Security Assessment of the University

Brian Hayes

GCIA Practical Assignment
Version 4.1 (revised September 22nd 2004)
Submitted
13 December 2004

Abstract

The University has requested an assessment of their current security posture, consisting of at least three days worth of data, including scan, alert and out-of-spec file types. The report is three sections, beginning with an executive summary that provides an overview of the findings, a list of compromised systems, and several recommendations to prevent future attacks. The second part is a detailed analysis that explains what is taking place on the Universities network. The report will then conclude with an explanation of the process used to perform the analysis.

Table of Contents

List of Figures

Part I - Executive Summary

The security posture of the University has been evaluated over a three day period and has been deemed an overall score of average. Although there is no perimeter access control and port scanning takes place constantly, only a few compromised hosts were confirmed.

A large number of attacks occurred hourly on the University network. Nearly one-fourth of all security alerts over a three day period were considered high severity (Figure 1). These high severity alerts were active attacks that can depreciate both the University network infrastructure as well as its reputation as a leader in next generation technology.

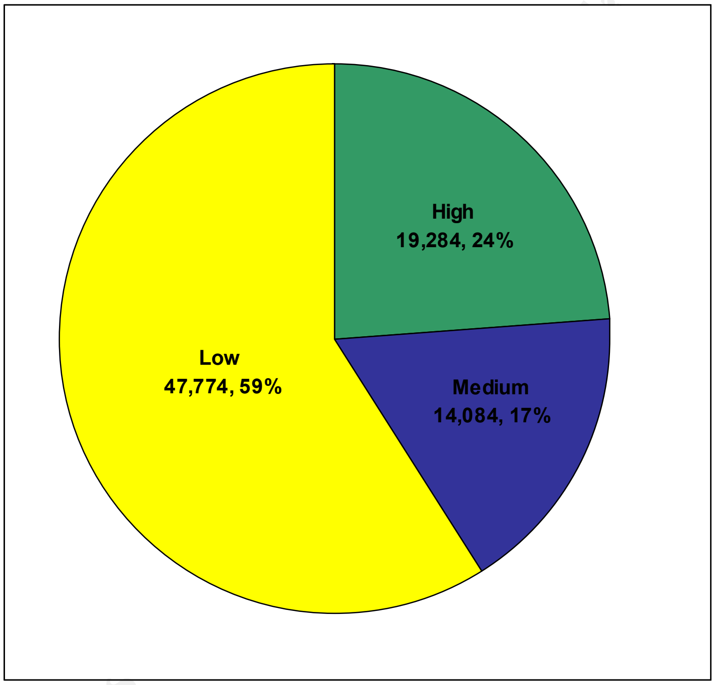

Figure 1. Total number of alerts by severity spanning three days.

Based on current IDS alerts associated with the host, several systems are suspected to be compromised (Table 1).

Table 1. Compromised hosts and their associated vulnerability.

IP Address	Vulnerability
MY.NET.5.20 MY.NET.5.45 MY.NET.83.98 MY.NET.189.62 MY.NET.190.97 MY.NET.190.102	Buffer Overflow
1,511 Hosts	Red worm

MY.NET.12.2	Fragmentation Attack, Incomplete Packets, Buffer Overflow
MY.NET.24.47	Fragments Discarded, FTP passwd attempt, Buffer Overflow, DDOS
MY.NET.12.6	MiMail
MY.NET.97.206	NIMDA
MY.NET.69.198	TFTP, Buffer Overflow, Incomplete Packet

A single alert, the Red worm is responsible for compromising 1,511 university hosts. This worm has currently infiltrated over 10% of the campus systems and spans the entire network (Figure 2). The University is strongly urged to allocate resources to contain and prevent this kind of security breach.

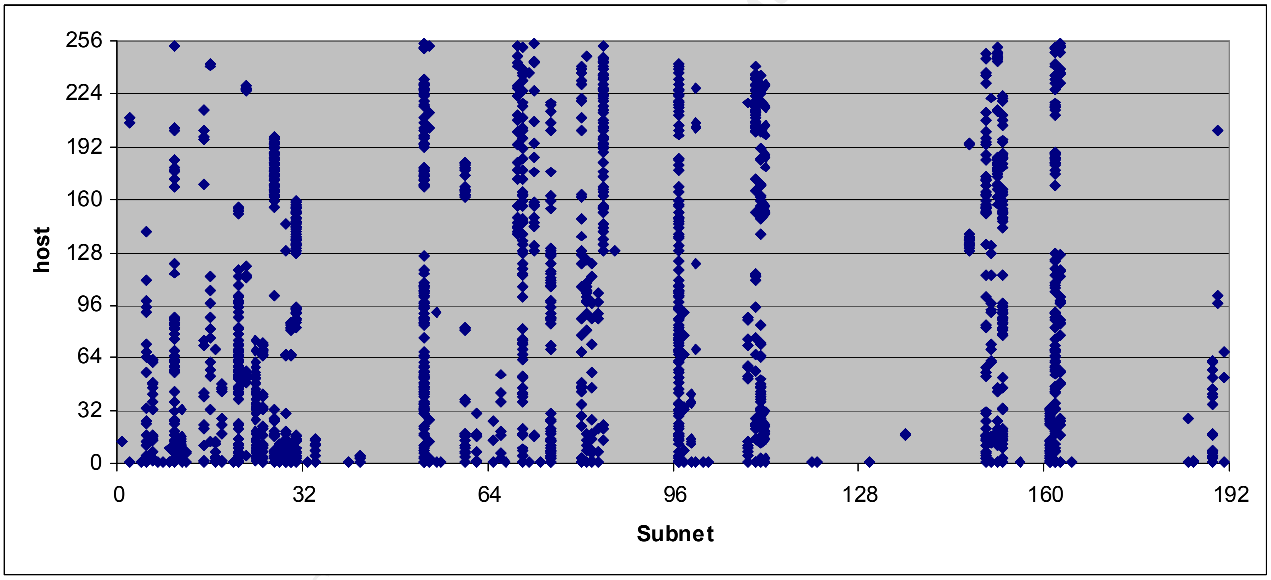

Figure 2. All Red worm infections on MY.NET.x.y.

The Red worm is just one example of many security breaches that currently exist in the University network. In order to prevent similar infections in the future, the following recommendations should be considered:

- Ensure all workstations and servers are up-to-date on security patches and Anti-Virus updates
- Install, configure, and monitor some type of access-control at the gateway
- Develop a CSIRC (Computer Security Incident Response Center) – as the current IDS (Intrusion Detection System) is worthless unless someone is reviewing and responding to the alerts and updating policy

Part II – Detailed Analysis

1 Log files

The University has requested that the following three days from 17 January to 19 January be reviewed for compromised systems and/or network issues. Three types of files were reviewed – scans, alerts, & out-of-spec (OOS) (Table 2). Note that OOS filenames do not correspond to the appropriate days, but the timestamps within the files do.

Table 2 - List of log files reviewed for security audit.

Day	Scans	Alerts	OOS
01/17/04	scans.040117	alert.040117	oos_report_040113
KB	308,392	41,73	1,335
lines	4,707,454	334,283	4,577
01/18/04	scans.040118	alert.040118	oos_report_040114
KB	278,668	38,456	1,060
lines	4,261,402	307,603	3,970
01/19/04	scans.040115	alert.040119	oos_report_040115
KB	329,316	44,902	1,050
lines	5,033,066	364,589	4,299
Total lines	14,001,922	1,006,475	12,846

2 Network topology

Based on Internet Protocol (IP) information contained in the log files and a whois [1] query, the University network has been assigned the class B network address MY.NET.0.0 with a subnet mask of 255.255.0.0 allowing 65,024 hosts. The University has further subnetted their network into 256 Class C networks, but are only using the space ranging from MY.NET.0.0 to MY.NET.192.255, providing 48,640 IP addresses. The log files analyzed have revealed 10,673 potential unique hosts in 89 different subnets (Table 3). While only approximately 1,500 university systems were confirmed to exist, attempted port scans revealed the rest. The assumption is that scanner software, i.e. nmap [2], will not scan a host without first receiving some sort of response from that host.

Table 3. Listing of University subnets with associated active host count.

Subnet (MY.NET.x.0)	# of active hosts	Subnet (MY.NET.x.0)	# of active hosts	Subnet (MY.NET.x.0)	# of active hosts
191	149	99	159	33	23
190	255	98	173	32	116
189	38	97	232	31	150
186	176	86	78	30	83
185	150	84	105	29	113
166	2	83	85	28	22
165	151	82	95	27	198
163	136	81	73	25	49
162	169	80	192	24	150
161	178	75	192	22	25
156	157	73	93	21	187
153	159	72	100	20	171
152	179	71	203	18	173
151	137	70	203	17	135
150	158	69	88	16	39
149	130	67	8	15	134
147	83	66	22	14	165
136	6	65	13	13	150
130	130	64	19	12	147
123	2	62	8	11	47
121	139	60	157	10	192
120	135	56	41	9	18
112	156	55	168	8	1
111	163	54	156	7	143
110	147	53	164	6	172
109	167	43	172	5	154
103	21	42	150	4	150
102	159	41	152	2	147
101	155	40	9	1	150
100	156	34	15	**89**	**10,673**

3 Alert Summary

Over one million alerts were detected over the span of three days, consisting of 26 unique alerts. The majority of those alerts were port scans, producing approximately 92% of the total alerts (Table 4).

Table 4. All alerts detected in three-day period, ordered by total number of occurrences.

	Total #	Alert type
1	925,289	spp_portscan
2	35,546	MY.NET.30.4 activity
3	16,938	High port 65535 udp/tcp
4	8,477	MY.NET.30.3 activity
5	5,238	Incomplete Packet Fragments Discarded
6	3,351	TFTP - Internal TCP connection to external tftp server
7	3,338	SMB Name Wildcard
8	2,432	connect to 515 from outside

9	1,770	EXPLOIT x86 NOOP
10	910	External RPC call
11	685	SUNRPC highport access!
12	605	NMAP TCP ping!
13	536	Null scan!
14	508	[UMBC NIDS IRC Alert] IRC user /kill detected, possible trojan.
15	241	TCP SRC and DST outside network
16	219	Possible trojan server activity
17	68	ICMP SRC and DST outside network
18	63	FTP passwd attempt
19	60	[UMBC NIDS] External MiMail alert
20	56	FTP DoS ftpd globbing
21	55	DDOS shaft client to handler
22	27	Tiny Fragments
23	10	RFB Possible WinVNC - 010708-1
24	4	NETBIOS NT NULL session
25	3	NIMDA - Attempt to execute cmd from campus host
26	2	Fragmentation Overflow Attack

However, Table 3 is misleading. After reviewing the network topology, filtering out the false positives and assigning a priority to each event, the alerts were reordered by severity (Table 5). Priorities were based on prevalence of vulnerability, ease of exploit, ease of mitigation, frequency and severity of alert.

Table 5. Prioritized alerts ordered by severity.

	#	**Alert**
1	16,938	High port 65535 udp/tcp
2	1,770	EXPLOIT x86 NOOP
3	63	FTP passwd attempt
4	3	NIMDA - Attempt to execute cmd from campus host
5	508	[UMBC NIDS IRC Alert] IRC user /kill detected, possible trojan.
6	2	Fragmentation Overflow Attack
7	2,432	connect to 515 from outside
8	925,289	spp_portscan
9	910	External RPC call
10	3,338	SMB Name Wildcard
11	685	SUNRPC highport access!
12	605	NMAP TCP ping!
13	536	Null scan!
14	241	TCP SRC and DST outside network
15	4	NETBIOS NT NULL session
16	68	ICMP SRC and DST outside network
17	5,238	Incomplete Packet Fragments Discarded
18	27	Tiny Fragments
19	55	DDOS shaft client to handler
20	35,546	MY.NET.30.4 activity
21	8,477	MY.NET.30.3 activity
22	3,351	TFTP - Internal TCP connection to external tftp server
23	219	Possible trojan server activity
24	60	[UMBC NIDS] External MiMail alert
25	56	FTP DoS ftpd globbing
26	10	RFB Possible WinVNC - 010708-1

The prioritized alerts reveal what the University must resolve.

- Alerts 1 – 6 are considered high risk alerts. They are active attacks that are active exploits and are being used to break into university systems. These alerts must be addressed immediately.
- Alerts 7 – 18 are medium level risk alerts. These result from an attacker probing the network and/or are network performance issues, but none of these alerts indicate a current compromise. These alerts should be fixed over time.
- Alerts 19 – 26 are low level risk alerts. The majority of the low level alerts are false positives, meaning the IDS misinterpreted the network traffic.

All 26 alerts need to resolved, but there are different approaches depending on the risk level. The section on defensive recommendations discusses several approaches.

4 In-Depth Analysis

4.1 Attack #1 – Red worm

Description of Detect

In April 2001 the Red worm was discovered in the wild. Not to be confused with Code Red [3], the Red worm is now referred to as Adore [4]. It spreads among Linux systems using four different types of vulnerabilities: BIND named [6] [7], wu-ftpd [8], rpc.stad [9] and lpd services [10] [5] [30]. Older worms that spread using similar vulnerabilities include Ramen [11] and Lion [12]. BID's associated with the Adore worm include 1712 [13], 1387 [14], 2302 [15], 1480 [16], & 7116 [29].

Reason for Further Analysis

The Red worm was significant for analysis, given the scope of infection. It was detected 16,938 times over the span of three days, interacting with 10,540 unique hosts (10,473 internal and 67 external). The campus likely has many compromised hosts that need to be addressed immediately.

Generated by

This attack was detected by a Snort network IDS and spanned all three days worth of logs. 191 alerts were detected on day one, 171 on day two, and 16,577 on day three. The alerts were logged in the Snort Fast format, as shown below:

```
01/17-10:47:21.683273  [**] High port 65535 tcp - possible Red Worm - traffic [**]
216.146.69.253:65535 -> MY.NET.97.83:6129
```

The format reveals the timestamp of the alert, general description, source IP and port and destination IP and port. This specific rule is customized to detect the Red worm likely matching on the source or destination port of 65535.

Probability of Spoofed Source Address

The source addresses of alerts associated with the Red worm are not likely spoofed. The Red worm communicates on TCP port 65535 and all the exploits require a TCP connection, thus all Red worm communications require a real source address.

Attack Mechanism

As mentioned above, the Red worm can use several different vectors to attack a system. All of the attacks are a form of stimuli. Then after compromise, each host immediately begins scanning for new hosts that may be vulnerable. The exploits themselves do not harm, but rather modify the system. After the worm has successful broken into a system, it downloads a rootkit and installs a trojaned ps binary. It then proceeds to email the output from the following files/programs to four different addresses: adore9000@21cn.com, adore9000@sina.com, adore9001@21cn.com, adore9001@sina.com:

- /etc/ftpusers
- ifconfig
- ps -aux (using original binary)
- /root/.bash_history
- /etc/hosts
- /etc/shadow

The worm then sets up a root shell on TCP port 65535 and removes all traces of itself and reboots the system.

Not only do the university alert logs show major scans of TCP port 65535, but they also clearly show that after a host is compromised, the worm contacts a web server (TCP port 80) to download the rootkit. The worm then proceeds to email the host information to the attacker (TCP port 25). TCP port 25 and 80 alerts are shown below:

```
01/17-08:08:33.170085  [**] High port 65535 tcp - possible Red Worm - traffic [**]
149.101.1.119:65535 -> MY.NET.5.20:80

01/17-00:31:48.277780  [**] High port 65535 tcp - possible Red Worm - traffic [**]
MY.NET.60.17:65535 -> 213.244.179.108:25
```

Probability of False Positive

One interesting observation made by Doug Kite in his GCIA practical [17] was that activity on port 65535 can also be caused by the file sharing program winmx and the network utility traceroute. Both applications create UDP packets destined for port 65535 and can easily confuse even the most well-intentioned Snort sensor. With that in mind, out of a total of 16,939 alerts on port 65535, UDP is only detected 26 times, leaving TCP with 16,913 alerts. If traceroute or winmx did cause a false positive, it is insignificant compared to the amount TCP alerts.

Correlations

There are other trojans that also use port 65535. Although not as abundant, RC1 [18] can be still found in the wild. RC1 runs under the Windows 95, 98, and NT platforms, but does not display the same characteristics as Adore. The log files are nearly one year old, yet in the last 70 days, the Internet Storm Center [36] is still observing traffic on port 65535 (Figure 3).

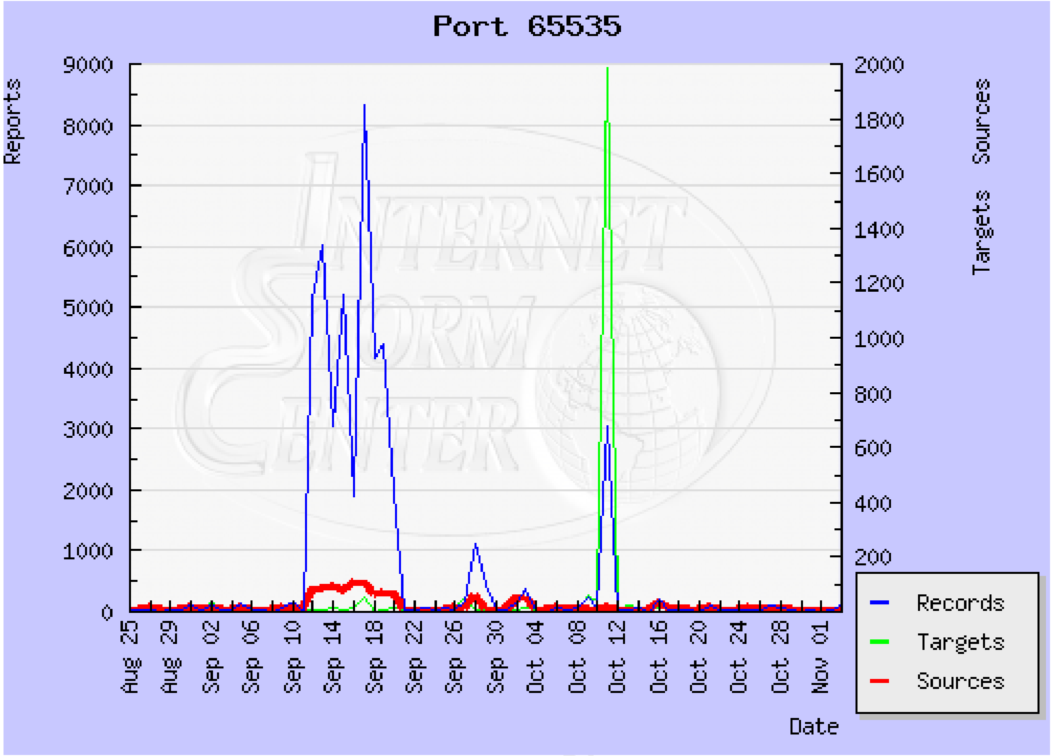

Figure 3. Recent Red worm activity on port 65535.

Evidence of Active Targeting

Due to the large address space the University uses and the lack of filtering at the gateway, these attacks do not appear to be targeted for a specific system. In fact, out of the 10,673 hosts on campus, 98% or 10,540 were scanned.

Severity

The severity of the Red worm was calculated to be 6 out of 10 (Table 6). The high criticality and lethality values are not offset as the countermeasures are both relatively low.

Table 6. Severity of Red worm.

Severity = (Criticality + Lethality) – (System Countermeasures + Network Countermeasures)		
Criticality	The target could be any system – a student's workstation or a production server. It is unknown, so you have to assume a server.	**5**
Lethality	The worm can completely take over the computer with a number of exploits, so the lethality is high.	**5**
System Countermeasures	The systems are not patched.	**2**
Network Countermeasures	Network countermeasures are lacking.	**2**
Total		**6**

Compromised Hosts

There were several attackers using this worm. The log files show 57 external hosts playing a part in the attack (Figure 4). The only host in that table that generated events besides those related to Red worm was 128.171.198.49, who added four SMB Name Wildcard alerts. This host also introduced the worm to the network, and from there, the compromised hosts initiated mail, auth, and web traffic and began spreading the worm themselves.

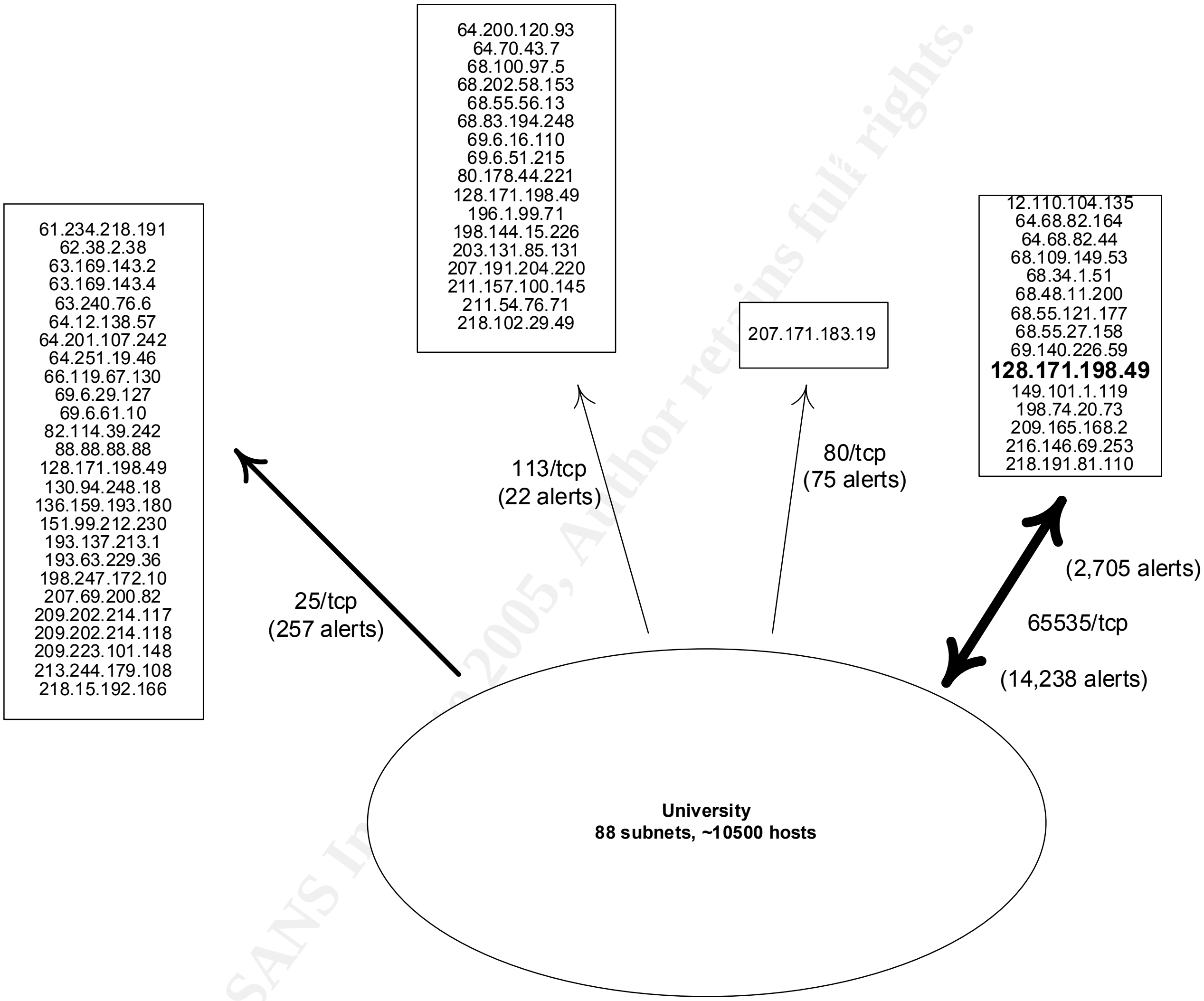

Figure 4. Link graph of Red worm traffic.

4.2 Attack #2 – EXPLOIT x86 NOOP

Description of Detect

The x86 NOOP (no-operation) detect refers to the Intel x86 character, 0x90. When found in the payload it may or may not indicate a malicious packet. It is quite common for the payload to contain the NOOP character during the transmission of binary files, but it can also be used to exploit several different vulnerabilities in remote services [19].

Table 7. EXPLOIT x86 NOOP top offenders.

Total # Unique Targets	Top Source IP's	Total # Unique Attackers	Top Destination IP's	Total # of Alerts	Top Source to Destination IP Flows
18	81.62.153.204	112	MY.NET.190.97	208	24.130.153.222 -> MY.NET.5.45
12	24.130.153.222	108	MY.NET.190.102	206	24.130.153.222 -> MY.NET.189.62
8	216.173.66.162	49	MY.NET.190.95	152	24.130.153.222 -> MY.NET.83.98
6	131.118.254.39	20	MY.NET.69.198	79	193.220.82.38 -> MY.NET.5.20
4	62.111.239.182	14	MY.NET.112.30	45	24.130.153.222 -> MY.NET.75.13
81	**246**	**246**	**81**	**2110**	**420**

The University log file shows there are many more external attackers (246) than internal targets (81) (Table 7). Based on the IP Flow, however, a single external attacker (24.130.153.222) is generating the many of the alerts.

Reason for Further Analysis

This detect was one of the more prevalent and dangerous attacks currently active on the University network. 81 university computers have already been targeted and although it is unknown if any have been compromised, the exploit can potentially give the attacker root access to the operating system.

Generated by

The detect was generated by a custom Snort rule, very similar to SHELLCODE x86 NOOP rule:

```
alert ip $EXTERNAL_NET $SHELLCODE_PORTS -> $HOME_NET any
(msg:"SHELLCODE x86 NOOP"; content:"|90 90 90 90 90 90 90 90 90 90 90 90 90 90|";
depth:128; reference:arachnids,181; classtype:shellcode-detect; sid:648; rev:7;)
```

Signatures used to detect this event are matched by the source port and packet payload.

An example of the alert is shown below:

```
01/17 23:45:01.702832  [**] EXPLOIT x86 NOOP [**] 24.130.153.222:42525 > MY.NET.189.62:80
```

The typical Snort fast alert format provides the timestamp, detect name, source address and port and destination address and port.

Probability of Spoofed Source Address

The success of this attack requires a source address that is not spoofed. Before the exploit can be launched, a TCP session must be established, which is highly unlikely if the source address is spoofed.

Attack Mechanism

The NOOP is a common component of many buffer overflow exploits. By stringing a number of 0x90 characters together, an attacker can interrupt the program flow of the running service and redirect the stack pointer to the attacker's code, located directly following the NOOP characters. If the stack pointer is misplaced, the service will crash.

Successful execution of the exploit, however, will typically generate a remote shell for the attacker running with the privileges of the exploited service, most often root.

The attack is initiated by the attacker, usually after some enumeration has occurred and listening ports have been discovered. A buffer overflow could technically occur on any service. The more common ones are found on web servers. One known vulnerability is MS03-007, a Microsoft Windows ntdll.dll Buffer Overflow that can be exploited through IIS (Internet Information Services) when running WebDAV [20] [28].

Probability of False Positive

This detect has the potential for many false positives. Whenever binary files like executables or jpeg's are transferred, they often contain NOOP's that can trigger this detect. Attention to the source and destination port numbers will help distinguish false positives from legitimate attacks.

The second highest source port is 80 which indicates someone is downloading content from a web page (Table 9). Web pages contain a number of images and other binaries, so this is very likely a false positive. On the other hand, the top destination port is also 80. In this case, the NOOP alert is triggering on traffic destined for a web server. This traffic is normally text and does not contain anything that would cause a false positive. In addition, the Microsoft WebDAV vulnerability is typically located on port 80 and will attract attention. Indeed, destination port 80 is responsible for over 65% of all NOOP alerts.

Table 9. Top three source and destination ports used in alerts.

Total # Alerts	Top Src Port	Common Use	Total # Alerts	Top Dst Port	Common Use	Total # Alerts	Top Src -> Dst Port Flow
45	51667	N/A	1151	80	HTTP	45	51667 -> 80
41	80	HTTP	266	135	MS-RPC	41	51611 -> 80
40	51611	N/A	50	445	MS-DS	40	3034 -> 80
2188	**498**		**1762**	**72**		**2235**	**545**

Correlations

This analysis of NOOP exploits is reinforced by Blaine Hein's GCIA 3.4 practical [21]. More information can also be found at snort.org [22] and whitehats.com [20].

There are 246 attackers (Table 7) and some have triggered other detects similar to NOOP in lethality and the potential for false positives (Table 10). All are triggered based on a specific payload and all result in root access for the attacker, as analyzed by [23].

Table 10. Similar alerts to EXPLOIT x86 NOOP.

Exploit Alert Name	Total # of Alerts	Total # Unique Source IP's	Total # Unique Destination IP's
EXPLOIT NTPDX buffer overflow	6	1	2
EXPLOIT x86 setgid 0	21	18	18
EXPLOIT x86 setuid 0	43	27	18
EXPLOIT x86 stealth noop	10	5	4

Evidence of Active Targeting

The alerts for this detect are clearly the result of active targeting. Known vulnerabilities exist on web servers, and TCP port 80 is the most popular target (Table 9). While other detects appear to be targeting obscure ports, it is unlikely this exploit would hit a host accidentally.

Severity

The severity of EXPLOIT x86 NOOP was calculated to be 4 out of 10 (Table 11). The high criticality and lethality values are partially offset as the countermeasures rate low to medium.

Table 11. Severity for EXPLOIT x86 NOOP.

Severity = (Criticality + Lethality) – (System Countermeasures + Network Countermeasures)		
Criticality	This attack targets well known services typically running on production servers that can not go offline.	**5**
Lethality	This is a moderately difficult root exploit.	**4**
System Countermeasures	Patches are available for known vulnerabilities, but new buffer overflows continue to be discovered. Given a universities typical small IT staff, it is likely the servers are not fully patched.	**3**
Network Countermeasures	A host based IDS could block this attack at the server, or a deep packet inspection firewall at the gateway should be able to detect and prevent this exploit. It does not appear either are in place.	**2**
Total		**4**

Compromised Hosts

With the data available, it is not clear what machines have been compromised. Based on other detects, nine hosts have a high probability of compromise (Table 12).

Table 12. EXPLOIT x86 NOOP compromised hosts.

MY.NET.12.2	MY.NET.190.102	MY.NET.190.97
MY.NET.24.47	MY.NET.5.45	MY.NET.83.98
MY.NET.69.198	MY.NET.189.62	MY.NET.5.20

4.3 Attack #3 – FTP Password Attempt

Description of Detect

The third critical event found in the data logs is an FTP password attempt. Fifty unique external hosts all tried to break into a single host's FTP server. The alerts spanned all three days with roughly the same number of alerts occurring each day (20, 14, 29, respectively) [24].

This alert is triggered when someone attempts to retrieve the password file from a FTP Server. There is a current BID [25] and ISS has additional information [26].

Reason for Further Analysis

This host not only was attacked many times via FTP, but eight other attacks were used by many different external attackers. In addition, several OOS packets were destined for this host. This looks like a potential compromised host. .

Generated by

The alert was generated by Snort, again using a custom ruleset. Although custom, it appears to be very similar to this:

```
ftp.rules:alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"FTP passwd retrieval
attempt"; flow:to_server,established; content:"RETR"; nocase; content:"passwd";
reference:arachnids,213; classtype:suspicious-filename-detect; sid:356; rev:5;)
```

This rule matches traffic from any external IP address destined for the FTP service on an internal host. A TCP session must already be established and the text 'RETR' and 'password' must be in the payload of the packet.

Probability of Spoofed Source Address

Typically with this type of alert, the IP address will not be spoofed because the attacker is requesting information back, specifically the password file. In addition, in order to create the TCP session, a real, responding IP address must be used.

Attack Mechanism

The basic procedure of the attack is to connect to the FTP server, then request the password file. In general, most FTP programs can be configured to deny this request, but if an FTP server is misconfigured or has a known vulnerability, the password file may be accessible. Once the attacker attains the password file, it can be cracked in little time and the host is now compromised.

Probability of False Positive

This host has nine different alerts in just three days from 62 different sources. The scans seem legitimate as are the FTP password attempts. In addition, there are many possible trojan alerts, and the port number resolves to the Ramen worm. This is interesting because many other hosts on the network are likely vulnerable to the Red worm, and both worms use the same vulnerabilities to spread. It is possible a second worm has infiltrated the University network. The rest of the alerts are likely false positives.

Correlation

Three portscans involved MY.NET.24.47 on 01/17:

```
01/17-08:06:47.616590  [**] spp_portscan: End of portscan from MY.NET.24.47: TOTAL
time(36s) hosts(1) TCP(192) UDP(0) [**]
01/17-08:08:29.300563  [**] spp_portscan: End of portscan from MY.NET.24.47: TOTAL
time(65s) hosts(1) TCP(365) UDP(0) [**]
01/17-08:17:41.168458  [**] spp_portscan: End of portscan from MY.NET.24.47: TOTAL
time(40s) hosts(1) TCP(195) UDP(0) [**]
```

In addition, several other alerts were targeted toward the FTP server (Table 13). Specifically, 62 external hosts sent 214 alerts (8 unique) to MY.NET.24.47 in three days.

The host also received some OOS packets. They were from three unique hosts, but there were still patterns. All three hosts targeted the FTP server, but alternated between port 21 and a higher port number between 2500 and 4200. The first host 199.184.165.136 set its source port number at 20 and sent a single packet once a day for all three days to an unknown high level port. 69.57.160.70 behaved similarly. Once a day either one or two packets were sent targeting port 21 and an unknown high level port. Lastly, 64.91.254.110 also sent between 1 and 4 packets at the same time each day, still targeting port 21 and a high level port. It is as if the same attacker is performing reconnaissance on the FTP server from multiple hosts.

Table 13. All alerts targeting MY.NET.24.47.

# Alerts	Source IP's	Alert	Time
135	68.55.251.133	Possible trojan server activity	01/17-22:30 - 01/17-22:31
63	12.47.47.2, 12.221.70.151 24.74.231.208, 24.91.193.35 24.189.92.167, 24.210.30.209 24.225.66.165, 62.3.217.250 63.88.31.40, 63.197.5.99 63.199.152.230, 64.45.236.72 65.103.48.236, 65.200.93.131 65.220.16.61, 66.1.139.47 66.57.67.156, 66.74.172.170 66.75.254.137, 66.143.167.205 66.160.67.22, 66.215.171.59 67.40.162.19, 67.85.74.18 67.100.203.178, 67.101.128.35 67.233.27.224, 68.19.94.200 68.38.196.162. 68.55.144.93 68.100.193.197, 68.120.154.117 68.121.146.106, 68.217.72.70 68.232.128.139, 82.32.44.118 128.6.25.153, 128.101.191.31 128.103.148.226, 129.107.2.248 142.151.132.91, 171.75.87.253 198.70.230.5, 199.243.85.90 202.149.208.110, 205.187.181.246 211.213.227.72, 211.223.97.254 216.72.131.104, 217.229.172.140	FTP password attempt	01/17-01:09 - 01/19:23:34
4	128.46.156.117 208.209.50.18	EXPLOIT x86 NOOP	01/17-21:30 - 01/19-07:21
3	64.91.254.110 69.57.160.70 199.184.165.136	OOS packet	01/17-00:43 - 01/19-02:30
3	138.88.17.245	Incomplete Packet Fragments	01/17-00:44 - 01/17-12:29
3	66.44.102.222 213.153.211.143 213.153.211.201	FTP DoS ftpd globbing	01/18-03:57 - 01/19-01:44
2	208.7.42.135	NMAP TCP ping!	01/17-14:18 - 01/19-15:20
1	138.88.17.245	Null scan!	01/17-02:50

Evidence of Active Targeting

This attack was targeted. An initial port scan of the system determined the FTP service to be listening. Then the attacker attempted to exploit the server. There are many known vulnerabilities associated with FTP. Determining the FTP server version number would indicate what vulnerabilities exist. An attack on an FTP server may begin as reconnaissance, but will likely end in a number of attempted exploits.

Severity

The severity of FTP passwd attempt was calculated to be 5 out of 10 (Table 11). The high criticality and lethality values are not offset as the countermeasures are both relatively low.

Table 14. Severity of FTP vulnerability.

Severity = (Criticality + Lethality) – (System Countermeasures + Network Countermeasures)		
Criticality	This FTP server could either be located on a University server or a student's workstation. Just to be safe, we assume it is a server.	**4**
Lethality	This exploit gives root access to the system.	**5**
System Countermeasures	The number of alerts targeting this host means a number of services are enabled and they are likely not patched.	**2**
Network Countermeasures	These alerts would be mitigated with any type of firewall, but one does not appear to exist.	**2**
Total		**5**

Compromised Hosts

Clearly, this host has generated a lot of interest. Based on the logs, it appears the server has been compromised, but it is not clear which one of the exploits worked, and the identity of the successful attacker. It appears that either this server is on a subnet that gets scanned often, or else it is a well-known box that is a favorite target for a lot of people.

5 Network Statistics

5.1 Top Talkers

The alert files were used to determine the top talkers. The number of alerts (not including port scans) were totaled for each host. Port scans were not included due to the massive amount of alerts they generate. Four of the top five internal hosts generated alerts for nearly the same targets (Table 15).

Table 15. Top five alert generating internal hosts.

Total # of Alerts	**Internal Hosts**	**Total # of Targets**	**Targeted Hosts**		
1,713	MY.NET.69.198	1	69.10.132.121	Memset Ltd.	GB
1,109	MY.NET.21.67	7	198.144.15.226	wine.codeweavers.com	US
			69.6.61.10	ProDot Networks	US
			64.201.107.242	Race Technologies	US
			63.169.143.4	star8.kindredkonnections.com	US
			69.6.51.215	mail1.4-stocknews.info	US

			209.223.101.148	Atjeu Publishing	US
			128.171.198.49	s198n49.soc.hawaii.edu	US
1,078	MY.NET.21.79	7	217.209.31.21	h21n2fls34o880.telia.com	US
			68.94.121.190	adsl-68-94-121-190.dsl.hstntx.swbell.net	US
			69.68.123.172	mn-69-68-123-172.dyn.sprint-hsd.net	US
			217.17.113.20	BOLTBLUE-BROADBAND	GB
			68.93.80.70	adsl-68-93-80-70.dsl.hstntx.swbell.net	US
			68.93.80.27	adsl-68-93-80-27.dsl.hstntx.swbell.net	US
			128.171.198.49	s198n49.soc.hawaii.edu	US
936	MY.NET.21.68	7	217.209.31.21	h21n2fls34o880.telia.com	US
			68.94.121.190	adsl-68-94-121-190.dsl.hstntx.swbell.net	US
			69.68.123.172	mn-69-68-123-172.dyn.sprint-hsd.net	US
			217.17.113.20	BOLTBLUE-BROADBAND	GB
			68.93.80.70	adsl-68-93-80-70.dsl.hstntx.swbell.net	US
			68.93.80.27	adsl-68-93-80-27.dsl.hstntx.swbell.net	US
			128.171.198.49	s198n49.soc.hawaii.edu	US
905	MY.NET.21.92	6	217.209.31.21	h21n2fls34o880.telia.com	US
			68.94.121.190	adsl-68-94-121-190.dsl.hstntx.swbell.net	US
			69.68.123.172	mn-69-68-123-172.dyn.sprint-hsd.net	US
			68.93.80.70	adsl-68-93-80-70.dsl.hstntx.swbell.net	US
			68.93.80.27	adsl-68-93-80-27.dsl.hstntx.swbell.net	US
			128.171.198.49	s198n49.soc.hawaii.edu	US
12,582	**1,546**				

A single host, 128.171.198.49 generated 57% of all external host alerts (Table 16). The same host also targeted 97% of all university hosts.

Table 16. Top five alert generating external hosts.

Total # of Alerts	External Hosts			Total # of Targets	Targeted Hosts
14,021	128.171.198.49	s198n49.soc.hawaii.edu	US	10,407	*Not Shown*
2,432	68.32.127.158	pcp0011023458pcs.arlngt01.va.comcast.net	US	1	MY.NET.24.15
1,628	69.10.132.121	Memset Ltd.	GB	1	MY.NET.69.198
901	24.130.153.222	c-24-130-153-222.we.client2.attbi.com	US	12	MY.NET.189.62
					MY.NET.5.44
					MY.NET.83.98
					MY.NET.5.67
					MY.NET.5.45
					MY.NET.5.95
					MY.NET.5.20
					MY.NET.29.18
					MY.NET.75.13
					MY.NET.5.46
					MY.NET.5.25
					MY.NET.29.8
748	68.167.238.6	sun.livetime.com	US	260	
24,509	**727**			**11,049**	

MY.NET.69.198 was very popular, receiving nearly 1,700 alerts from 36 different sources (Table 17). Although the majority of the attackers are from the US, hosts from Germany and Austria were also attacking the University.

Table 17. Top five most targeted internal hosts

Total # of Alerts	Internal Hosts	Total # of Sources	Attacking Hosts		
2,434	MY.NET.24.15	2	68.32.127.158 128.171.198.49	pcp0011023458pcs.arlngt01.va.comcast.net s198n49.soc.hawaii.edu	US US
1,698	MY.NET.69.198	36	*Not Shown*		
451	MY.NET.97.123	2	66.98.168.220 128.171.198.49	shared-primary.alterhosting.com s198n49.soc.hawaii.edu	US US
368	MY.NET.97.35	2	128.122.20.14 128.171.198.49	SLINKY.CS.NYU.EDU s198n49.soc.hawaii.edu	US US
334	MY.NET.153.149	8	63.251.52.75 69.44.118.145 63.250.195.10 128.171.198.49 128.220.39.217 129.27.9.247 129.27.9.248 80.237.176.16	www.shockwave.com 69-44-118-145.wcg.net l8.cache.vip.dal.yahoo.com s198n49.soc.hawaii.edu x1-6-00-c0-9f-11-31-65.resnet.jhu.edu zidpc247.tu-graz.ac.at zidpc248.tu-graz.ac.at n80-237-176-16.iblknet.hosteurope.de	US US US US US AT AT DE
24,509	**10,576**				

The same five internal hosts can be seen attacking three different external hosts (Table 18). The hosts they are attacking actually all belong to the same ISP.

Table 18. Top five most targeted external hosts

Total # of Alerts	External Hosts			Total # of Sources	Attacking Hosts
2,298	128.171.198.49	s198n49.soc.hawaii.edu	US	1,509	*Not Shown*
1,711	69.10.132.121	Memset Ltd.	GB	1	MY.NET.69.198
1,539	68.93.80.70	adsl-68-93-80-0.dsl.hstntx.swbell.net	US	5	MY.NET.21.67 MY.NET.21.68 MY.NET.21.69 MY.NET.21.79 MY.NET.21.92
1,037	68.93.80.27	adsl-68-93-80-27.dsl.hstntx.swbell.net	US	5	MY.NET.21.67 MY.NET.21.68 MY.NET.21.69 MY.NET.21.79 MY.NET.21.92
967	68.94.121.190	adsl-68-94-121-190.dsl.hstntx.swbell.net	US	5	MY.NET.21.67 MY.NET.21.68 MY.NET.21.69 MY.NET.21.79 MY.NET.21.92
12,582	**473**			**2,273**	

It is surprising to see so much port scanning originating from the University network (Table 19). Detecting many more external hosts (1,434) than internal hosts (203) performing the scans is more understandable.

Table 19. Top five internal and external port scanning hosts.

Total # of Hosts Scanned	**Internal Hosts**	**Total # of Hosts Scanned**	**External Hosts**		
1,815,818	MY.NET.111.72	55,968	61.130.20.178	Cixi Developing Area Committee	CN
1,815,062	MY.NET.162.92	47,424	61.56.69.18	Diyixian.com(TW)Ltd.	TW
1,753,522	MY.NET.84.194	42,349	218.200.163.129	China Mobile Communications Corporation	CN
364,262	MY.NET.1.4	42,213	62.39.237.249	249.237.39-62.rev.gaoland.net	FR
122,882	MY.NET.34.14	40,834	218.237.65.19	Hanaro Telecom Inc.	ROK
6,516,271	**203**	**2,246,367**	**1,434**		

TCP SYN scans are the most popular enumerating technique (Table 20). Systems running Microsoft Windows are targeted most often due to the information available on TCP port 135 (Table 21).

Table 20. List of port scan types.

Total #	**Type of Scan**	**% of Total**
7,947,344	TCP SYN	70
7,941,492	******S*	
5,851	12****S*	
1	*2****S*	
3,384,525	UDP	29
6,131	TCP FIN	> .01
653	INVALIDACK	> .01
291	NULL	> .01
11,339,275		**99**

Table 21. Top six services scanned for.

Total #	**Service**	**Common**
5,472,977	135/tcp	RPC
2,885,546	53/udp	DNS
1,056,230	6129/tcp	Trojan
416,660	25/tcp	SMTP
239,049	4000/tcp	Trojan
113,445	80/tcp	HTTP

5.2 Profile of the three most suspicious external sources

128.171.198.49
In the span of three days, “Hawaii” managed to scan the University’s entire IP address space and happen to infect 1,500 users with the Red worm. This single host generated over 14,000 alerts (Red worm & SMB Name Wildcard) and attempted connecting to 10,407 university systems. The IP address resolves to a student dorm room at the University of Hawaii, so it is very possible that this IP address is part of a DHCP pool and our attacker can no longer be held accountable (Table 22).

193.220.82.38

This host, "Tanzania," does not appear to be currently online. This attacker scanned 6,711 hosts and then followed with 120 EXPLOIT x86 NOOP attempts against three different University hosts.

66.225.198.20
This host, "Chicago," did not generate any alerts and only performed one port scan against a single host. What makes this host suspicious is how it connected to 10 University systems, continually connects to an internal mail server, replies on TCP port 113 and UDP port 53, the source port for DNS queries is always the same, and 116 OOS packets have been detected with this host as the source. Further investigation is required.

Table 22. Whois lookup findings.

	128.171.198.49	193.220.82.38	66.225.198.20
NetRange:	128.171.0.0 - 128.171.255.255	193.220.82.0 - 193.220.83.191	66.225.192.0 - 66.225.255.255
NetName:	HAWAII	CATS-NET	SCN-2
Country:	US	TZ	US
Descr:	University of Hawaii	Internet Service Provider in Dar es Salaam, Tanzania	Server Central Network
Tech-c:	ZU32-ARIN	GHC12	JL1890-ARIN
RegDate:	1988-06-06	1997-06-18	2003-06-10
Updated:	2000-10-25	1999-04-01	2004-04-29
Source:	ARIN	RIPE	ARIN
NameServer:	DNS1.HAWAII.EDU		NS1.SCSERVERS.COM NS2.SCSERVERS.COM
Contact			
Role:	University of Hawaii Keller Hall	Gulam Chagani	Server Central Network
Address:	202 2565 The Mall, Honolulu, HI, 96822	P.O. Box 2569 Dar es Salaam	2002 W Chicago PMB 101, Chicago IL, 60622
Country:	US	Tanzania	US
Phone:	+1-808-521-2879	+255 51 112631	+1-312-829-1111
E-mail:	netcontact@hawaii.edu	rimas@taide.net	scsupport@servercentral.net
Other			
DNS	S198n49.soc.hawaii.edu		unknown.splashhost.net
# of hops away	14	18	15
RRT (avg)	139 ms	682 ms	38 ms
OS		*nix (Linux, FreeBSD, Solaris)	

6 Correlations

In addition to the correlations listed in each of the three network detects analyzed in the in-depth analysis, GCIA practicals from Jamell Creque [30], Hee So [31], Tim Kroeger [32], Les Gord [33], Peter Storm [34], and Wouter Clarie [35] were reviewed and influenced the analysis and report.

7 Compromised Internal Hosts

A listing of compromised hosts can be found in the Executive Summary (Table 1). A discussion of those hosts takes place in the in-depth analysis. See Appendix 2 for a comprehensive list of compromised Red worm hosts.

8 Defensive Recommendations

It is recommended the University consider implementing a system that requires every machine connected to the network to be fully patched and contain no software vulnerabilities.

Products currently exist that intercept any user that plugs into the network. After a quick patch scan, the product will either allow or disallow that user to browse the network. It is basically an authenticated DHCP solution using Nessus [27] for the security scan.

In addition to patching, providing virus and spam filtering at the gateway would be another preventative measure. The University may even consider purchasing a site license and provide free of charge anti-virus software for all faculty, staff, and students.

It is very important to also implement some kind of traffic filtering choke point between the Internet and internal LAN. A policy must be created that allows informational freedom in an academic environment, yet still protects computing assets.

Anti-Virus and access-control will mitigate the high level alerts discussed above in Table 5. In order to tackle the medium level alerts, a CSIRC must be created. A CSIRC does not necessarily require dozens of analysts in a state-of-the-art facility continuously monitoring the entire network. The University simply needs the capability to detect security events when they happen, and know how to respond. To do this, syslog should be configured to monitor all access points, such as routers, switches, and firewalls. IDS logs should be reviewed daily. Additionally, proper network monitoring tools should be in use. Tracking bandwidth, latency, pps (packet per second), etc. can provide valuable information about an event, perhaps even before it is detected by the IDS.

The low level alerts are generally false positives. Time must be spent with the IDS to fine-tune the policy to enable it to be as efficient as possible. An initial 30-day baseline is recommended to build an accurate, site-specific policy for the University network. Periodic updates of the policy must then be performed given the dynamic nature of the network.

Part III – Analysis Process

The goal in this analysis was to decide how to manage such a large data set, while still extracting meaningful results. Without a solid methodology, considerable amounts of time could be wasted performing the same analysis over and over again.

All three types of files were initially reviewed. The scans files were analyzed first because the content was the simplest, despite being the largest. The scans files provided a sense of the IP address space and the scope of the network before tackling specific alerts.

Perl was chosen as the main analysis tool after reading a number of practicals and GIAC study guides. Existing scripts from past practicals were considered for use, but were decided against: writing one's own code is usually easier and a greater learning experience than deciphering another's.

It was clear that analysis would be the simplest if all days of data could be aggregated into a single file. The problem is processing that data. The primary analysis machine was a Sony 2.4 GHz Pentium 4 Laptop with 1 Gigabyte of RAM running RedHat Linux 2.4 and Windows XP sp1. After aggregating the scans files together, the new data set was a 900 Megabyte beast, running over 14 million lines. In addition, the initial Perl scripts failed miserably because they were attempting to read the entire file into memory before processing. A solution was to pipe the file to the program as STDIN to avoid the memory bottleneck. After several optimizations, a report on the entire 14 million lines of data could be completed in under 60 minutes.

To expedite the reporting time, the alerts files were broken into smaller pieces for analysis. Due to already analyzing the scans file, the port scan alerts were removed into a separate file while the rest of the alerts were analyzed. This approach conferred several advantages. Reports ran much more rapidly because the data files were smaller. In addition, a port scan could be quickly confirmed because it was in its own file. A script was created to de-obfuscate all the University IP addresses. This allowed for simpler scripts, but all final reports re-obfuscate the addresses. By the end of the analysis, scripts were running on a number of different files including the original alert, scan and OOS types, searching for relational information and exacting real flows from the limited amount of data available.

In addition to Perl, the following UNIX command line tools were heavily utilized: grep, cat, uniq, wc, head, tail, vi, dig, whois. The majority of the analysis was done in Linux, while the writing of the report was done using Microsoft Word 2002 in Windows XP. Figures were created using Microsoft Excel 2002 and Visio 2002.

Other tools such as SnortSnarf or Analysis Console for Intrusion Databases (ACID) were not used; the results of the custom Perl programs were better understood in the process of coding them as opposed to interpreting the results of a static template report. The most often used Perl scripts are detailed in Appendix A.

References

[1] ARIN “ARIN WHOIS Database Search”
URL: http://whois.arin.net (3 Dec 04)

[2] Nmap “Nmap – Free Security Scanner For Network Exploration & Security Audits”
URL: http://www.insecure.org/nmap/ (12 Dec 04)

[3] CAIDA “CAIDA Analysis of Code-Red”
URL: http://www.caida.org/analysis/security/code-red/ (27 Oct 04)

[4] SANS “SANS Institute: Adore Worm”
URL: http://www.sans.org/y2k/adore.htm (27 Oct 04)

[5] F-Secure “F-Secure Computer Virus Information Pages: Adore”
URL: http://www.europe.f-secure.com/v-descs/adore.shtml (27 Oct 04)

[6] CERT “CERT Advisory CA-2001-02 Multiple Vulnerabilities in BIND”
URL: http://www.cert.org/advisories/CA-2001-02.html (28 Oct 04)

[7] Redhat “Red Hat Support”
URL: http://rhn.redhat.com/errata/RHSA-2001-007.html (27 Oct 04)

[8] Redhat “Red Hat, Inc.”
URL: http://www.redhat.com/archives/redhat-watch-list/2000-June/msg00009.html (1 Nov 04)

[9] Insecure.org “Bugtraq: [RHSA-2000:043-03] Revised advisory: Updated package for nfs-utils available”
URL: http://seclists.org/lists/bugtraq/2000/Jul/0305.html (27 Oct 04)

[10] Hideaway
URL: http://www.hideaway.net/newsletter/lpring.txt (27 Oct 04)

[11] SANS “SANS Global Incident Analysis Center > Ramen Worm”
URL: http://www.sans.org/y2k/ramen.htm (3 Nov 04)

[12] SANS “SANS Institute – Lion Worm”
URL: http://www.sans.org/y2k/lion.htm (3 Nov 04)

[13] SecurityFocus “Multiple Vendor LPRng User-Supplied Format String”
URL: http://www.securityfocus.com/bid/1712 (27 Oct 04)

[14] SecurityFocus “Wu-Ftpd Remote Format String Stack Overwrite Vulne”
URL: http://www.securityfocus.com/bid/1387 (27 Oct 04)

[15] SecurityFocus “ISC Bind 8 Transaction Signatures Buffer Overflow”
URL: http://www.securityfocus.com/bid/2302 (27 Oct 04)

[16] SecurityFocus “Multiple Linux Vendor rpc.statd Remote Format Stri”
URL: http://www.securityfocus.com/bid/1480 (27 Oct 04)

[17] Kite, Doug. “Intrusion Detection in Depth (GCIA). Practical Assignment.” July 2002.
URL: http://www.giac.org/practical/GCIA/Doug_Kite_GCIA.pdf (12 Dec 04)

[18] Simovits “RC1 trojan”
URL: http://www.simovits.com/trojans/tr_data/y2724.html (27 Oct 04)

[19] Whitehats ”IDS181”
URL: http://www.whitehats.com/info/IDS181 (3 Nov 04)

[20] Microsoft “Microsoft Security Bulletin MS03-007”
URL: http://www.microsoft.com/technet/security/bulletin/MS03-007.mspx (28 Oct 04)

[21] Hein, Blaine. “GIAC GCIA Certification. Practical Assignment.” 21 May 2004.
URL: http://www.giac.org/practical/GCIA/Blaine_Hein_GCIA.pdf (11 Dec 04)

[22] Snort “Snort.org”
URL: http://www.snort.org/snort-db/sid.html?sid=648 (12 Dec 04)

[23] Affeld, James. “GIAC Certified Intrusion Analyst (GCIA). Practical Assignment.” 3 June 2004.
URL: http://www.giac.org/practical/GCIA/James_Affeld_GCIA.pdf (12 Dec 04)

[24] Digitaltrust “Full details for ftp-passwd-retrieval-retr”
URL: http://www.digitaltrust.it/arachnids/IDS213/event.html (3 Nov 04)

[25] SecurityFocus “Mini SQL w3-msql Vulnerability”
URL: http://www.securityfocus.com/bid/591 (12 Dec 04)

[26] ISS “2003601”
URL: http://www.iss.net/security_center/advice/Intrusions/2003601/default.htm (3 Nov 04)

[27] Nessus
URL: http://www.nessus.org/ (12 Dec 04)

[28] SecurityFocus “Microsoft Windows ntdll.dll Buffer Overflow Vulner”
URL: http://www.securityfocus.com/bid/7116 (28 Oct 04)

[29] LWN.net "Adore Worm a little more…."
URL: http://lwn.net/2001/0405/a/adore-ARIS.php3 (3 Nov 04)

[30] Creque, Jamell. "SANS GICA CERTIFICATION. Practical Assignment." 3 March 2003.
URL: http://www.giac.org/practical/GSEC/Jamell_Creque_GCIA.pdf (12 Dec 04)

[31] So, Hee. "GIAC Intrusion Detection In Depth. Practical Assignment." 16 Feb 2002.
URL: http://www.giac.org/practical/GSEC/Hee_So_G_GCIA.doc (27 Oct 04)

[32] Kroeger, Tim. "Security Information Management Systems (GCIA). Practical Assignment"
URL: http://www.giac.org/practical/GSEC/Tim_Kroeger_GCIA.pdf (10 Dec 04)

[33] Gordon, Les. "Intrusion Analysis – The Director's Cut! Practical Assignment." 22 Nov 2002.
URL: http://www.giac.org/practical/GCIA/Les_Gordon_GCIA.doc (4 Nov 04)

[34] Storm, Peter. "GIAC Certified Intrusion Analyst (GCIA). Practical Assignment" 15 Nov 2003.
URL: http://www.giac.org/practical/GCIA/Pete_Storm_GCIA.pdf (15 Oct 04)

[35] Clarie, Wouter. "GIAC Certified Intrusion Analyst (GCIA). Practical Assignment." 6 Oct 2004.
URL: http://www.giac.org/practical/GCIA/Wouter_Clarie_GCIA.pdf (12 Dec 04)

[36] SANS "SANS – Internet Storm Center"
URL: http://isc.sans.org/ (2 Nov 04)

Appendix A – Perl scripts

Code 1. portscan.pl - generate host list based on port scans.

```
#!/usr/bin/perl

#parse portscan alerts and find number of active hosts in each subnet

my $line, $subnet, $host, $hosts, $subnets;
my @A;
my %scans;

while ($line = <STDIN>) {
   @A = ();
   push @A, split (' ', $line);
   ($_, $_, $subnet, $host) = split ('\.', $A[2]);
   $scans{$subnet}++;
   $hosts++;
}

#create report
open (OUT, '>net_sum') or die "Can't open file: $!";
print OUT "\nNumber of hosts scanned from subnet\n";
print OUT "------------------------------\n";
foreach $subnet ( sort keys %scans ) {
   print OUT "$scans{$key} = MY.NET.$key.x\n";
   $subnets++;
}
print OUT "\n$subnets = Number of internal subnets\n";
print OUT "$hosts = Total number of hosts scanned\n";
close (OUT);
```

Code 2. scans.pl - parse file and generate reports.

```
#!/usr/bin/perl

#read in text files, parse and output as directed

my @A, @dst_ip;
my $line, $src_ip, $src_port, $dst_ip, $dst_port, $prot, $scan_count, $key,
$error_count, $i, $dst_ip_count, $src_ip_count, $total_scans, $total_dst_scans,
$usrc_ip_count, $total_u_scans, $src_count, $flags;
my %ip, %Sip, %port, %pro, %HoA;

open (SUM, '>summary') or die "Can't open file: $!";
open (ERROR, '>error') or die "Can't open file: $!";

while ($line = <STDIN>) {
   @A = ();
   push @A, split (' ', $line);
   ($src_ip, $src_port) = split (':', $A[3]);
   ($dst_ip, $dst_port) = split (':', $A[5]);
   $prot = $A[6];
   $flags = $A[7];
   $scan_count++;

   if ($src_ip =~ m/^([01]?\d\d?|2[0-4]\d|25[0-5])\.([01]?\d\d?|2[0-4]\d|25[0-
5])\.([01]?\d\d?|2[0-4]\d|25[0-5])\.([01]?\d\d?|2[0-4]\d|25[0-5])$/ and $dst_ip
=~ m/^([01]?\d\d?|2[0-4]\d|25[0-5])\.([01]?\d\d?|2[0-4]\d|25[0-
5])\.([01]?\d\d?|2[0-4]\d|25[0-5])\.([01]?\d\d?|2[0-4]\d|25[0-5])$/) {
      #insert line into hash
      $port{"$src_port:$dst_port"}++;
      $port{"s $src_port"}++;
      $port{"d $dst_port"}++;
      if ($prot eq "SYN") {
         $pro{$prot}{"count"}++;
         $pro{$prot}{$flags}++;
      } else {
         $pro{$prot}{"count"}++;
      }
      $Dip{$dst_ip}++;

      next unless !exists $HoA{$src_ip}{$dst_ip};
      $HoA{$src_ip}{$dst_ip} = 1;
      $HoA{$src_ip}{"count"}++;
      $src_count++;
   } else {
      #copy line to error file
      print ERROR "$line";
      $error_count++;
   }
}

#create reports
print "Creating reports...\n";
print "  [usrc_ip]";
open (OUT, '>usrc_ip') or die "Can't open file: $!";
print OUT "\nSRC IP = # of unique IPs scanned\n";
print OUT "-------------------------\n";
foreach $src ( keys %HoA ) {
  print OUT "$HoA{$src}{count} = $src\n";
  print ".";
  #$total = ++$#{ $HoA{$key} };
  #print "\n$key [$total] -> @{ $Sip{$key} }\n";
}
print SUM "$src_count = Number of unique src Ips found scanning from uSRC\n";
close (OUT);
print "done!\n";

print "  [dst_ip]";
open (OUT, '>dst_ip') or die "Can't open file: $!";
print OUT "\nDST IP = # of times hit\n";
print OUT "-----------------------\n";
foreach $key ( keys %Dip ) {
   if ($Dip{$key} > 999) {
      print OUT "$Dip{$key} = $key\n";
      print ".";
   }
   $total_dst_scans += $Dip{$key};
   $dst_ip_count++;
}
```

```
print SUM "$total_dst_scans = total number of scans from DST\n";
print SUM "$dst_ip_count = total dst ips scanned from DST\n";
close (OUT);
print "done!\n";

print "  [port]";
open (OUT, '>port') or die "Can't open file: $!";
print OUT "\nSRC and DST port comb = # times used\n";
print OUT "-----------------------------------\n";
foreach $key ( keys %port ) {
   print OUT "$port{$key} = $key\n";
   print ".";
}
close (OUT);
print "done!\n";

print "  [protocol]";
open (OUT, '>protocol') or die "Can't open file: $!";
print OUT "\nProtocol used = # of times\n";
print OUT "-------------------------\n";
foreach $protocol ( keys %pro ) {
   print OUT "$pro{$protocol}{count} = $protocol\n";
   for $type (keys %{ $pro{$protocol} }) {
      print OUT "$pro{$protocol}{$type} = $type\n";
      $i++;
      print ".";
   }
}
print SUM "$i = total protocol\n";
close (OUT);
print "done!\n";

print SUM "$error_count = total errors found\n";
print SUM "$scan_count = total lines processed\n";

close (ERROR);
close (SUM);
```

Code 3. alerts.pl - parse file and sort number of alerts.

```
#!/usr/bin/perl

#parse file for alerts, and count the occurance of each

my @A;
my $line, $alert;
my %hash;

#read in single line at a time
while ($line = <STDIN>) {
   ($_, $_, $alert) = split ('[**]', $line);
   $hash{$alert}++;
}

#create report
open (OUT, '>unique_alert.count') or die "Can't open file: $!";
```

```
foreach $alert ( keys %hash ) {
   $num = $hash{$key};
   print OUT "$num $key\n";
   $alerts++;
   $total += $num;
}
print "$alerts unique alerts found\n";
print "$total total alerts found";
close (OUT);
```

Code 4. top_talker.pl - parse alert file and find top talkers.

```
#!/usr/bin/perl

#parse alert files and determine the number of alerts generated by each IP
address in file by source and destination

my $line, $i, $sip, $sport, $dip, $dport, $a, $b, $key, $count;
my @A;
my %sip, %dip;

while ($line = <STDIN>) {
   @A = ();
   push @A, split (' ', $line);
   $i=0;
   foreach $key (@A) {
      ($sip, $sport) = split (':', $key);
      if ($sip =~ m/^([01]?\d\d?|2[0-4]\d|25[0-5])\.([01]?\d\d?|2[0-4]\d|25[0-
5])\.([01]?\d\d?|2[0-4]\d|25[0-5])\.([01]?\d\d?|2[0-4]\d|25[0-5])$/) {
         ($dip, $dport) = split (':', $A[$i+2]);
         last if ($dip eq "");
         #print "Adding $line... $sip $sport -> $dip $dport\n";
         $a = 1;
         foreach $ip (@{ $sip{$sip} }) {
            $a = 0 if ($ip eq $dip);
         }
         push @{ $sip{$sip} }, $dip if $a;

         $b = 1;
         foreach $ip (@{ $dip{$dip} }) {
            $b = 0 if ($ip eq $sip);
         }
         push @{ $dip{$dip} }, $sip if $b;
         last;
      }
      $i++;
   }
}

#create report
open (OUT, '>top_talkers.src') or die "Can't open file: $!";
foreach $key ( keys %sip ) {
   $count = $#{ $sip{$key} } + 1;
   #print OUT "$count $key -> @{ $sip{$key} }\n";
   print OUT "$count $key\n";
   $src++;
   $dst += $count;
}
print "$src = total src\n";
print "$dst = total hosts hit (not unique)\n";
close (OUT);

$src=0;
$dst=0;
open (OUT, '>top_talkers.dst') or die "Can't open file: $!";
foreach $key ( keys %dip ) {
   $count = $#{ $dip{$key} } + 1;
   #print OUT "$count $key -> @{ $dip{$key} }\n";
   print OUT "$count $key\n";
   $src++;
   $dst += $count;
}
print "$src = total src\n";
print "$dst = total hosts hit (not unique)\n";
close (OUT);
```

Appendix B – Red worm infected hosts

130.85.1.13	130.85.147.193	130.85.161.9	130.85.21.98	130.85.31.17	130.85.65.14
130.85.10.1	130.85.147.194	130.85.162.1	130.85.21.99	130.85.31.2	130.85.65.25
130.85.10.115	130.85.15.1	130.85.162.100	130.85.22.112	130.85.31.3	130.85.66.17
130.85.10.12	130.85.15.11	130.85.162.104	130.85.22.113	130.85.31.4	130.85.66.19
130.85.10.121	130.85.15.169	130.85.162.106	130.85.22.114	130.85.31.5	130.85.66.3
130.85.10.13	130.85.15.196	130.85.162.108	130.85.22.119	130.85.31.6	130.85.66.38
130.85.10.14	130.85.15.198	130.85.162.109	130.85.22.225	130.85.31.7	130.85.66.43
130.85.10.167	130.85.15.200	130.85.162.114	130.85.22.226	130.85.31.83	130.85.66.54
130.85.10.17	130.85.15.202	130.85.162.118	130.85.22.227	130.85.31.86	130.85.66.6
130.85.10.172	130.85.15.21	130.85.162.12	130.85.22.228	130.85.31.87	130.85.67.10
130.85.10.176	130.85.15.214	130.85.162.122	130.85.22.49	130.85.31.88	130.85.69.139
130.85.10.177	130.85.15.23	130.85.162.123	130.85.22.50	130.85.31.9	130.85.69.141
130.85.10.179	130.85.15.41	130.85.162.127	130.85.22.51	130.85.31.90	130.85.69.143
130.85.10.184	130.85.15.43	130.85.162.168	130.85.22.52	130.85.31.91	130.85.69.144
130.85.10.19	130.85.15.71	130.85.162.175	130.85.22.53	130.85.31.92	130.85.69.146
130.85.10.202	130.85.15.74	130.85.162.177	130.85.22.54	130.85.31.93	130.85.69.149
130.85.10.203	130.85.150.1	130.85.162.180	130.85.22.55	130.85.31.94	130.85.69.156
130.85.10.24	130.85.150.101	130.85.162.181	130.85.22.56	130.85.31.95	130.85.69.172
130.85.10.25	130.85.150.11	130.85.162.182	130.85.24.11	130.85.33.1	130.85.69.177
130.85.10.253	130.85.150.114	130.85.162.183	130.85.24.13	130.85.34.1	130.85.69.183
130.85.10.27	130.85.150.133	130.85.162.184	130.85.24.14	130.85.34.11	130.85.69.193
130.85.10.30	130.85.150.14	130.85.162.185	130.85.24.15	130.85.34.12	130.85.69.201
130.85.10.32	130.85.150.150	130.85.162.186	130.85.24.18	130.85.34.14	130.85.69.208
130.85.10.38	130.85.150.151	130.85.162.187	130.85.24.19	130.85.34.15	130.85.69.211
130.85.10.44	130.85.150.152	130.85.162.188	130.85.24.20	130.85.34.5	130.85.69.222
130.85.10.55	130.85.150.153	130.85.162.189	130.85.24.27	130.85.34.8	130.85.69.227
130.85.10.56	130.85.150.154	130.85.162.19	130.85.24.3	130.85.4.1	130.85.69.228
130.85.10.57	130.85.150.155	130.85.162.20	130.85.24.30	130.85.40.1	130.85.69.241
130.85.10.58	130.85.150.156	130.85.162.211	130.85.24.31	130.85.42.1	130.85.69.243
130.85.10.59	130.85.150.157	130.85.162.214	130.85.24.33	130.85.42.3	130.85.69.247
130.85.10.60	130.85.150.159	130.85.162.215	130.85.24.34	130.85.42.4	130.85.69.253
130.85.10.61	130.85.150.16	130.85.162.216	130.85.24.35	130.85.42.5	130.85.7.1
130.85.10.62	130.85.150.162	130.85.162.217	130.85.24.36	130.85.5.1	130.85.70.1
130.85.10.63	130.85.150.163	130.85.162.218	130.85.24.37	130.85.5.11	130.85.70.101
130.85.10.65	130.85.150.164	130.85.162.22	130.85.24.39	130.85.5.111	130.85.70.107
130.85.10.68	130.85.150.168	130.85.162.226	130.85.24.4	130.85.5.13	130.85.70.114
130.85.10.75	130.85.150.17	130.85.162.231	130.85.24.40	130.85.5.141	130.85.70.115
130.85.10.79	130.85.150.170	130.85.162.233	130.85.24.42	130.85.5.17	130.85.70.118
130.85.10.82	130.85.150.171	130.85.162.235	130.85.24.43	130.85.5.20	130.85.70.121
130.85.10.83	130.85.150.172	130.85.162.240	130.85.24.44	130.85.5.24	130.85.70.128
130.85.10.84	130.85.150.173	130.85.162.241	130.85.24.45	130.85.5.25	130.85.70.129
130.85.10.85	130.85.150.184	130.85.162.242	130.85.24.48	130.85.5.26	130.85.70.133
130.85.10.86	130.85.150.187	130.85.162.249	130.85.24.49	130.85.5.34	130.85.70.135
130.85.10.87	130.85.150.193	130.85.162.251	130.85.24.51	130.85.5.50	130.85.70.139
130.85.10.88	130.85.150.195	130.85.162.252	130.85.24.52	130.85.5.55	130.85.70.146
130.85.10.89	130.85.150.197	130.85.162.33	130.85.24.54	130.85.5.64	130.85.70.147

130.85.10.9	130.85.150.201	130.85.162.34	130.85.24.55	130.85.5.67	130.85.70.148
130.85.100.1	130.85.150.208	130.85.162.37	130.85.24.58	130.85.5.72	130.85.70.156
130.85.100.121	130.85.150.210	130.85.162.43	130.85.24.6	130.85.5.92	130.85.70.159
130.85.100.203	130.85.150.212	130.85.162.44	130.85.24.61	130.85.5.95	130.85.70.162
130.85.100.204	130.85.150.231	130.85.162.45	130.85.24.68	130.85.5.99	130.85.70.163
130.85.100.206	130.85.150.235	130.85.162.47	130.85.24.7	130.85.53.1	130.85.70.164
130.85.100.227	130.85.150.237	130.85.162.54	130.85.24.70	130.85.53.10	130.85.70.170
130.85.100.69	130.85.150.245	130.85.162.56	130.85.24.74	130.85.53.100	130.85.70.172
130.85.101.1	130.85.150.248	130.85.162.57	130.85.24.8	130.85.53.101	130.85.70.177
130.85.102.1	130.85.150.250	130.85.162.58	130.85.24.9	130.85.53.102	130.85.70.18
130.85.109.1	130.85.150.3	130.85.162.59	130.85.25.1	130.85.53.103	130.85.70.180
130.85.109.110	130.85.150.30	130.85.162.61	130.85.25.10	130.85.53.104	130.85.70.185
130.85.109.13	130.85.150.31	130.85.162.62	130.85.25.11	130.85.53.105	130.85.70.191
130.85.109.218	130.85.150.32	130.85.162.64	130.85.25.12	130.85.53.106	130.85.70.197
130.85.109.50	130.85.150.50	130.85.162.65	130.85.25.17	130.85.53.107	130.85.70.202
130.85.109.51	130.85.150.53	130.85.162.67	130.85.25.21	130.85.53.108	130.85.70.203
130.85.109.53	130.85.150.55	130.85.162.68	130.85.25.22	130.85.53.109	130.85.70.209
130.85.109.58	130.85.150.58	130.85.162.69	130.85.25.3	130.85.53.110	130.85.70.210
130.85.109.59	130.85.150.6	130.85.162.70	130.85.25.33	130.85.53.115	130.85.70.216
130.85.109.70	130.85.150.70	130.85.162.71	130.85.25.34	130.85.53.117	130.85.70.218
130.85.109.71	130.85.150.83	130.85.162.75	130.85.25.35	130.85.53.125	130.85.70.225
130.85.109.75	130.85.150.84	130.85.162.80	130.85.25.4	130.85.53.167	130.85.70.232
130.85.109.87	130.85.151.1	130.85.162.83	130.85.25.41	130.85.53.168	130.85.70.235
130.85.109.89	130.85.151.114	130.85.162.87	130.85.25.42	130.85.53.169	130.85.70.237
130.85.109.9	130.85.151.12	130.85.162.89	130.85.25.65	130.85.53.170	130.85.70.238
130.85.11.1	130.85.151.128	130.85.162.90	130.85.25.66	130.85.53.171	130.85.70.239
130.85.11.11	130.85.151.132	130.85.162.91	130.85.25.67	130.85.53.172	130.85.70.252
130.85.11.12	130.85.151.16	130.85.162.92	130.85.25.68	130.85.53.173	130.85.70.38
130.85.11.13	130.85.151.221	130.85.163.1	130.85.25.69	130.85.53.174	130.85.70.41
130.85.11.15	130.85.151.61	130.85.163.100	130.85.25.70	130.85.53.175	130.85.70.42
130.85.11.16	130.85.151.62	130.85.163.101	130.85.25.71	130.85.53.176	130.85.70.43
130.85.11.2	130.85.151.69	130.85.163.113	130.85.25.72	130.85.53.177	130.85.70.46
130.85.11.3	130.85.151.72	130.85.163.116	130.85.25.73	130.85.53.178	130.85.70.5
130.85.11.33	130.85.151.92	130.85.163.117	130.85.25.9	130.85.53.179	130.85.70.50
130.85.11.4	130.85.151.93	130.85.163.126	130.85.27.1	130.85.53.180	130.85.70.52
130.85.11.5	130.85.151.97	130.85.163.17	130.85.27.102	130.85.53.192	130.85.70.53
130.85.11.6	130.85.152.1	130.85.163.23	130.85.27.155	130.85.53.193	130.85.70.63
130.85.11.7	130.85.152.10	130.85.163.231	130.85.27.159	130.85.53.194	130.85.70.66
130.85.11.9	130.85.152.11	130.85.163.236	130.85.27.160	130.85.53.197	130.85.70.69
130.85.110.1	130.85.152.12	130.85.163.237	130.85.27.161	130.85.53.198	130.85.70.72
130.85.110.100	130.85.152.13	130.85.163.239	130.85.27.162	130.85.53.199	130.85.70.73
130.85.110.111	130.85.152.14	130.85.163.249	130.85.27.163	130.85.53.202	130.85.70.74
130.85.110.113	130.85.152.15	130.85.163.25	130.85.27.164	130.85.53.203	130.85.70.75
130.85.110.114	130.85.152.157	130.85.163.252	130.85.27.165	130.85.53.206	130.85.70.80
130.85.110.115	130.85.152.16	130.85.163.253	130.85.27.166	130.85.53.209	130.85.70.82
130.85.110.150	130.85.152.161	130.85.163.254	130.85.27.167	130.85.53.210	130.85.70.9
130.85.110.152	130.85.152.166	130.85.163.26	130.85.27.168	130.85.53.216	130.85.71.1
130.85.110.165	130.85.152.168	130.85.163.28	130.85.27.169	130.85.53.217	130.85.71.237

130.85.110.172	130.85.152.169	130.85.163.48	130.85.27.170	130.85.53.219	130.85.72.129
130.85.110.201	130.85.152.170	130.85.163.49	130.85.27.171	130.85.53.220	130.85.72.132
130.85.110.202	130.85.152.173	130.85.163.55	130.85.27.172	130.85.53.222	130.85.72.144
130.85.110.203	130.85.152.175	130.85.163.56	130.85.27.173	130.85.53.223	130.85.72.146
130.85.110.204	130.85.152.176	130.85.163.78	130.85.27.174	130.85.53.224	130.85.72.149
130.85.110.205	130.85.152.177	130.85.163.85	130.85.27.175	130.85.53.225	130.85.72.156
130.85.110.206	130.85.152.178	130.85.163.86	130.85.27.176	130.85.53.226	130.85.72.157
130.85.110.207	130.85.152.179	130.85.163.87	130.85.27.177	130.85.53.227	130.85.72.158
130.85.110.209	130.85.152.18	130.85.163.97	130.85.27.178	130.85.53.228	130.85.72.160
130.85.110.210	130.85.152.180	130.85.163.98	130.85.27.179	130.85.53.229	130.85.72.170
130.85.110.211	130.85.152.181	130.85.163.99	130.85.27.180	130.85.53.231	130.85.72.176
130.85.110.212	130.85.152.182	130.85.165.1	130.85.27.181	130.85.53.233	130.85.72.186
130.85.110.213	130.85.152.183	130.85.17.1	130.85.27.182	130.85.53.251	130.85.72.194
130.85.110.214	130.85.152.184	130.85.17.10	130.85.27.183	130.85.53.252	130.85.72.207
130.85.110.215	130.85.152.185	130.85.17.12	130.85.27.184	130.85.53.254	130.85.72.225
130.85.110.216	130.85.152.186	130.85.17.13	130.85.27.185	130.85.53.30	130.85.72.243
130.85.110.217	130.85.152.19	130.85.17.2	130.85.27.186	130.85.53.31	130.85.72.244
130.85.110.219	130.85.152.21	130.85.17.20	130.85.27.187	130.85.53.32	130.85.72.254
130.85.110.22	130.85.152.213	130.85.17.3	130.85.27.188	130.85.53.33	130.85.73.1
130.85.110.220	130.85.152.214	130.85.17.4	130.85.27.189	130.85.53.34	130.85.75.1
130.85.110.222	130.85.152.244	130.85.17.69	130.85.27.190	130.85.53.35	130.85.75.10
130.85.110.225	130.85.152.245	130.85.17.70	130.85.27.191	130.85.53.36	130.85.75.107
130.85.110.226	130.85.152.246	130.85.18.1	130.85.27.192	130.85.53.37	130.85.75.108
130.85.110.228	130.85.152.247	130.85.18.18	130.85.27.193	130.85.53.38	130.85.75.109
130.85.110.229	130.85.152.248	130.85.18.2	130.85.27.194	130.85.53.40	130.85.75.11
130.85.110.23	130.85.152.249	130.85.18.23	130.85.27.195	130.85.53.41	130.85.75.111
130.85.110.230	130.85.152.250	130.85.18.28	130.85.27.196	130.85.53.42	130.85.75.112
130.85.110.233	130.85.152.252	130.85.18.44	130.85.27.197	130.85.53.43	130.85.75.115
130.85.110.234	130.85.152.44	130.85.18.45	130.85.27.198	130.85.53.44	130.85.75.116
130.85.110.235	130.85.152.46	130.85.18.46	130.85.27.25	130.85.53.45	130.85.75.121
130.85.110.236	130.85.153.1	130.85.18.48	130.85.27.26	130.85.53.46	130.85.75.125
130.85.110.240	130.85.153.114	130.85.185.1	130.85.27.27	130.85.53.47	130.85.75.126
130.85.110.241	130.85.153.12	130.85.185.28	130.85.27.28	130.85.53.48	130.85.75.127
130.85.110.28	130.85.153.140	130.85.186.1	130.85.27.3	130.85.53.49	130.85.75.128
130.85.110.56	130.85.153.143	130.85.186.20	130.85.27.33	130.85.53.51	130.85.75.129
130.85.110.66	130.85.153.147	130.85.189.1	130.85.27.5	130.85.53.52	130.85.75.13
130.85.110.76	130.85.153.148	130.85.189.17	130.85.27.6	130.85.53.53	130.85.75.131
130.85.110.95	130.85.153.149	130.85.189.18	130.85.27.7	130.85.53.54	130.85.75.14
130.85.111.1	130.85.153.150	130.85.189.30	130.85.27.8	130.85.53.55	130.85.75.140
130.85.111.12	130.85.153.151	130.85.189.36	130.85.28.1	130.85.53.56	130.85.75.15
130.85.111.139	130.85.153.152	130.85.189.40	130.85.28.10	130.85.53.58	130.85.75.154
130.85.111.140	130.85.153.153	130.85.189.41	130.85.28.11	130.85.53.59	130.85.75.159
130.85.111.148	130.85.153.154	130.85.189.42	130.85.28.12	130.85.53.60	130.85.75.162
130.85.111.15	130.85.153.157	130.85.189.45	130.85.28.2	130.85.53.61	130.85.75.176
130.85.111.156	130.85.153.159	130.85.189.5	130.85.28.3	130.85.53.64	130.85.75.18
130.85.111.159	130.85.153.16	130.85.189.52	130.85.28.4	130.85.53.65	130.85.75.19
130.85.111.160	130.85.153.163	130.85.189.57	130.85.28.5	130.85.53.67	130.85.75.202
130.85.111.161	130.85.153.164	130.85.189.6	130.85.28.6	130.85.53.76	130.85.75.206

130.85.111.162	130.85.153.166	130.85.189.61	130.85.28.7	130.85.53.8	130.85.75.210
130.85.111.168	130.85.153.179	130.85.189.62	130.85.28.8	130.85.53.84	130.85.75.213
130.85.111.169	130.85.153.180	130.85.189.7	130.85.28.9	130.85.53.85	130.85.75.217
130.85.111.184	130.85.153.182	130.85.189.8	130.85.29.1	130.85.53.86	130.85.75.218
130.85.111.185	130.85.153.185	130.85.190.102	130.85.29.10	130.85.53.87	130.85.75.25
130.85.111.191	130.85.153.186	130.85.190.202	130.85.29.12	130.85.53.88	130.85.75.26
130.85.111.20	130.85.153.187	130.85.190.97	130.85.29.129	130.85.53.89	130.85.75.27
130.85.111.201	130.85.153.188	130.85.191.1	130.85.29.13	130.85.53.90	130.85.75.3
130.85.111.202	130.85.153.190	130.85.191.52	130.85.29.130	130.85.53.91	130.85.75.30
130.85.111.21	130.85.153.195	130.85.191.67	130.85.29.14	130.85.53.94	130.85.75.31
130.85.111.219	130.85.153.196	130.85.2.1	130.85.29.145	130.85.53.95	130.85.75.4
130.85.111.22	130.85.153.205	130.85.2.206	130.85.29.15	130.85.53.96	130.85.75.5
130.85.111.224	130.85.153.208	130.85.2.209	130.85.29.18	130.85.53.97	130.85.75.6
130.85.111.225	130.85.153.210	130.85.20.1	130.85.29.19	130.85.53.98	130.85.75.69
130.85.111.228	130.85.153.211	130.85.21.1	130.85.29.2	130.85.54.1	130.85.75.7
130.85.111.229	130.85.153.219	130.85.21.10	130.85.29.3	130.85.54.13	130.85.75.71
130.85.111.23	130.85.153.221	130.85.21.100	130.85.29.30	130.85.54.203	130.85.75.8
130.85.111.235	130.85.153.222	130.85.21.101	130.85.29.31	130.85.54.212	130.85.75.85
130.85.111.28	130.85.153.30	130.85.21.102	130.85.29.4	130.85.54.253	130.85.75.87
130.85.111.29	130.85.153.33	130.85.21.108	130.85.29.5	130.85.54.27	130.85.75.88
130.85.111.30	130.85.153.34	130.85.21.11	130.85.29.65	130.85.54.30	130.85.75.89
130.85.111.31	130.85.153.46	130.85.21.113	130.85.29.66	130.85.55.1	130.85.75.9
130.85.111.32	130.85.153.52	130.85.21.117	130.85.29.8	130.85.55.92	130.85.75.91
130.85.111.33	130.85.153.78	130.85.21.12	130.85.29.9	130.85.56.1	130.85.75.95
130.85.111.34	130.85.153.79	130.85.21.120	130.85.30.1	130.85.6.14	130.85.75.98
130.85.111.38	130.85.153.81	130.85.21.150	130.85.30.10	130.85.6.15	130.85.75.99
130.85.111.39	130.85.153.82	130.85.21.151	130.85.30.11	130.85.6.16	130.85.8.1
130.85.111.41	130.85.153.83	130.85.21.153	130.85.30.3	130.85.6.17	130.85.80.1
130.85.111.42	130.85.153.85	130.85.21.154	130.85.30.4	130.85.6.20	130.85.80.107
130.85.111.44	130.85.153.86	130.85.21.155	130.85.30.5	130.85.6.30	130.85.80.121
130.85.111.46	130.85.153.87	130.85.21.2	130.85.30.6	130.85.6.33	130.85.80.126
130.85.111.47	130.85.153.88	130.85.21.20	130.85.30.65	130.85.6.38	130.85.80.129
130.85.111.48	130.85.153.89	130.85.21.21	130.85.30.66	130.85.6.42	130.85.80.138
130.85.111.51	130.85.153.90	130.85.21.23	130.85.30.7	130.85.6.46	130.85.80.148
130.85.111.64	130.85.153.91	130.85.21.24	130.85.30.8	130.85.6.48	130.85.80.161
130.85.111.65	130.85.153.92	130.85.21.3	130.85.30.81	130.85.6.49	130.85.80.163
130.85.111.72	130.85.153.93	130.85.21.39	130.85.30.82	130.85.6.61	130.85.80.202
130.85.111.73	130.85.153.95	130.85.21.4	130.85.30.83	130.85.6.62	130.85.80.209
130.85.111.84	130.85.153.96	130.85.21.40	130.85.30.84	130.85.6.63	130.85.80.219
130.85.112.1	130.85.153.97	130.85.21.42	130.85.30.85	130.85.6.7	130.85.80.220
130.85.112.150	130.85.156.1	130.85.21.43	130.85.30.86	130.85.60.1	130.85.80.221
130.85.112.151	130.85.16.105	130.85.21.44	130.85.30.9	130.85.60.11	130.85.80.229
130.85.112.152	130.85.16.113	130.85.21.45	130.85.31.1	130.85.60.14	130.85.80.232
130.85.112.153	130.85.16.13	130.85.21.46	130.85.31.128	130.85.60.16	130.85.80.237
130.85.112.156	130.85.16.241	130.85.21.47	130.85.31.129	130.85.60.161	130.85.80.239
130.85.112.179	130.85.16.242	130.85.21.5	130.85.31.130	130.85.60.162	130.85.80.241
130.85.112.180	130.85.16.33	130.85.21.51	130.85.31.131	130.85.60.163	130.85.80.29
130.85.112.186	130.85.16.53	130.85.21.52	130.85.31.132	130.85.60.164	130.85.80.3

130.85.112.187	130.85.16.57	130.85.21.53	130.85.31.133	130.85.60.165	130.85.80.30
130.85.112.190	130.85.16.61	130.85.21.54	130.85.31.134	130.85.60.166	130.85.80.36
130.85.112.199	130.85.16.77	130.85.21.55	130.85.31.135	130.85.60.167	130.85.80.44
130.85.112.205	130.85.16.82	130.85.21.56	130.85.31.136	130.85.60.17	130.85.80.46
130.85.112.215	130.85.16.89	130.85.21.57	130.85.31.137	130.85.60.174	130.85.80.47
130.85.112.216	130.85.16.97	130.85.21.58	130.85.31.138	130.85.60.177	130.85.80.49
130.85.112.22	130.85.161.1	130.85.21.59	130.85.31.139	130.85.60.178	130.85.80.67
130.85.112.228	130.85.161.10	130.85.21.6	130.85.31.14	130.85.60.179	130.85.80.78
130.85.112.229	130.85.161.11	130.85.21.60	130.85.31.140	130.85.60.18	130.85.80.88
130.85.112.230	130.85.161.12	130.85.21.61	130.85.31.141	130.85.60.180	130.85.81.1
130.85.112.30	130.85.161.13	130.85.21.62	130.85.31.142	130.85.60.181	130.85.81.101
130.85.112.32	130.85.161.14	130.85.21.63	130.85.31.143	130.85.60.182	130.85.81.103
130.85.12.1	130.85.161.2	130.85.21.64	130.85.31.144	130.85.60.183	130.85.81.104
130.85.12.6	130.85.161.23	130.85.21.65	130.85.31.145	130.85.60.38	130.85.81.105
130.85.12.7	130.85.161.24	130.85.21.66	130.85.31.146	130.85.60.39	130.85.81.107
130.85.120.1	130.85.161.25	130.85.21.67	130.85.31.147	130.85.60.40	130.85.81.109
130.85.121.1	130.85.161.27	130.85.21.68	130.85.31.148	130.85.60.6	130.85.81.110
130.85.130.1	130.85.161.28	130.85.21.69	130.85.31.149	130.85.60.7	130.85.81.123
130.85.136.17	130.85.161.29	130.85.21.7	130.85.31.15	130.85.60.81	130.85.81.14
130.85.136.18	130.85.161.3	130.85.21.71	130.85.31.150	130.85.60.82	130.85.81.18
130.85.147.129	130.85.161.30	130.85.21.72	130.85.31.151	130.85.60.83	130.85.81.247
130.85.147.131	130.85.161.31	130.85.21.74	130.85.31.152	130.85.60.9	130.85.81.80
130.85.147.132	130.85.161.32	130.85.21.79	130.85.31.153	130.85.62.1	130.85.81.81
130.85.147.133	130.85.161.33	130.85.21.82	130.85.31.154	130.85.62.16	130.85.81.91
130.85.147.134	130.85.161.34	130.85.21.83	130.85.31.155	130.85.62.17	130.85.81.98
130.85.82.121	130.85.82.15	130.85.65.1	130.85.82.113	130.85.82.1	130.85.81.99
130.85.98.35	130.85.97.36	130.85.97.17	130.85.9.1	130.85.84.192	130.85.82.18
130.85.98.66	130.85.97.37	130.85.97.177	130.85.9.9	130.85.84.193	130.85.82.2
130.85.98.78	130.85.97.40	130.85.97.18	130.85.97.1	130.85.84.194	130.85.82.27
130.85.98.80	130.85.97.43	130.85.97.180	130.85.97.100	130.85.84.196	130.85.82.46
130.85.98.92	130.85.97.45	130.85.97.181	130.85.97.101	130.85.84.197	130.85.82.55
130.85.99.1	130.85.97.49	130.85.97.184	130.85.97.102	130.85.84.198	130.85.82.60
130.85.99.120	130.85.97.50	130.85.97.185	130.85.97.103	130.85.84.202	130.85.82.70
130.85.99.130	130.85.97.52	130.85.97.199	130.85.97.104	130.85.84.203	130.85.82.72
130.85.99.150	130.85.97.55	130.85.97.20	130.85.97.105	130.85.84.204	130.85.82.8
130.85.99.37	130.85.97.57	130.85.97.202	130.85.97.107	130.85.84.206	130.85.82.88
130.85.99.38	130.85.97.61	130.85.97.205	130.85.97.108	130.85.84.208	130.85.82.97
130.85.99.42	130.85.97.62	130.85.97.21	130.85.97.111	130.85.84.210	130.85.82.98
130.85.147.135	130.85.97.66	130.85.97.211	130.85.97.117	130.85.84.212	130.85.83.1
130.85.147.136	130.85.97.67	130.85.97.213	130.85.97.12	130.85.84.214	130.85.83.103
130.85.147.137	130.85.97.68	130.85.97.215	130.85.97.122	130.85.84.216	130.85.83.21
130.85.147.138	130.85.97.69	130.85.97.217	130.85.97.129	130.85.84.219	130.85.83.70
130.85.147.139	130.85.97.70	130.85.97.218	130.85.97.132	130.85.84.221	130.85.83.88
130.85.161.4	130.85.97.71	130.85.97.219	130.85.97.137	130.85.84.222	130.85.83.91
130.85.161.5	130.85.97.73	130.85.97.22	130.85.97.138	130.85.84.223	130.85.83.98
130.85.161.6	130.85.97.74	130.85.97.222	130.85.97.139	130.85.84.225	130.85.84.129
130.85.161.7	130.85.97.75	130.85.97.223	130.85.97.140	130.85.84.226	130.85.84.133
130.85.161.8	130.85.97.77	130.85.97.225	130.85.97.143	130.85.84.227	130.85.84.136

130.85.21.89	130.85.97.78	130.85.97.226	130.85.97.145	130.85.84.229	130.85.84.140
130.85.21.9	130.85.97.79	130.85.97.229	130.85.97.147	130.85.84.230	130.85.84.141
130.85.21.92	130.85.97.81	130.85.97.233	130.85.97.148	130.85.84.233	130.85.84.143
130.85.21.95	130.85.97.83	130.85.97.237	130.85.97.149	130.85.84.234	130.85.84.145
130.85.21.97	130.85.97.84	130.85.97.239	130.85.97.15	130.85.84.235	130.85.84.152
130.85.31.156	130.85.97.87	130.85.97.24	130.85.97.152	130.85.84.236	130.85.84.154
130.85.31.157	130.85.97.88	130.85.97.241	130.85.97.156	130.85.84.239	130.85.84.155
130.85.31.158	130.85.97.93	130.85.97.242	130.85.97.157	130.85.84.241	130.85.84.156
130.85.31.159	130.85.97.94	130.85.97.29	130.85.97.159	130.85.84.243	130.85.84.162
130.85.31.16	130.85.97.95	130.85.97.30	130.85.97.160	130.85.84.244	130.85.84.164
130.85.62.18	130.85.97.98	130.85.97.31	130.85.97.164	130.85.84.245	130.85.84.166
130.85.62.2	130.85.98.1	130.85.97.32	130.85.97.167	130.85.84.246	130.85.84.167
130.85.62.31	130.85.98.33	130.85.97.33	130.85.84.183	130.85.84.253	130.85.84.173
130.85.62.7	130.85.84.191	130.85.84.189	130.85.84.176	130.85.86.129	[redacted]