Network Traffic Audit

COMP 8006 – Final Project

By:

Jeffrey Sasaki

British Columbia Institute of Technology

Aman Abdulla

March 26, 2015

Disclaimer's Note:

This document contains confidential information that should only be seen by readers authorized by the author. All sensitive information have been sanitized due to privacy matters.

For inquiries regarding this document, please contact the author.

CONTENTS

SUMMARY

The purpose of this project is to audit three separate networks. The goal of this project is to apply the practical principles and knowledge of intrusion detection and packet analysis.

The tools used in this project include Snort, SnortSnarf, Splunk, Microsoft Excel and Wireshark.

All three networks examined have been compromised in one form or another.

After examining Network 1's alert files, there are evidence showing that the firewall machine has been compromised.

Network 2 showed UPnP traffic which alerted the snort system. The UPnP scan came up as a false positive, and it appears that no harm has been done.

Network 3 has been compromised and is sending out MS-SQL Worms out to external IP's, the timestamps shown in the alert file reports that the worms are being sent rapidly by the milliseconds.

This project only covers a marginal amount of exploits caught out of the full dataset. Due to time constraints and processing time of large data, more exploits may arise.

INTRODUCTION

In 1989, a young, and yet to be knighted then, Tim Berners-Lee revolutionized the computing world and brought to us the World Wide Web. Sir Tim Berners-Lee's vision of the World Wide Web was to promote creativity and invent a system where people can communicate across the globe with each other. That vision was quickly diminished, as people begin to find ways of exploiting the Internet, for the benefit of their own. As technology became more sophisticated, people that were able to manipulate and abuse the system reigned havoc onto those that are gullible enough to expose themselves. Hence, it is the role of network security analysts to protect those that are vulnerable against exploits and to provide defense against hackers.

The purpose of this project is to audit three separate networks. The goal of this project is to apply the practical principles and knowledge of intrusion detection and packet analysis. The process of this project includes identifying, observing and analyzing malicious activities for each network. The networks contains a significant number of files, which includes pcap network traffic files, various log files (eg. secure, Snort, syslog, etc.), and other additional files readily available to contribute towards network auditing.

REQUIREMENTS

The following are the requirements for this project, specified by the hand out provided:

- A summary of detects prioritized by number of occurrences for each of the three networks.
- Malicious traffic, reconnaissance traffic, and benign traffic.
- The top sources of traffic to and from each network.
- A list of source addresses together with their registration information. These are selected on the basis of posing a high risk to the security of the network.

TECHNOLOGIES

The following are tools used to analyze the network traffic data:

- **Snort** – Snort is an open-source intrusion detection system (IDS) tool which follows a set of commercial or community made rules to prevent a machine from being compromised. Snort is the most important tools used in this project, since it processes pcap files then generate alert data in text form.
- **SnortSnarf** – SnortSnarf is another open-source project aimed at analyzing and recreating alert files in a legible HTML format. It is a third-party perl script that works solely with Snort alert files.
- **Splunk** – Splunk is a web-based, log monitoring and analysis tools used by businesses. Splunk generally creates statistics of data and provides useful information for system analysts and administrators. Splunk supports various files including Linux secure logs and Snort logs
- **Microsoft Excel** – Excel is a spreadsheet program which can calculate and create graphical charts.
- **Wireshark** – Wireshark is a network traffic capturing tool, which provides extensive detail for each packet that is being sent.

METHODOLOGY

It is important to note that this project simulates a real-life network setting. As such, analysts are unable to determine what they are looking for, nor should they know without first analyzing the log files.

The following below is the procedure taken for inspecting each network:

1. **Process log files**.
2. **Process pcap files.**
3. **Note any suspicious activities for the process log files and pcap files.**
4. **Apply network theories to draw a working hypothesis.**
5. **Validate working hypothesis with supporting evidence from noted observations.**

I processed the secure and alert file, since it contains relevant information related to authorized and unauthorized remote access.

Pcaps were processed by replaying them in Snort, then outputs them in a Snort alert file. The log files generated by Snort was again processed to produce a csv spreadsheet format for processing in Excel Alert files were processed again in SnortSnarf to produce a readable HTML format report. Splunk was used to generate reports for Linux secure files which can also output CSV file format.

It should be noted that all alert files were not examined, due to the massive data obtained in this project, with the addition to the time constraint. Two Snort alert log files chosen at random was examined to demonstrate the basic techniques of intrusion detection.

NETWORK 1

Network 1's infrastructure consists of a firewall and a workstation. The workstation is protected behind the firewall machine, which is evident through the pcap captures and secure log files.

After examining Network 1's alert files, there are evidence showing that the firewall machine has been compromised and the attacker attempted to access port 0 from the workstation as well as the firewall machine. The attacker has managed to log into the firewall machine via ssh, where the firewall allowed the connection to carry over onto the workstation machine.

NETWORK 1 – OBSERVATIONS

The following is a breakdown of the alerts generated with Snort on the firewall machine:

Alert Message	**No. of Occurrence**	**Percentage**
BAD-TRAFFIC tcp port 0 traffic	531416	98.14%
ICMP Destination Unreachable Port Unreachable	5211	0.96%
ICMP PING	1182	0.22%
ICMP PING *NIX	992	0.18%
ICMP PING BSDtype	992	0.18%
ICMP Destination Unreachable Communication with Destination Host is Administratively Prohibited	530	0.10%
ICMP Destination Unreachable Host Unreachable	222	0.04%
ICMP Time-To-Live Exceeded in Transit	165	0.03%

ICMP PING BayRS Router	80	0.01%
ICMP PING Flowpoint2200 or Network Management Software	80	0.01%
SNMP request udp	64	0.01%
ICMP PING NMAP	62	0.01%
SNMP public access udp	60	0.01%
ICMP Echo Reply	52	0.01%
ICMP Destination Unreachable Communication Administratively Prohibited	51	0.01%
MS-SQL version overflow attempt	45	0.01%
MS-SQL Worm propagation attempt	45	0.01%
MS-SQL Worm propagation attempt OUTBOUND	45	0.01%
SHELLCODE x86 NOOP	32	0.01%
SCAN UPnP service discover attempt	29	0.01%
ICMP Destination Unreachable Network Unreachable	19	0.00%
MISC Source Port 20 to <1024	14	0.00%
MISC source port 53 to <1024	14	0.00%
SHELLCODE x86 inc ebx NOOP	10	0.00%
ICMP redirect host	8	0.00%
ICMP PING speedera	6	0.00%
ICMP PING Windows	6	0.00%
ICMP traceroute	6	0.00%
MS-SQL ping attempt	6	0.00%
EXPLOIT ntpdx overflow attempt	5	0.00%

ICMP PING undefined code	4	0.00%
ICMP Source Quench	4	0.00%
SNMP private access udp	4	0.00%
ICMP Timestamp Request	3	0.00%
BAD-TRAFFIC 0 ttl	2	0.00%
BAD-TRAFFIC same SRC/DST	2	0.00%
ICMP Destination Unreachable Protocol Unreachable	2	0.00%
RPC portmap listing UDP 111	2	0.00%
SNMP AgentX/tcp request	2	0.00%
SNMP request tcp	2	0.00%
Grand Total	**541476**	

Network 1 – Firewall Overview	
Number of distinct source IP's	5622
Number of distinct destination IP's	1 (■■■.■■■.■■■.■■■)
Number of distinct alerts generated	40

The following is a breakdown of the alerts generated with Snort on the workstation machine:

Alert Message	**No. of Occurrence**	**Percentage**
BAD-TRAFFIC tcp port 0 traffic	684554	99.99%

MISC Source Port 20 to <1024	10	0.00%
MISC source port 53 to <1024	10	0.00%
SNMP AgentX/tcp request	10	0.00%
SNMP request tcp	10	0.00%
SNMP trap tcp	10	0.00%
ICMP Destination Unreachable Communication with Destination Host is Administratively Prohibited	3	0.00%
ICMP Destination Unreachable Port Unreachable	1	0.00%
Grand Total	**684608**	

Network 1 – Workstation Overview	
Number of distinct source IP's	5
Number of distinct destination IP's	2 (10.10.10.1 & 10.10.10.253)
Number of distinct alerts generated	8

NETWORK 1 – ANALYSIS

Majority of the alerts generated by this Snort log indicates that the IP ■■■.■■■.■■■.■■■ attempted to gain access through port 0. Generally TCP traffic do not go through port 0; however, the primary purpose of entering through port 0 is to exploit developer-made error. Firewall implementation may

completely ignore port 0, as it is possible that the firewall implementation may start inspection from port 1 instead of port 0.[1]

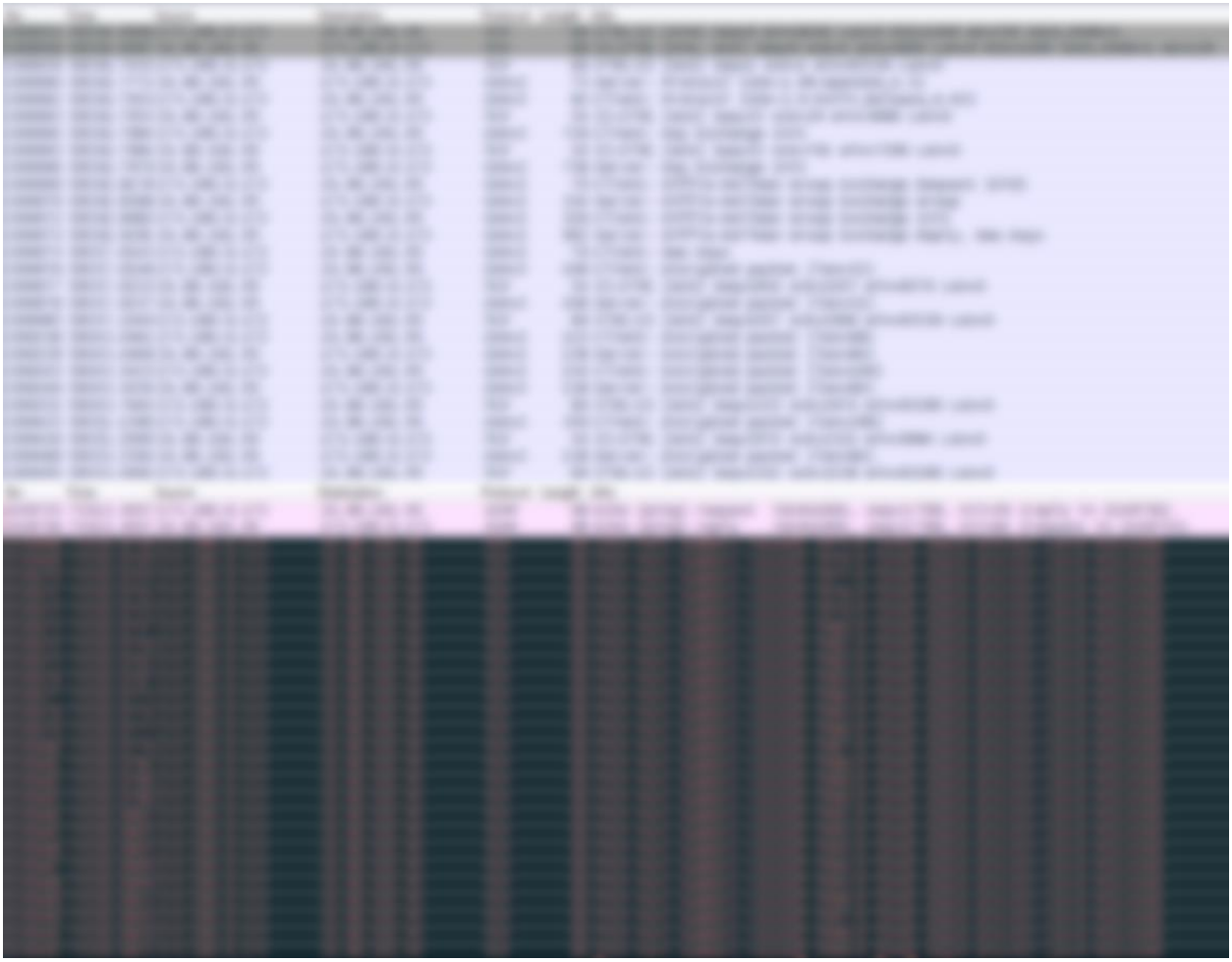
The second most generated alert is the ICMP Destination Unreachable Port Unreachable. This is also significant such that a port scan was initiated. The port scan has been traced back to multiple IP addresses.

NETWORK 1 – INFERENCE

By analyzing the network behavior of the firewall machine through Wireshark and the secure file, we can assume that the source IP ■■■.■■■.■■■.■■■ is a potential attacker. There are multiple instances where the user from IP ■■■.■■■.■■■.■■■ was logging into the network machine via SSH prior to sending Bad TCP Traffic to port 0. It is important to note that it is still an alert generated by Snort and that the user should be contacted. In addition to this, the Bad-traffic to port 0 continues inside the workstation machine.

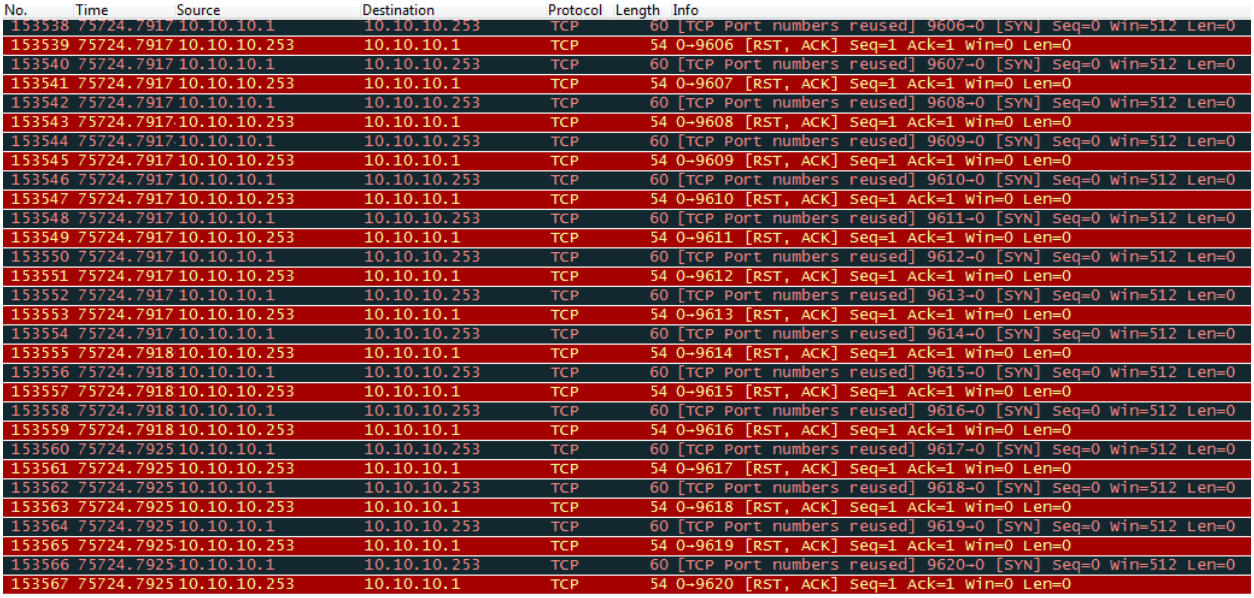
Below is a screenshot of the attacker gaining access to the firewall machine, followed by the port 0 attack:

[1] http://marc.info/?l=Snort-users&m=103584385717802



Below is the screenshot of the attacker accessing the workstation and carrying on the port 0 attack.

Note that the time intervals are close related to each other:



No.	Time	Source	Destination	Protocol	Length	Info
153538	75724.7917	10.10.10.1	10.10.10.253	TCP	60	[TCP Port numbers reused] 9606→0 [SYN] Seq=0 Win=512 Len=0
153539	75724.7917	10.10.10.253	10.10.10.1	TCP	54	0→9606 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
153540	75724.7917	10.10.10.1	10.10.10.253	TCP	60	[TCP Port numbers reused] 9607→0 [SYN] Seq=0 Win=512 Len=0
153541	75724.7917	10.10.10.253	10.10.10.1	TCP	54	0→9607 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
153542	75724.7917	10.10.10.1	10.10.10.253	TCP	60	[TCP Port numbers reused] 9608→0 [SYN] Seq=0 Win=512 Len=0
153543	75724.7917	10.10.10.253	10.10.10.1	TCP	54	0→9608 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
153544	75724.7917	10.10.10.1	10.10.10.253	TCP	60	[TCP Port numbers reused] 9609→0 [SYN] Seq=0 Win=512 Len=0
153545	75724.7917	10.10.10.253	10.10.10.1	TCP	54	0→9609 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
153546	75724.7917	10.10.10.1	10.10.10.253	TCP	60	[TCP Port numbers reused] 9610→0 [SYN] Seq=0 Win=512 Len=0
153547	75724.7917	10.10.10.253	10.10.10.1	TCP	54	0→9610 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
153548	75724.7917	10.10.10.1	10.10.10.253	TCP	60	[TCP Port numbers reused] 9611→0 [SYN] Seq=0 Win=512 Len=0
153549	75724.7917	10.10.10.253	10.10.10.1	TCP	54	0→9611 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
153550	75724.7917	10.10.10.1	10.10.10.253	TCP	60	[TCP Port numbers reused] 9612→0 [SYN] Seq=0 Win=512 Len=0
153551	75724.7917	10.10.10.253	10.10.10.1	TCP	54	0→9612 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
153552	75724.7917	10.10.10.1	10.10.10.253	TCP	60	[TCP Port numbers reused] 9613→0 [SYN] Seq=0 Win=512 Len=0
153553	75724.7917	10.10.10.253	10.10.10.1	TCP	54	0→9613 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
153554	75724.7917	10.10.10.1	10.10.10.253	TCP	60	[TCP Port numbers reused] 9614→0 [SYN] Seq=0 Win=512 Len=0
153555	75724.7918	10.10.10.253	10.10.10.1	TCP	54	0→9614 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
153556	75724.7918	10.10.10.1	10.10.10.253	TCP	60	[TCP Port numbers reused] 9615→0 [SYN] Seq=0 Win=512 Len=0
153557	75724.7918	10.10.10.253	10.10.10.1	TCP	54	0→9615 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
153558	75724.7918	10.10.10.1	10.10.10.253	TCP	60	[TCP Port numbers reused] 9616→0 [SYN] Seq=0 Win=512 Len=0
153559	75724.7918	10.10.10.253	10.10.10.1	TCP	54	0→9616 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
153560	75724.7925	10.10.10.1	10.10.10.253	TCP	60	[TCP Port numbers reused] 9617→0 [SYN] Seq=0 Win=512 Len=0
153561	75724.7925	10.10.10.253	10.10.10.1	TCP	54	0→9617 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
153562	75724.7925	10.10.10.1	10.10.10.253	TCP	60	[TCP Port numbers reused] 9618→0 [SYN] Seq=0 Win=512 Len=0
153563	75724.7925	10.10.10.253	10.10.10.1	TCP	54	0→9618 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
153564	75724.7925	10.10.10.1	10.10.10.253	TCP	60	[TCP Port numbers reused] 9619→0 [SYN] Seq=0 Win=512 Len=0
153565	75724.7925	10.10.10.253	10.10.10.1	TCP	54	0→9619 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
153566	75724.7925	10.10.10.1	10.10.10.253	TCP	60	[TCP Port numbers reused] 9620→0 [SYN] Seq=0 Win=512 Len=0
153567	75724.7925	10.10.10.253	10.10.10.1	TCP	54	0→9620 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

The attacker is compromising a machine that is behind a firewall and is continuing his/her attacks from a remote machine. In essence, a backdoor was implemented to gain access to the network firewall machine and ultimately into the workstation machine.

The lookup for IP ■■■.■■■.■■■.■■■ is provided below:[2]

Country: Canada Region: British Columbia City: Surrey Postal Code: N/A Latitude/Longitude: (removed) ISP: "Telus Communications"

[2] https://ipdb.at/ip/■■■.■■■.■■■.■■■

Organization: "Telus Communications" Host Name: (removed)

NETWORK 1 – CONCLUSION

Knowing that the user connecting from IP ■■■.■■■.■■■.■■■ has established an SSH connection with the network machine, we can assume that the bad traffic to port 0 is a malicious activity. However, as noted above, it is important to notify the user from ■■■.■■■.■■■.■■■ (if possible) immediately.

NETWORK 2

By looking at Network 2's pcap files, we can immediately state that the traffic took place in an internal network environment. Primarily speaking, we find evidence leading to a significant amount of UPnP malformed advertisement alerts. Universal Plug and Play (UPnP) is a protocol that allows machines on the same Wi-Fi network to discover each other. In essence, it is a broadcast to other network to advertise itself.

NETWORK 2 – OBSERVATIONS

The following is a breakdown of the alerts generated with the first alert file:

Alert Message	**No. of Occurrence**	**Percentage**
MISC UPnP malformed advertisement	15132	97.18%
ICMP Destination Unreachable Port Unreachable	291	1.87%
BAD-TRAFFIC same SRC/DST	130	0.83%
ICMP Destination Unreachable Host Unreachable	4	0.03%
MS-SQL version overflow attempt	3	0.02%
MS-SQL Worm propagation attempt	3	0.02%
MS-SQL Worm propagation attempt OUTBOUND	3	0.02%
SCAN UPnP service discover attempt	2	0.01%
ICMP Destination Unreachable Communication with Destination Host is Administratively Prohibited	1	0.01%

SHELLCODE x86 inc ebx NOOP	1	0.01%
SHELLCODE x86 NOOP	1	0.01%
Grand Total	**15571**	

Network 2 – Alert File 1 Overview	
Number of distinct source IP's	9
Number of distinct destination IP's	185
Number of distinct alerts generated	12

The following is a breakdown of the alerts generated with the second alert file:

Alert Message	**No. of Occurrence**	**Percentage**
MISC UPnP malformed advertisement	36146	88.79%
SCAN UPnP service discover attempt	4366	10.73%
BAD-TRAFFIC same SRC/DST	176	0.43%
ICMP Destination Unreachable Communication with Destination Host is Administratively Prohibited	19	0.05%
BAD-TRAFFIC Unassigned/Reserved IP protocol	1	0.00%
Grand Total	**40708**	

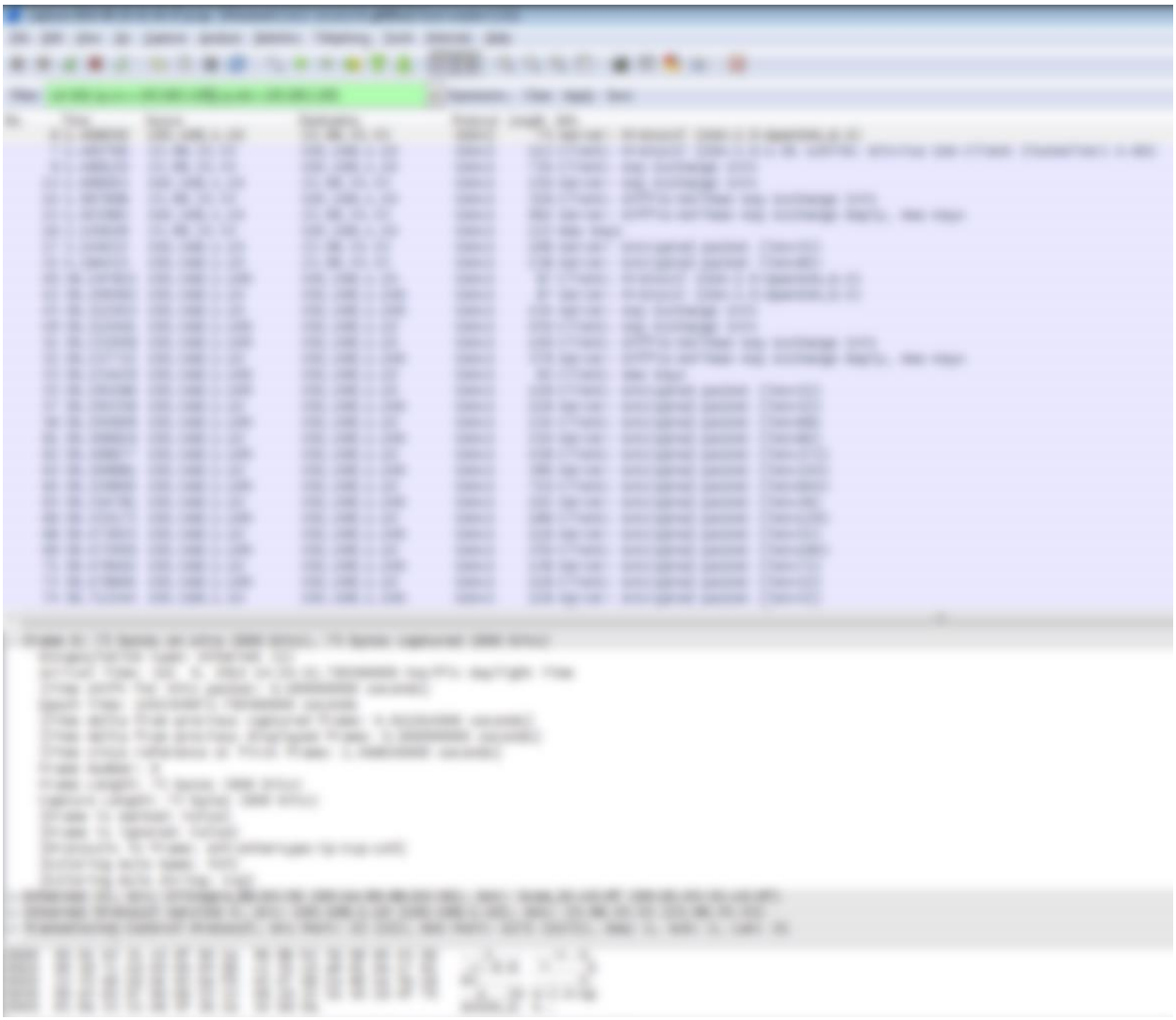
Network 2 – Alert File 2 Overview

Number of distinct source IP's	16
Number of distinct destination IP's	8
Number of distinct alerts generated	5

NETWORK 2 – ANALYSIS

The alert files show that the attacker is attempting a network scan of the internal network; the alert message "SCAN UPnP service discover attempt" implies just that. Further investigations show that the user remotely connected via ssh to perform this network scan. This can be found in the pcap file (see screenshot below).

However, after tracing the packet once again, the attacker ssh'd one more time into 192.168.1.100.



NETWORK 2 – INFERENCE

The purpose of this attack is to scan for hosts and potentially exploit any vulnerabilities in the network. However, there is not enough evidence to show that anything has been compromised. The UPnP scan came up as a false positive, and it appears that no harm has been done.

NETWORK 2 – CONCLUSION

There has been an exploit unveiled at the 2011 Defcon hacker's convention, which allows outside machines to enter an internal machine and exploit the machines inside the network.[3] Although it appears that no harm has been done, a quick fix to prevent UPnP from signaling a broadcast is to block the port. According to the alert file, UDP port 1900 is generating UPnP traffic; hence, users inside the network should block port 1900 to avoid getting compromised.

[3] https://www.defcon.org/images/defcon-19/dc-19-presentations/Garcia/DEFCON-19-Garcia-UPnP-Mapping.pdf

NETWORK 3

It is estimated that Network 3 has over 51,000,000 alerts logged. Due to the size of data in this network, only a fraction of the traffic could be analyzed. But although, network 3 contains a massive amount of data, majority of the alert files examined show an important pattern (and an interesting one nonetheless).

Network 3 contained two large pcap files (one being 1GB and the other being 23GB in size) and 20 smaller pcap files. I combined the entire 20 pcap files into one and processed them as a group. I completely negated the 23GB pcap, due to processing time constraint and processed the 1GB pcap file instead.

NETWORK 3 – OBSERVATIONS

The following is a breakdown of the alerts generated with the processed smaller pcap:

Alert Message	**No. of Occurrence**	**Percentage**
ICMP Destination Unreachable Port Unreachable	1752	73.15%
BAD-TRAFFIC same SRC/DST	284	11.86%
SNMP request udp	100	4.18%
SNMP public access udp	96	4.01%
ICMP PING	42	1.75%
ICMP PING *NIX	42	1.75%
ICMP PING BSDtype	42	1.75%
ICMP Echo Reply	14	0.58%

SCAN UPnP service discover attempt	6	0.25%
SNMP private access udp	4	0.17%
MS-SQL version overflow attempt	3	0.13%
MS-SQL Worm propagation attempt	3	0.13%
MS-SQL Worm propagation attempt OUTBOUND	3	0.13%
SHELLCODE x86 inc ebx NOOP	2	0.08%
SHELLCODE x86 NOOP	2	0.08%
Grand Total	**2395**	

Network 3 – Smaller pcap's Overview	
Number of distinct source IP's	23
Number of distinct destination IP's	13
Number of distinct alerts generated	15

The following is a breakdown of the alerts generated with the processed smaller pcap:

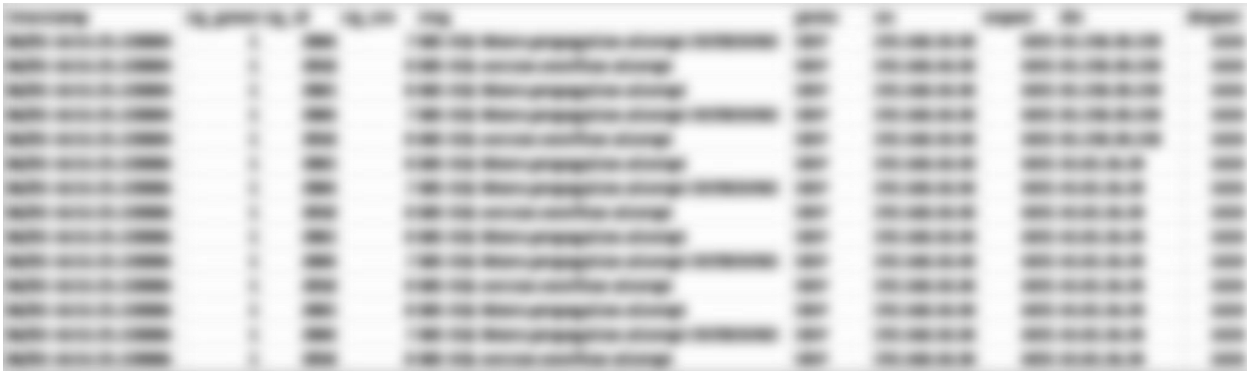
Alert Message	**No. of Occurrence**	**Percentage**
MS-SQL Worm propagation attempt OUTBOUND	241869	33.33%
MS-SQL version overflow attempt	241868	33.33%
MS-SQL Worm propagation attempt	241868	33.33%
Grand Total	**725605**	

Network 3 – Smaller pcap's Overview	
Number of distinct source IP's	1 (192.168.10.30)
Number of distinct destination IP's	80624
Number of distinct alerts generated	3

NETWORK 3 – ANALYSIS

Network 3 has been compromised and is sending out MS-SQL Worms out to external IP's, the timestamps shown in the alert file reports that the worms are being sent rapidly by the milliseconds.

Below is a screenshot of the host IP spamming worms to external IP's:



After examining 4 other alert files (out of 71 other ones), they all follow a pattern of sending out malicious traffic, specifically MS-SQL Worm propagation attempt OUTBOUND, MS-SQL version overflow attempt and MS-SQL Worm propagation attempt. Below are the additional 3 alert files that were processed.

Alert Message	No. of Occurrence	Percentage
MS-SQL version overflow attempt	241872	33.33338%
MS-SQL Worm propagation attempt	241872	33.33338%
MS-SQL Worm propagation attempt OUTBOUND	241871	33.33324%
Src IP	**No. of Occurrence**	**Percentage**
192.168.10.30	725615	100.00%

Alert Message	No. of Occurrence	Percentag
MS-SQL version overflow attempt	241868	33.33%
MS-SQL Worm propagation attempt	241867	33.33%
MS-SQL Worm propagation attempt OUTBOUND	241867	33.33%
Src IP	**No. of Occurrence**	**Percentag**
192.168.10.30	725602	100.00%

NETWORK 3 – INFERENCE

It is clear as to why the pcap files for network 3 are significantly larger than the other two networks. The machine has been compromised and is sending out worm at a rapid rate from a single host. Although I did not examine the 23GB pcap file, it is safe to assume that the traffic will be similar in nature.

NETWORK 3 – CONCLUSION

Network 3 has been marked malicious, and is sending malicious MS-SQL worm traffic to other external IP's; it is unknown as to whether or not it is the attacker's intent. The host computer should be fully formatted and cleaned immediately, prior to booting it up again.

CONCLUSION

All three networks examined have been compromised in one form or another. It is important to note that all three networks have been subject to brute force ssh login attempts from external sources outside the network.

CALL TO ACTION

- All networks should implement a netfilter script that blocks any IP's that failed to log into ssh. This is due to the fact that the secure file shows outside traffic attempting to login as root or other users with priviliges.
- Network 1 is a subject of a backdoor-like intrusion where the attacker is scanning and sending bad traffic to port 0 across multiple internal IP's. The user of the IP specified should be contacted immediately and ensure that malicious activities from that machine come to a halt.
- Network 2 was found to be a false positive by sending UPnP scan across internal networks. The machines inside the internal network has the option of blocking these UPnP broadcast, or the host can ultimately avert all UPnP broadcasts.
- Network 3 was found to be compromised and dangerous. Network traffic indicated that it was the source of MS-SQL worm spamming and the machine should be shut off and cleaned immediately.

This project only covers a marginal amount of exploits caught out of the full dataset. Due to time constraints and processing time of large data, more exploits can be extracted, should one wish continue with analyzing the entire log files. Refer to Appendix A for codes that allows full extraction of data and log processing.

APPENDIX A – SCRIPTS

PCAPLOGGER.SH

```
# pcaplogger.sh
# By: Jeffrey Sasaki
#
# Finds pcap files and perform a snort scan that logs to /var/log/snort
# The tcpdump.logs are then reprocessed and convereted to csv format.
# pcaps can be found in the network folders

NETWORK=n3
LOGPATH=/run/media/root/Passport/$NETWORK-importantfiles/big-pcaps
WORKPATH=/run/media/root/Passport/workfile-$NETWORK-b/final-log/big

pcap_alert()
{
      find $LOGPATH -name 'june3-2.pcap' | while read line
            do
                  snort -A full -r "$line" -c /etc/snort/snort.conf -l
$WORKPATH
                        done
}

# find tcpdump log files in /var/log/snort and perform alert logging
tcpdump_snort()
{
      find $WORKPATH -name 'tcpdump.log.*' | while read line
            do
                  snort -r $line -c /etc/snort/snort.conf -l $WORKPATH
                        done
}
```

```
# move alert.csv and alert.log file from /var/log/snort to the workpath
move_csv()
{
      mv /var/log/snort/alert.* $WORKPATH/final-log
}

# sequence of script
pcap_alert
tcpdump_snort
move_csv
```

SECURELOGGER.SH

```
# securelogger.sh
# By: Jeffrey Sasaki
#
# Finds /var/log/secure logs and concatenate all notable secure files into
# one file

NETWORK=n1
FILENAME=testsecure
LOGPATH=/run/media/root/Passport/$NETWORK-importantfiles/log
WORKPATH=/run/media/root/Passport/workfile-$NETWORK

# find tcpdump log files in /var/log/snort and perform alert logging

concat_secure()
{
      cat $LOGPATH/secure* >> $WORKPATH/final-log/$FILENAME
}
```

```
# sequence of script
concat_secure
```

SNORTSNARFER.SH

```
# snortsnarfer.sh
# By: Jeffrey Sasaki
#
# Performs SnortSnarf on multiple alert files

NETWORK=n3
SNARFBINPATH=/root/Downloads/SnortSnarf-1.0
LOGPATH=/run/media/root/Passport/$NETWORK-importantfiles/pcap
WORKPATH=/run/media/root/Passport/workfile-$NETWORK/final-log


# find tcpdump log files in /var/log/snort and perform alert logging
snortsnarfer()
{
      find $WORKPATH -name 'alert.full*' | while read line
            do
                  cd $SNARFBINPATH
                        ./snortsnarf.pl $line -d $WORKPATH/snortsnarf
                        done
}

# sequence of script
snortsnarfer
```

APPENDIX B – LIST OF TABLES AND GRAPHS

NETWORK 1

EXPLOITS SORTED BY NUMBER OF OCCURRENCE – FIREWALL MACHINE

Alert Message	No. of Occurrence	Percentage
BAD-TRAFFIC tcp port 0 traffic	531416	98.14212%
ICMP Destination Unreachable Port Unreachable	5211	0.96237%
ICMP PING	1182	0.21829%
ICMP PING *NIX	992	0.18320%
ICMP PING BSDtype	992	0.18320%
ICMP Destination Unreachable Communication with Destination Host is Administratively Prohibited	530	0.09788%
ICMP Destination Unreachable Host Unreachable	222	0.04100%
ICMP Time-To-Live Exceeded in Transit	165	0.03047%
ICMP PING BayRS Router	80	0.01477%
ICMP PING Flowpoint2200 or Network Management Software	80	0.01477%
SNMP request udp	64	0.01182%
ICMP PING NMAP	62	0.01145%
SNMP public access udp	60	0.01108%
ICMP Echo Reply	52	0.00960%
ICMP Destination Unreachable Communication Administratively Prohibited	51	0.00942%
MS-SQL version overflow attempt	45	0.00831%
MS-SQL Worm propagation attempt	45	0.00831%
MS-SQL Worm propagation attempt OUTBOUND	45	0.00831%
SHELLCODE x86 NOOP	32	0.00591%
SCAN UPnP service discover attempt	29	0.00536%
ICMP Destination Unreachable Network Unreachable	19	0.00351%
MISC Source Port 20 to <1024	14	0.00259%
MISC source port 53 to <1024	14	0.00259%
SHELLCODE x86 inc ebx NOOP	10	0.00185%
ICMP redirect host	8	0.00148%
ICMP PING speedera	6	0.00111%
ICMP PING Windows	6	0.00111%
ICMP traceroute	6	0.00111%
MS-SQL ping attempt	6	0.00111%
EXPLOIT ntpdx overflow attempt	5	0.00092%
ICMP PING undefined code	4	0.00074%
ICMP Source Quench	4	0.00074%
SNMP private access udp	4	0.00074%
ICMP Timestamp Request	3	0.00055%
BAD-TRAFFIC 0 ttl	2	0.00037%
BAD-TRAFFIC same SRC/DST	2	0.00037%
ICMP Destination Unreachable Protocol Unreachable	2	0.00037%
RPC portmap listing UDP 111	2	0.00037%
SNMP AgentX/tcp request	2	0.00037%
SNMP request tcp	2	0.00037%
Grand Total	**541476**	

TOP SOURCES – FIREWALL MACHINE

Rank	Total # Alerts	**Source IP**	# Signatures triggered	Destinations involved
rank #1	443972 alerts	■■■.■■■.■■■.■■■	7 signatures	■■■.■■■.■■■.■■■
rank #2	328 alerts	■■■.■■■.■■■.■■■	5 signatures	(145 destination IPs)
rank #3	21 alerts	■■■.■■■.■■■.■■■	8 signatures	■■■.■■■.■■■.■■■
rank #4	9 alerts	■■■.■■■.■■■.■■■	1 signatures	■■■.■■■.■■■.■■■
rank #5	5 alerts	■■■.■■■.■■■.■■■	1 signatures	■■■.■■■.■■■.■■■
		■■■.■■■.■■■.■■■	1 signatures	■■■.■■■.■■■.■■■
rank #7	4 alerts	■■■.■■■.■■■.■■■	1 signatures	■■■.■■■.■■■.■■■
rank #8	3 alerts	■■■.■■■.■■■.■■■	3 signatures	■■■.■■■.■■■.■■■
		■■■.■■■.■■■.■■■	3 signatures	■■■.■■■.■■■.■■■
rank #10	2 alerts	■■■.■■■.■■■.■■■	2 signatures	■■■.■■■.■■■.■■■
		■■■.■■■.■■■.■■■	2 signatures	■■■.■■■.■■■.■■■
		■■■.■■■.■■■.■■■	2 signatures	■■■.■■■.■■■.■■■

		■■■.■■■.■■■.■■■	2 signatures	■■■.■■■.■■■.■■■
		■■■.■■■.■■■.■■■	1 signatures	■■■.■■■.■■■.■■■
		■■■.■■■.■■■.■■■	1 signatures	■■■.■■■.■■■.■■■
		■■■.■■■.■■■.■■■	1 signatures	■■■.■■■.■■■.■■■
		■■■.■■■.■■■.■■■	1 signatures	■■■.■■■.■■■.■■■
rank #18	1 alerts	■■■.■■■.■■■.■■■	1 signatures	■■■.■■■.■■■.■■■
		■■■.■■■.■■■.■■■	1 signatures	■■■.■■■.■■■.■■■
		■■■.■■■.■■■.■■■	1 signatures	■■■.■■■.■■■.■■■
		■■■.■■■.■■■.■■■	1 signatures	■■■.■■■.■■■.■■■
		■■■.■■■.■■■.■■■	1 signatures	■■■.■■■.■■■.■■■

TOP DESTINATIONS – FIREWALL MACHINE

Rank	Total # Alerts	**Destination IP**	# Signatures triggered	Originating sources
rank #1	444699 alerts	■■■.■■■.■■■.■■■	32 signatures	(677 source IPs)
rank #2	74 alerts	■■■.■■■.■■■.■■■	3 signatures	■■■.■■■.■■■.■■■
rank #3	33 alerts	■■■.■■■.■■■.■■■	1 signatures	■■■.■■■.■■■.■■■

rank #4	18 alerts	■■■.■■■.■■■.■■■	1 signatures	■■■.■■■.■■■.■■■
rank #5	13 alerts	■■■.■■■.■■■.■■■	1 signatures	■■■.■■■.■■■.■■■
		■■■.■■■.■■■.■■■	1 signatures	■■■.■■■.■■■.■■■
rank #7	8 alerts	■■■.■■■.■■■.■■■	1 signatures	■■■.■■■.■■■.■■■
rank #8	5 alerts	■■■.■■■.■■■.■■■	1 signatures	■■■.■■■.■■■.■■■
		■■■.■■■.■■■.■■■	1 signatures	■■■.■■■.■■■.■■■
		■■■.■■■.■■■.■■■	1 signatures	■■■.■■■.■■■.■■■
		■■■.■■■.■■■.■■■	1 signatures	■■■.■■■.■■■.■■■
		■■■.■■■.■■■.■■■	1 signatures	■■■.■■■.■■■.■■■
		■■■.■■■.■■■.■■■	1 signatures	■■■.■■■.■■■.■■■
rank #14	3 alerts	■■■.■■■.■■■.■■■	2 signatures	■■■.■■■.■■■.■■■
rank #15	2 alerts	■■■.■■■.■■■.■■■	1 signatures	■■■.■■■.■■■.■■■
		■■■.■■■.■■■.■■■	1 signatures	■■■.■■■.■■■.■■■

		■■■.■■■.■■■.■■■	1 signatures	■■■.■■■.■■■.■■■
		■■■.■■■.■■■.■■■	1 signatures	■■■.■■■.■■■.■■■
rank #19	1 alerts	■■■.■■■.■■■.■■■	1 signatures	■■■.■■■.■■■.■■■
		■■■.■■■.■■■.■■■	1 signatures	■■■.■■■.■■■.■■■

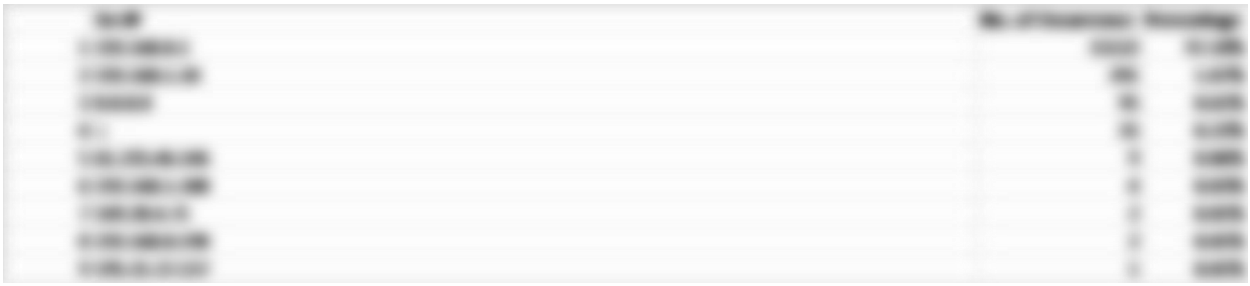
NETWORK 2

EXPLOITS SORTED BY NUMBER OF OCCURRENCE

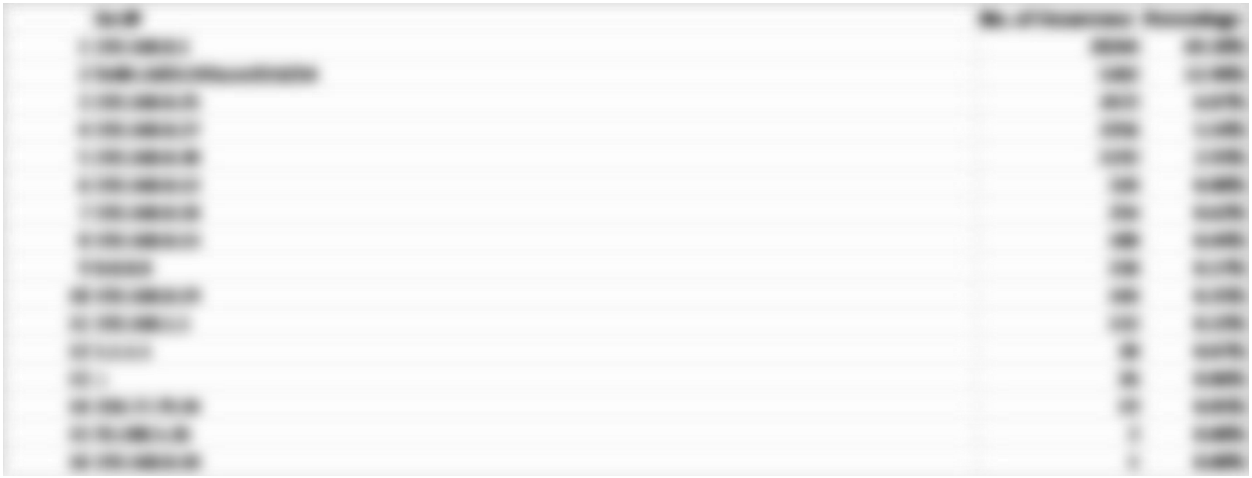
Alert Message	No. of Occurrence	Percentage
MISC UPnP malformed advertisement	15132	97.18%
ICMP Destination Unreachable Port Unreachable	291	1.87%
BAD-TRAFFIC same SRC/DST	130	0.83%
ICMP Destination Unreachable Host Unreachable	4	0.03%
MS-SQL version overflow attempt	3	0.02%
MS-SQL Worm propagation attempt	3	0.02%
MS-SQL Worm propagation attempt OUTBOUND	3	0.02%
SCAN UPnP service discover attempt	2	0.01%
ICMP Destination Unreachable Communication with Destination Host is Administratively Prohibited	1	0.01%
SHELLCODE x86 inc ebx NOOP	1	0.01%
SHELLCODE x86 NOOP	1	0.01%
Grand Total	**15571**	

TOP SOURCES

First Alert File

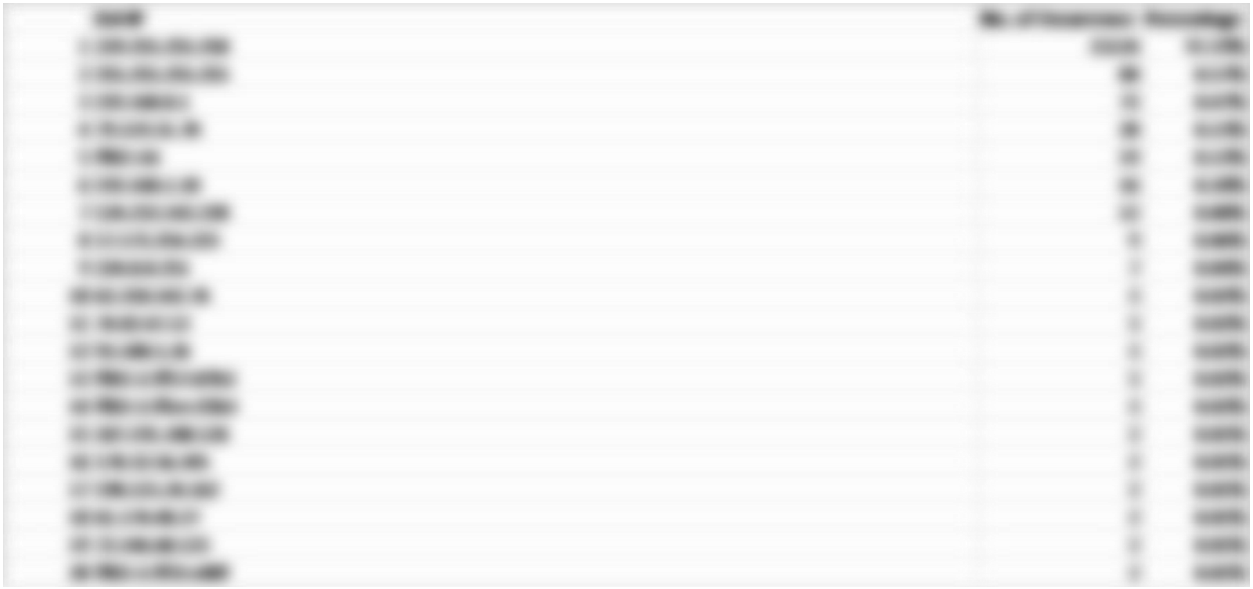


Second Alert File

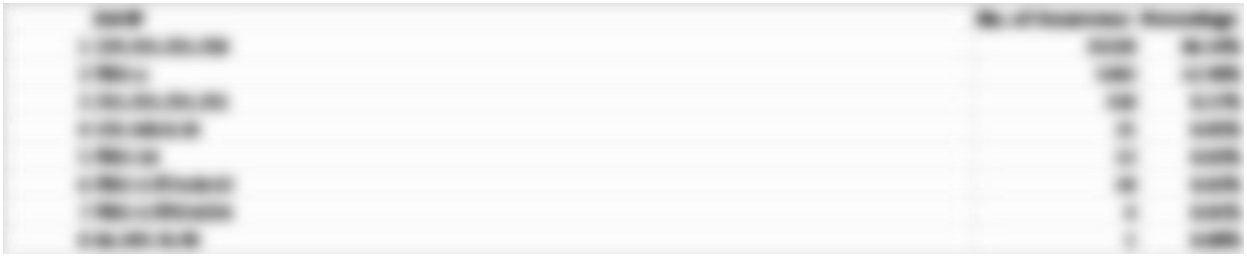


TOP DESTINATIONS

First Alert File



Second Alert File



NETWORK 3

EXPLOITS SORTED BY NUMBER OF OCCURRENCE

Smaller pcap's

Alert Message	No. of Occurrence	Percentag
ICMP Destination Unreachable Port Unreachable	1752	73.15%
BAD-TRAFFIC same SRC/DST	284	11.86%
SNMP request udp	100	4.18%
SNMP public access udp	96	4.01%
ICMP PING	42	1.75%
ICMP PING *NIX	42	1.75%
ICMP PING BSDtype	42	1.75%
ICMP Echo Reply	14	0.58%
SCAN UPnP service discover attempt	6	0.25%
SNMP private access udp	4	0.17%
MS-SQL version overflow attempt	3	0.13%
MS-SQL Worm propagation attempt	3	0.13%
MS-SQL Worm propagation attempt OUTBOUND	3	0.13%
SHELLCODE x86 inc ebx NOOP	2	0.08%
SHELLCODE x86 NOOP	2	0.08%
Grand Total	**2395**	

Big pcap

Alert Message	No. of Occ	Percentag
MS-SQL Worm propagation attempt OUTBOUND	241869	33.33%
MS-SQL version overflow attempt	241868	33.33%
MS-SQL Worm propagation attempt	241868	33.33%
Grand Total	**725605**	

TOP SOURCES

Smaller pcap's

Big pcap

	Src IP	No. of Occurrence	Percentage
1	192.168.10.30	725602	100.00%

TOP DESTINATIONS

Smaller pcap's

Big pcap

Sample Screenshot of a Processed Secure log File Using Splunk