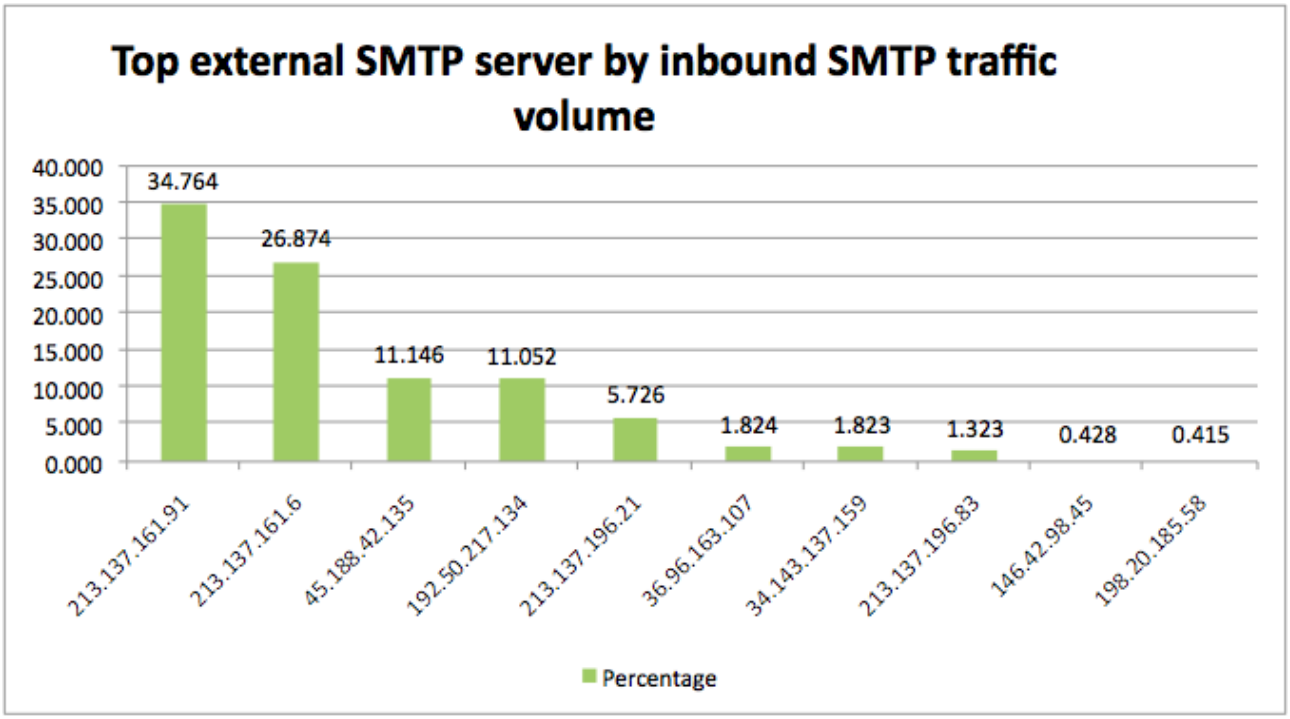
SMTP traffic accounted for < 1% of the traffic amount. The graph shown above indicate the SMTP activity highest at 01:00-04:00, then slightly went down from 04:00. The traffic pattern indicates nothing particularly suspicious.

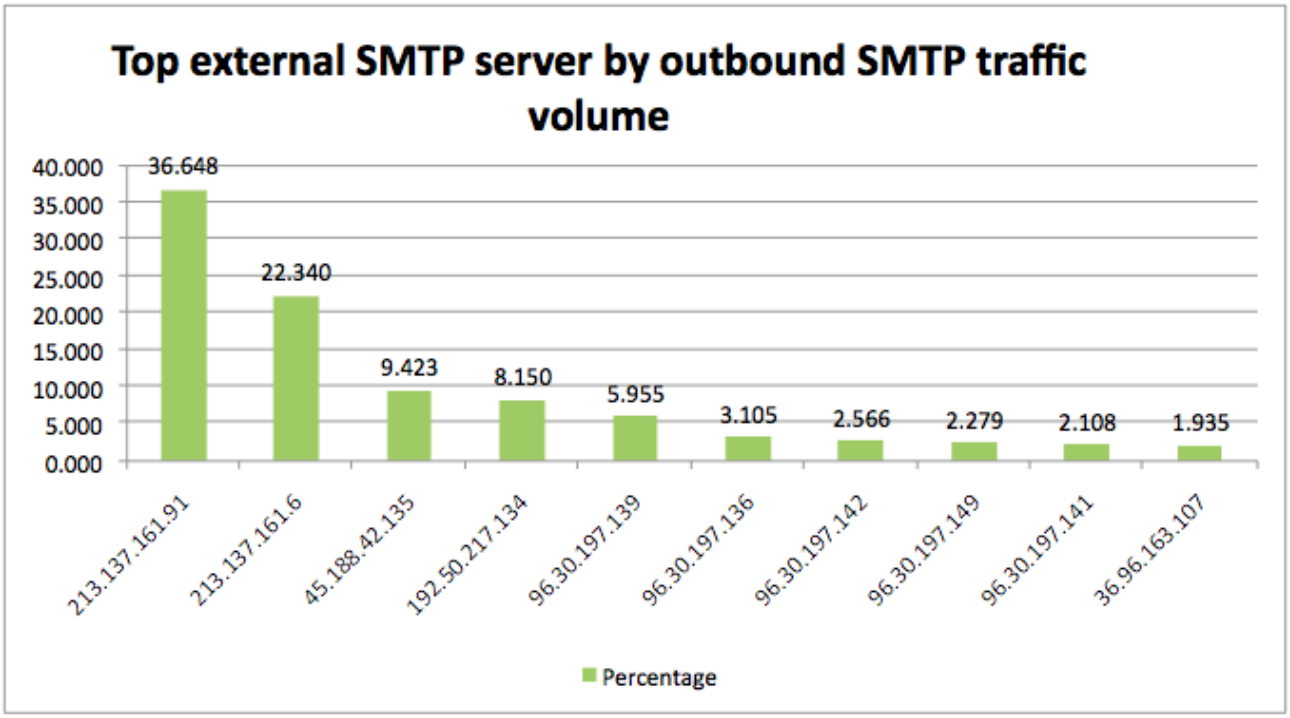
The statistical data showing the SMTP traffic from/to the internal and external SMTP server is provided below,





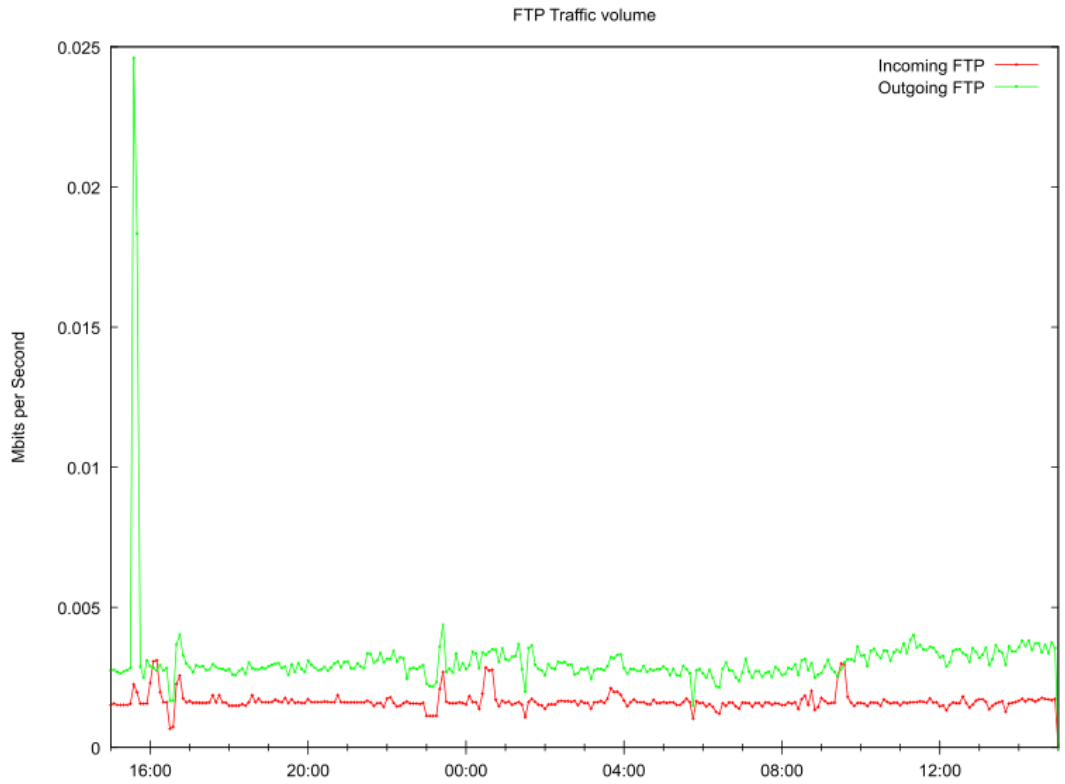
The graph provided above indicate that there's only 2 major SMTP server resided in our network, 173.94.164.194 and 173.94.167.7. With 173.94.164.194 accounted for the most SMTP traffic volume received and sent.





The traffic shown above indicated that our network used the SMTP service mostly offered by 213.137.161.91 (about 35% of inbound/outbound volume), 213.137.161.6, 45.188.42.135,192.50.217.134 and 213.137.196.21 in order of the traffic volume.

FTP

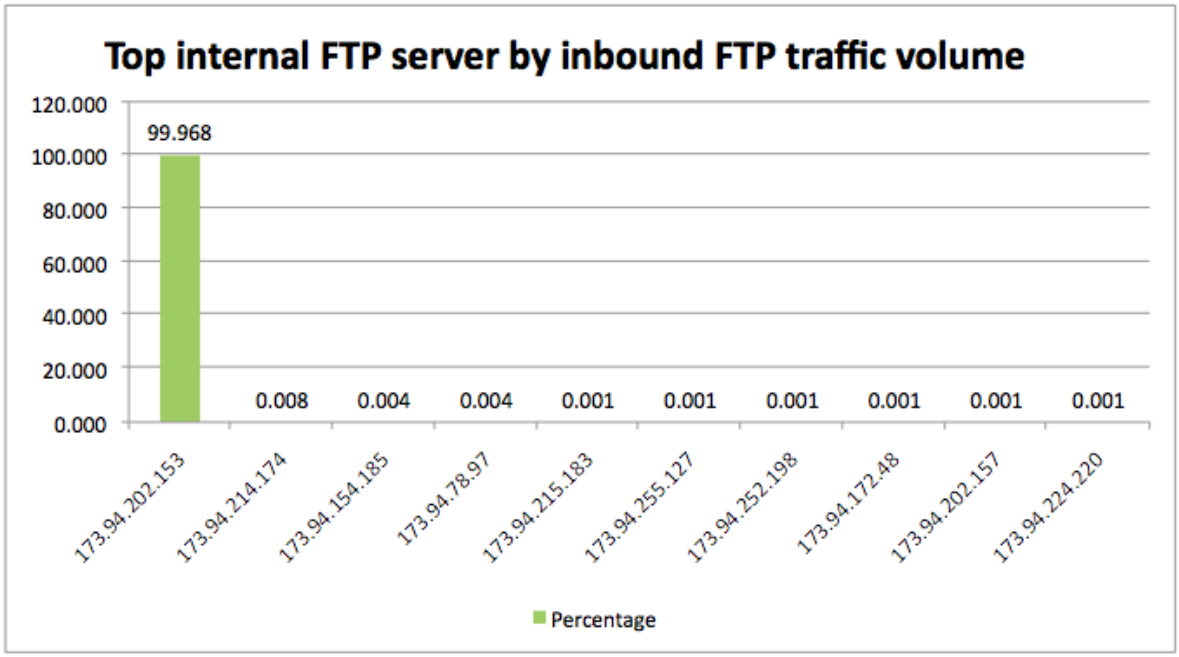


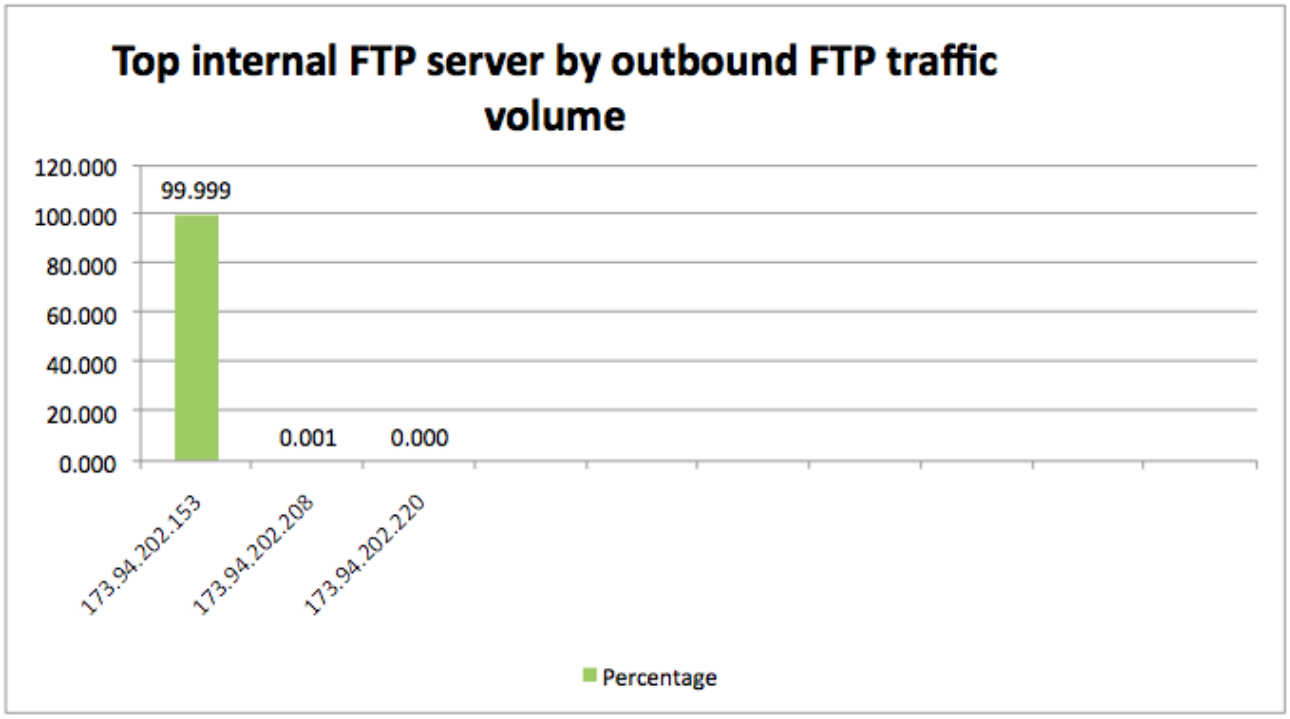
FTP accounted for less than 1% of the volume with normal traffic activity for inbound traffic. The outbound traffic also looks normal except the narrow spike around 15:30.

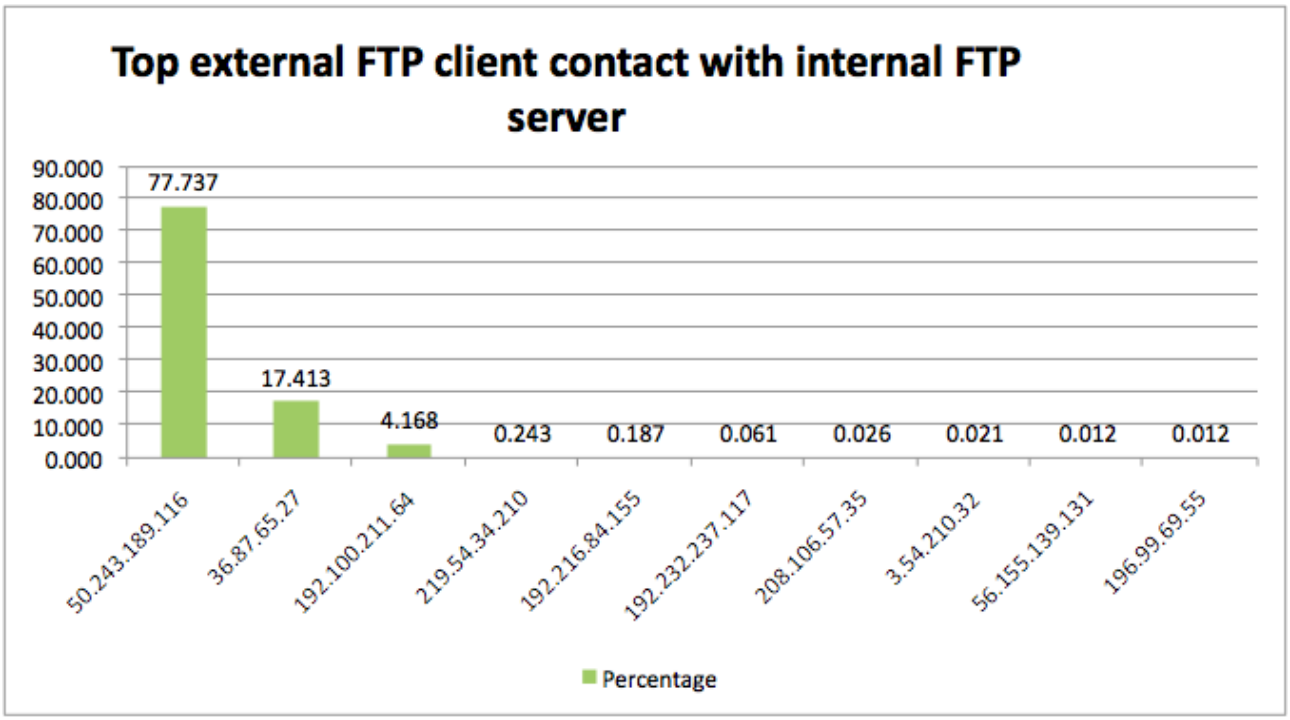
Note on the spike appeared in the graph:

FTP traffic from internal FTP server to 36.87.65.27 and 192.100.211.64 on various ports with FSPA flags set. Note that although the spike is outlined from overall FTP traffic, its traffic volume is very small (less than 0.025 Mbps). One possible explanation is that these two external hosts were using FTP accelerator to download large file from the network's FTP server at that time. See appendix A for the sample flow data around the time of the spike

The statistical data showing the FTP traffic from/to the internal FTP server is provided below,

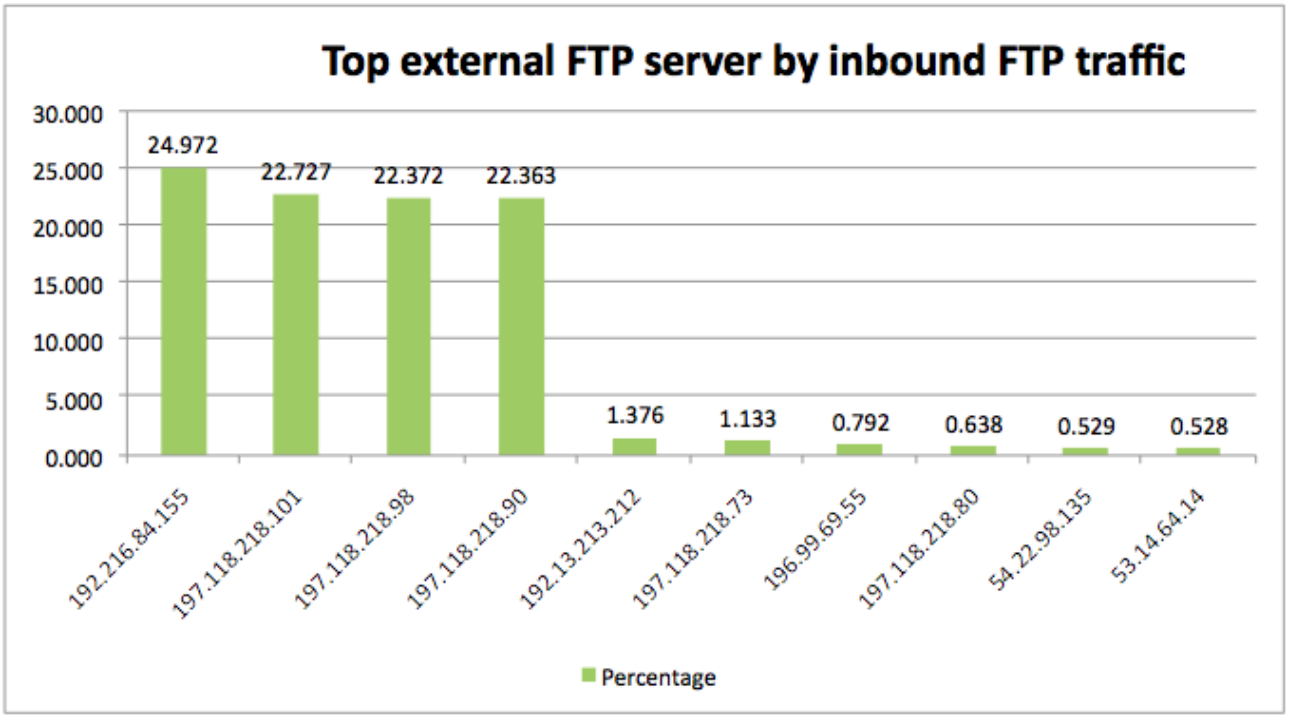


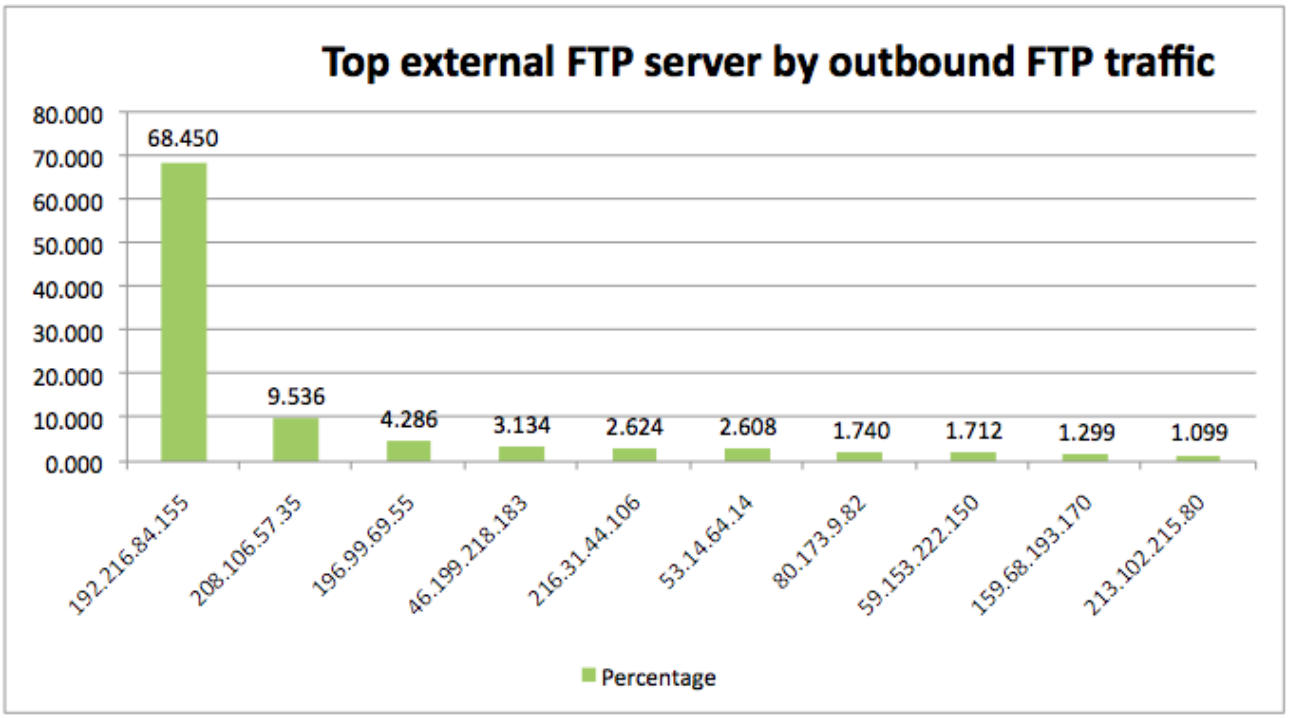




The data shown above indicated that almost all(>99.9%) FTP traffic from/to our FTP internal server went to/from 173.94.202.153. We found out that there're 37 external clients contact with our internal FTP server. Among these 37 clients, 50.243.189.116 accounted for 78% of the traffic, 36.87.65.27 for 17.4% and 192.100.211.64 for 4%. Therefore, there're correlation dependency between our internal FTP server and these three external clients.

The graphical data showing the FTP traffic from/to the external FTP server is provided below,

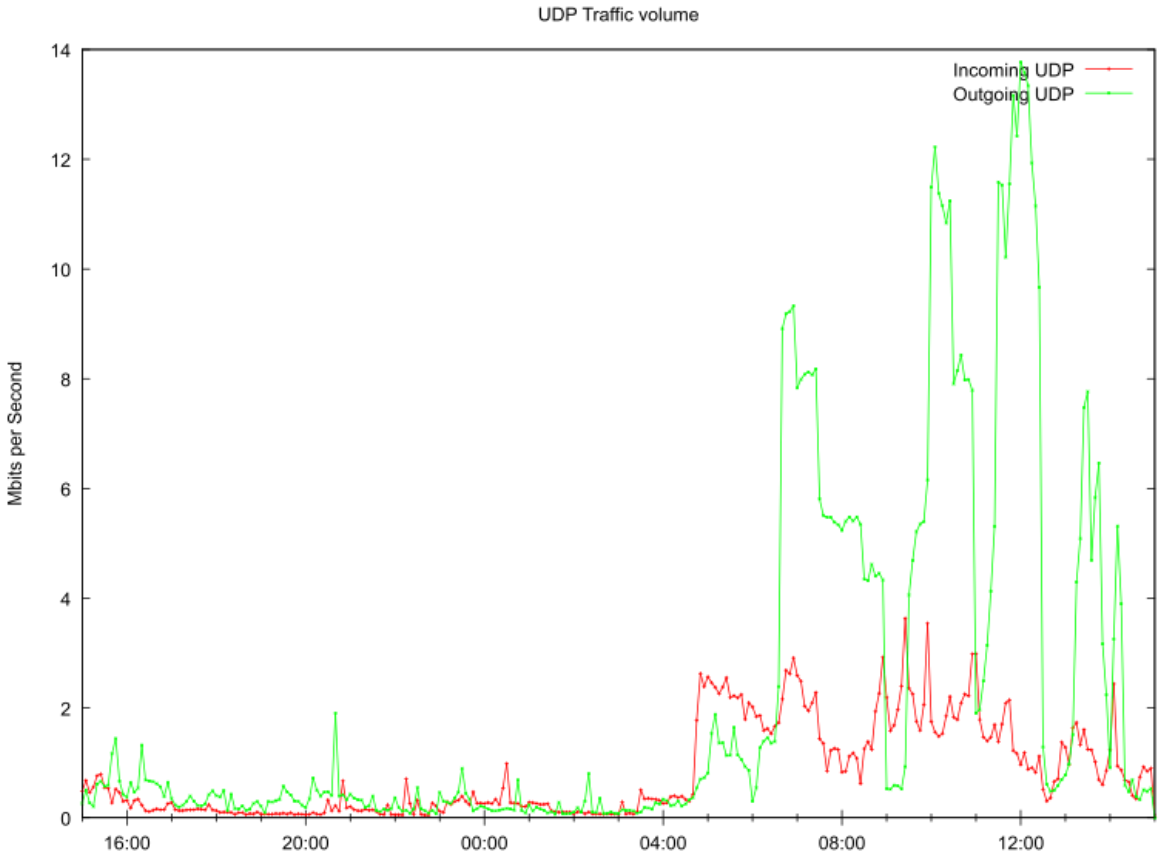


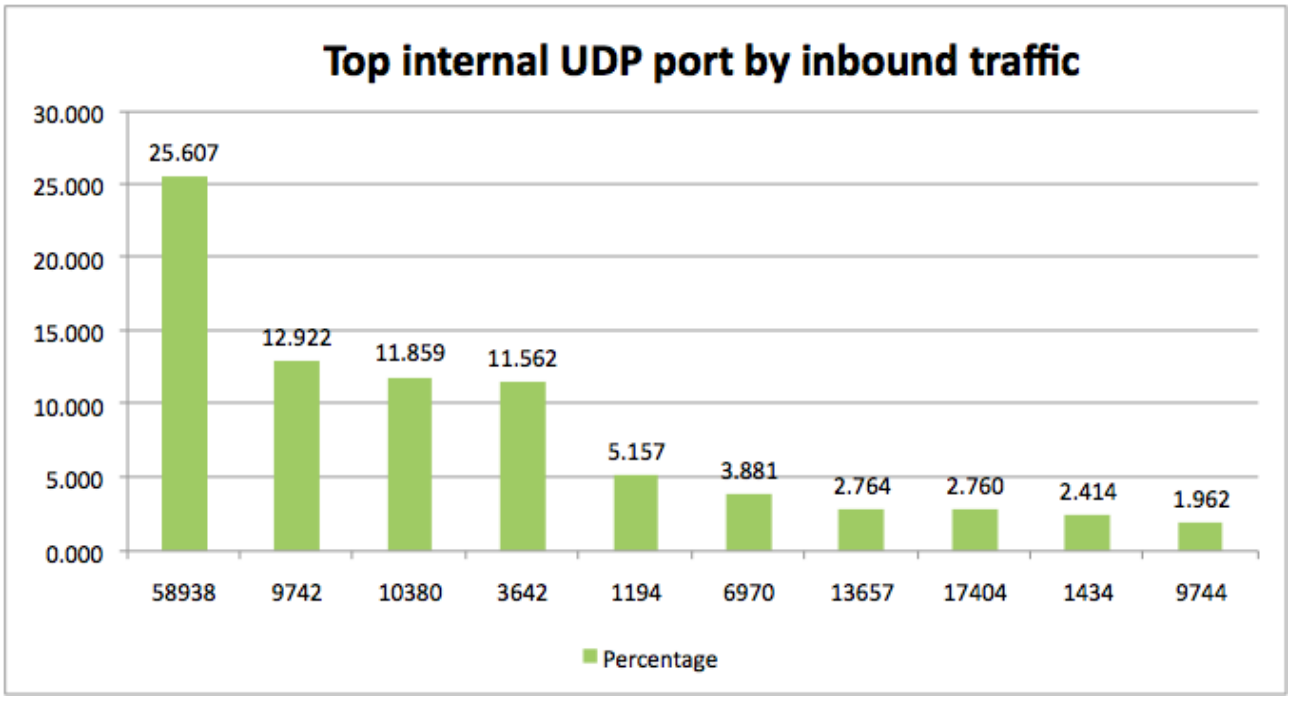


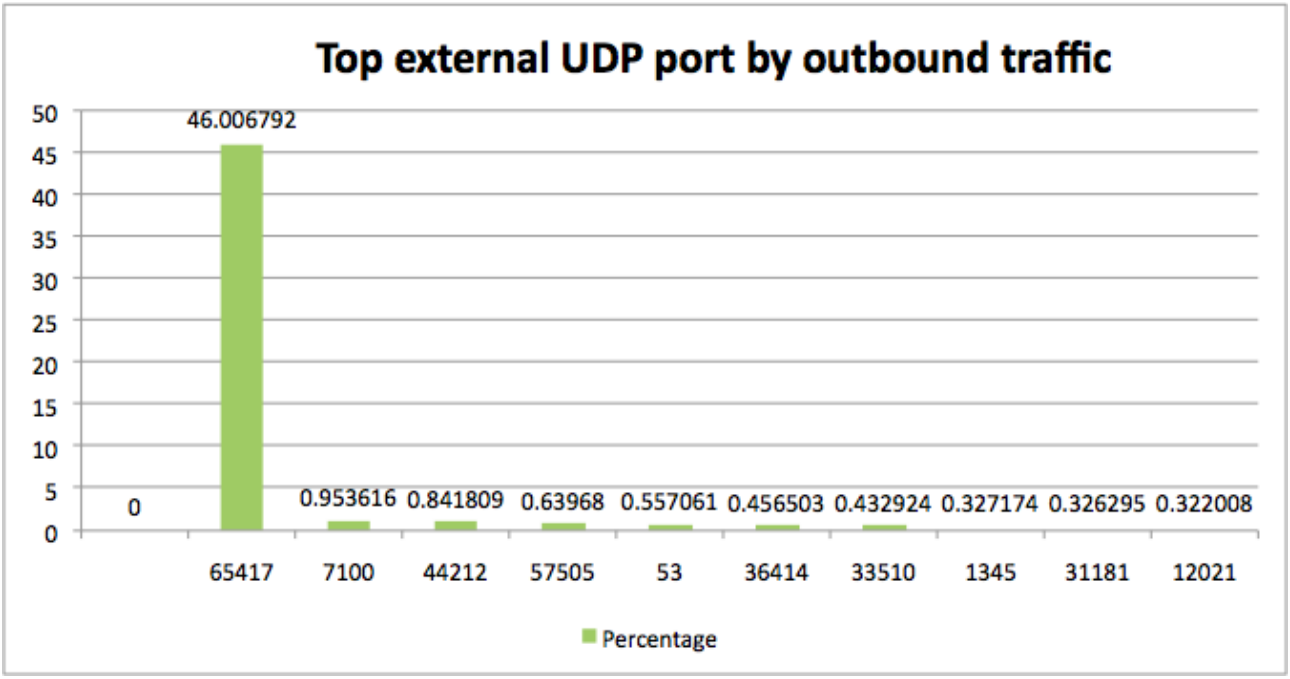
The graphical data above show that our host on the 173.94.x.x/16 network requested the FTP service mostly to 192.216.84.155 in term of the traffic to the external FTP server. The traffic from external FTP server to our network were served mostly by 192.216.84.155, 197.118.218.101, 197118.218.98 and 197.118.218.90 which accounted for 22-25% each. this suggest the dependencies of the FTP service request between our network and those external FTP servers.

UDP

Here's the graphical representation showing the UDP traffic in timely manner along with the Top ten internal/external port for the inbound/outbound traffic.



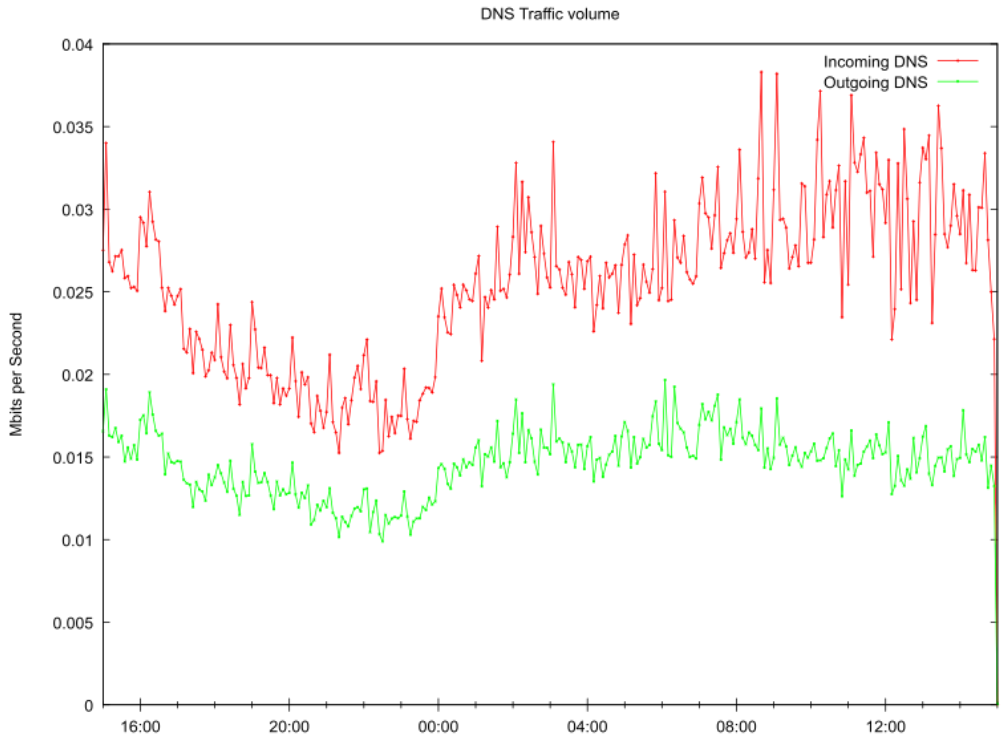




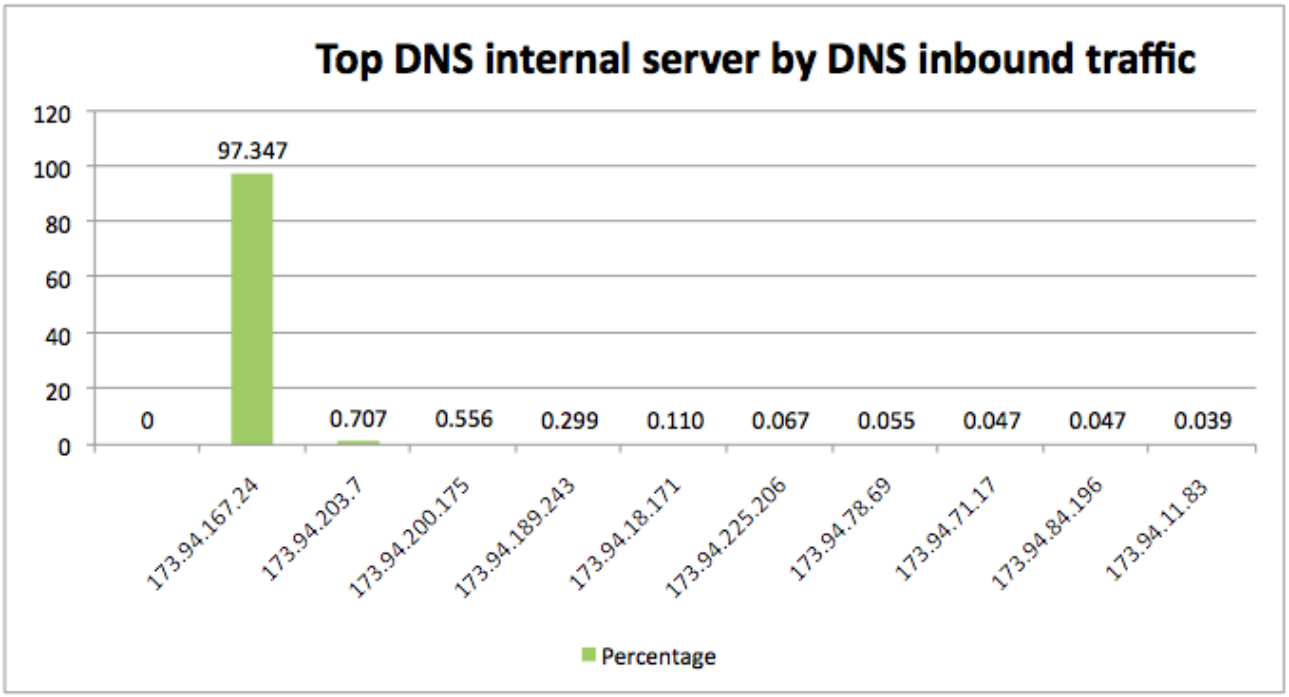
The UDP traffic accounted for 20% of the overall traffic volume by packets and 15% by bytes. The UDP traffic was higher during 06:00-15:00 for both inbound and outbound traffic. We can see that port 65417 was accounted for 46% of the UDP outbound traffic while the UDP outbound traffic on other ports was distributed evenly. We found that the traffic on the external port 65417 is associated with OpenVPN traffic on internal server 173.94.210.209 (port 1194). Similarly, internal UDP port 58937, was accounted for 26% while the others were distributed in a regular fashion. The traffic associated with internal port 58937 was mostly originated from host 173.94.89.99 to many distinct external hosts and ports. This may indicate a UDP scan from our network.

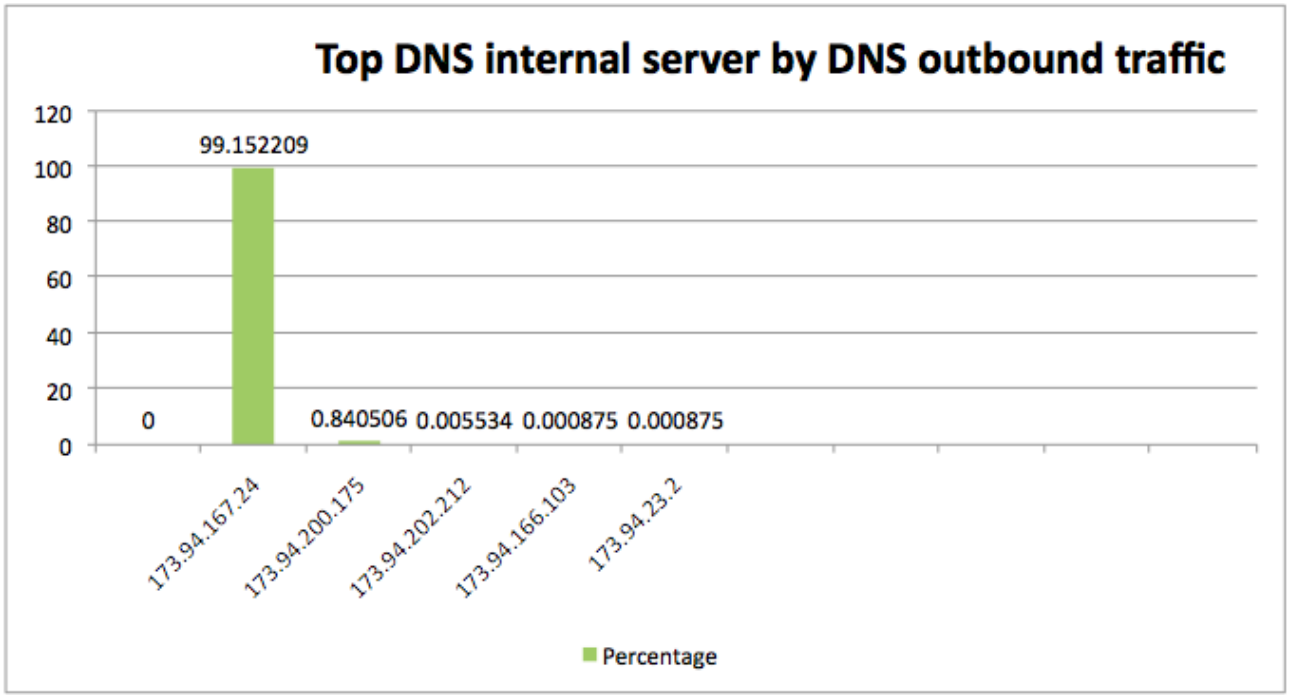
DNS

Here's the graphical representation showing the DNS traffic in timely manner along with the Top ten internal/external port for the inbound/outbound traffic.

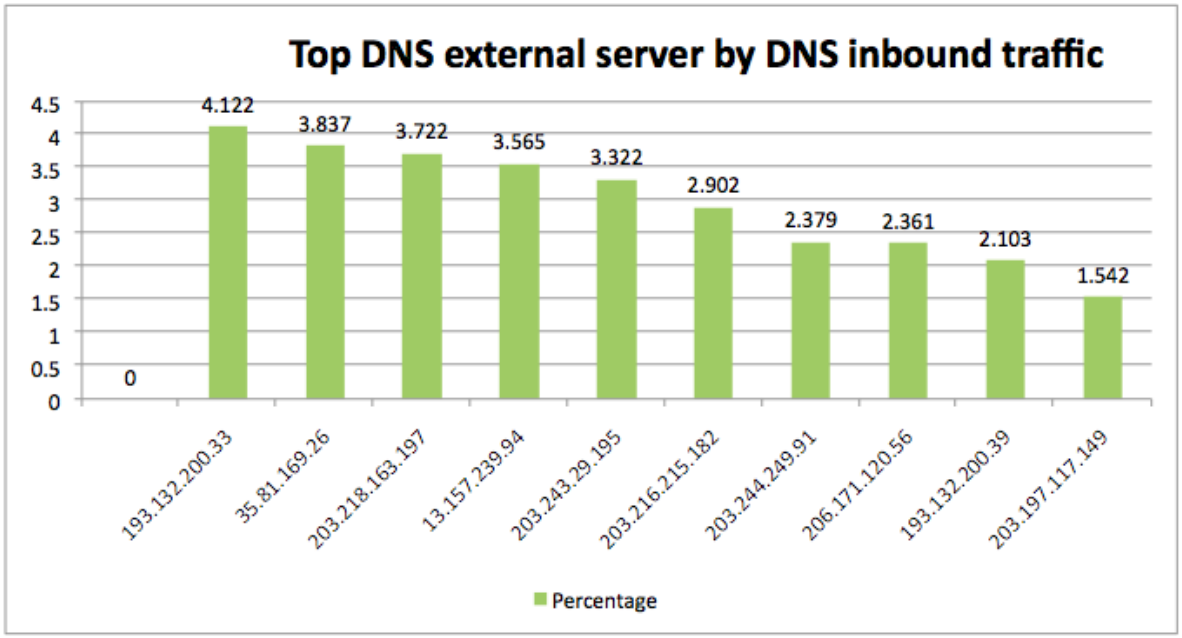


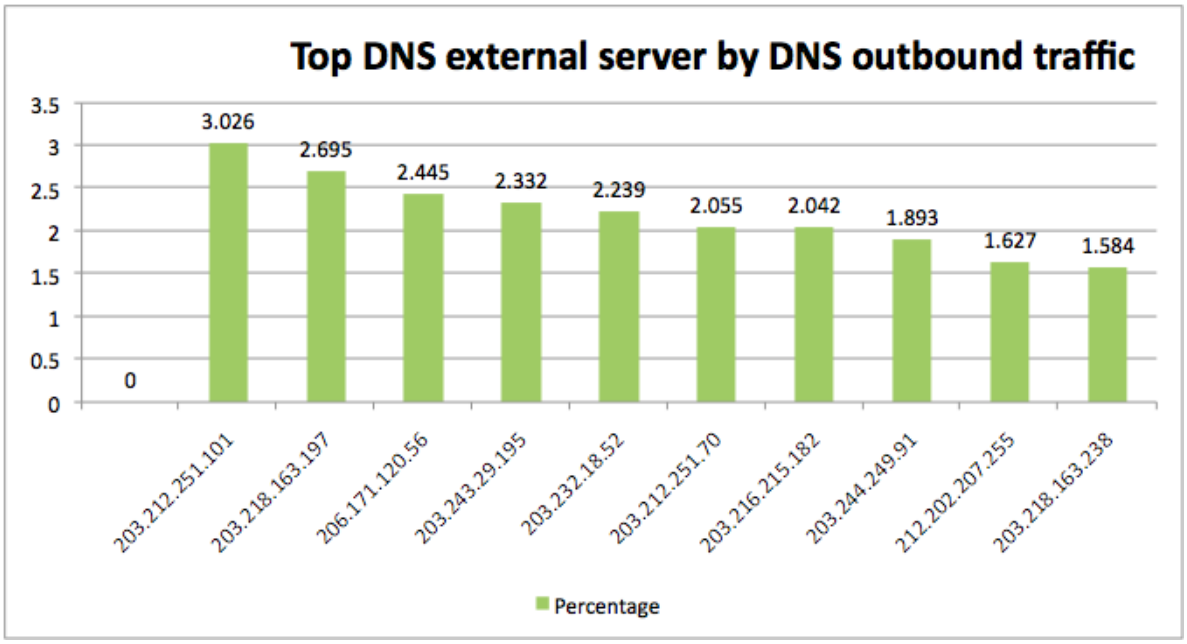
DNS traffic was accounted for 1% of traffic volume by packet. We can see that the inbound DNS traffic is 2 times higher than the outbound DNS traffic. With slightly higher DNS traffic volume in the working hours.





It is obvious from the data shown above that 173.94.167.24 is definitely the major DNS server in the network serving 99% of the DNS traffic to the outsiders. This has a serious drawback which will discuss later in the next section.

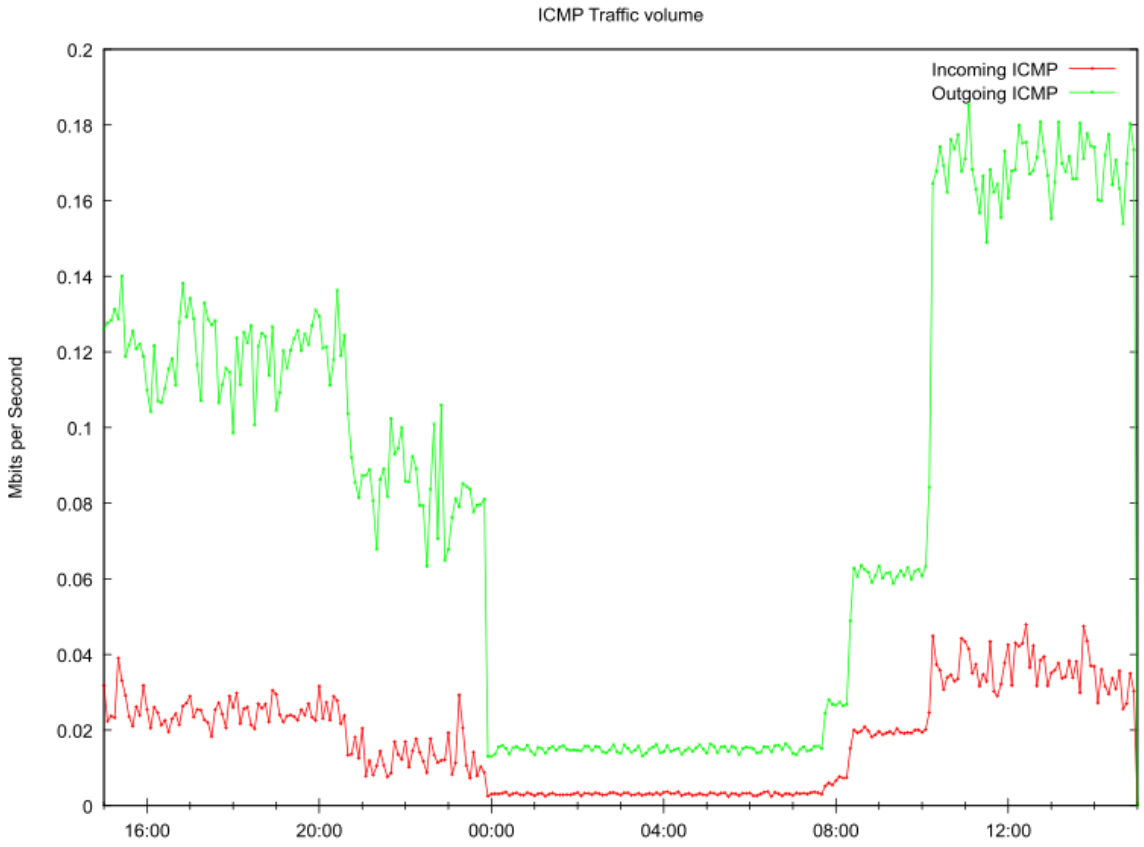




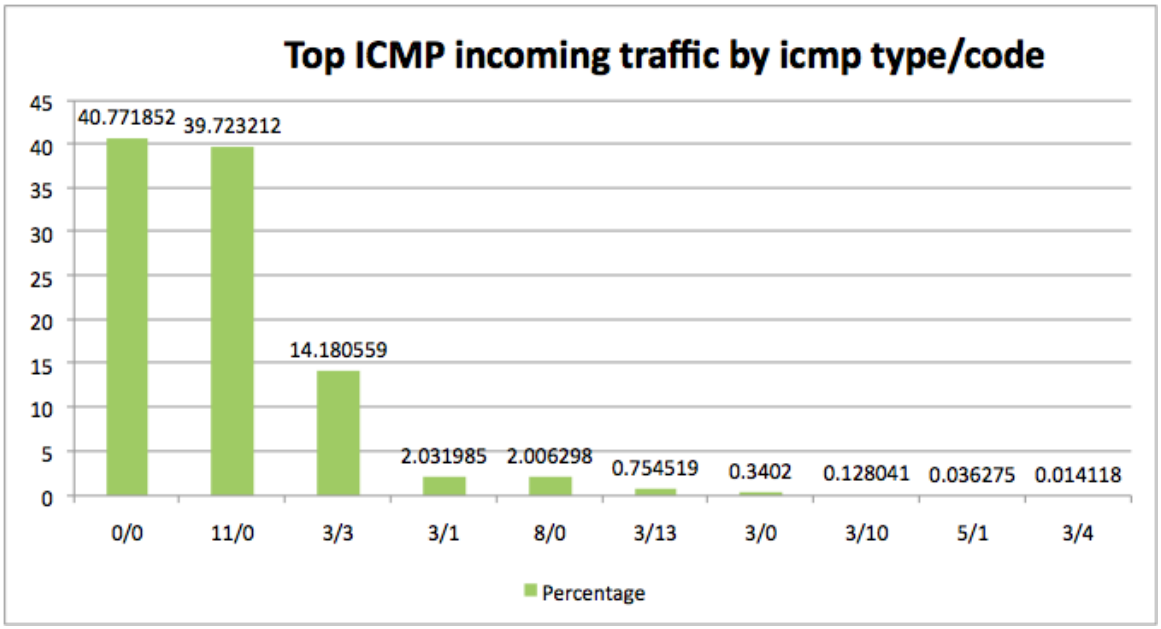
The outbound traffic activity looks normal to us. With regular distribution between hosts, it means that there're DNS requests from our network which distribute evenly across the neighbor network's DNS servers.

ICMP

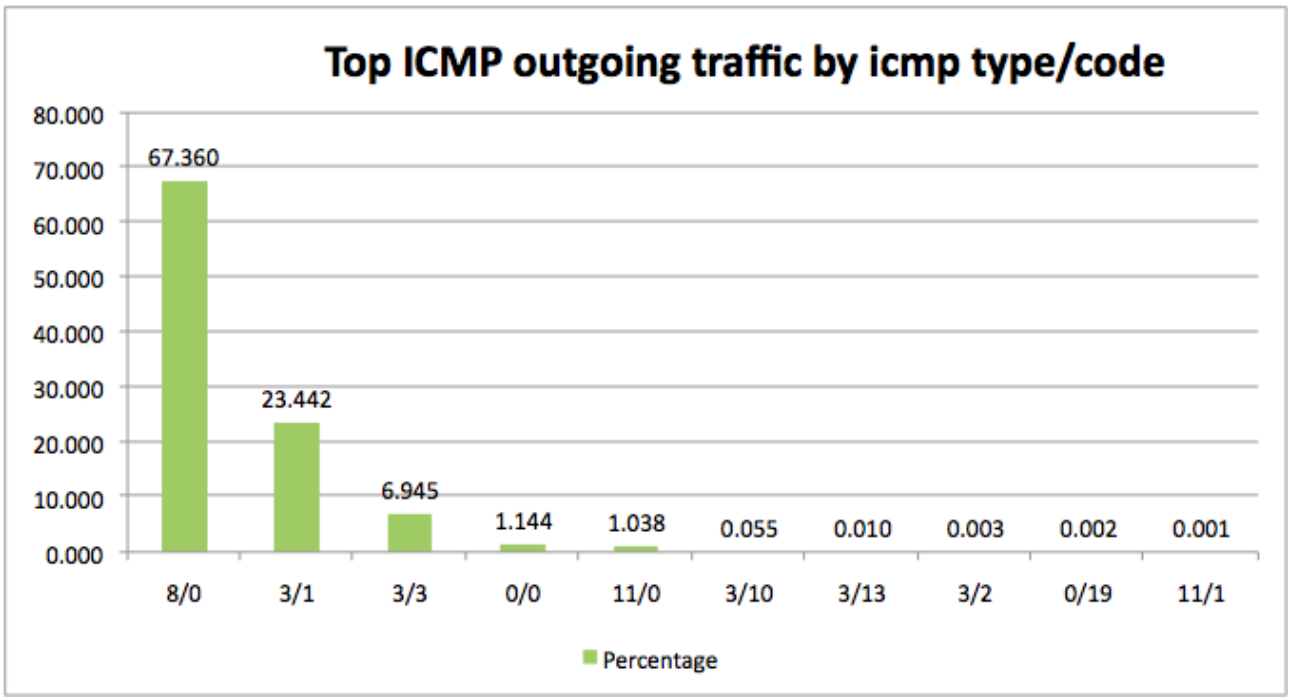
ICMP traffic is accounted for 2% of traffic volume by packets and 0-1% by bytes. The overall ICMP traffic volume is shown the following graph. We can see that there is a drop in ICMP traffic between 0.00 am to 8.00 am. This might occur from some router misconfiguration in that time period so the ICMP packet did not transmit to a proper route through the transit point. Obviously, this misconfiguration was fixed between 8.00 am to 10.00 am.



We perform a thorough inspection on the proportion of the ICMP type on both incoming and outgoing traffic. The result will be shown below,



The inbound traffic proportion graph above show a large (40%) proportion of echo reply (ICMP type 0 code 0) and nearly identical volume of ICMP time exceed(ICMP type 11 code 0). Note that about 20% of ICMP traffic are of type 3 (destination unreachable). 14.18% are of type 3 code 3 which is port unreachable. This indicates that many hosts within our network tried to connect to a closed or blocked port.



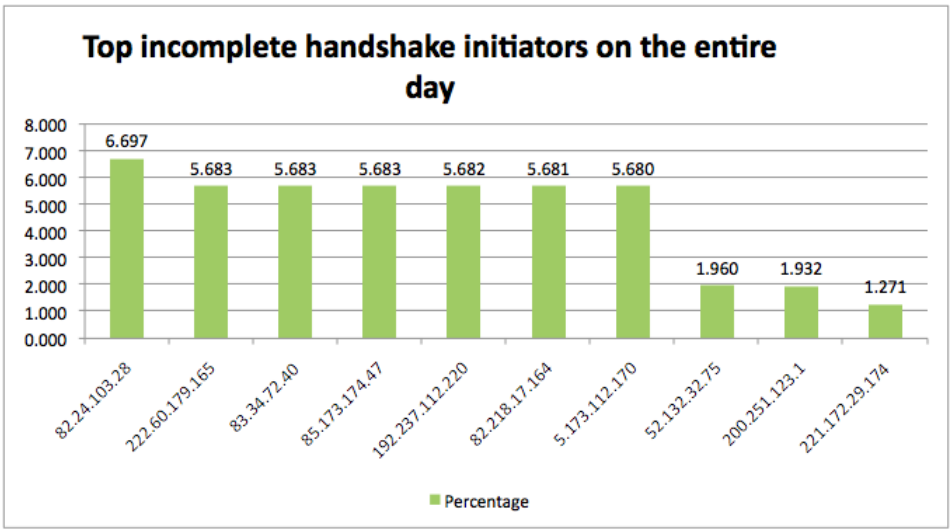
67% of the ICMP outbound traffic is ICMP echo message. This could indicate many things from regular network activity to check the availability of the outside network to a ping scanning from our network to other network. Further investigation is needed to be conducted. 23.4% of the ICMP outbound traffic is ICMP type 3 code 1 - host unreachable and 6.9% are type 3 code 3 - Destination unreachable.

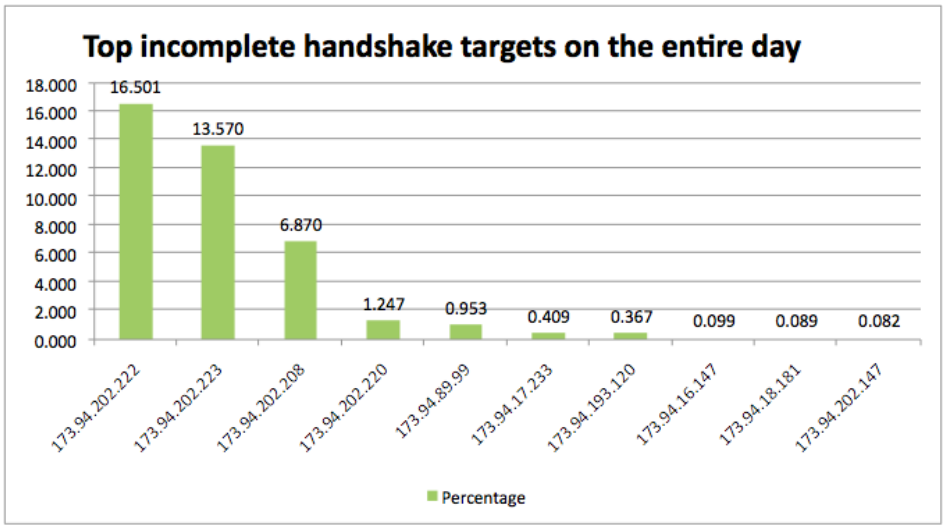
Note that our network sent 583206 flows for the ping message (type 8 code 0, check appendix A for the amount of flow on the traffic data) while received only 207934 echo reply back to the network. This might indicate that our network tried to ping a unreachable host (not existed or blocked) many times. In other hand, there are 10200 ping message to our network and 9909 echo reply back from our network to the outsider. Although the difference is not obvious as the outbound ping/ inbound echo reply, it also indicates that there're somebody outside ping the unreachable address within our network range.

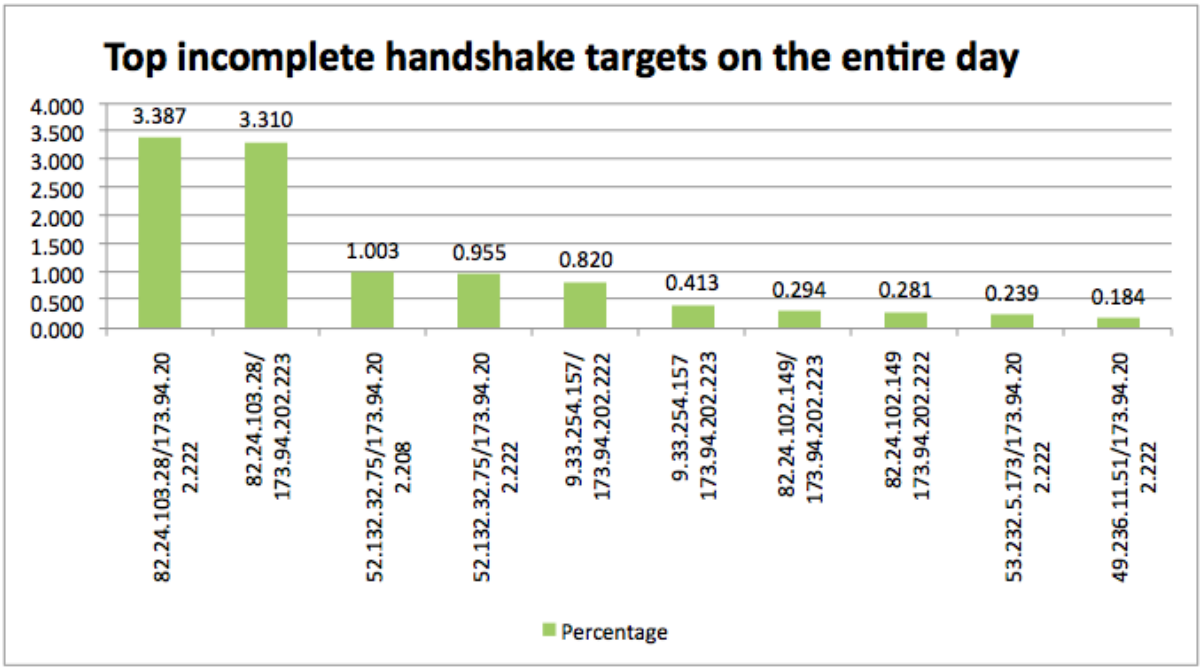
Network incident inspection

1. Syn Scanning

These data will be used to perform our analysis.

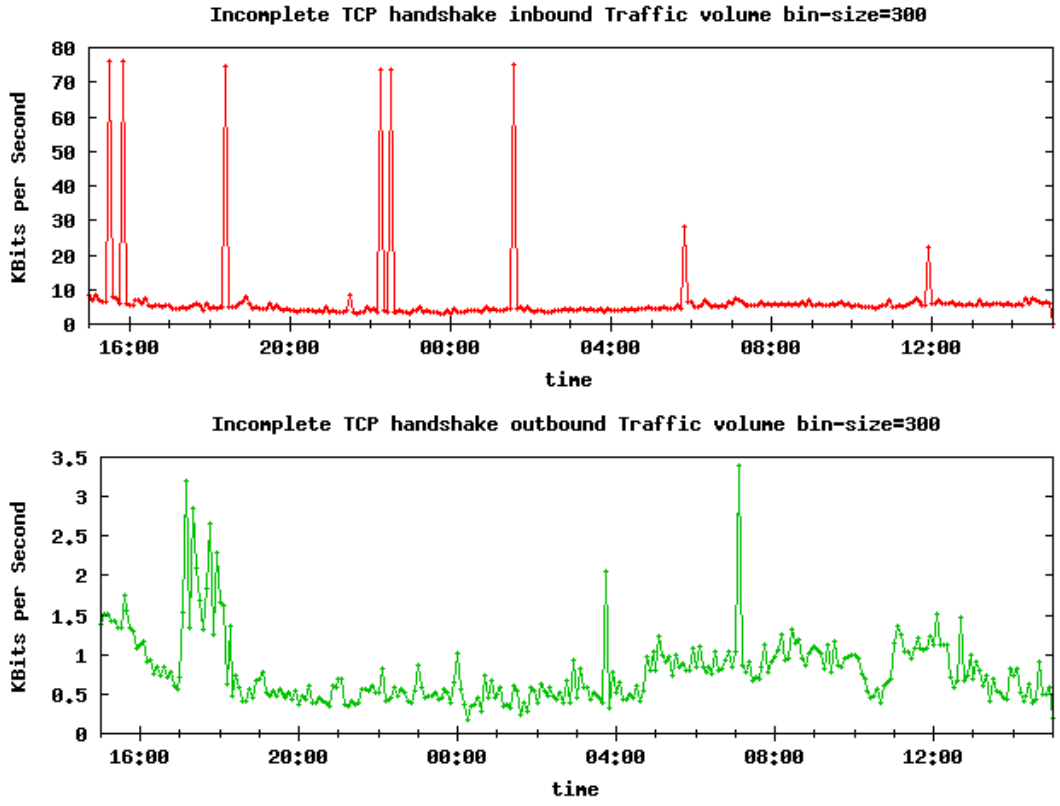






We found 2 scanning patterns in the data collected on that day. First,

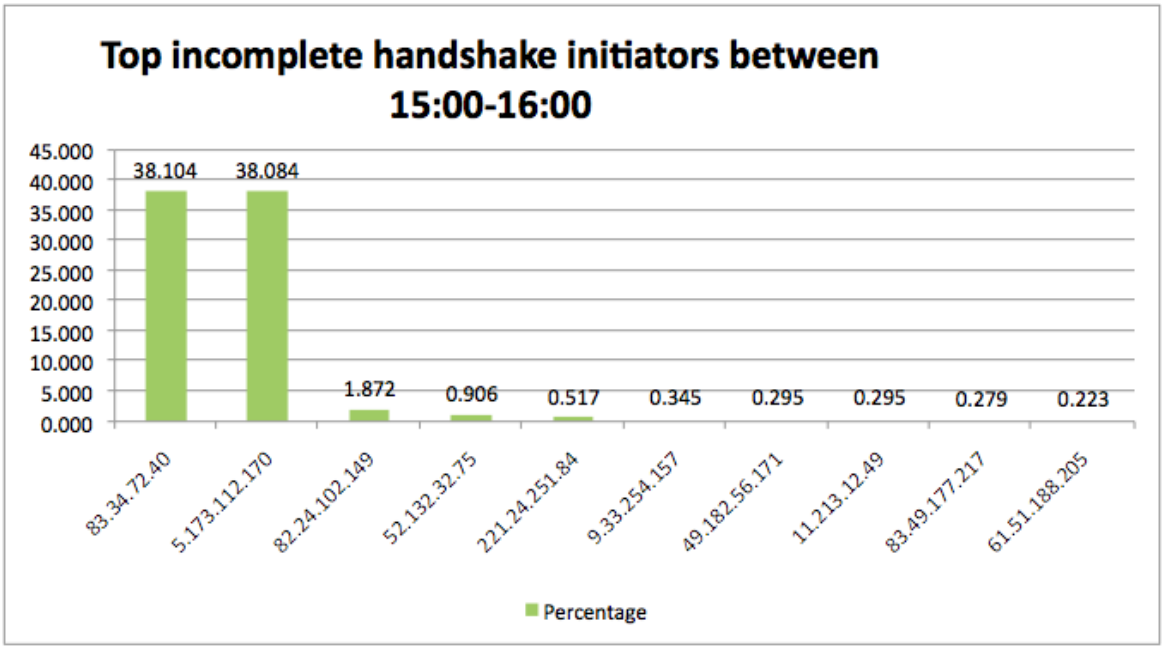
a. Looking into the time series SYN inbound traffic volume, we saw the significantly increasing in traffic volume making up a peak for 8 times across the entire day. This pattern also showed



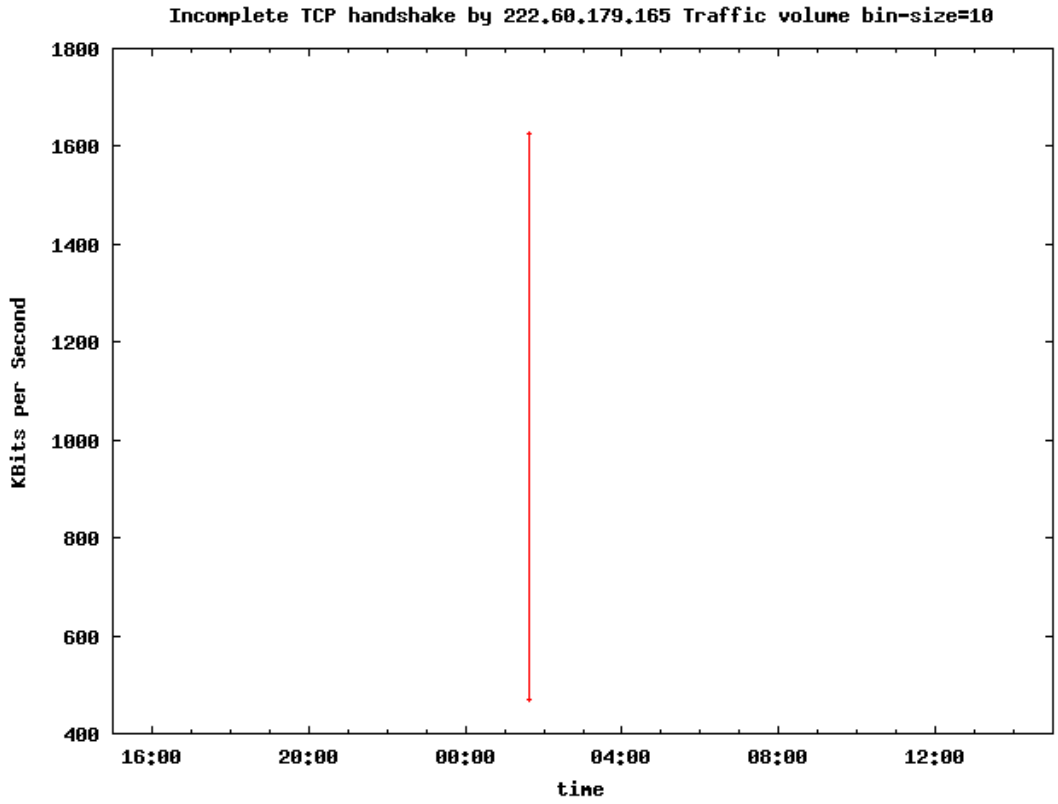
up in the incomplete TCP handshake traffic volume.

b. We made an inspection on the cause of that peak and found the pattern of SYN scanning on the entire range of our network. Each of the SYN scanning was conducted in a very brief

period of time (< 1 sec). Below is an inspection on 15:00-16:00. we found 2 hosts scanning our network.



Incomplete handshake pattern of 222.60.179.165 (This holds true for 202.251.123.1, 83.34.72.40,



85.173.174.47 and many more) on 173.94.0.0/16 network.

```
sIP|            dIP|sPort|dPort|                  sTime|
 222.60.179.165|     173.94.0.0| 6000| 2967|2009/03/31T01:38:08.989|
 222.60.179.165|     173.94.0.1| 6000| 2967|2009/03/31T01:38:08.991|
 222.60.179.165|     173.94.0.2| 6000| 2967|2009/03/31T01:38:08.989|
 222.60.179.165|     173.94.0.3| 6000| 2967|2009/03/31T01:38:08.991|
 222.60.179.165|     173.94.0.4| 6000| 2967|2009/03/31T01:38:08.991|
```

```
222.60.179.165|     173.94.0.5| 6000| 2967|2009/03/31T01:38:08.991|
222.60.179.165|     173.94.0.6| 6000| 2967|2009/03/31T01:38:08.991|
222.60.179.165|     173.94.0.7| 6000| 2967|2009/03/31T01:38:08.988|
222.60.179.165|     173.94.0.8| 6000| 2967|2009/03/31T01:38:08.991|
222.60.179.165|     173.94.0.9| 6000| 2967|2009/03/31T01:38:08.990|
222.60.179.165|    173.94.0.10| 6000| 2967|2009/03/31T01:38:08.991|
222.60.179.165|    173.94.0.11| 6000| 2967|2009/03/31T01:38:08.988|
222.60.179.165|    173.94.0.12| 6000| 2967|2009/03/31T01:38:08.990|
```

We can associate each scanning ip with each spikes,

Time	Source ip	Destination port
15:34	5.173.112.170	1433
15:52	83.34.72.40	2967
18:29	82.218.17.164	1433
22:15	192.237.112.220	8080
22:30	85.173.174.47	2967
01:38	222.60.179.165	3389
05:50	200.251.123.1	8080
11:55	221.172.29.174	2967

c. The host scanning our network resides in both class A,B and C networks with different network address. We found no connection between these hosts.

d. However, the source ports used for scanning our network between those scanning host are the same, the 6000 port.

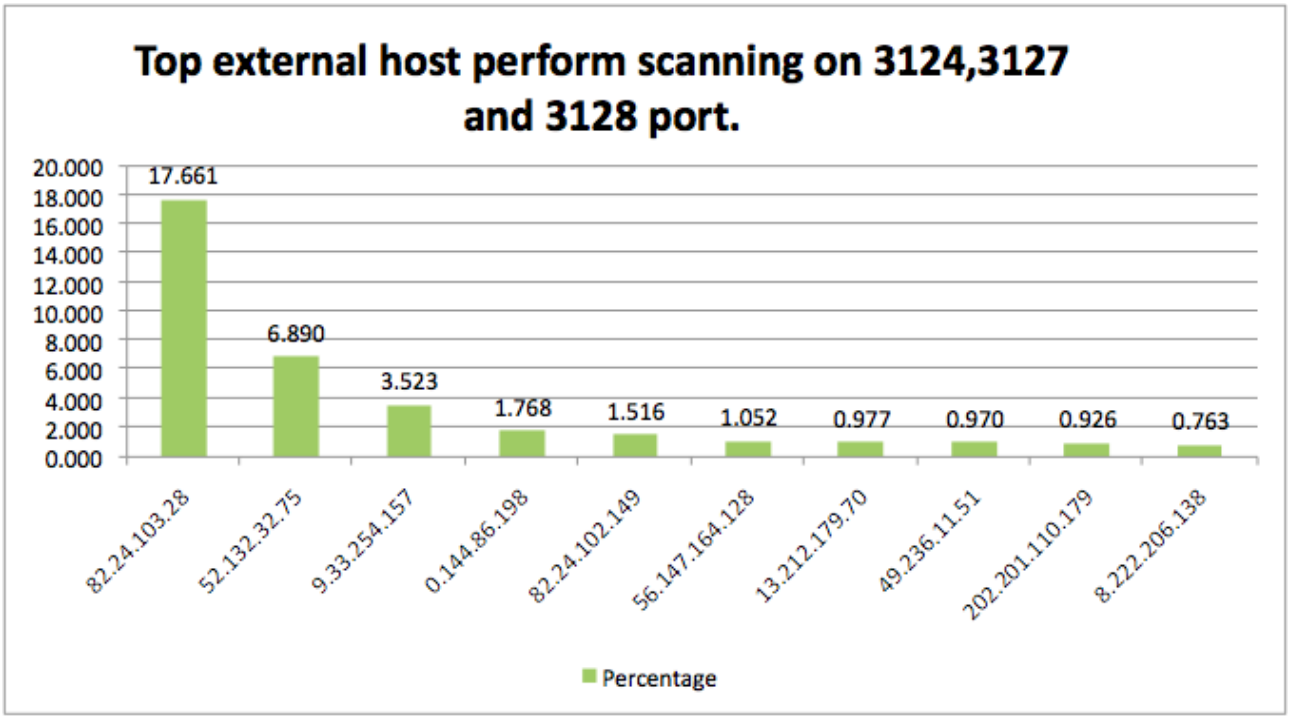
e. Our network ports being scanned are 1433, 2967,3389 and 8080 port. (Note : the vulnerabilities associated with these port are summarized in the appendix B)

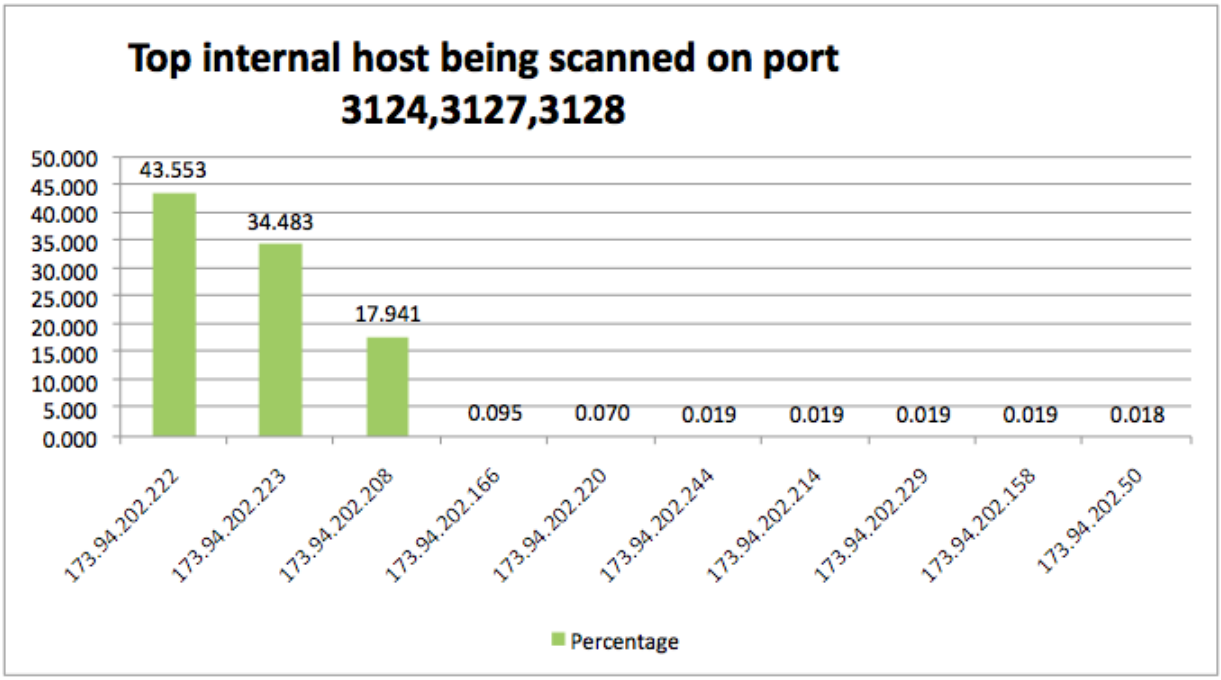
f. The scanning traffic volume is approximately 1600 kb (in 5 seconds bucket, which means the actual scan can take up to 8000 kb in 1 seconds at most). Comparing to the overall traffic, there's still nothing to worry since the traffic generated from the scanning plus the normal traffic at the time of being scanned is not exceed the maximum amount of traffic that the network can handle (Assuming that the amount of the traffic our network can handle is at least 22,000, the highest point in the overall traffic of that day).

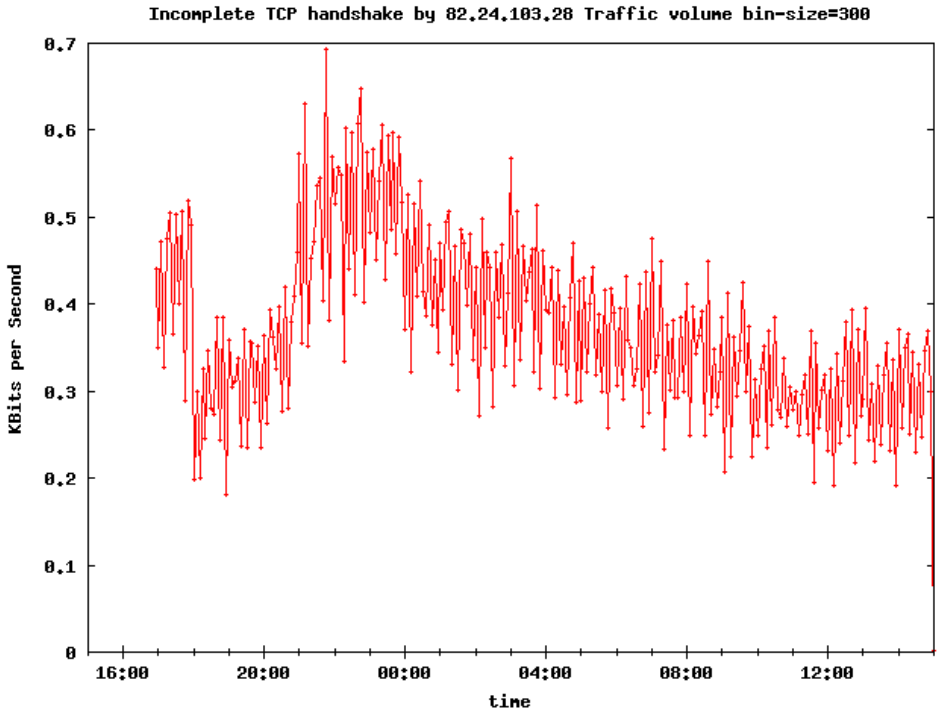
g. The number of host sending out the traffic from port 1433,2967,3389,8080 to any outside port is 192 hosts while the number of the host responding from port 1433,2967,3389,8080 to a scan from port 6000 is only 32 hosts. This means that there might be an ACL setting up on somewhere that allow only the traffic on the legitimate port to the 1433,2967,3389,8080 ports (Hence, drop packet from the suspicious port, port 6000).

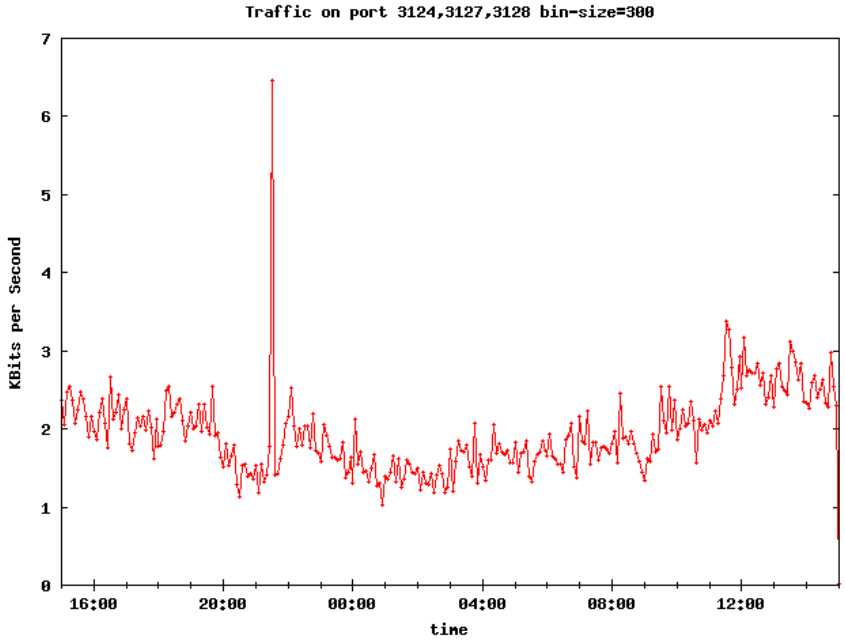
h. The remaining 32 machine that the SYN scanning packet made it way to the machine mostly sent out the RST packet as a response to those scans except 173.94.202.192 on port 3389, 173.94.202.162,169 on port 8080 which sent the SYN-ACK packet as a response.

Secondly, there're consistent very-low-volume scan throughout the day mostly on the host 173.94.202.208,222,223 on uncommon port 3124,3127 and 3128 as indicated by the suspicious trend of the below graph and rwfilter data.


Top external host perform scanning on 3124,3127 and 3128 port.
20.000
18.000
16.000
14.000
12.000
10.000
8.000
6.000
4.000
2.000
0.000
17.661
6.890
3.523
1.768
1.516
1.052
0.977
0.970
0.926
0.763
82.24.103.28
52.132.32.75
9.33.254.157
0.144.86.198
82.24.102.149
56.147.164.128
13.212.179.70
49.236.11.51
202.201.110.179
8.222.206.138
Percentage


Top internal host being scanned on port 3124,3127,3128
50.000
45.000
40.000
35.000
30.000
25.000
20.000
15.000
10.000
5.000
0.000
43.553
34.483
17.941
0.095
0.070
0.019
0.019
0.019
0.019
0.018
173.94.202.222
173.94.202.223
173.94.202.208
173.94.202.166
173.94.202.220
173.94.202.244
173.94.202.214
173.94.202.229
173.94.202.158
173.94.202.50
Percentage





Example of the scanning pattern by 82.24.103.28

sIP	dIP	sPort	dPort	pro	sTime
82.24.103.28	173.94.202.223	1486	3128	6	2009/03/30T16:55:25.579
82.24.103.28	173.94.202.223	1486	3128	6	2009/03/30T16:55:26.316
82.24.103.28	173.94.202.223	1486	3128	6	2009/03/30T16:55:27.025
82.24.103.28	173.94.202.223	2564	3127	6	2009/03/30T16:55:31.878
82.24.103.28	173.94.202.223	2564	3127	6	2009/03/30T16:55:32.656
82.24.103.28	173.94.202.222	4332	3124	6	2009/03/30T16:55:33.472
82.24.103.28	173.94.202.223	2564	3127	6	2009/03/30T16:55:38.591
82.24.103.28	173.94.202.223	4871	3127	6	2009/03/30T16:55:39.164
82.24.103.28	173.94.202.223	1573	3128	6	2009/03/30T16:55:40.932
82.24.103.28	173.94.202.223	4871	3127	6	2009/03/30T16:55:42.116

```
  82.24.103.28| 173.94.202.223| 4871| 3127|  6|2009/03/30T16:55:42.825|
  82.24.103.28| 173.94.202.223| 1573| 3128|  6|2009/03/30T16:55:43.933|
  82.24.103.28| 173.94.202.223| 1573| 3128|  6|2009/03/30T16:55:44.738|
  82.24.103.28| 173.94.202.222| 4529| 3128|  6|2009/03/30T16:55:46.363|
  82.24.103.28| 173.94.202.222| 4613| 3128|  6|2009/03/30T16:55:46.473|
  82.24.103.28| 173.94.202.223| 1326| 3127|  6|2009/03/30T16:55:47.195|
  82.24.103.28| 173.94.202.222| 4613| 3128|  6|2009/03/30T16:55:47.343|
```

There are many scanning host following this pattern (at least 20 hosts and up to 4000 hosts) The scanning host accounted for the most scanning volume is 52.132.32.75 and `82.24.103.28` . The top 20 scanning hosts on port 3124,3127,3128 took up to 25% scanning traffic volume of all scanning traffic.

i. As far as we see, all the scanning on those port was responded with RST packet.

j. There're some seem-to-be legitimate traffic running on those port with low volume comparing to the scanning traffic volume.

k. This scanning volume is very low (< 10 kb / s) comparing to the overall traffic of the network. However, it happens throughout the day consistently.

l. It's not clear that this pattern of scanning is the malicious traffic or just keep-alive traffic sent to server listening on these ports.

2. Backscattering analysis

Looking for SYN/ACK in TCP handshake sent to/generate from our network

```
[nratanas@unix36 ~/proj2]$ rwfilter --flags-all=AS/ASRF --packets=1 --
pass=stdout ../proj/anytcp.txt | rwstats --sip --count=10
INPUT SIZE: 37880 records for 1072 unique keys
SOURCE IP Key: Top 10 flow counts
            sIP|             Records|%_of_total|   cumul_%|
     43.22.0.99|                4210| 11.114044| 11.114044|
  61.51.188.205|                2664|  7.032735| 18.146779|
 82.184.170.148|                1356|  3.579725| 21.726505|
   83.49.186.26|                1283|  3.387012| 25.113516|
 173.94.202.220|                1100|  2.903907| 28.017423|
 80.128.152.194|                 916|  2.418163| 30.435586|
   8.78.114.221|                 694|  1.832101| 32.267687|
   56.180.80.75|                 651|  1.718585| 33.986272|
    83.34.84.44|                 637|  1.681626| 35.667899|
  61.51.173.197|                 580|  1.531151| 37.199050|
```

Looking for ACK from our network in response to the above SYN/ACK sent by 43.22.0.99

```
 rwfilter --flags-all=A/ASRF --pass=stdout
-daddr=43.22.0.99 ../proj/anytcp.txt | rwstats --sip --count=10
INPUT SIZE: 0 records for 0 unique keys
SOURCE IP Key: Top 10 flow counts
            sIP|             Records|%_of_total|   cumul_%|

 rwfilter --flags-all=A/ASRF --pass=stdout
--daddr=61.51.188.205 ../proj/anytcp.txt | rwstats --sip --count=10
INPUT SIZE: 0 records for 0 unique keys
SOURCE IP Key: Top 10 flow counts
            sIP|             Records|%_of_total|   cumul_%
```

The result shows no ips in our network sending ACK message to 43.22.0.99 and 61.51.188.205. Instead, when we investigate further more, they sent RST to 43.22.0.99. This

indicate that these handshakes wasn't first originated (SYN initiation) from our network but SYN/ACK was sent back ,in corresponding to that SYN, to our network. This indicates that there're some backscattering in our network (We can also see this backscattering evidence every ips shown above by repeating the above process again with different ips)

Furthermore, there's backscattering occur in the converse way. We can see from the data shown above that there're SYN/ACKs sent from our network(173.94.202.220) to the outside networks. However, there's no ACK response from most of those network to 173.94.202.220. This also justify the fact that there're some backscattering incident associated with our network. However, because the volume is miniscule and it's ordinary for the large network to have some tiny amount of backscattering on the network. We can conclude that there's nothing suspicious in term of the backscattering volume on our network.

Suggestions for Improvement

Based on protocol and port inspection

1. We could build redundant web servers, DNS servers and FTP server on our network since most of the traffic (>70%) on each service is rely on only one or two server resided in our network. This make the availability of this service susceptible to an absence of these server due to malfunction, DDoS attack and so on. In other word, if these server are down, these services offered by the network will be terminated definitely.
2. We should implement a load-balancing for the SMTP,FTP server as well since, again, the SMTP and FTP service offered by our network resides in only two host with unevenly traffic (91% and 9 % for inbound traffic and 66% and 33% for outbound traffic). We might implement load balancer to distribute the load between these two host evenly. Moreover, if one internal SMTP server is down, the load balancer can redirect those traffic destined to the failed server to another server. This scheme will make our SMTP and FTP services more robust.
3. Dependencies between our network and other network were found. Our network used SMTP and FTP service offered by a small amount of host -- FTP service provided mostly(>90%) by two host on the external network while SMTP service provided by 5-6 hosts outside the external network. If these host are down or the path between our network to these host are cut off, the FTP and SMTP service used by our network will be ruined. Therefore, the network administrator should find and implement the alternate route to these services, either by finding more server provided the service or establish another route to the existing service

Based on network incident inspection

1. Make sure that the firewall ruleset on the network is configured properly - not allowing the traffic from illegitimate port destined for the common service port used in the network to get into our network.
2. The host 173.94.202.192 and 173.94.202.162,169 which responses to the SYN-sweep scan by sending SYN-ACK back to the scanning host might be already exploited by the attacker. Therefore, the administrator should checked and fixed these host as soon as possible. Thorough inspection should be conducted in order to make sure that this host is cleaned and is not harmful to the health of our network.
3. If the above hosts had not already been exploited We can expect the exploitation on 173.94.202.192 / Port 3389 and 173.94.202.162,169/ Port 8080 in the near future. The workaround this prospective attack is (1) or simply configure the host to deny the traffic to those port. This should be done after consulting with the system administrator. Moreover, after thorough analysis on those host, we should consider defending our network against the vulnerabilities on port 1433, 2967, 3389 and 8080. Patching the system and well-configure firewall, most of the time, can defend the network against the vulnerabilities on those port.
4. Checking whether there're squid server or proxy server running on 173.94.202.208,222 and 223. If so, then check whether the scanning traffic pattern we found on those hosts conforms with the

legitimate traffic running on the same ports in the legitimate hosts. If not or if there're not squid servers or proxy server associated with port 3124,3127,3128 running on those hosts, we can conclude that the traffic is suspicious. We then can inform the network administrator to investigate further on the traffic on those hosts.

Note : There are lot of vulnerabilities associated with these port. One of these is the MyDoom virus. it will open port 3127 through 3198, since 2 out of 3 port being scanned are 3127,3128. We should inspect on whether those host are infected with this virus. if not, then we should consider the other possible vulnerabilities on these port.

5. Make sure that we applied the most recent vulnerabilities patch on each host on our network especially on the vulnerabilities associated with port 1433,2967,3869,8080, 3124,3127 and 3128 because, basing on our analysis, the most potential ports that might be exploited in the near future are these ports.

Recent Event Study

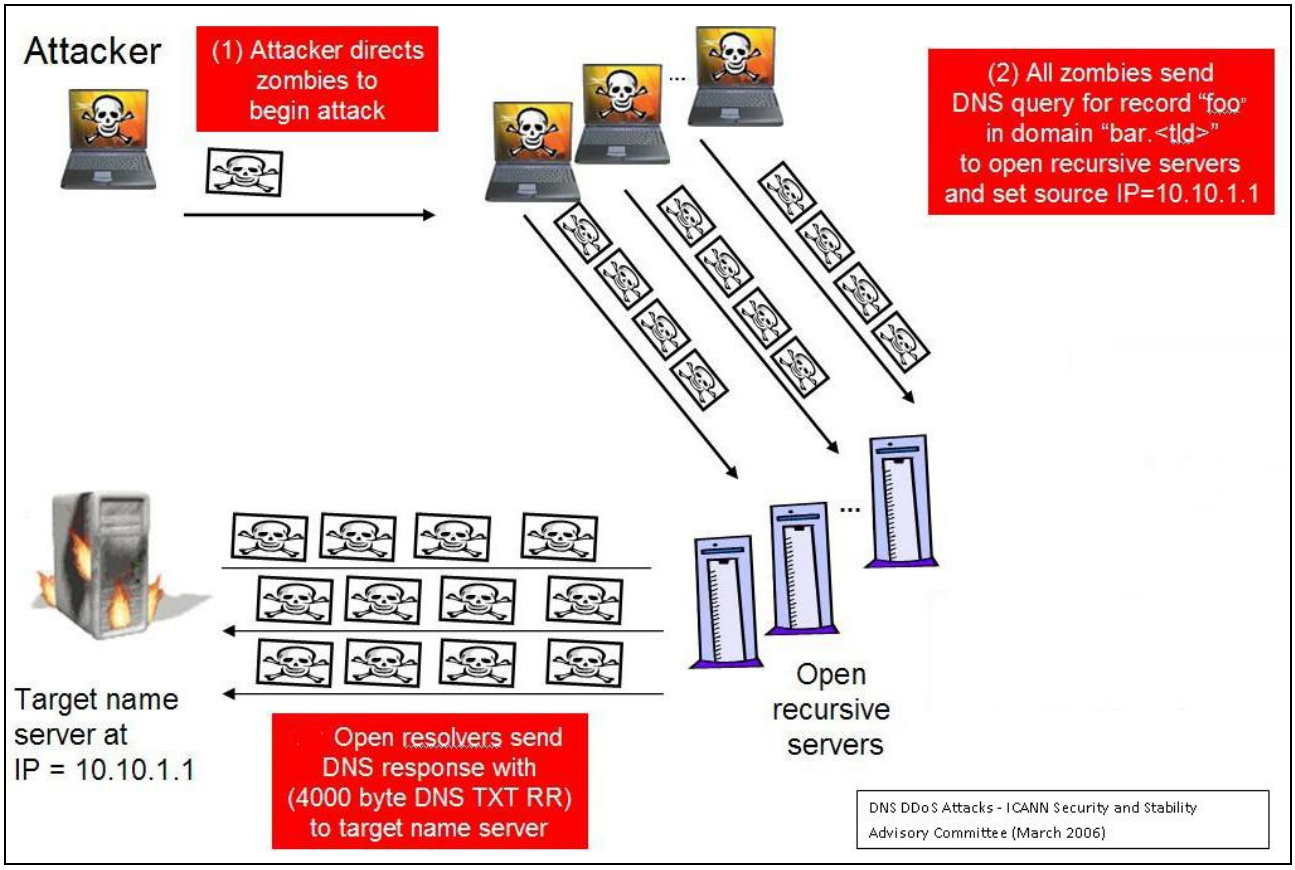
Event Description

As reported in a SANS ISC Diary entry[1] and many posts to the North American Network Operators Group (NONAG) mailing list[2], on January 20th, 2009, network administrators around the internet reported odd queries hitting their DNS servers at a steady rate of about two or more per second. The queries asked for the name server of the domain "." (NS query for a single dot). Since "." is a query for the root name servers, it has a very short query packet but a fairly long answer. It appeared that this was a denial of service (DoS) attack in progress, where the DNS servers are used as amplifiers and unwittingly flood the (spoofed) source by providing a long answer to a system which never asked. Amplification is a process whereby the attacker sends a small request with the expectation of invoking a much larger response directed to the target.

However, the attack will only be amplified if the queried DNS server responds with a full answer if recursion is enabled and open to any requestor. "Recursion is a method of processing a DNS query in which a name server pursues the query for a client at the authoritative name server for the name. When recursion is performed for any client as opposed to a trusted set of clients, a name server is said to be an open recursive server."[3]

If recursion is not enabled, then the response will be very similar in size to the request. Looking at example queries using Wireshark, we observed that the reply packet only contains the original request and no answer. The Flags in the DNS application layer state that Recursion was requested, but that the server does not support it, and the Reply Code then works out to be 'Refused' (60 byte request, 60 byte answer). This 1:1 size does not take advantage of amplification; however it does still send data to the targeted DNS server.

If recursion is enabled, the 60 byte request from the attacker yields a 250 byte packet to the target server. In general, this is not a particularly large amplification attack. It is possible to generate larger ones in the area of 4000 bytes with DNS by using a custom TXT Record, which would also cause the data to be fragmented into several 1500 sized packets. Still, this particular attack is a 5x increase (60:250) and is distributed from many sources, which can result in the Denial of Service.

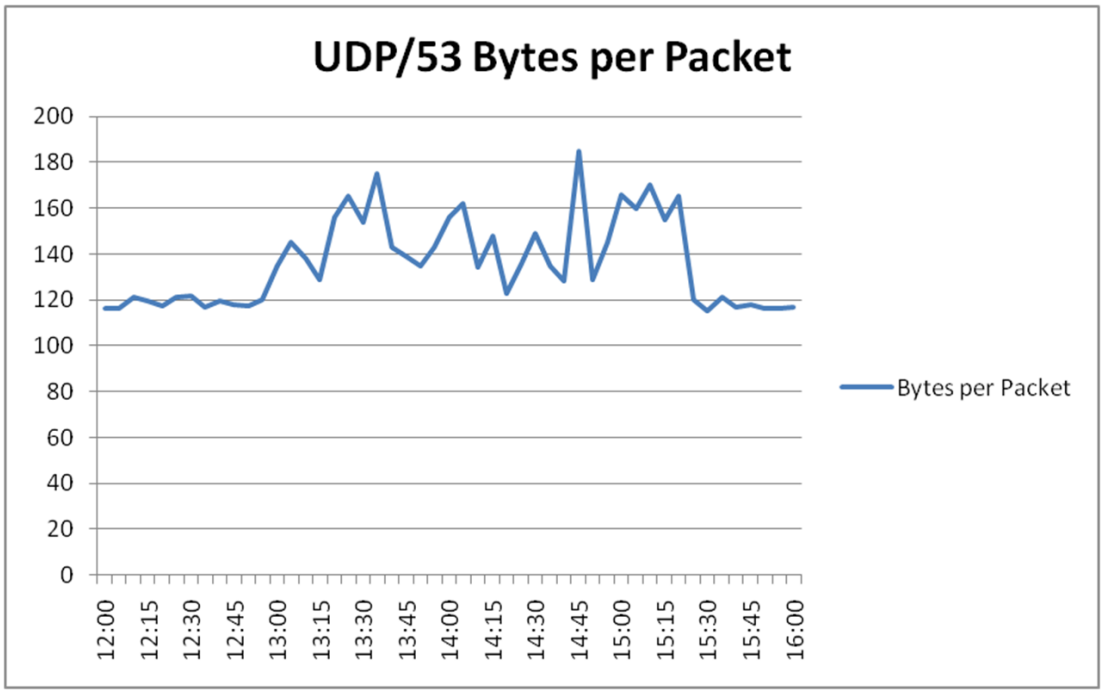


Since many internet services rely on DNS, this kind of attack can have a large impact. In this particular attack, the authoritative DNS servers for Network Solutions were one of the targets. So, any web browser client that attempted to view a web site hosted by Network Solutions would not be able to locate it.

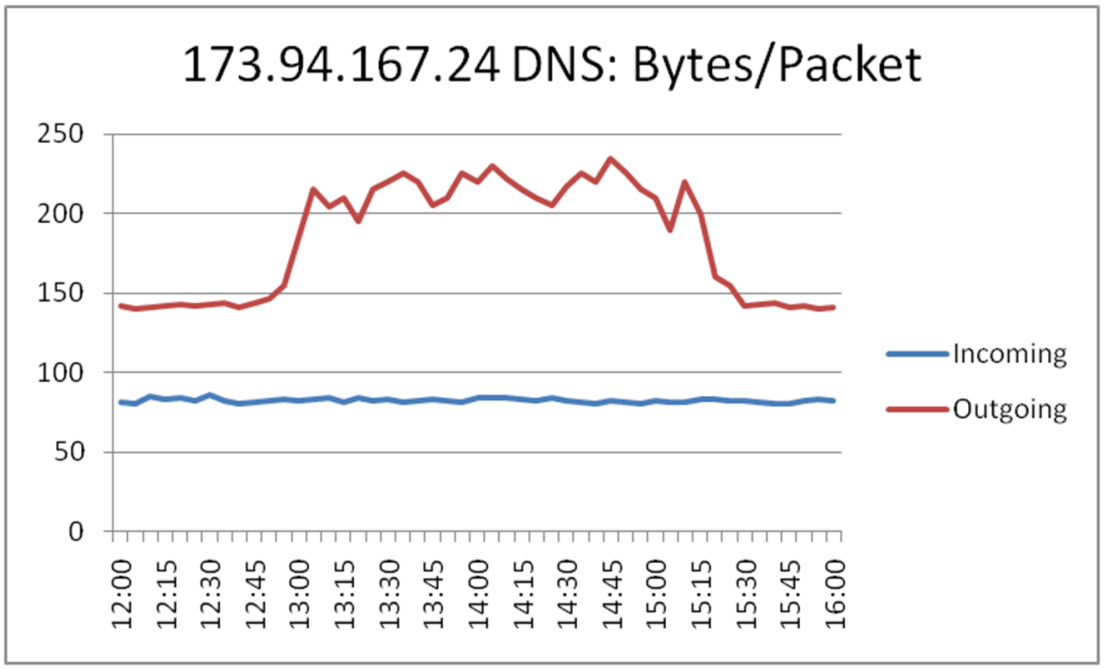
Circle ID reported that major domain registrar Network Solutions experienced a massive DDOS UDP/53 attack on their domain servers for approximately 48 hours. The Network Solutions blog confirms this: "There is a spike in DNS query volumes that is causing latency for the delay in web sites resolving. This is a result of a DDOS attack. We are taking measures to mitigate the attack and speed up queries."[4]

Theories for Manifestation in our Data Set

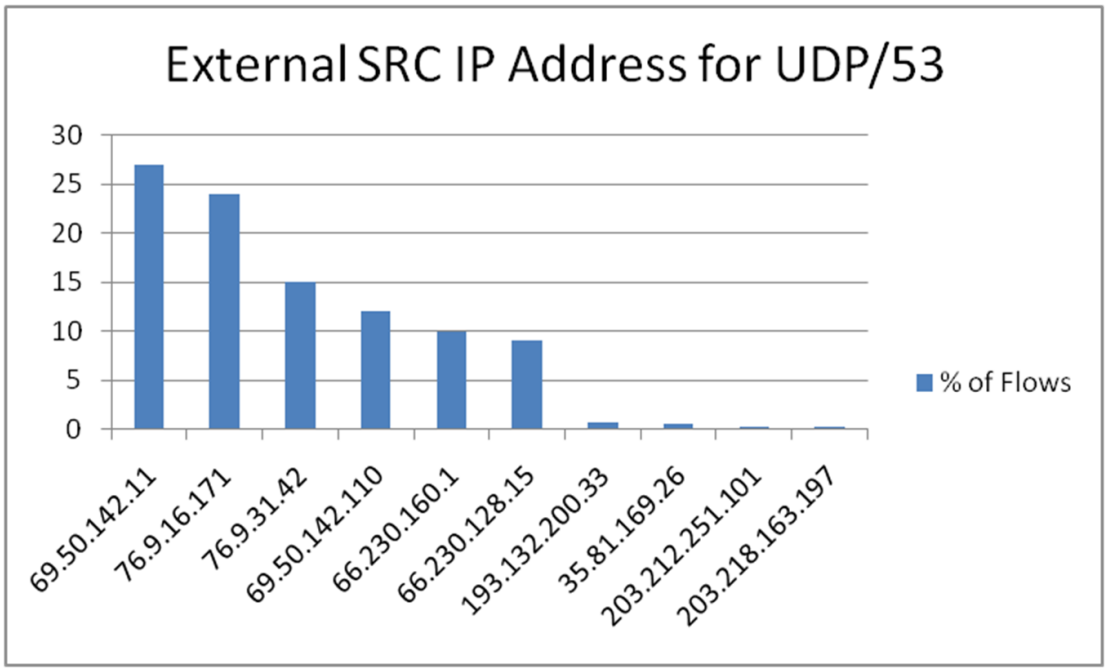
For this section, we've made hypothetical data sets and charts that we can use to detect/analyze the attack and effects of the attack. This is not based on any actual data, but just example data used for thought exercises. The hypothetical DNS DDoS attack occurs from approximately 12:50 – 15:25.



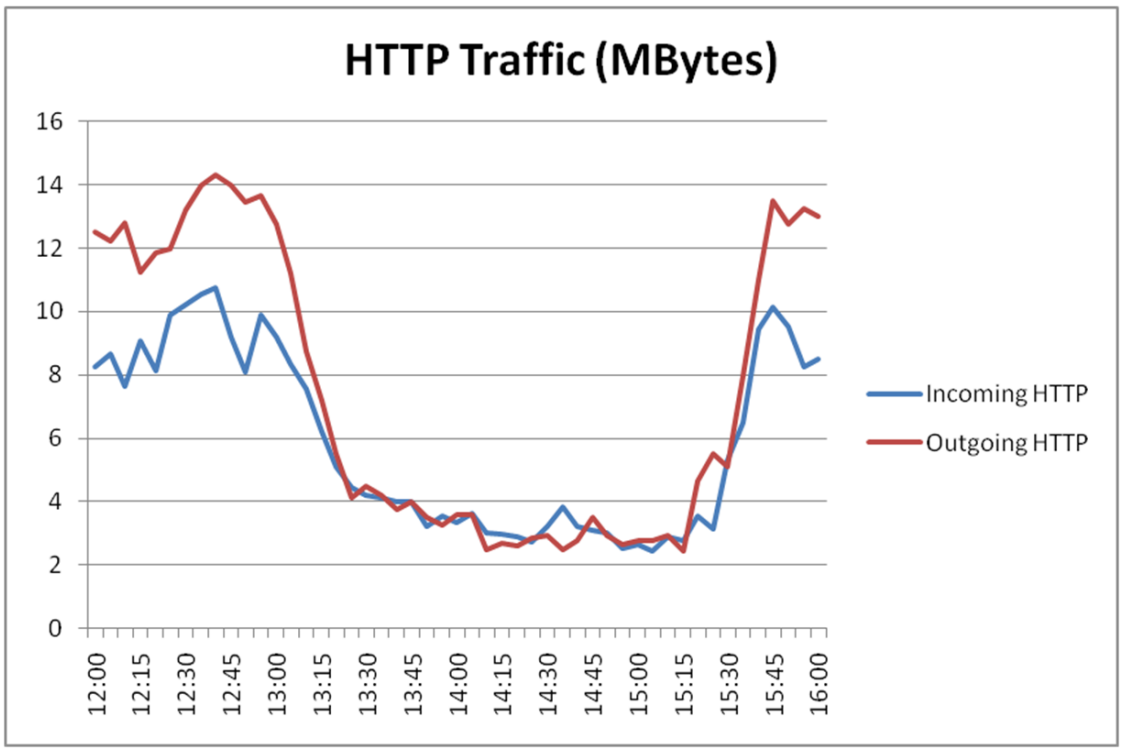
Since this is an amplification attack against DNS servers, we will look at flow data to see if the average bytes/packet changes. We can see in this chart that the average packet size increases during the attack period. This indicates that we are seeing effects of the amplification attack in our network. So, we should continue the inspection into other services.



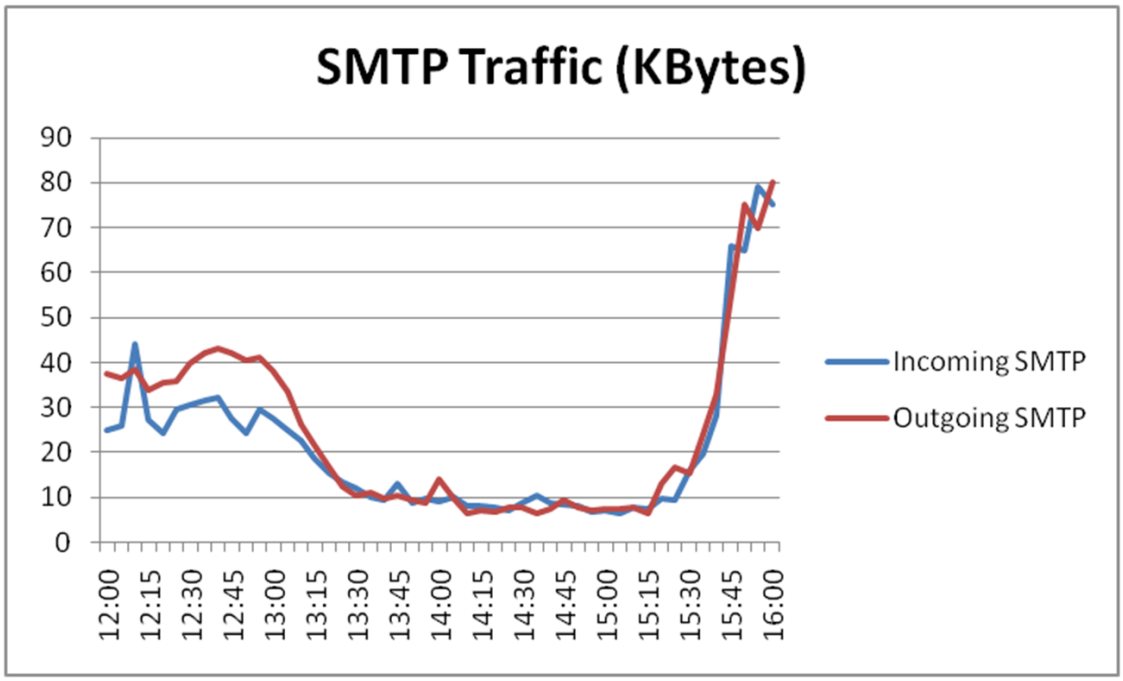
According to our profiling, the host 173.94.167.24 is by far our most used DNS server. We can use network flows to compare incoming vs. outgoing UDP/53. Since Incoming remains steady, our server is not a target of the DDoS. However, since Outgoing increases it leads us to believe that it has Recursion enabled and is being used by bots to attack.



In our normal traffic Network Profile, Source IP Addresses for DNS queries are very evenly spread (1.5% is the max for a host). During the DDoS, the IP Addressed in the chart above are found in the Network Flow data. Checking the SANS blogs, these top six IP Addresses are reported by other network administrators as spoofed addresses that are targets. Again, we are seeing lots of attack traffic in our network.



As the DDoS attack begins, clients are unable to resolve hostnames for websites, caches expire, and HTTP traffic falls. Since both Incoming and Outgoing drops, the effects are very widespread, and most likely our DNS server (173.94.167.24) is being slowed by the bots using it to amplify attacks against the target DNS servers.



Similar to HTTP, email relies on the DNS service to look up MX records for domains in order to deliver email. And, as the attack begins the Mail Transfer Agents (MTAs) face delays and difficulty obtaining the MX records, caches expire, and email volume falls. Once the DDoS attack ends, there's a slight surge in SMTP traffic as queues empty.

There are many services on the internet that rely on DNS; HTTP and SMTP are just two common examples. So, we would expect to see many services affected. Some services would be able to maintain connectivity if their DNS cache maintains through the outage, but any prolonged outage will have a far-reaching affect.

Remediation Steps

- Network Ingress Filtering (BCP 38 / RFC 2827) - Perform source IP address verification at the edge, so that ISPs block any traffic not in their networks. This will help to prevent IP Address spoofing.
- Disable Open Recursive DNS - Disabling open recursion on name servers from external sources and only accepting recursive DNS from trusted sources greatly reduces the amplification vector. We must fix our DNS server (173.94.167.24) as soon as possible. We will want to send notices to our DNS server administrators and suggest they use an online tool for scanning DNS servers on isc.sans.org. Also, we could use a scanner (Nessus, etc.) to check for this and alert the system owners.
- Securely configure DNS Servers - Operating securely configured DNS application services on servers running securely configured operating systems reduces the number of servers attackers can exploit through DNS cache poisoning and privilege escalation and other

system compromise attacks. This reduces the number of innocent systems that can host large DNS resource records used as amplification domain records.

- Configure Network Filtering - Block invalid DNS messages at the network edge and Rate Limit client and server requests. Rate limiting client requests at the border can ease the effects on DNS servers.

Conclusion

Analyzing flow data provides us with a method to profile our large network. Network Situational Awareness gives us the concepts and skills to gain an understanding of our network, and to identify vulnerabilities and weaknesses which could be exploited.

Appendix

A. Command used to produce common protocol and port inspection and network incident inspection and their detailed result.

Top protocols for incoming traffic

```
$ rwfilter ext1/*.rw ext2/*.rw --daddress=173.94.x.x --pass=stdout | rwstats --count=10 -
-protocol
INPUT SIZE: 5924184 records for 5 unique keys
PROTOCOL Key: Top 10 flow counts
       protocol|             Records|%_of_total|   cumul_%|
             17|             3030140| 51.148648| 51.148648|
              6|             2383947| 40.240934| 91.389582|
              1|              509994|  8.608679| 99.998261|
              0|                 100|  0.001688| 99.999949|
             46|                   3|  0.000051|100.000000|


$ rwfilter ext1/*.rw ext2/*.rw --daddress=173.94.x.x --pass=stdout | rwstats --count=10 -
-bytes --protocol
INPUT SIZE: 5924184 records for 5 unique keys
PROTOCOL Key: Top 10 byte counts
       protocol|               Bytes|%_of_total|   cumul_%|
              6|         58333629085| 86.537929| 86.537929|
             17|          8885014149| 13.180917| 99.718846|
              1|           189509988|  0.281138| 99.999984|
              0|               10200|  0.000015| 99.999999|
             46|                 680|  0.000001|100.000000|
```

Top protocols for outgoing traffic

```
$ rwfilter ext1/*.rw ext2/*.rw --saddress=173.94.x.x --pass=stdout | rwstats --count=10 -
-protocol
INPUT SIZE: 5791380 records for 4 unique keys
PROTOCOL Key: Top 10 flow counts
       protocol|             Records|%_of_total|   cumul_%|
             17|             2779650| 47.996332| 47.996332|
              6|             2145928| 37.053828| 85.050161|
              1|              865801| 14.949822| 99.999983|
             41|                   1|  0.000017|100.000000|


$ rwfilter ext1/*.rw ext2/*.rw --saddress=173.94.x.x --pass=stdout | rwstats --count=10 -
-bytes --protocol
INPUT SIZE: 5791380 records for 4 unique keys
PROTOCOL Key: Top 10 byte counts
       protocol|               Bytes|%_of_total|   cumul_%|
              6|        133183989975| 84.211893| 84.211893|
             17|         24063659865| 15.215390| 99.427283|
              1|           905770910|  0.572717|100.000000|
             41|                 136|  0.000000|100.000000|
```

Top Internal TCP Ports

```
$ rwfilter ext1/*.rw ext2/*.rw --daddress=173.94.x.x --proto=6 --pass=stdout | rwstats --
count=10 --bytes --dport
INPUT SIZE: 2383947 records for 63405 unique keys
```

```
DESTINATION PORT Key: Top 10 byte counts
          dPort|               Bytes|%_of_total|   cumul_%|
             80|          1784359657|  3.058887|  3.058887|
           1898|           885007740|  1.517148|  4.576035|
          54347|           523795945|  0.897931|  5.473967|
          63821|           511539184|  0.876920|  6.350886|
          57850|           431865781|  0.740338|  7.091224|
          53711|           381615080|  0.654194|  7.745418|
          53981|           380747058|  0.652706|  8.398124|
          52591|           380545819|  0.652361|  9.050485|
          54306|           380449574|  0.652196|  9.702681|
          53402|           379884990|  0.651228| 10.353909|
```

Top External TCP Ports

```
$ rwfilter ext1/*.rw ext2/*.rw --saddress=173.94.x.x --proto=6 --pass=stdout | rwstats --
count=10 --bytes --dport
INPUT SIZE: 2145928 records for 63349 unique keys
DESTINATION PORT Key: Top 10 byte counts
          dPort|               Bytes|%_of_total|   cumul_%|
          49168|          3842021182|  2.884747|  2.884747|
          49167|          3669974081|  2.755567|  5.640314|
             80|          2136851549|  1.604436|  7.244750|
            443|           245021093|  0.183972|  7.428722|
            993|           228504060|  0.171570|  7.600292|
             25|           194455184|  0.146005|  7.746297|
          39328|           158733185|  0.119183|  7.865480|
          32326|           126059999|  0.094651|  7.960131|
          56343|           118642351|  0.089082|  8.049213|
           1054|            99523567|  0.074726|  8.123939|
```

Top internal web server

```
$ rwfilter ext1/*.rw ext2/*.rw --daddress=173.94.x.x --proto=6 --dport=80,443 --
pass=stdout | rwstats --count=10 --bytes --dip
INPUT SIZE: 540766 records for 3839 unique keys
DESTINATION IP Key: Top 10 byte counts
             dIP|               Bytes|%_of_total|   cumul_%|
 173.94.202.147|          1241412322| 69.455023| 69.455023|
 173.94.202.157|           324423801| 18.150990| 87.606013|
 173.94.202.162|            36293519|  2.030564| 89.636577|
 173.94.202.220|            15821241|  0.885173| 90.521750|
 173.94.229.151|            13310580|  0.744706| 91.266455|
 173.94.202.208|            12179049|  0.681398| 91.947853|
    173.94.2.10|            12093960|  0.676638| 92.624491|
 173.94.202.222|            11489807|  0.642836| 93.267327|
 173.94.202.223|            11440745|  0.640091| 93.907418|
  173.94.50.165|             9993744|  0.559134| 94.466552|
```

```
$ rwfilter ext1/*.rw ext2/*.rw --saddress=173.94.x.x --proto=6 --sport=80,443 --
pass=stdout | rwstats --count=10 --bytes --sip
INPUT SIZE: 585165 records for 95 unique keys
SOURCE IP Key: Top 10 byte counts
             sIP|               Bytes|%_of_total|   cumul_%|
 173.94.202.147|        100785504558| 84.295259| 84.295259|
  173.94.36.236|          7782762243|  6.509368| 90.804627|
 173.94.202.157|          4516250251|  3.777314| 94.581941|
 173.94.202.220|           555372077|  0.464504| 95.046445|
 173.94.202.162|           549217770|  0.459356| 95.505801|
  173.94.154.85|           548196516|  0.458502| 95.964303|
```

```
 173.94.229.151|           488847063|  0.408863| 96.373167|
    173.94.2.10|           431093186|  0.360559| 96.733725|
 173.94.202.208|           419853688|  0.351158| 97.084884|
 173.94.202.222|           398368627|  0.333189| 97.418073|
```

Top external web server

```
$ rwfilter ext1/*.rw ext2/*.rw --saddress=173.94.x.x --proto=6 --dport=80,443 --
pass=stdout | rwstats --count=10 --bytes --dip
INPUT SIZE: 728623 records for 12449 unique keys
DESTINATION IP Key: Top 10 byte counts
            dIP|               Bytes|%_of_total|   cumul_%|
   47.89.29.112|            63314389|  2.658177|  2.658177|
  96.115.87.160|            60966982|  2.559624|  5.217801|
 200.41.249.245|            54517616|  2.288855|  7.506656|
   207.81.17.52|            30825371|  1.294165|  8.800821|
     47.89.2.12|            30704449|  1.289089| 10.089910|
 203.250.155.46|            25982070|  1.090825| 11.180735|
212.149.160.116|            19943377|  0.837298| 12.018034|
    47.89.72.65|            19775671|  0.830257| 12.848291|
   42.86.144.17|            18703299|  0.785235| 13.633526|
  35.44.210.128|            18233189|  0.765498| 14.399024|


$ rwfilter ext1/*.rw ext2/*.rw --daddress=173.94.x.x --proto=6 --sport=80,443 --
pass=stdout | rwstats --count=10 --bytes --sip
INPUT SIZE: 523547 records for 9996 unique keys
SOURCE IP Key: Top 10 byte counts
            sIP|               Bytes|%_of_total|   cumul_%|
   65.86.19.221|           876728344|  1.712805|  1.712805|
 164.154.230.76|           511518329|  0.999319|  2.712125|
 164.154.231.62|           486867802|  0.951161|  3.663286|
  50.20.170.211|           431668356|  0.843322|  4.506607|
 36.136.116.155|           430958408|  0.841935|  5.348542|
 36.136.116.222|           430930156|  0.841879|  6.190421|
  56.149.13.210|           428376498|  0.836890|  7.027312|
   65.86.21.231|           405866864|  0.792915|  7.820226|
 164.154.231.47|           389186271|  0.760327|  8.580554|
164.154.230.113|           381119594|  0.744568|  9.325121|
```

Internal SMTP Server

```
$ rwfilter ext1/*.rw ext2/*.rw --saddress=173.94.x.x --proto=6 --sport=25 --pass=stdout |
rwstats --count=10 --bytes --sip
INPUT SIZE: 39962 records for 2 unique keys
SOURCE IP Key: Top 10 byte counts
            sIP|               Bytes|%_of_total|   cumul_%|
 173.94.164.194|            23301167| 66.658171| 66.658171|
   173.94.167.7|            11655038| 33.341829|100.000000|


$ rwfilter ext1/*.rw ext2/*.rw --daddress=173.94.x.x --proto=6 --dport=25 --pass=stdout |
rwstats --count=10 --bytes --dip
INPUT SIZE: 28214 records for 49 unique keys
DESTINATION IP Key: Top 10 byte counts
            dIP|               Bytes|%_of_total|   cumul_%|
 173.94.164.194|            96861970| 91.454320| 91.454320|
   173.94.167.7|             9037234|  8.532700| 99.987020|
  173.94.167.24|                7020|  0.006628| 99.993648|
  173.94.154.85|                 576|  0.000544| 99.994191|
 173.94.246.100|                 416|  0.000393| 99.994584|
  173.94.223.17|                 180|  0.000170| 99.994754|
```

```
  173.94.131.34|                180|  0.000170| 99.994924|
  173.94.38.220|                144|  0.000136| 99.995060|
  173.94.170.25|                144|  0.000136| 99.995196|
  173.94.34.105|                144|  0.000136| 99.995332|
```

External SMTP Server

```
$ rwfilter ext1/*.rw ext2/*.rw --daddress=173.94.x.x --proto=6 --sport=25 --pass=stdout |
rwstats --count=10 --bytes --sip
INPUT SIZE: 2248 records for 100 unique keys
SOURCE IP Key: Top 10 byte counts
             sIP|               Bytes|%_of_total|   cumul_%|
 213.137.161.91|             1383935| 34.763606| 34.763606|
  213.137.161.6|             1069835| 26.873605| 61.637212|
  45.188.42.135|              443733| 11.146303| 72.783515|
 192.50.217.134|              439998| 11.052482| 83.835997|
 213.137.196.21|              227949|  5.725940| 89.561938|
  36.96.163.107|               72617|  1.824095| 91.386033|
 34.143.137.159|               72575|  1.823040| 93.209073|
 213.137.196.83|               52680|  1.323290| 94.532362|
   146.42.98.45|               17032|  0.427833| 94.960196|
  198.20.185.58|               16517|  0.414897| 95.375093|


$ rwfilter ext1/*.rw ext2/*.rw --saddress=173.94.x.x --proto=6 --dport=25 --pass=stdout |
rwstats --count=10 --bytes --dip
INPUT SIZE: 3189 records for 177 unique keys
DESTINATION IP Key: Top 10 byte counts
             dIP|               Bytes|%_of_total|   cumul_%|
 213.137.161.91|            71264000| 36.648033| 36.648033|
  213.137.161.6|            43441704| 22.340214| 58.988247|
  45.188.42.135|            18322902|  9.422686| 68.410933|
 192.50.217.134|            15847977|  8.149938| 76.560871|
  96.30.197.139|            11580465|  5.955339| 82.516210|
  96.30.197.136|             6038756|  3.105474| 85.621684|
  96.30.197.142|             4988998|  2.565629| 88.187313|
  96.30.197.149|             4432407|  2.279398| 90.466711|
  96.30.197.141|             4098969|  2.107925| 92.574636|
  36.96.163.107|             3761959|  1.934615| 94.509251|
```

Internal FTP Server

```
$ rwfilter ext1/*.rw ext2/*.rw --daddress=173.94.x.x --proto=6 --dport=20,21 --
pass=stdout | rwstats --count=10 --bytes --dip
INPUT SIZE: 10902 records for 44 unique keys
DESTINATION IP Key: Top 10 byte counts
             dIP|               Bytes|%_of_total|   cumul_%|
 173.94.202.153|            17029162| 99.968347| 99.968347|
 173.94.214.174|                1328|  0.007796| 99.976143|
 173.94.154.185|                 720|  0.004227| 99.980369|
   173.94.78.97|                 612|  0.003593| 99.983962|
 173.94.215.183|                 192|  0.001127| 99.985089|
 173.94.255.127|                 144|  0.000845| 99.985934|
 173.94.252.198|                 144|  0.000845| 99.986780|
  173.94.172.48|                 144|  0.000845| 99.987625|
 173.94.202.157|                 144|  0.000845| 99.988470|
 173.94.224.220|                 144|  0.000845| 99.989316|


$ rwfilter ext1/*.rw ext2/*.rw --saddress=173.94.x.x --proto=6 --sport=20,21 --
pass=stdout | rwstats --count=10 --bytes --sip
```

```
INPUT SIZE: 13146 records for 3 unique keys
SOURCE IP Key: Top 10 byte counts
            sIP|               Bytes|%_of_total|   cumul_%|
 173.94.202.153|            33542942| 99.998808| 99.998808|
 173.94.202.208|                 360|  0.001073| 99.999881|
 173.94.202.220|                  40|  0.000119|100.000000|
```

External Clients Contact with Internal FTP Server

```
$ rwfilter ext1/*.rw ext2/*.rw --proto=6 --aport=20,21 --saddress=173.94.x.x --
pass=stdout | rwstats --bytes --dip --count=10
INPUT SIZE: 13302 records for 37 unique keys
DESTINATION IP Key: Top 10 byte counts
            dIP|               Bytes|%_of_total|   cumul_%|
 50.243.189.116|            26147101| 77.736713| 77.736713|
    36.87.65.27|             5856786| 17.412534| 95.149247|
 192.100.211.64|             1401835|  4.167730| 99.316977|
  219.54.34.210|               81729|  0.242985| 99.559961|
 192.216.84.155|               63055|  0.187466| 99.747427|
192.232.237.117|               20644|  0.061376| 99.808803|
  208.106.57.35|                8784|  0.026115| 99.834918|
    3.54.210.32|                6929|  0.020600| 99.855519|
 56.155.139.131|                4032|  0.011987| 99.867506|
   196.99.69.55|                3948|  0.011738| 99.879244|
```

External FTP Server

```
$ rwfilter ext1/*.rw ext2/*.rw --daddress=173.94.x.x --proto=6 --sport=20,21 --
pass=stdout | rwstats --count=10 --bytes --sip
INPUT SIZE: 466 records for 20 unique keys
SOURCE IP Key: Top 10 byte counts
            sIP|               Bytes|%_of_total|   cumul_%|
 192.216.84.155|              171202| 24.972104| 24.972104|
197.118.218.101|              155810| 22.726974| 47.699078|
 197.118.218.98|              153375| 22.371797| 70.070875|
 197.118.218.90|              153312| 22.362608| 92.433483|
 192.13.213.212|                9436|  1.376367| 93.809850|
 197.118.218.73|                7768|  1.133067| 94.942916|
   196.99.69.55|                5428|  0.791746| 95.734663|
 197.118.218.80|                4371|  0.637569| 96.372232|
   54.22.98.135|                3628|  0.529192| 96.901424|
    53.14.64.14|                3619|  0.527880| 97.429304|

$ rwfilter ext1/*.rw ext2/*.rw --saddress=173.94.x.x --proto=6 --dport=20,21 --
pass=stdout | rwstats --count=10 --bytes --dip
INPUT SIZE: 156 records for 15 unique keys
DESTINATION IP Key: Top 10 byte counts
            dIP|               Bytes|%_of_total|   cumul_%|
 192.216.84.155|               63055| 68.450249| 68.450249|
  208.106.57.35|                8784|  9.535596| 77.985844|
   196.99.69.55|                3948|  4.285807| 82.271652|
 46.199.218.183|                2887|  3.134024| 85.405675|
  216.31.44.106|                2417|  2.623809| 88.029484|
    53.14.64.14|                2402|  2.607525| 90.637009|
    80.173.9.82|                1603|  1.740159| 92.377168|
 59.153.222.150|                1577|  1.711935| 94.089103|
 159.68.193.170|                1197|  1.299420| 95.388523|
 213.102.215.80|                1012|  1.098591| 96.487114|
```

Top Internal UDP Ports

```
$ rwfilter ext1/*.rw ext2/*.rw --daddress=173.94.x.x --proto=17 --pass=stdout | rwstats --count=10 --bytes --dport
INPUT SIZE: 3030140 records for 64554 unique keys
DESTINATION PORT Key: Top 10 byte counts
          dPort|               Bytes|%_of_total|   cumul_%|
          58938|          2275166143| 25.606781| 25.606781|
           9742|          1148140466| 12.922213| 38.528994|
          10380|          1053716575| 11.859481| 50.388476|
           3642|          1027249437| 11.561596| 61.950072|
           1194|           458161784|  5.156568| 67.106639|
           6970|           344835785|  3.881094| 70.987734|
          13657|           245566632|  2.763829| 73.751563|
          17404|           245187860|  2.759566| 76.511130|
           1434|           214442291|  2.413528| 78.924657|
           9744|           174305063|  1.961787| 80.886444|
```

Top External UDP Ports

```
$ rwfilter ext1/*.rw ext2/*.rw --saddress=173.94.x.x --proto=17 --pass=stdout | rwstats --count=10 --bytes --dport
INPUT SIZE: 2779650 records for 64254 unique keys
DESTINATION PORT Key: Top 10 byte counts
          dPort|               Bytes|%_of_total|   cumul_%|
          65417|         11070917978| 46.006792| 46.006792|
           7100|           229474849|  0.953616| 46.960408|
          44212|           202570138|  0.841809| 47.802217|
          57505|           153930435|  0.639680| 48.441897|
             53|           134049194|  0.557061| 48.998958|
          36414|           109851292|  0.456503| 49.455461|
          33510|           104177270|  0.432924| 49.888384|
           1345|            78729978|  0.327174| 50.215558|
          31181|            78518619|  0.326295| 50.541854|
          12021|            77486832|  0.322008| 50.863861|
```

Internal DNS Server

```
$ rwfilter ext1/*.rw ext2/*.rw --daddress=173.94.x.x --proto=17 --dport=53 --pass=stdout | rwstats --count=10 --bytes --dip
INPUT SIZE: 83040 records for 79 unique keys
DESTINATION IP Key: Top 10 byte counts
            dIP|               Bytes|%_of_total|   cumul_%|
  173.94.167.24|             6671119| 97.347087| 97.347087|
   173.94.203.7|               48438|  0.706823| 98.053910|
 173.94.200.175|               38086|  0.555763| 98.609673|
 173.94.189.243|               20520|  0.299434| 98.909108|
  173.94.18.171|                7518|  0.109705| 99.018813|
 173.94.225.206|                4575|  0.066760| 99.085572|
   173.94.78.69|                3780|  0.055159| 99.140731|
   173.94.71.17|                3240|  0.047279| 99.188010|
  173.94.84.196|                3240|  0.047279| 99.235290|
   173.94.11.83|                2700|  0.039399| 99.274689|
```

```
$ rwfilter ext1/*.rw ext2/*.rw --saddress=173.94.x.x --proto=17 --sport=53 --pass=stdout | rwstats --count=10 --bytes --sip
INPUT SIZE: 146207 records for 5 unique keys
SOURCE IP Key: Top 10 byte counts
            sIP|               Bytes|%_of_total|   cumul_%|
  173.94.167.24|            24473372| 99.152209| 99.152209|
 173.94.200.175|              207459|  0.840506| 99.992716|
 173.94.202.212|                1366|  0.005534| 99.998250|
 173.94.166.103|                 216|  0.000875| 99.999125|
```

```
   173.94.23.2|                216|  0.000875|100.000000|
```

External DNS Server

```
$ rwfilter ext1/*.rw ext2/*.rw --daddress=173.94.x.x --proto=17 --sport=53 --pass=stdout
| rwstats --count=10 --bytes --sip
INPUT SIZE: 1123459 records for 10648 unique keys
SOURCE IP Key: Top 10 byte counts
            sIP|               Bytes|%_of_total|   cumul_%|
 193.132.200.33|            11051454|  4.122339|  4.122339|
   35.81.169.26|            10287139|  3.837239|  7.959579|
203.218.163.197|             9978718|  3.722194| 11.681773|
  13.157.239.94|             9556671|  3.564765| 15.246538|
 203.243.29.195|             8906430|  3.322217| 18.568755|
203.216.215.182|             7780588|  2.902263| 21.471017|
 203.244.249.91|             6376949|  2.378687| 23.849704|
 206.171.120.56|             6330407|  2.361326| 26.211030|
 193.132.200.39|             5637675|  2.102928| 28.313957|
203.197.117.149|             4133872|  1.541989| 29.855947|
```

```
$ rwfilter ext1/*.rw ext2/*.rw --saddress=173.94.x.x --proto=17 --dport=53 --pass=stdout
| rwstats --count=10 --bytes --dip
INPUT SIZE: 1513045 records for 16449 unique keys
DESTINATION IP Key: Top 10 byte counts
            dIP|               Bytes|%_of_total|   cumul_%|
203.212.251.101|             4056566|  3.026177|  3.026177|
203.218.163.197|             3612573|  2.694961|  5.721138|
 206.171.120.56|             3276947|  2.444585|  8.165723|
 203.243.29.195|             3126597|  2.332425| 10.498148|
  203.232.18.52|             3000974|  2.238711| 12.736859|
 203.212.251.70|             2754133|  2.054569| 14.791428|
203.216.215.182|             2737155|  2.041903| 16.833331|
 203.244.249.91|             2537105|  1.892667| 18.725998|
212.202.207.255|             2180625|  1.626735| 20.352733|
203.218.163.238|             2122817|  1.583610| 21.936344|
```

Incoming ICMP

```
$ rwfilter ext1/*.rw ext2/*.rw --daddress=173.94.x.x --proto=1 --pass=stdout | rwstats --
icmp --count=10
INPUT SIZE: 509994 records for 28 unique keys
ICMP TYPE/CODE Key: Top 10 flow counts
       icmpType|       icmpCode|             Records|%_of_total|   cumul_%|
              0|              0|              207934| 40.771852| 40.771852|
             11|              0|              202586| 39.723212| 80.495065|
              3|              3|               72320| 14.180559| 94.675624|
              3|              1|               10363|  2.031985| 96.707608|
              8|              0|               10232|  2.006298| 98.713906|
              3|             13|                3848|  0.754519| 99.468425|
              3|              0|                1735|  0.340200| 99.808625|
              3|             10|                 653|  0.128041| 99.936666|
              5|              1|                 185|  0.036275| 99.972941|
              3|              4|                  72|  0.014118| 99.987059|
```

Outgoing ICMP

```
$ rwfilter ext1/*.rw ext2/*.rw --saddress=173.94.x.x --proto=1 --pass=stdout | rwstats --
icmp --count=10
INPUT SIZE: 865801 records for 10 unique keys
ICMP TYPE/CODE Key: Top 10 flow counts
       icmpType|       icmpCode|             Records|%_of_total|   cumul_%|
```

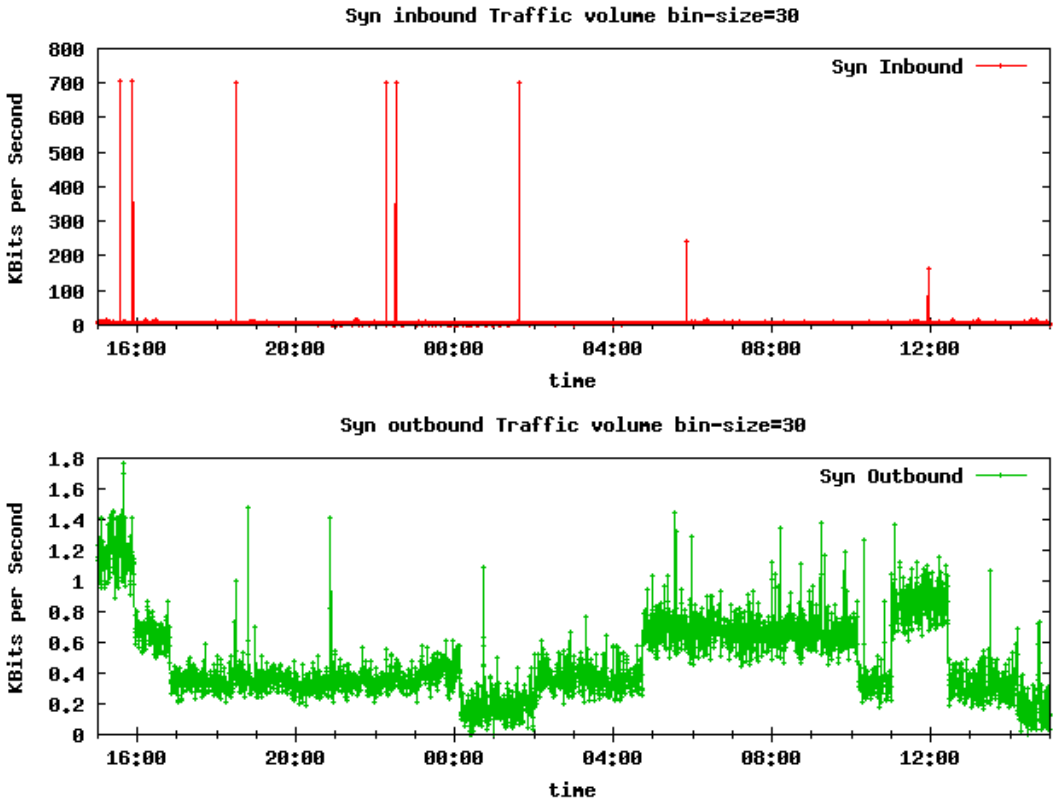
8|	0|	583206| 67.360283| 67.360283
3|	1|	202959| 23.441761| 90.802043
3|	3|	60131| 6.945129| 97.747173
0|	0|	9909| 1.144489| 98.891662
11|	0|	8984| 1.037652| 99.929314
3|	10|	476| 0.054978| 99.984292
3|	13|	90| 0.010395| 99.994687
3|	2|	24| 0.002772| 99.997459
0|	19|	13| 0.001501| 99.998961
11|	1|	9| 0.001039|100.000000

SYN-only traffic

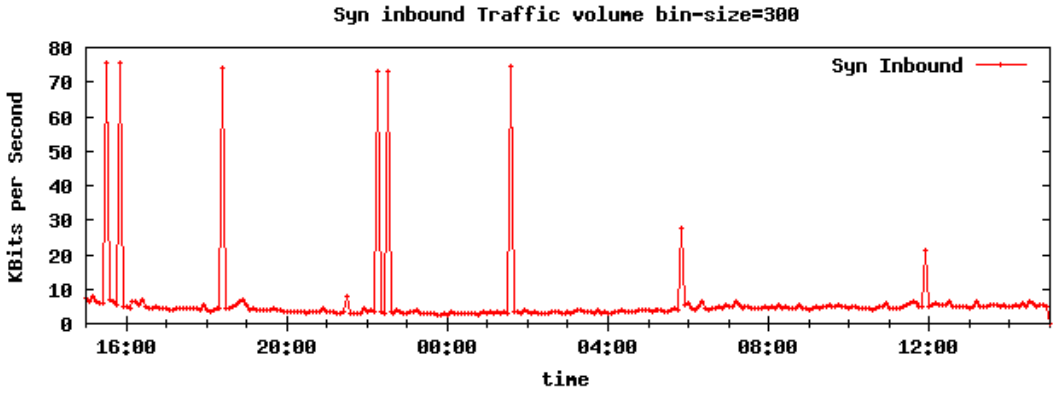
Command used:

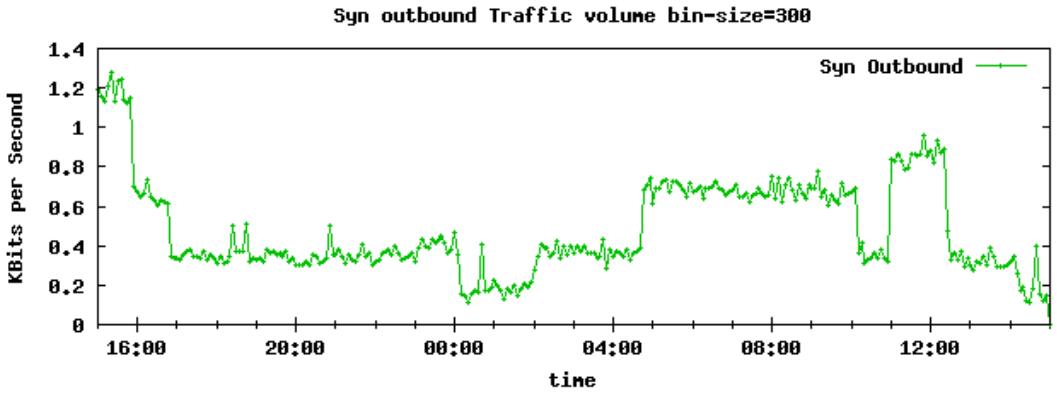
rwfilter anytcp.txt --saddr=173.94.x.x --flags-all=S/SAFR --packet=1-3 --pass=stdout | rwcount --bin-size=30 --delim=" " --output-path=OutSynOneToThree30.stats

rwfilter anytcp.txt --daddr=173.94.x.x --flags-all=S/SAFR --packet=1-3 --pass=stdout | rwcount --



bin-size=30 --delim=" " --output-path=InRstOneToThree30.stats





Top TCP Syn Sender/Incoming Flows

INPUT SIZE: 1101198 records for 140095 unique keys
SOURCE IP Key: Top 20 flow counts

sIP	Records	%_of_total	cumul_%
82.24.103.28	77238	7.013997	7.013997
83.34.72.40	65536	5.951337	12.965334
222.60.179.165	65536	5.951337	18.916671
85.173.174.47	65535	5.951246	24.867917
192.237.112.220	65530	5.950792	30.818708
82.218.17.164	65512	5.949157	36.767866
5.173.112.170	65502	5.948249	42.716115
52.132.32.75	22599	2.052219	44.768334
200.251.123.1	22276	2.022888	46.791222
221.172.29.174	14656	1.330914	48.122136
9.33.254.157	14217	1.291048	49.413185
82.24.102.149	6631	0.602162	50.015347
60.165.163.70	6590	0.598439	50.613786
13.212.179.70	4271	0.387850	51.001636
49.236.11.51	4242	0.385217	51.386853
56.147.164.128	3682	0.334363	51.721216
8.222.206.138	3336	0.302943	52.024159
220.176.74.68	3270	0.296949	52.321108
62.110.59.13	3256	0.295678	52.616786
202.201.110.179	3239	0.294134	52.910921

Top TCP Syn Receiver/Incoming Flows

INPUT SIZE: 1101198 records for 65536 unique keys
DESTINATION IP Key: Top 20 flow counts

dIP	Records	%_of_total	cumul_%

173.94.202.222	190110	17.263925	17.263925
173.94.202.223	156358	14.198900	31.462825
173.94.202.208	79142	7.186900	38.649725
173.94.202.220	13943	1.266166	39.915892
173.94.89.99	10864	0.986562	40.902454
173.94.193.120	4231	0.384218	41.286671
173.94.17.233	4111	0.373321	41.659992
173.94.18.181	1021	0.092717	41.752709
173.94.16.147	729	0.066201	41.818910
173.94.50.165	720	0.065383	41.884293
173.94.17.222	696	0.063204	41.947497
173.94.202.147	692	0.062841	42.010338
173.94.154.85	556	0.050490	42.060828
173.94.202.157	544	0.049401	42.110229
173.94.167.7	530	0.048129	42.158358
173.94.175.14	512	0.046495	42.204853
173.94.241.90	457	0.041500	42.246354
173.94.154.185	424	0.038504	42.284857
173.94.178.186	377	0.034235	42.319092
173.94.225.175	368	0.033418	42.352511

TOP TCP Syn Sender/Outgoing Flows

INPUT SIZE: 54768 records for 607 unique keys

SOURCE IP Key: Top 20 flow counts

sIP	Records	%_of_total	cumul_%
173.94.229.4	12825	23.416959	23.416959
173.94.89.99	10524	19.215600	42.632559
173.94.17.233	7175	13.100716	55.733275
173.94.18.189	6685	12.206033	67.939308
173.94.17.84	2682	4.897020	72.836328
173.94.202.220	1102	2.012124	74.848452
173.94.87.95	1093	1.995691	76.844143
173.94.18.187	989	1.805799	78.649942
173.94.202.208	910	1.661554	80.311496
173.94.202.222	906	1.654251	81.965746
173.94.202.223	881	1.608604	83.574350
173.94.18.162	462	0.843558	84.417908
173.94.87.184	334	0.609845	85.027753
173.94.16.147	285	0.520377	85.548130
173.94.106.157	205	0.374306	85.922436
173.94.69.182	189	0.345092	86.267528
173.94.229.116	141	0.257450	86.524978
173.94.111.42	140	0.255624	86.780602
173.94.232.33	140	0.255624	87.036226
173.94.88.47	138	0.251972	87.288197

TOP TCP Syn Receiver/Outgoing Flows

INPUT SIZE: 54768 records for 4191 unique keys

DESTINATION IP Key: Top 20 flow counts

dIP	Records	%_of_total	cumul_%
82.1.94.38	9473	17.296597	17.296597
54.10.36.102	3197	5.837350	23.133947
36.98.151.254	3188	5.820917	28.954864
45.157.74.99	3188	5.820917	34.775781
219.68.90.223	3186	5.817266	40.593047
81.12.233.246	2044	3.732106	44.325153
197.116.199.83	1559	2.846553	47.171706
36.36.225.145	517	0.943982	48.115688

80.243.89.143	447	0.816170	48.931858
196.212.52.13	370	0.675577	49.607435
39.166.213.90	314	0.573327	50.180762
154.44.101.188	194	0.354221	50.534984
145.193.156.179	186	0.339614	50.874598
119.192.115.166	183	0.334137	51.208735
119.149.19.241	183	0.334137	51.542872
119.192.115.164	183	0.334137	51.877008
196.17.40.139	181	0.330485	52.207493
137.75.22.144	176	0.321356	52.528849
145.193.156.186	176	0.321356	52.850204
49.29.236.51	164	0.299445	53.149649

TOP TCP Syn Sender-Receiver/Incoming Flows

INPUT SIZE: 1101198 records for 627988 unique keys

SIP/DIP PAIR Key: Top 20 flow counts

sIP	dIP	Records	%_of_total	cumul_%
82.24.103.28	173.94.202.222	39060	3.547046	3.547046
82.24.103.28	173.94.202.223	38178	3.466951	7.013997
52.132.32.75	173.94.202.208	11572	1.050856	8.064853
52.132.32.75	173.94.202.222	11017	1.000456	9.065309
9.33.254.157	173.94.202.222	9455	0.858610	9.923919
9.33.254.157	173.94.202.223	4762	0.432438	10.356357
82.24.102.149	173.94.202.223	3396	0.308391	10.664749
82.24.102.149	173.94.202.222	3235	0.293771	10.958520
53.232.5.173	173.94.202.222	2760	0.250636	11.209156
49.236.11.51	173.94.202.222	2123	0.192790	11.401946
49.236.11.51	173.94.202.223	2119	0.192427	11.594373
62.182.166.13	173.94.202.222	1896	0.172176	11.766549
13.212.179.70	173.94.202.222	1884	0.171086	11.937635
202.201.110.179	173.94.202.222	1623	0.147385	12.085020
50.182.85.163	173.94.202.222	1538	0.139666	12.224686
56.147.164.128	173.94.202.223	1464	0.132946	12.357632
62.110.59.13	173.94.202.223	1458	0.132401	12.490034
56.147.164.128	173.94.202.222	1331	0.120868	12.610902
13.212.179.70	173.94.202.208	1218	0.110607	12.721509
50.182.85.163	173.94.202.223	1196	0.108609	12.830118

TOP TCP Syn Sender-Receiver/Outgoing Flows

INPUT SIZE: 54768 records for 5109 unique keys

SIP/DIP PAIR Key: Top 20 flow counts

sIP	dIP	Records	%_of_total	cumul_%
173.94.229.4	82.1.94.38	7741	14.134166	14.134166
173.94.17.84	82.1.94.38	1678	3.063833	17.197999
173.94.18.189	54.10.36.102	1676	3.060181	20.258180
173.94.18.189	45.157.74.99	1670	3.049226	23.307406
173.94.18.189	36.98.151.254	1670	3.049226	26.356632
173.94.18.189	219.68.90.223	1669	3.047400	29.404032
173.94.229.4	54.10.36.102	1265	2.309743	31.713774
173.94.229.4	36.98.151.254	1263	2.306091	34.019866
173.94.229.4	45.157.74.99	1263	2.306091	36.325957
173.94.229.4	219.68.90.223	1262	2.304265	38.630222
173.94.87.95	197.116.199.83	817	1.491747	40.121969
173.94.18.187	197.116.199.83	742	1.354806	41.476775
173.94.18.162	80.243.89.143	447	0.816170	42.292945
173.94.87.95	36.36.225.145	272	0.496640	42.789585
173.94.17.84	54.10.36.102	250	0.456471	43.246056
173.94.17.84	36.98.151.254	249	0.454645	43.700701
173.94.17.84	219.68.90.223	249	0.454645	44.155346

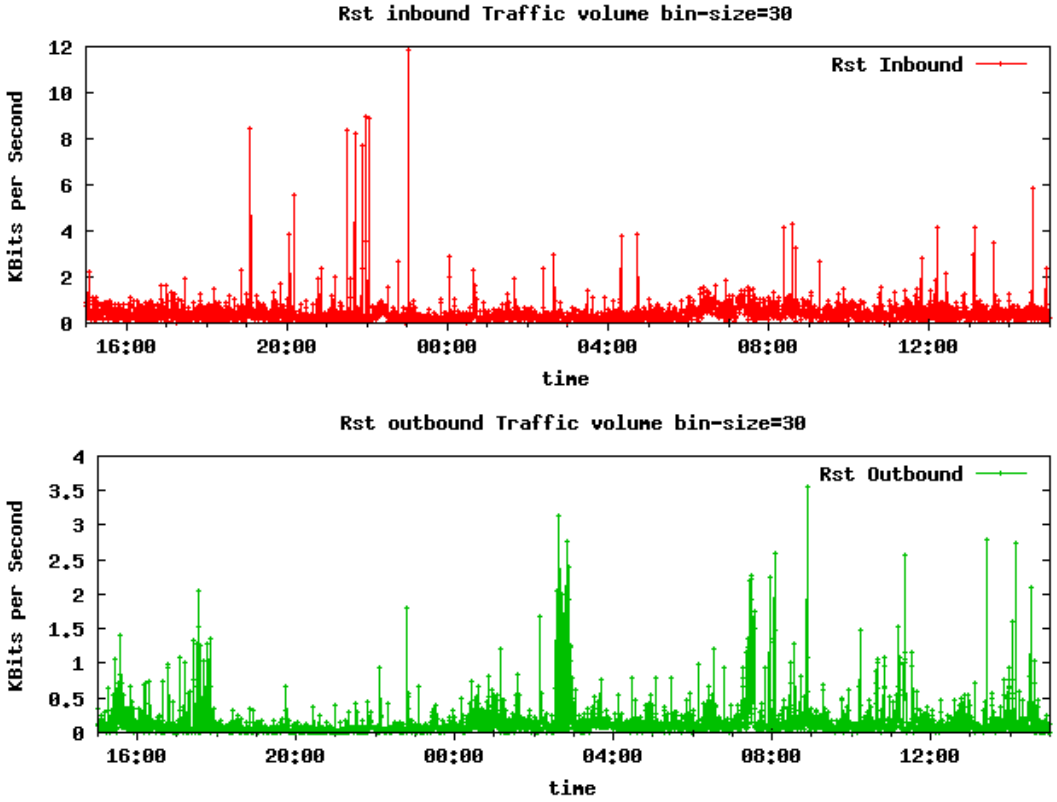
```
  173.94.17.84|   45.157.74.99|          249|  0.454645| 44.609991|
 173.94.18.187|  36.36.225.145|          245|  0.447342| 45.057333|
173.94.202.220|  196.212.52.13|          142|  0.259275| 45.316608|
```

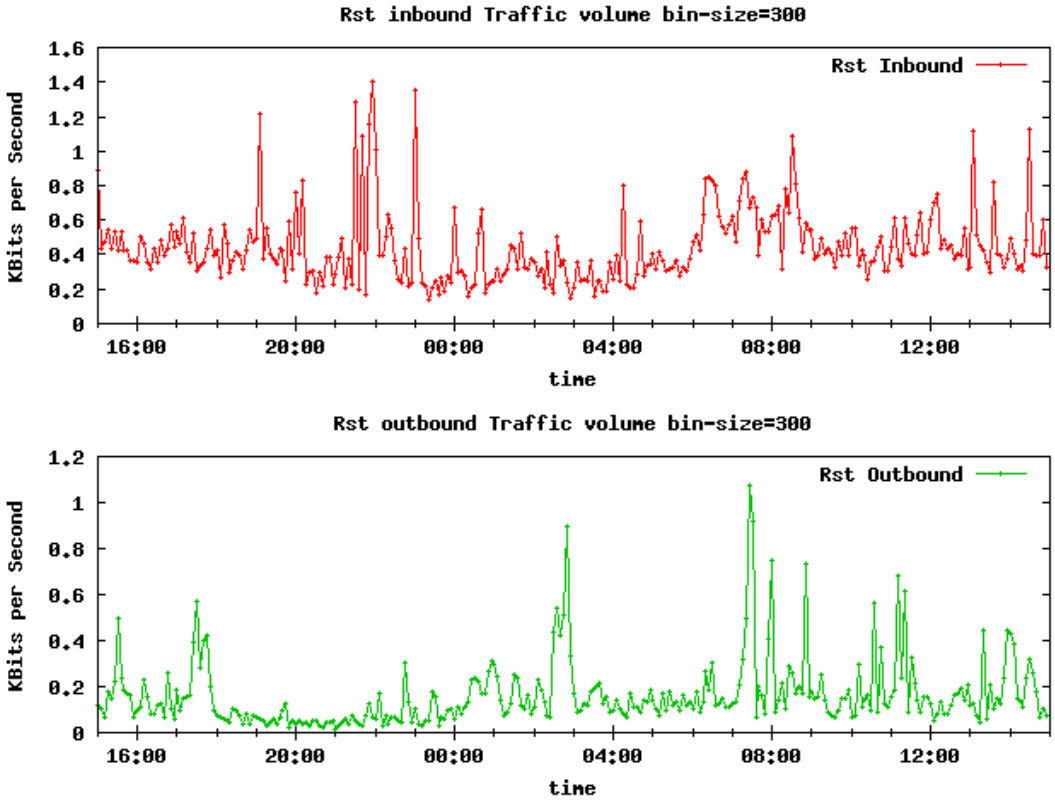
RST-only traffic

Command used:

rwfilter anytcp.txt --saddr=173.94.x.x --flags-all=R/SAFR --packet=1-3 --pass=stdout | rwcount --bin-size=30 --delim=" " --output-path=OutSynOneToThree30.stats

rwfilter anytcp.txt --daddr=173.94.x.x --flags-all=R/SAFR --packet=1-3 --pass=stdout | rwcount --bin-size=30 --delim=" " --output-path=InRstOneToThree30.stats





Top TCP-Rst Sender/Incoming Flows

INPUT SIZE: 118899 records for 7381 unique keys

SOURCE IP Key: Top 20 flow counts

sIP	Records	%_of_total	cumul_%
45.174.1.134	8293	6.974827	6.974827
42.86.144.65	8033	6.756154	13.730982
40.178.77.75	6161	5.181709	18.912691
36.87.68.136	4044	3.401206	22.313897
83.20.190.158	3929	3.304485	25.618382
213.137.196.21	2974	2.501283	28.119665
222.56.162.143	1597	1.343157	29.462821
221.188.110.212	1257	1.057200	30.520021
201.108.43.10	1253	1.053836	31.573857
36.87.64.41	1222	1.027763	32.601620
83.29.48.61	1200	1.009260	33.610880
36.87.75.21	973	0.818342	34.429221
36.87.68.192	864	0.726667	35.155889
1.105.26.29	788	0.662747	35.818636
83.29.41.213	786	0.661065	36.479701
46.249.117.47	613	0.515564	36.995265
36.87.64.225	542	0.455849	37.451114
36.87.64.128	417	0.350718	37.801832
178.45.39.130	417	0.350718	38.152550
220.19.211.30	415	0.349036	38.501585

Top TCP-Rst Receiver/Incoming Flows

INPUT SIZE: 118899 records for 4520 unique keys

DESTINATION IP Key: Top 20 flow counts

dIP	Records	%_of_total	cumul_%

173.94.202.147	61975	52.124072	52.124072
173.94.16.163	7426	6.245637	58.369709
173.94.36.236	4479	3.767063	62.136772
173.94.50.165	3887	3.269161	65.405933
173.94.202.157	2801	2.355781	67.761714
173.94.202.220	2324	1.954600	69.716314
173.94.154.85	2011	1.691351	71.407665
173.94.229.151	1972	1.658551	73.066216
173.94.164.194	1232	1.036174	74.102389
173.94.167.109	1067	0.897400	74.999790
173.94.202.223	922	0.775448	75.775238
173.94.164.145	769	0.646767	76.422005
173.94.202.208	765	0.643403	77.065408
173.94.50.128	730	0.613966	77.679375
173.94.38.214	701	0.589576	78.268951
173.94.90.48	639	0.537431	78.806382
173.94.154.23	627	0.527338	79.333720
173.94.202.162	585	0.492014	79.825734
173.94.202.222	561	0.471829	80.297563
173.94.133.228	500	0.420525	80.718088

Top TCP-Rst Sender/Outgoing Flows

INPUT SIZE: 43663 records for 1751 unique keys

SOURCE IP Key: Top 20 flow counts

sIP	Records	%_of_total	cumul_%
173.94.16.199	4341	9.942056	9.942056
173.94.202.157	2834	6.490621	16.432678
173.94.16.182	2556	5.853927	22.286604
173.94.71.210	2365	5.416485	27.703090
173.94.202.220	1795	4.111032	31.814122
173.94.202.147	1406	3.220118	35.034240
173.94.202.223	909	2.081854	37.116094
173.94.32.85	902	2.065822	39.181916
173.94.18.187	845	1.935277	41.117193
173.94.202.208	828	1.896342	43.013535
173.94.202.222	815	1.866569	44.880104
173.94.16.91	603	1.381032	46.261136
173.94.246.145	526	1.204681	47.465818
173.94.50.217	514	1.177198	48.643016
173.94.21.86	512	1.172618	49.815633
173.94.17.189	506	1.158876	50.974509
173.94.77.237	469	1.074136	52.048645
173.94.144.76	465	1.064975	53.113620
173.94.119.255	452	1.035201	54.148822
173.94.214.148	351	0.803884	54.952706

Top TCP-Rst Receiver/Outgoing Flows

INPUT SIZE: 43663 records for 3032 unique keys

DESTINATION IP Key: Top 20 flow counts

dIP	Records	%_of_total	cumul_%
212.134.67.8	1388	3.178893	3.178893
212.130.130.66	1148	2.629228	5.808121
199.202.185.86	1039	2.379589	8.187710
212.130.130.65	1015	2.324623	10.512333
212.130.130.64	963	2.205529	12.717862
96.115.87.3	957	2.191787	14.909649
212.134.67.9	929	2.127660	17.037308
96.30.194.92	768	1.758926	18.796235

196.97.30.143	657	1.504707	20.300941
197.116.199.83	626	1.433708	21.734649
137.75.22.158	589	1.348968	23.083618
212.130.130.85	584	1.337517	24.421135
96.115.87.160	562	1.287131	25.708266
137.75.22.144	537	1.229874	26.938140
212.149.160.116	415	0.950461	27.888601
43.22.0.99	382	0.874883	28.763484
212.134.67.20	357	0.817626	29.581110
39.166.213.91	352	0.806175	30.387284
40.43.6.215	319	0.730596	31.117880
212.134.67.0	309	0.707693	31.825573

TOP TCP Rst Sender-Receiver/Incoming Flows

INPUT SIZE: 118899 records for 11183 unique keys

SIP/DIP PAIR Key: Top 20 flow counts

sIP	dIP	Records	%_of_total	cumul_%
45.174.1.134	173.94.202.147	8293	6.974827	6.974827
42.86.144.65	173.94.16.163	6940	5.836887	12.811714
40.178.77.75	173.94.202.147	6161	5.181709	17.993423
36.87.68.136	173.94.36.236	4044	3.401206	21.394629
36.87.64.41	173.94.50.165	1222	1.027763	22.422392
36.87.75.21	173.94.229.151	973	0.818342	23.240734
36.87.68.192	173.94.167.109	864	0.726667	23.967401
1.105.26.29	173.94.202.147	788	0.662747	24.630148
83.29.41.213	173.94.202.220	786	0.661065	25.291214
213.137.196.21	173.94.50.128	706	0.593781	25.884995
46.249.117.47	173.94.229.151	613	0.515564	26.400558
42.86.144.65	173.94.154.23	612	0.514723	26.915281
36.87.64.225	173.94.202.162	542	0.455849	27.371130
83.20.190.158	173.94.133.228	500	0.420525	27.791655
42.86.144.65	173.94.154.220	468	0.393611	28.185266
36.87.64.128	173.94.154.85	417	0.350718	28.535984
178.45.39.130	173.94.202.147	417	0.350718	28.886702
220.19.211.30	173.94.202.147	415	0.349036	29.235738
221.188.91.141	173.94.202.220	405	0.340625	29.576363
83.20.190.158	173.94.250.187	396	0.333056	29.909419

TOP TCP Rst Sender-Receiver/Outgoing Flows

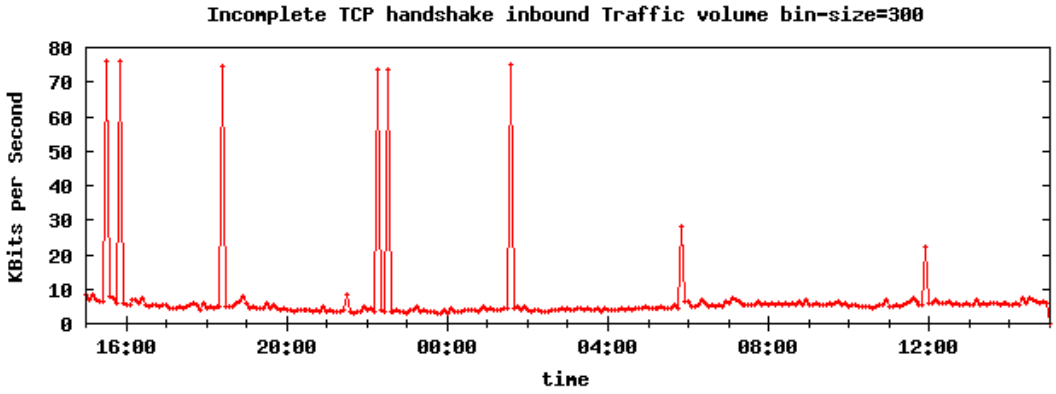
INPUT SIZE: 43663 records for 5926 unique keys

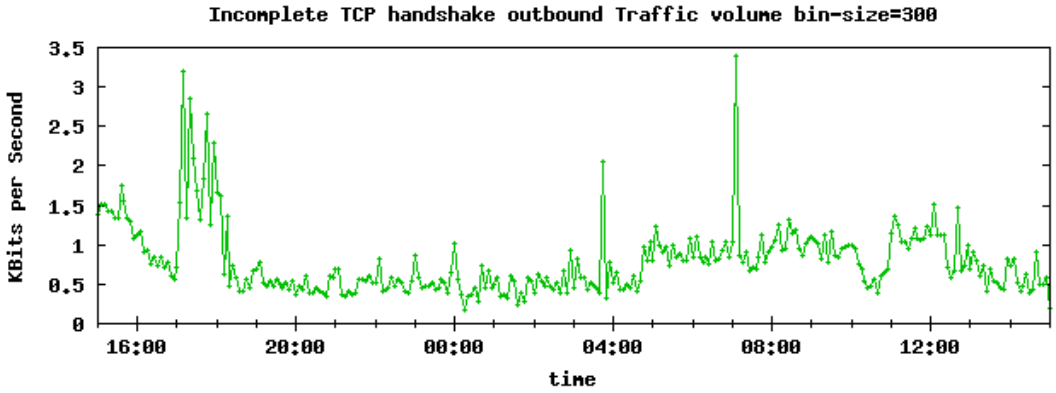
SIP/DIP PAIR Key: Top 20 flow counts

sIP	dIP	Records	%_of_total	cumul_%
173.94.16.182	212.130.130.65	900	2.061242	2.061242
173.94.16.182	212.134.67.8	738	1.690218	3.751460
173.94.16.199	212.130.130.64	738	1.690218	5.441678
173.94.32.85	96.30.194.92	733	1.678767	7.120445
173.94.16.199	212.134.67.8	650	1.488675	8.609120
173.94.18.187	197.116.199.83	626	1.433708	10.042828
173.94.16.199	212.130.130.85	584	1.337517	11.380345
173.94.16.199	212.134.67.9	579	1.326066	12.706410
173.94.16.199	212.130.130.66	570	1.305453	14.011864
173.94.16.182	212.130.130.66	521	1.193230	15.205094
173.94.21.86	96.115.87.3	487	1.115361	16.320454
173.94.144.76	212.149.160.116	370	0.847399	17.167854
173.94.119.255	199.202.185.86	369	0.845109	18.012963
173.94.16.199	212.134.67.20	357	0.817626	18.830589
173.94.16.182	212.134.67.9	350	0.801594	19.632183
173.94.16.199	40.43.6.215	319	0.730596	20.362779
173.94.16.199	212.134.67.0	309	0.707693	21.070472

```
173.94.202.220|  39.166.213.91|                300|  0.687081| 21.757552|
173.94.202.220| 140.148.107.72|                287|  0.657307| 22.414859|
  173.94.16.91|  196.97.30.143|                262|  0.600050| 23.014910|
```

Incomplete TCP Handshake analysis





Top incomplete handshake initiators for entire day

```
[nratanas@unix32 ~/proj2]$ rwfilter --flags-all=S/SRF --packets=1-3 --
daddr=173.94.x.x --pass=stdout ../proj/anytcp.txt | rwstats --sip --count=10
INPUT SIZE: 1153254 records for 142292 unique keys
SOURCE IP Key: Top 10 flow counts
             sIP|             Records|%_of_total|   cumul_%|
    82.24.103.28|               77238|  6.697397|  6.697397|
 222.60.179.165|               65536|  5.682703| 12.380100|
    83.34.72.40|               65536|  5.682703| 18.062803|
  85.173.174.47|               65535|  5.682616| 23.745419|
192.237.112.220|               65530|  5.682183| 29.427602|
  82.218.17.164|               65512|  5.680622| 35.108224|
  5.173.112.170|               65502|  5.679755| 40.787979|
   52.132.32.75|               22599|  1.959586| 42.747565|
  200.251.123.1|               22277|  1.931665| 44.679229|
 221.172.29.174|               14656|  1.270839| 45.950068|
```

Top incomplete handshake initiators between 15:00-16:00

```
nratanas@unix32 ext1]$ rwfilter --flags-all=S/SRF --packets=1-3 --
daddr=173.94.x.x --pass=stdout 2009033100.rw | rwstats --sip --count=10
INPUT SIZE: 171991 records for 10117 unique keys
SOURCE IP Key: Top 10 flow counts
             sIP|             Records|%_of_total|   cumul_%|
    83.34.72.40|               65536| 38.104319| 38.104319|
```

```
 5.173.112.170|               65501| 38.083970| 76.188289|
 82.24.102.149|                3220|  1.872191| 78.060480|
  52.132.32.75|                1558|  0.905861| 78.966341|
 221.24.251.84|                 889|  0.516888| 79.483229|
  9.33.254.157|                 594|  0.345367| 79.828596|
 49.182.56.171|                 508|  0.295364| 80.123960|
  11.213.12.49|                 508|  0.295364| 80.419324|
 83.49.177.217|                 480|  0.279084| 80.698409|
 61.51.188.205|                 383|  0.222686| 80.921095|
```

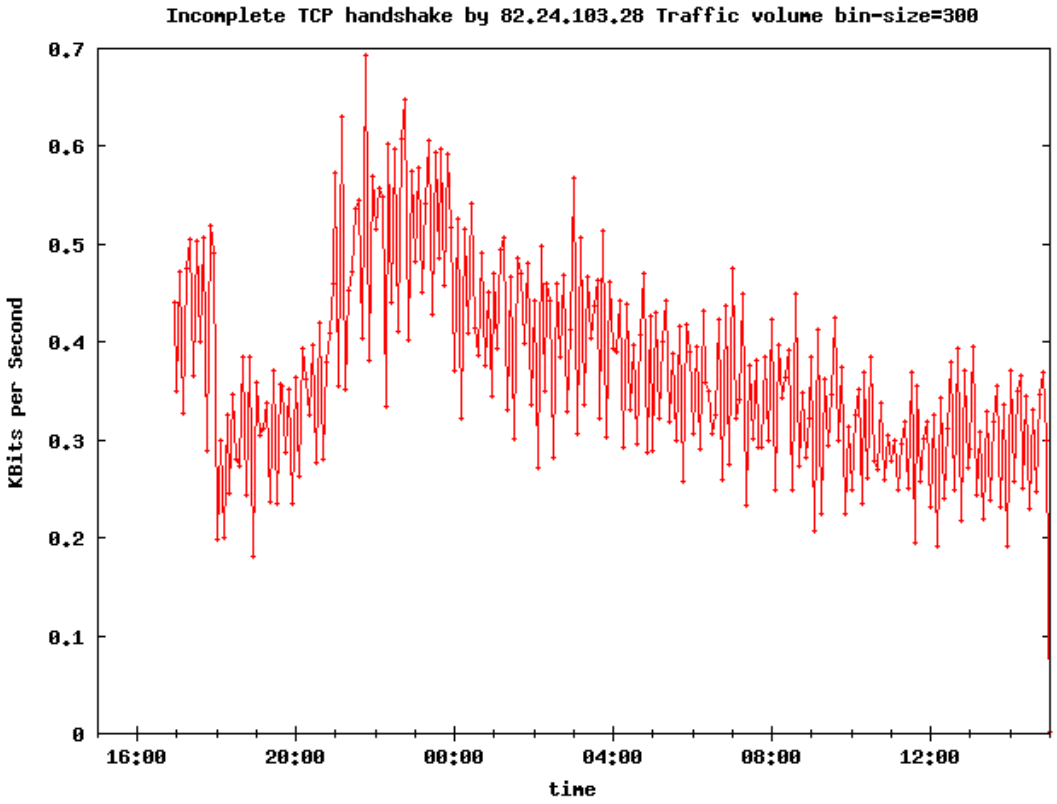
Top Incomplete handshake targets for entire day

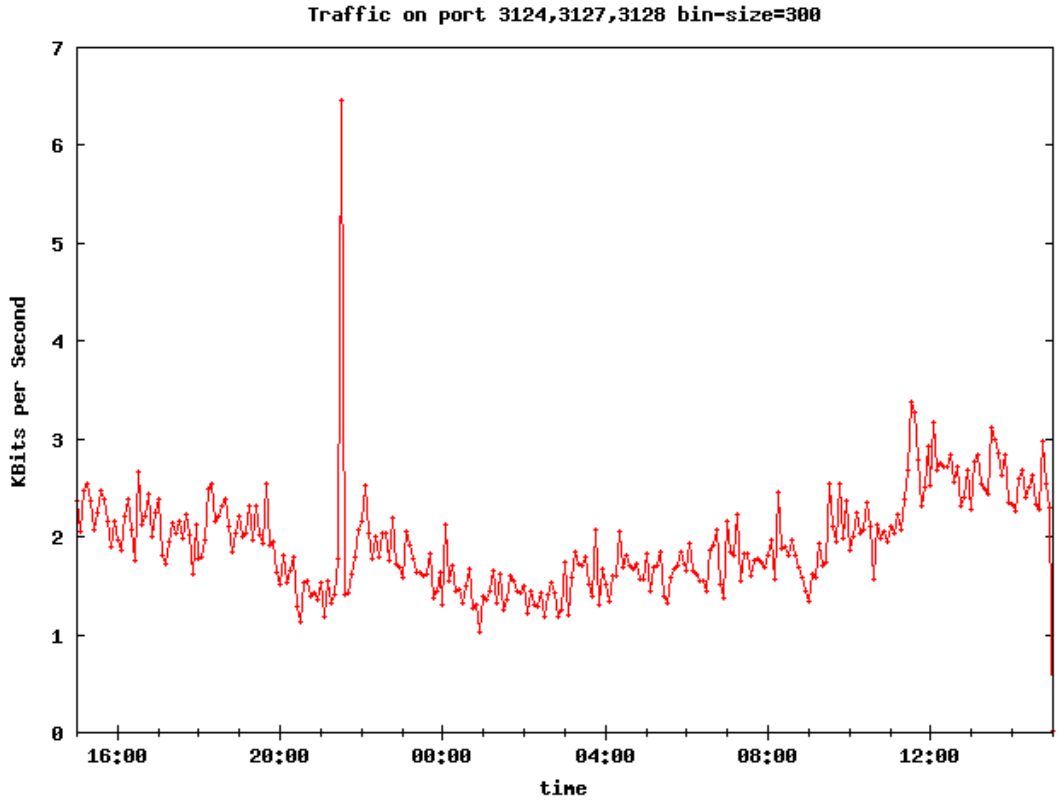
```
[nfatanas@unix32 ~/proj2]$ rwfilter --flags-all=S/SRF --packets=1-3 --
daddr=173.94.x.x --pass=stdout ../proj/anytcp.txt | rwstats --dip --count=10
INPUT SIZE: 1153254 records for 65536 unique keys
DESTINATION IP Key: Top 10 flow counts
            dIP|             Records|%_of_total|   cumul_%|
 173.94.202.222|              190296| 16.500788| 16.500788|
 173.94.202.223|              156491| 13.569517| 30.070305|
 173.94.202.208|               79227|  6.869866| 36.940171|
 173.94.202.220|               14380|  1.246907| 38.187078|
   173.94.89.99|               10986|  0.952609| 39.139686|
  173.94.17.233|                4720|  0.409277| 39.548963|
 173.94.193.120|                4232|  0.366962| 39.915925|
  173.94.16.147|                1139|  0.098764| 40.014689|
  173.94.18.181|                1023|  0.088706| 40.103394|
 173.94.202.147|                 950|  0.082376| 40.185770|
```

Top Incomplete handshake pairs for entire day

```
[nfatanas@unix32 ~/proj2]$ rwfilter --flags-all=S/SARF --packets=1-3 --
daddr=173.94.x.x --pass=stdout ../proj/anytcp.txt | rwstats --sip --dip --
count=10
INPUT SIZE: 1153254 records for 671728 unique keys
SIP/DIP PAIR Key: Top 10 flow counts
            sIP|            dIP|             Records|%_of_total|   cumul_%|
   82.24.103.28| 173.94.202.222|               39060|  3.386938|  3.386938|
   82.24.103.28| 173.94.202.223|               38178|  3.310459|  6.697397|
   52.132.32.75| 173.94.202.208|               11572|  1.003422|  7.700819|
   52.132.32.75| 173.94.202.222|               11017|  0.955297|  8.656116|
   9.33.254.157| 173.94.202.222|                9455|  0.819854|  9.475970|
   9.33.254.157| 173.94.202.223|                4762|  0.412919|  9.888888|
  82.24.102.149| 173.94.202.223|                3396|  0.294471| 10.183359|
  82.24.102.149| 173.94.202.222|                3235|  0.280511| 10.463870|
   53.232.5.173| 173.94.202.222|                2760|  0.239323| 10.703193|
   49.236.11.51| 173.94.202.222|                2123|  0.184088| 10.887281|
```

Incomplete handshake pattern of 82.24.103.28 (This holds true for 52.132.32.75, 9.33.254.157, 82.24.102.149, and many more) on 173.94.202.222,223,208


Incomplete TCP handshake by 82.24.103.28 Traffic volume bin-size=300
KBits per Second
0.7
0.6
0.5
0.4
0.3
0.2
0.1
0
16:00
20:00
00:00
04:00
08:00
12:00
time



The scanning traffic between 82.24.103.28 and our network

```
[nratanas@unix37 ~/proj]$ rwfilter --flags-all=S/SARF --packets=1-3 --
daddr=173.94.x.x --saddr=82.24.103.28 --pass=stdout ../proj/anytcp.txt | rwcut
--fields=1,2,3,4,5,9 | more
            sIP|            dIP|sPort|dPort|pro|                  sTime|
   82.24.103.28| 173.94.202.223| 1486| 3128|  6|2009/03/30T16:55:25.579|
   82.24.103.28| 173.94.202.223| 1486| 3128|  6|2009/03/30T16:55:26.316|
   82.24.103.28| 173.94.202.223| 1486| 3128|  6|2009/03/30T16:55:27.025|
   82.24.103.28| 173.94.202.223| 2564| 3127|  6|2009/03/30T16:55:31.878|
   82.24.103.28| 173.94.202.223| 2564| 3127|  6|2009/03/30T16:55:32.656|
   82.24.103.28| 173.94.202.222| 4332| 3124|  6|2009/03/30T16:55:33.472|
   82.24.103.28| 173.94.202.223| 2564| 3127|  6|2009/03/30T16:55:38.591|
   82.24.103.28| 173.94.202.223| 4871| 3127|  6|2009/03/30T16:55:39.164|
   82.24.103.28| 173.94.202.223| 1573| 3128|  6|2009/03/30T16:55:40.932|
   82.24.103.28| 173.94.202.223| 4871| 3127|  6|2009/03/30T16:55:42.116|
   82.24.103.28| 173.94.202.223| 4871| 3127|  6|2009/03/30T16:55:42.825|
   82.24.103.28| 173.94.202.223| 1573| 3128|  6|2009/03/30T16:55:43.933|
   82.24.103.28| 173.94.202.223| 1573| 3128|  6|2009/03/30T16:55:44.738|
   82.24.103.28| 173.94.202.222| 4529| 3128|  6|2009/03/30T16:55:46.363|
   82.24.103.28| 173.94.202.222| 4613| 3128|  6|2009/03/30T16:55:46.473|
   82.24.103.28| 173.94.202.223| 1326| 3127|  6|2009/03/30T16:55:47.195|
   82.24.103.28| 173.94.202.222| 4613| 3128|  6|2009/03/30T16:55:47.343|
```

Top scanning traffic to our network on port 3124,3127,3128 by scanning host ip

```
[nratanas@unix36 ~/proj]$ rwfilter --flags-all=S/SARF --packets=1-3 --
daddr=173.94.x.x --dport=3128,3124,3127 --pass=stdout anytcp.txt | rwstats --sip
--bytes --count=10
INPUT SIZE: 396805 records for 4809 unique keys
SOURCE IP Key: Top 10 byte counts
            sIP|               Bytes|%_of_total|   cumul_%|
   82.24.103.28|             3707520| 17.660865| 17.660865|
   52.132.32.75|             1446336|  6.889658| 24.550523|
   9.33.254.157|              739596|  3.523084| 28.073608|
   0.144.86.198|              371136|  1.767916| 29.841523|
```

```
  82.24.102.149|              318288|  1.516173| 31.357696|
 56.147.164.128|              220920|  1.052358| 32.410054|
  13.212.179.70|              205008|  0.976561| 33.386615|
   49.236.11.51|              203616|  0.969930| 34.356545|
202.201.110.179|              194340|  0.925744| 35.282288|
  8.222.206.138|              160128|  0.762774| 36.045062|
```

Top scanning traffic on port 3124,3127 and 3128 by victim ip

```
[nratanas@unix37 ~/proj]$ rwfilter --flags-all=S/SARF --packets=1-3 --
dport=3128,3124,3127 --pass=stdout anytcp.txt | rwstats --dip --bytes --count=10
INPUT SIZE: 396925 records for 3111 unique keys
DESTINATION IP Key: Top 10 byte counts
            dIP|               Bytes|%_of_total|   cumul_%|
 173.94.202.222|             9147044| 43.552964| 43.552964|
 173.94.202.223|             7242236| 34.483363| 78.036327|
 173.94.202.208|             3767968| 17.940897| 95.977224|
 173.94.202.166|               19952|  0.095000| 96.072224|
 173.94.202.220|               14644|  0.069726| 96.141951|
 173.94.202.244|                4032|  0.019198| 96.161149|
 173.94.202.214|                4032|  0.019198| 96.180347|
 173.94.202.229|                3888|  0.018512| 96.198859|
 173.94.202.158|                3888|  0.018512| 96.217372|
  173.94.202.50|                3744|  0.017827| 96.235198|
```

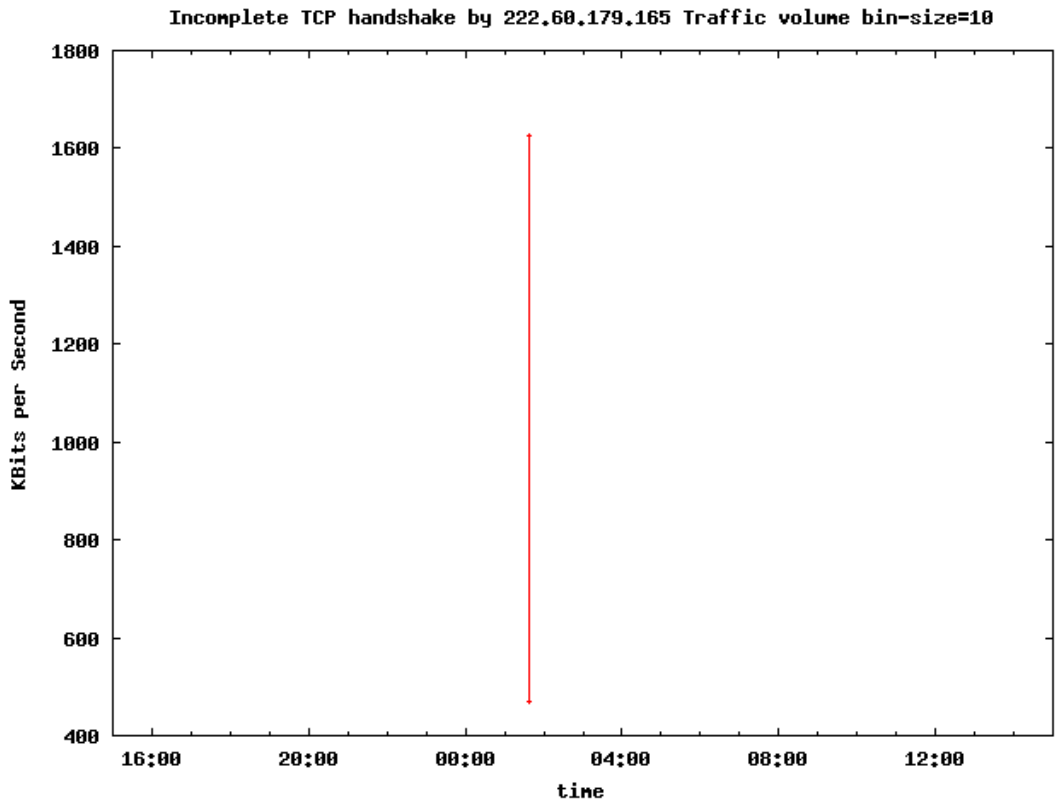
The scanning traffic between 82.24.103.28 and our network

```
[nratanas@unix32 ~/proj2]$ rwfilter --flags-all=S/SRF --packets=1-3 --
daddr=173.94.x.x --saddr=82.24.103.28 --pass=stdout ../proj/anytcp.txt | rwstats
--sip --dip --count=10
INPUT SIZE: 77238 records for 2 unique keys
SIP/DIP PAIR Key: Top 10 flow counts
            sIP|            dIP|             Records|%_of_total|   cumul_%|
   82.24.103.28| 173.94.202.222|               39060| 50.570962| 50.570962|
   82.24.103.28| 173.94.202.223|               38178| 49.429038|100.000000|
```

The port being scanned by 82.24.103.28

```
[nratanas@unix32 ~/proj2]$ rwfilter --flags-all=S/SRF --packets=1-3 --
daddr=173.94.x.x --saddr=82.24.103.28 --pass=stdout ../proj/anytcp.txt | rwstats
--dport --count=10
INPUT SIZE: 77238 records for 3 unique keys
DESTINATION PORT Key: Top 10 flow counts
          dPort|             Records|%_of_total|   cumul_%|
           3128|               38659| 50.051788| 50.051788|
           3127|               19329| 25.025247| 75.077035|
           3124|               19250| 24.922965|100.000000|
```

Incomplete handshake pattern of 222.60.179.165 (This holds true for 202.251.123.1, 83.34.72.40, 85.173.174.47 and many more) on 173.94.0.0/16 network.



Scanning traffic pattern between 222.60.179.165 and our network

[nratanas@unix37 ~/proj]$ rwfilter --flags-all=S/SRF --packets=1-3 --
daddr=173.94.x.x --saddr=222.60.179.165 --pass=stdout ../proj/anytcp.txt |
rwsort --fields=2 | rwcut --fields=1,2,3,4,9 | more
rwsort: Warning: Using default temporary directory /tmp

sIP	dIP	sPort	dPort	sTime
222.60.179.165	173.94.0.0	6000	2967	2009/03/31T01:38:08.989
222.60.179.165	173.94.0.1	6000	2967	2009/03/31T01:38:08.991
222.60.179.165	173.94.0.2	6000	2967	2009/03/31T01:38:08.989
222.60.179.165	173.94.0.3	6000	2967	2009/03/31T01:38:08.991
222.60.179.165	173.94.0.4	6000	2967	2009/03/31T01:38:08.991
222.60.179.165	173.94.0.5	6000	2967	2009/03/31T01:38:08.991
222.60.179.165	173.94.0.6	6000	2967	2009/03/31T01:38:08.991
222.60.179.165	173.94.0.7	6000	2967	2009/03/31T01:38:08.988
222.60.179.165	173.94.0.8	6000	2967	2009/03/31T01:38:08.991
222.60.179.165	173.94.0.9	6000	2967	2009/03/31T01:38:08.990
222.60.179.165	173.94.0.10	6000	2967	2009/03/31T01:38:08.991
222.60.179.165	173.94.0.11	6000	2967	2009/03/31T01:38:08.988
222.60.179.165	173.94.0.12	6000	2967	2009/03/31T01:38:08.990
222.60.179.165	173.94.0.13	6000	2967	2009/03/31T01:38:08.988
222.60.179.165	173.94.0.14	6000	2967	2009/03/31T01:38:08.993
222.60.179.165	173.94.0.15	6000	2967	2009/03/31T01:38:08.988
222.60.179.165	173.94.0.16	6000	2967	2009/03/31T01:38:08.989

Inspection on the response from our network to the scanning host, 222.60.179.165

[nratanas@unix37 ~/proj]$ rwfilter anytcp.txt --daddr=222.60.179.165 --
saddr=173.94.x.x --pass=stdout | rwcut --fields=1,2,3,4,5,8,9 | more

sIP	dIP	sPort	dPort	pro	flags	sTime
173.94.196.120	222.60.179.165	2967	6000	6	R A	2009/03/31T01:38:06.858

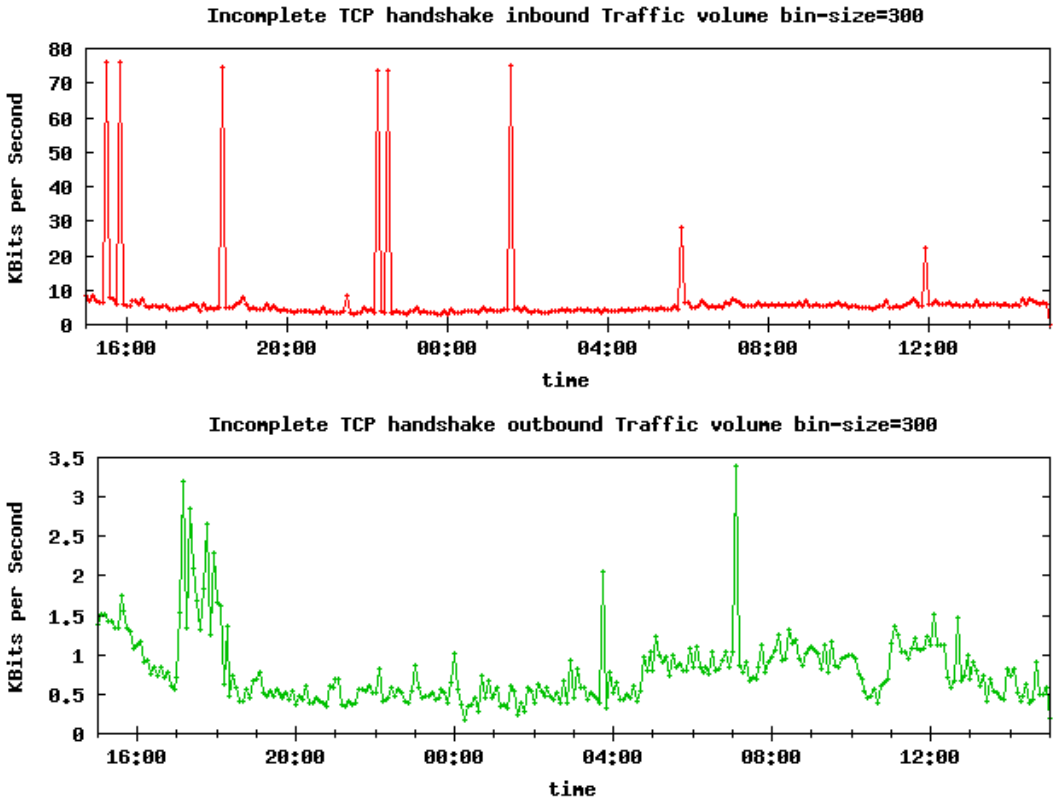
```
|
  173.94.203.23| 222.60.179.165| 2967| 6000|  6|  R A   |2009/03/31T01:38:06.993
|
  173.94.203.30| 222.60.179.165| 2967| 6000|  6|  R A   |2009/03/31T01:38:06.996
|
 173.94.202.147| 222.60.179.165| 2967| 6000|  6|  R A   |2009/03/31T01:38:07.007
|
 173.94.202.153| 222.60.179.165| 2967| 6000|  6|  R A   |2009/03/31T01:38:07.008
```

Top ten host being connected on port 1433,2967,3389,8080

```
[nratanas@unix37 ~/proj]$ rwfilter anytcp.txt --sport=2967,1433,3389,8080 --
saddr=173.94.x.x --pass=stdout | rwstats --sip --count=10
INPUT SIZE: 10544 records for 165 unique keys
SOURCE IP Key: Top 10 flow counts
            sIP|             Records|%_of_total|   cumul_%|
 173.94.202.220|                3200| 30.349014| 30.349014|
 173.94.202.208|                2447| 23.207511| 53.556525|
 173.94.202.223|                2351| 22.297041| 75.853566|
 173.94.202.222|                2180| 20.675266| 96.528832|
 173.94.202.153|                  11|  0.104325| 96.633156|
 173.94.202.169|                   7|  0.066388| 96.699545|
  173.94.16.128|                   7|  0.066388| 96.765933|
 173.94.202.145|                   6|  0.056904| 96.822838|
 173.94.202.168|                   6|  0.056904| 96.879742|
 173.94.202.163|                   6|  0.056904| 96.936646|
```

Traffic pattern of the response from our network to the external network on port 6000.

```
[nratanas@unix37 ~/proj]$ rwfilter anytcp.txt --dport=6000 --flags-all=AS/ASRF
 --saddr=173.94.x.x --pass=stdout | rwcut --fields=1,2,3,4,5,6,7,8,9 | more
            sIP|            dIP|sPort|dPort|pro|   packets|     bytes|   flags|
              sTime|
 173.94.202.192|  5.173.112.170| 3389| 6000|  6|         1|        44| S  A   |2
009/03/30T15:34:12.071|
 173.94.202.147| 48.235.139.189|   80| 6000|  6|        20|     27190| S PA   |2
009/03/30T20:13:10.020|
 173.94.202.169|  200.251.123.1| 8080| 6000|  6|         1|        44| S  A   |2
009/03/31T05:50:09.424|
 173.94.202.162|  200.251.123.1| 8080| 6000|  6|         1|        40| S  A   |2
009/03/31T05:50:09.435|
```



Considering the incomplete TCP handshake inbound traffic above, we will see 8 peaks. We can associate the IP of the scanner with each peak,

15:34 - 5.173.112.170 - 1433

15:52 - 83.34.72.40 - 2967

18:29 - 82.218.17.164 -1433

22:15 - 192.237.112.220 - 8080

22:30 - 85.173.174.47 - 2967

01:38 - 222.60.179.165 - 3389

05:50 - 200.251.123.1 - 8080

11:55 - 221.172.29.174 - 2967

All of these scan was conducted using the same source port = 6000 and destination port = 1433,2967,3389,8080. These destination port are common to be scanned for vulnerabilities nowadays.

Top port associated with incomplete handshake

```
[nfatanas@unix37 ~/proj2]$ rwfilter --flags-all=S/SRF --packets=1-3 --
daddr=173.94.x.x --pass=stdout ../proj/anytcp.txt | rwstats --dport --count=10
INPUT SIZE: 1153254 records for 54378 unique keys
DESTINATION PORT Key: Top 10 flow counts
          dPort|             Records|%_of_total|   cumul_%|
          3128|              172207| 14.932270| 14.932270|
          2967|              145708| 12.634511| 27.566781|
          1433|              131167| 11.373644| 38.940424|
          3124|              121643| 10.547806| 49.488231|
          3127|              102985|  8.929950| 58.418180|
          8080|               91120|  7.901122| 66.319302|
          3389|               65794|  5.705075| 72.024376|
         15078|               10853|  0.941076| 72.965453|
```

```
445|              10810|  0.937348| 73.902800|
 80|               8760|  0.759590| 74.662390|
```

B. Vulnerabilities associated with port 1433,2967,3389 (taken from the internet article)

Port 1433(www.linklogger.com/TCP1433.htm)

Common Use
Microsoft SQL Server port used typically for remote connections to the database.

Inbound Scan
Inbound scans are typically looking for Microsoft SQL Server installations with weak password protection and if successful are looking to steal or corrupt data or use some features with SQL Server to compromise the host system. There are some worms which scan this port but mostly tools.

Outbound Scan
Outbound scans if occurring in volume should be considered an indication of a possible worm infection on the source computer and should be investigated.

This port's adjacent UDP cousin (port 1434) hosted the fastest spreading Internet worm ever seen at the time. What's interesting about this port (1433) is that a less well known, and significantly less prolific SQL worm, known as the "SQL Snake" was discovered to be exploiting a different SQL server vulnerability almost a year earlier. It didn't make headlines, but it did come to the attention of the Internet security community. Microsoft generated patches for their SQL server products but, as shown by the later success of the SQL Slammer worm, they apparently didn't examine all of the SQL Server Internet interface code. Whoops.

Needless to say, if our port analysis found your port 1433 open, and if you are not deliberately offering SQL services to the global Internet (who would be that insane?), you will definitely want to either shut down the secret SQL server running in your machine, or arrange to have a personal firewall or NAT router block that port from all external access. (And do the same for port 1434 while you're at it!)

Port 2967

Common vulnerability
“Exploits an overflow condition in Symantec AV Corp. Masquerades as msupdates.exe, nod33.exe and wauclt.exe. Bot also connects back to an IRC server on a non-standard port. Lives in %windir%\system32 and is set as hidden and read only. Makes many registry changes to the netbt hive under HKLM\System\CurrentControlSet\Services and to the HKLM\SOFTWARE\Microsoft\Windows run and OLE keys. Runs IP scans en mass to discover other hosts to infect.”

Example of relate worm that exploits this port.
“Symantec: W32.Rinbot.BC
http://www.symantec.com/enterprise/security_response/writeup.jsp?docid=2007-041701-3720-99

QUOTE: The worm opens a random port and waits for a connection from shell code. The worm scans network for computers vulnerable to the following vulnerabilities and exploits them:

* The Microsoft DNS Server Service Could Allow Remote Code Execution (BID 23470) on TCP port 1025
* The Microsoft Windows Server Service Remote Buffer Overflow Vulnerability (BID 19409) on TCP port 139

* Symantec Client Security and Symantec AntiVirus Elevation of Privilege (BID 18107) on TCP port 2967"

Port 3389

This port is use by The Remote Desktop Protocol (RDP) service. The unpatched MS window platform which open this port either by default or by user might susceptible to the DDoS attack or any other attacks as stated below.

"The vulnerability, thought at first to affect only Windows XP SP2, is now believed to affect all current Windows editions, including Windows 2000, Windows XP SP1, Windows XP Professional x64, Windows Server 2003, Windows Server 2003 SP1, and Windows Server x64.

The Remote Desktop Protocol (RDP) is not enabled by default, however if the service is enabled, a Denial of Service attack could cause the OS to restart unexpectedly according to Microsoft, or experience buffer overflows according to Symantec. The RDP is enabled by default on Windows XP Media Center Edition.

Microsoft suggests users block TCP port 3389 (the port used by RDP) on their firewall, or disable Terminal Services or Remote Desktop if not required by the user. The remote desktop connections could also be secured using either Internet Protocol Security or a virtual private network connection until a patch is ready."

C. References

Usage and vulnerabilities on port

1433 http://www.linklogger.com/TCP1433.htm

2967 - http://www.symantec.com/enterprise/security_response/writeup.jsp?docid=2007-041701-3720-99

3389 - http://isc.sans.org/diary.html?storyid=599

Recent Event Case Study:

1. http://isc.sans.org/diary.html?storyid=5713

2. http://www.merit.edu/mail.archives/nanog/2009-01

3. http://www.icann.org/en/committees/security/dns-ddos-advisory-31mar06.pdf

4. http://www.circleid.com/posts/20090123_network_solutions_down_ddos_attack/