Global Information Assurance Certification Paper

GIAC Certified Intrusion Analyst (GCIA)
Practical Assignment Version 4.1

Jason D. Gordon
March 2005

Table of Contents

Abstract

This document represents the student's practical assignment for the GIAC Certified Intrusion Analyst (GCIA) certification. The assignment is based on the premise of performing an audit and analysis of a university's intrusion detection logs for a period of three days. Observations and recommendations about the network security of the university are then presented to the university's management.

The University of the Northwest Territories located in Inuvik, Northwest Territories, Canada has contracted Inuk Data Security to audit the university's intrusion detection logs. The university's board of directors is concerned that their network is not as secure as they believe and would like a third party observation of their security position.

The University of the Northwest Territories and Inuk Data Security are fictional organizations used for the purpose of attaching an identity to the events contained in the various log files.

Part I – Executive Summary

This intrusion report is based on the intrusion detection logs provided to Inuk Data Security by the University of the Northwest Territories for the period of April 20 – 22, 2004. The intrusion detection logs did not contain enough information to determine the degree that UNWT systems have been compromised, but does provide enough information to give an idea of the type of traffic passing through the UNWT network, raise some concerns and identify areas for improvement.

Types of traffic

- Typical core infrastructure traffic such as DNS, SMTP, HTTP, HTTPS. This traffic is normal, but these systems should be monitored for attacks as they are some of the first systems that attackers use to compromise networks.
- Internet Relay Chat, online gaming, Peer 2 Peer file sharing. This traffic should raise some flags because many viruses, Trojans, worms and other types of attacks can originate from these networks. Additionally, the UNWT has to be aware of the legal issues regarding the use of file sharing systems on the UNWT network.
- Virus, Worm and Trojan activity. This should be very alarming to the UNWT because several hosts on the UNWT network appear to have been compromised and are attempting to compromise other networks. For example, the Adore/Red Worm has triggered 22% of the entries in the alert logs by itself.
- Host and port scanning is also very prevalent on the UNWT network. While this is becoming more normal most networks, this traffic should be monitored to warn of any students or faculty that are misusing UNWT resources and potentially damaging the reputation of the UNWT.
- Miscellaneous scatter or noise. This type of traffic is indicative of misconfigured systems and should not be ignored completely because proper system administration and resource management are important responsibilities of running a network.
- Other types of scans and attacks. Most of the rest of the traffic could be categorized here. This does not diminish the seriousness of this traffic, and this traffic should also be monitored.

Areas of concern

While no core infrastructure systems appeared to be compromised, several systems appear to have been compromised by Trojans or worms, and given that the UNWT has not yet subscribed to defense in depth methodologies of mitigation, it is only a matter of time before there is a serious electronic incident at the UNWT.

The UNWT understandably has an open philosophy regarding enforcing network usage policies, but given the direction that other networks are taking in this era of the hostile

Internet, the UNWT has to take more proactive steps of protecting its core infrastructure systems and be a good Internet citizen. It is not necessary for the UNWT to adopt a "deny all, except that which is explicitly permitted" security policy, but just allowing users to do whatever they want with UNWT resources is not acceptable and would probably be a liability legally.

Areas for improvement

There are several areas that the UNWT should work towards that can improve network security and make intrusion detection more meaningful and easier to manage.

The UNWT intrusion detection system should be upgraded to the most current stable version and the rule set should be kept up to date as well. The intrusion detection system is generating too many alerts for UNWT analysts to keep up with and make meaningful analysis of the data. Additionally, the intrusion detection system is generating far too many false positives because there are too many custom signatures that are configured to alert on any traffic to several hosts. These false positives accounted for approximately 46% of all entries in the alert logs.

The UNWT will have to review the placement of the intrusion detection systems and work towards creating log fusion with firewall, router, mail and web access logs. This will help the analysts see the UNWT network from a 40,000 foot view and will pay great dividends in the end. Security will not be the only improvement if the UNWT is aware of all traffic on the network; improvements in performance and bandwidth utilization will also be realized. This will be a sense of pride for UNWT administrators and the UNWT should put strong emphasis on this immediately.

There were no TCPDUMP audit trails available to use for corroboration. This is something that the UNWT administrators should also consider implementing in some form. At a minimum, the intrusion detection system should be configured to also log in binary mode because this will dump the packets that trigger the alerts.

Conclusion

The UNWT is no different than other organizations and universities in the respect that they are only now realizing that responsibility must be taken when connecting systems to the Internet and that they must be aware of what their users are doing and what types of traffic is passing through their networks. The UNWT reputation is important and if a major Internet incident were to originate from the UNWT network because of negligence, the repercussions would take a long time to recover from.

Part II – Detailed Analysis

2.1 – Log files

The UNWT requested that log files generated by their intrusion detection system from April 20 to April 22, 2004 be audited and analyzed. The log files were generated by the Snort Intrusion Detection System. Based on the output of the alert files, it is believed that the version of Snort that the UNWT is running is probably 1.8[1] or earlier. The log files were downloaded from http://isc.incidents.org/logs and are detailed in the following table.

The file types that were audited and analyzed were Snort alert, scan and OOS (Out of Specification) log files. The alert files are generated when running Snort in NIDS mode and are in ASCII format. Based on the format of the alert files, it is obvious that the UNWT is logging their alerts in fast mode. The scan files are generated when the portscan preprocessor is used in the snort.conf file. Based on the format of the scan files, it is assumed that the UNWT is using Snort's older portscan preprocessor. The OOS files contain detailed entries for datagrams that do not conform to the RFC standards.

Each of the log files were corrupt to varying degrees and contained other oddities such as the timestamp jumping back and forth in several locations. Several other analysts have suggested that the issue with the timestamp is likely caused by multiple Snort instances writing to the same log files[2]. Each of the alert files contained entries up to approximately 7 minutes past midnight of the next day. It is assumed that this is an issue with the size of the files and time the log rotation starts being too close to the start of the next day. The timestamps within the OOS files do not correspond with the dates of the actual files. It is not exactly known why this has occurred.

Table 2.1.1 contains the files used, their respective sizes and line counts. It should be noted that the line counts are reflective of the analyst's manual corrections.

Table 2.1.1

Alert	Size	Lines	Scan	Size	Lines	OOS	Size	Lines
alert.040420	14M	112,300	scans.040420	130M	2,042,776	oos_report_040416	344K	7,952
alert.040421	27M	221,443	scans.040421	260M	4,103,067	oos_report_040417	320K	7,406
alert.040422	26M	217,318	scans.040422	183M	2,950,648	oos_report_040418	1.7M	5,559

2.2 – Topology

[1] SANS Intrusion Detection In Depth 3.5/3.6, Page B-13
[2] Credit to Brett Hutley, http://www.giac.org/certified_professionals/practicals/gcia/0775.php

The UNWT has the Class B address space of MY.NET.0.0/16 and appears to have segmented their network into several semi-contiguous Class C subnets. There are 15,747 unique MY.NET.x.x addresses in 85 Class C subnets in all the alert, scan and OOS files, with an average of 185 hosts per subnet. However, since some of the addresses are illegal addresses, it is estimated that there are actually 15,577 valid hosts with an average of 183 hosts per subnet.

The alerts files contained 734 unique hosts in 76 different subnets. On average, there are 9.6 hosts per subnet and there is an average of 149.6 alerts generated per subnet. There are 2 subnets that have 50 or more hosts, and there are 10 subnets that have 20 or more hosts. The subnets with the fewest hosts contained 1 host, and the subnet with the highest number of hosts contained 70 hosts.

Table 2.2.1 details the 76 subnets contained in the alerts files. Columns 2, 3 and 4 detail the number of hosts, alerts and average number of alerts per host. Columns 5 and 6 indicate whether the hosts from MY.NET.x.x were the source or destination of the triggering alerts, and the number of occurrences in each direction.

Table 2.2.1

Subnet	Hosts	Alerts	Average	Source	Destination
MY.NET.1.0	9	486	54.0	0	486
MY.NET.2.0	4	11	2.8	0	11
MY.NET.4.0	1	4	4.0	0	4
MY.NET.5.0	14	708	50.6	95	613
MY.NET.6.0	6	141	23.5	5	136
MY.NET.7.0	4	11	2.8	0	11
MY.NET.9.0	4	259	64.8	0	259
MY.NET.10.0	9	88	9.8	4	84
MY.NET.11.0	10	4453	445.3	4407	46
MY.NET.12.0	5	442	88.4	65	377
MY.NET.13.0	3	6	2.0	0	6
MY.NET.14.0	3	8	2.7	0	8
MY.NET.15.0	7	108	15.4	1	107
MY.NET.16.0	3	4	1.3	0	4
MY.NET.17.0	9	1139	126.6	14	1125
MY.NET.18.0	7	75	10.7	0	75
MY.NET.20.0	1	1	1.0	0	1
MY.NET.21.0	2	6	3.0	0	6
MY.NET.22.0	8	31	3.9	0	31
MY.NET.24.0	20	962	48.1	242	720
MY.NET.25.0	13	576	44.3	347	229
MY.NET.27.0	60	380	6.3	1	379
MY.NET.29.0	8	499	62.4	71	428
MY.NET.30.0	5	40194	8038.8	3	40191

MY.NET.31.0	7	365	52.1	0	365
MY.NET.32.0	37	1645	44.5	0	1645
MY.NET.34.0	4	184	46.0	96	88
MY.NET.40.0	1	41	41.0	0	41
MY.NET.41.0	1	3	3.0	0	3
MY.NET.42.0	4	5	1.3	0	5
MY.NET.43.0	16	11691	730.7	5887	5804
MY.NET.53.0	28	952	34.0	26	925
MY.NET.54.0	1	1	1.0	0	1
MY.NET.55.0	4	6	1.5	0	6
MY.NET.60.0	8	195	24.4	19	176
MY.NET.62.0	3	67	22.3	3	64
MY.NET.64.0	3	6	2.0	0	6
MY.NET.65.0	2	117	58.5	0	117
MY.NET.66.0	6	27	4.5	3	24
MY.NET.69.0	27	4817	178.4	3003	1814
MY.NET.70.0	30	2241	74.7	715	1526
MY.NET.71.0	5	253	50.6	123	130
MY.NET.75.0	11	489	44.5	381	108
MY.NET.80.0	26	98	3.8	25	73
MY.NET.81.0	4	722	180.5	1	721
MY.NET.82.0	16	890	55.6	194	696
MY.NET.83.0	5	347	69.4	0	347
MY.NET.84.0	14	430	30.7	36	394
MY.NET.86.0	1	1	1.0	0	1
MY.NET.97.0	70	4426	63.2	23	4403
MY.NET.98.0	7	57	8.1	8	49
MY.NET.99.0	7	102	14.6	0	102
MY.NET.100.0	4	9	2.3	0	9
MY.NET.101.0	2	2	1.0	0	2
MY.NET.102.0	4	5	1.3	0	5
MY.NET.103.0	1	2	2.0	0	2
MY.NET.109.0	5	240	48.0	92	148
MY.NET.110.0	8	166	20.8	0	166
MY.NET.111.0	22	1050	47.7	193	857
MY.NET.112.0	15	759	50.6	20	739
MY.NET.120.0	1	5	5.0	0	5
MY.NET.121.0	2	4	2.0	0	4
MY.NET.130.0	1	2	2.0	0	2
MY.NET.147.0	9	39	4.3	0	39
MY.NET.149.0	1	2	2.0	0	2
MY.NET.150.0	27	989	36.6	553	436
MY.NET.151.0	10	167	16.7	5	162
MY.NET.152.0	8	44	5.5	40	4
MY.NET.153.0	27	2531	93.7	960	1571
MY.NET.156.0	1	2	2.0	0	2
MY.NET.165.0	3	7	2.3	0	7
MY.NET.185.0	5	12	2.4	0	12
MY.NET.186.0	1	1	1.0	0	1
MY.NET.189.0	3	78	26.0	3	75

MY.NET.190.0	7	220	31.4	40	180
MY.NET.191.0	3	46	15.3	0	46

Based on the analysis of the traffic direction, ports and number of occurrences of the alerts, and the premise that most attackers know what they are looking for, the inferred roles of core network services is detailed in Table 2.2.2

Table 2.2.2

Service	**Hosts**
DNS	MY.NET.1.3 MY.NET.1.4
SMTP	MY.NET.12.6
WWW	MY.NET.24.34 MY.NET.34.11 MY.NET.24.44 MY.NET.5.44
FTP	MY.NET.24.47 MY.NET.24.27
HelpDesk	MY.NET.53.29 MY.NET.70.49 MY.NET.70.50
Novell iFolder/Web Storage[3]	MY.NET.30.4 MY.NET.30.3

It is important to note that the identification of the above network services is based on inference and educated guesses, and that actual qualification should be made by a UNWT network administrator.

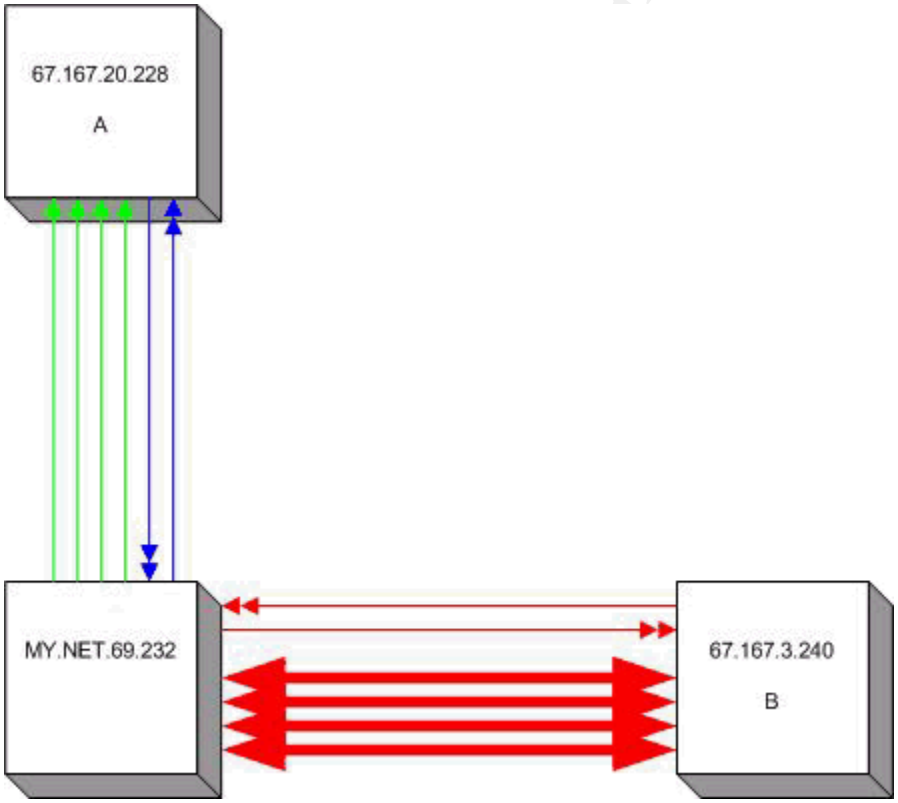
2.3 – Link Graph

The link graph below will help visualize the Adore/Red Worm being propagated within the UNWT network. In the sample log files below, the first three entries are from the scans file and remaining entries are from the alert file. What is seen are 3 UDP scans from MY.NET.69.232 to 67.167.20.228, next two TFTP alerts are triggered, followed by several Red Worm alerts from 67.167.3.240 to MY.NET.69.232. Next these two hosts generate several thousand Adore/Red Worm alerts in both directions.

Apr 21 20:04:11 MY.NET.69.232:2894 -> 67.167.20.228:4309 UDP
Apr 21 20:08:39 MY.NET.69.232:2894 -> 67.167.20.228:4309 UDP
Apr 21 20:20:42 MY.NET.69.232:2894 -> 67.167.20.228:4309 UDP
04/21-20:25:00.524278 [**] TFTP - Internal UDP connection to external tftp server [**] 67.167.20.228:69 -> MY.NET.69.232:2894

[3] Educated guess based on comments in http://www.novell.com/coolsolutions/qna/8443.html

04/21-20:25:00.525036 [**] TFTP - Internal UDP connection to external tftp server [**] MY.NET.69.232:2894 -> 67.167.20.228:69
04/21-20:30:21.459264 [**] High port 65535 tcp - possible Red Worm - traffic [**] 67.167.3.240:65535 -> MY.NET.69.232:2894
04/21-20:30:21.459885 [**] High port 65535 tcp - possible Red Worm - traffic [**] MY.NET.69.232:2894 -> 67.167.3.240:65535
04/21-20:30:21.508484 [**] High port 65535 tcp - possible Red Worm - traffic [**] 67.167.3.240:65535 -> MY.NET.69.232:2894
04/21-20:30:21.558389 [**] High port 65535 tcp - possible Red Worm - traffic [**] 67.167.3.240:65535 -> MY.NET.69.232:2894
04/21-20:30:21.603449 [**] High port 65535 tcp - possible Red Worm - traffic [**] 67.167.3.240:65535 -> MY.NET.69.232:2894
04/21-20:30:21.656869 [**] High port 65535 tcp - possible Red Worm - traffic [**] MY.NET.69.232:2894 -> 67.167.3.240:65535
04/21-20:30:21.656913 [**] High port 65535 tcp - possible Red Worm - traffic [**] MY.NET.69.232:2894 -> 67.167.3.240:65535



3.1 – Overview of Detects

3.1.1 – Alerts

There were 50 unique events that generated 87,276 alerts[4]. Table 3.1.1.1 details each of

the alerts and their frequency.

Table 3.1.1.1

Frequency	Alert Description
30844	MY.NET.30.4 activity
19253	High port 65535 tcp - possible Red Worm - traffic
11174	EXPLOIT x86 NOOP
9269	MY.NET.30.3 activity
5979	SMB Name Wildcard
4387	Tiny Fragments - Possible Hostile Activity
2357	RFB - Possible WinVNC - 010708-1
1728	Null scan!
627	NMAP TCP ping!
374	Possible trojan server activity
243	SUNRPC highport access!
145	DDOS shaft client to handler
106	High port 65535 udp - possible Red Worm - traffic
98	UMBC NIDS IRC Alert IRC user /kill detected
97	TCP SMTP Source Port traffic
77	TCP SRC and DST outside network
67	Incomplete Packet Fragments Discarded
60	FTP passwd attempt
57	UMBC NIDS IRC Alert Possible sdbot floodnet detected attempting to IRC
43	ICMP SRC and DST outside network
40	SMB C access
31	TFTP - Internal UDP connection to external tftp server
23	External RPC call
18	EXPLOIT x86 setgid 0
17	UMBC NIDS IRC Alert Possible drone command detected.
16	TFTP - External TCP connection to internal tftp server
16	EXPLOIT x86 setuid 0
15	NIMDA - Attempt to execute cmd from campus host
15	FTP DoS ftpd globbing
13	DDOS mstream client to handler
9	UMBC NIDS IRC Alert XDCC client detected attempting to IRC
9	EXPLOIT NTPDX buffer overflow
8	UMBC NIDS Internal MiMail alert
8	UMBC NIDS External MiMail alert
7	IRC evil - running XDCC
6	UMBC NIDS IRC Alert Possible Incoming XDCC Send Request Detected.
6	TFTP - Internal TCP connection to external tftp server
6	Attempted Sun RPC high port access
4	EXPLOIT x86 stealth noop
4	DDOS mstream handler to client
4	connect to 515 from inside
3	SYN-FIN scan!
2	Probable NMAP fingerprint attempt

[4] Scans are accounted for separately

2	NETBIOS NT NULL session
1	Traffic from port 53 to port 123
1	TFTP - External UDP connection to internal tftp server
1	External FTP to HelpDesk MY.NET.70.50
1	External FTP to HelpDesk MY.NET.70.49
1	External FTP to HelpDesk MY.NET.53.29
1	Back Orifice

17,699 alerts originated from the UNWT network and the remaining 69,445 alerts originated from external networks. 130 hosts within the UNWT network generated an outbound alert, and the top 6 hosts accounted for 77% of all outbound alerts. It should also be noted that these top 6 hosts also belonged to the overall Top 20 Source IP's. 9,227 of the alerts were generated by the "High port 65535 tcp – possible Red Worm – traffic" signature. 4,337 alerts were generated by the "SMB Name Wildcard" signature and 1 alert was generated by the "TFTP – Internal UDP connection to external tftp server" signature. Table 3.1.1.2 details the top 6 source hosts and triggering signatures.

Table 3.1.1.2

Alerts	Host	Signature
3230	MY.NET.43.8	100% High port 65535 tcp -possible Red Worm - traffic
3108	MY.NET.11.4	100% SMB Name Wildcard
2990	MY.NET.69.232	99% tcp Red Worm, 1 tftp internal to external event
2124	MY.NET.43.13	100% High port 65535 tcp -possible Red Worm - traffic
1229	MY.NET.11.7	100% SMB Name Wildcard
883	MY.NET.153.81	100% High port 65535 tcp -possible Red Worm - traffic

This information is important because it is indicative of probable Internet worm propagation, misconfigured network systems and probable compromise. The "High port 65535 tcp – possible Red Worm – traffic" alerts are probably generated by Adore/Red Worm traffic. This particular worm affects vulnerable Linux systems and has also spread to other universities consuming significant bandwidth[5]. The "SMB Name Wildcard" alerts are probably misconfigured Windows hosts trying to register themselves or make themselves known to other Windows hosts. This can be inferred because one of the hosts generating these alerts was trying to connect from port 137 to port 137 on only one destination host and there was no evidence of incoming scans to this host during these three days. The other host generating these alerts was trying to connect to port 137 on hosts in the Automatic Private IP Address (APIPA) space[6]. The "TFTP – Internal UDP connection to external tftp server" is indicative of some sort of compromise because many worms or malware will use the TFTP protocol to further propagate itself.
688 different hosts were the destination recipients in the remaining 69,445 alerts. The top 6 UNWT destination hosts accounted for 71% of the alerts. It should be noted that these top 6 hosts also belong to the overall Top 20 Destination IP's. 40,101 of the alerts were generated by two custom Snort rules that appear to trigger alerts for any activity to the

[5] http://linux0.cs.uaf.edu/archive31Jul01/msg00102.html
[6] http://wiki.ethereal.com/APIPA

MY.NET.30.4 and MY.NET.30.3 hosts. Obviously these two hosts are important to the UNWT, but because the Snort rule appears to trigger on any activity, there is an extremely high degree for false positives with these alerts. The "Tiny Fragments – Possible Hostile Activity" signature generated 3,628 alerts. These alerts were likely generated using nmap and are an evasive scan that is typically used to fool older firewalls or firewalls that do simple packet filtering[7]. The "Null scan!" signature is also likely generated by nmap. Table 3.1.1.3 details the 6 hosts and triggering signatures.

Table 3.1.1.3

Alerts	Host	Signature
30833	MY.NET.30.4	100% "MY.NET.30.4 activity"
9270	MY.NET.30.3	99.9% "MY.NET.30.3 activity", 2 "NMAP TCP ping"
3429	MY.NET.43.8	100% "High port 65535 tcp - possible Red Worm - traffic
2160	MY.NET.97.43	91% "Tiny Fragments", 8.5% "Null scan!", 1 "SYN-FIN scan!", 1 "EXPLOIT x86 NOOP"
2099	MY.NET.43.13	100% "High port 65535 tcp - possible Red Worm - traffic
1803	MY.NET.97.55	91% "Tiny Fragments", 8% "Null scan!", 4 "SUNRPC highport access!"

Interestingly, this list does not include the third overall largest number of alerts; the "EXPLOIT x86 NOOP" signature. This signature did not make the top 6 list because it is spread out over 502 different hosts on the UNWT network, and each host generated an average of 22 alerts. Host MY.NET.43.8 is both a top source and destination for "High port 65535 tcp – possible Red Worm" alerts, and is almost assuredly compromised with the Adore/Red Worm. The rest of the top 6 alerts are either the result of scanning using crafted packets or in the case of the two servers on the MY.NET.30.0 subnet, noise.

3.1.2 – Scans

Throughout the 3 days, there were 9,106,295 scans recorded. Although 13 different scan types were detected, SYN and UDP scans accounted for 99.78% of all scans. FIN scans accounted for 0.08% of the scans and the remaining scans were comprised of different stealth scans that craft various properties of the packets. Table 3.1.2.1 details the detected scans. Columns 3 and 4 detail the number of scans that originated or terminated within the UNWT network and columns 5 and 6 indicate the number of source and destination UNWT hosts that participated in the scans.

Table 3.1.2.1

Scans	Scan Type	Sources	Destination	Src Hosts	Dst Hosts
5298782	SYN	4739848	558981	156	15746
3787865	UDP	3785006	2874	76	266

[7] SANS Introduction to Logfile Analysis, Page A-25

6971	FIN	3695	3276	12	52
800	NULL	4	796	2	44
739	UNKNOWN	45	694	4	417
578	NOACK	0	578	0	43
492	INVALIDACK	0	492	0	74
157	VECNA	0	157	0	32
43	XMAS	0	43	0	11
18	FULLXMAS	0	18	0	6
12	SPAU	0	12	0	7
7	NMAPID	0	7	0	5
7	SYNFIN	0	7	0	4

Hosts MY.NET.1.4 and MY.NET.1.3 are responsible for 38.5% of the outbound scans. These hosts are almost certainly the UNWT DNS servers, and the UDP scans that they are triggering are most likely valid DNS traffic. Reverse DNS lookups on the destination addresses proves that the destination hosts are valid DNS servers.

8 of the top 10 source hosts are responsible for approximately 48% of the outbound scans. The majority of these scans have the characteristics of Trojan, worm, online gaming and P2P file sharing traffic. Table 3.1.2.2 details the top 10 source hosts and the number of scans.

Table 3.1.2.2

Scans	Host
2536677	MY.NET.1.3
1179156	MY.NET.17.45
747940	MY.NET.1.4
713579	MY.NET.112.189
694877	MY.NET.81.39
553272	MY.NET.112.193
447524	MY.NET.84.186
291773	MY.NET.43.10
122802	MY.NET.53.225
114201	MY.NET.69.210

The inbound scans are spread out across 15,765 destination addresses and because of this, the top 10 destination hosts only comprise 9% of the total ingress scans. Table 3.1.2.3 details the top 10 destination hosts and the number of scans.

Table 3.1.2.3

Scans	Host

22003	MY.NET.97.65
14510	MY.NET.97.159
4933	MY.NET.66.30
1945	MY.NET.12.6
1793	MY.NET.97.93
1768	MY.NET.18.25
1768	MY.NET.112.204
1265	MY.NET.6.7
684	MY.NET.97.73
539	MY.NET.97.52

Curiously, there are 1,245 scans to host MY.NET.12.6, which is believed to be one of the UNWT mail servers. The traffic triggering these alerts is most likely valid SMTP traffic because reverse DNS lookups of the source hosts reveal that the majority are valid mail servers. It is possible that these alerts were triggered because of the ECN bits being set, but this needs further investigation.

3.1.3 – OOS

There were 2,972 Out Of Specification packets generated by 57 unique UNWT hosts. 3 source hosts are responsible for 25 outbound OOS packets and 56 destination hosts are responsible for the remaining 2947 OOS packets. Table 3.1.3.1 details the source hosts that generated OOS packets and table 3.1.3.2 details the top 10 destinations hosts that generated OOS packets.

Table 3.1.3.1

OOS	Host
21	MY.NET.12.6
3	MY.NET.12.4
1	MY.NET.17.30

Table 3.1.3.2

OOS	Host
1001	MY.NET.6.7
944	MY.NET.12.6
137	MY.NET.24.44
126	MY.NET.71.246
117	MY.NET.5.67
96	MY.NET.43.5
63	MY.NET.34.14
60	MY.NET.24.34
56	MY.NET.34.11

45	MY.NET.12.4

3.2 – Detects

3.2.1 – Detect 1: High port 65535 tcp – possible Red Worm - traffic

- Description of detect

The Adore/Red Worm is a worm that affects Linux systems by attacking vulnerabilities in rpc.statd, bind, LPRng and wuftpd26.

The following description is taken directly from http://www.sans.org/y2k/adore.htm

"Adore is a worm that we originally called the Red Worm. It is similar to the Ramen and Lion worms. Adore scans the Internet checking Linux hosts to determine whether they are vulnerable to any of the following well-known exploits: LPRng, rpc-statd, wu-ftpd and BIND. LPRng is installed by default on Red Hat 7.0 systems. From the reports so far, Adore appears to have started its spread on April 1.

Adore worm replaces only one system binary (ps), with a trojaned version and moves the original to /usr/bin/adore. It installs the files in /usr/lib/lib . It then sends an email to the following addresses: adore9000@21cn.com, adore9000@sina.com, adore9001@21cn.com, adore9001@sina.com Attempts have been made to get these addresses taken offline, but no response so far from the provider. It attempts to send the following information:

- */etc/ftpusers*
- *ifconfig*
- *ps -aux (using the original binary in /usr/bin/adore)*
- */root/.bash_history*
- */etc/hosts*
- */etc/shadow*

Adore then runs a package called icmp. With the options provided with the tarball, it by default sets the port to listen too, and the packet length to watch for. When it sees this information it then sets a rootshell to allow connections. It also sets up a cronjob in cron daily (which runs at 04:02 am local time) to run and remove all traces of its existence and then reboots your system. However, it does not remove the backdoor." – SANS Institute

- Reason this detect was selected

The Adore/Red Worm detect was selected because 19,253 alerts were generated between 100 source IP's and 124 destination IP's. This signature caused the number 2 overall amount of alerts to be generated, and is arguably number 1 because the overall top alert is more than likely a false positive. Several other universities have stated that this worm has consumed considerable amounts of their network bandwidth; this is a concern because if too many machines on the UNWT network become compromised, the UNWT network bandwidth will surely suffer.

5 of the top 10 source hosts generating these alerts are hosts on the UNWT network and account for 49% of all alerts. 4 of the top 10 destination hosts generating these alerts are hosts on the UNWT network and account for 44% of all alerts. 4 of these hosts are on both the source and destination lists and are most certainly compromised because they are also generating many signatures in the scan files.

Since this worm attacks some common Linux services, the UNWT has to be concerned that none of their critical servers become compromised. The chance for denial of service, loss of data and loss of reputation to the UNWT is high.

- Detect was generated by

This detect was generated by a custom Snort rule written by the UNWT system administrators. There was a signature for both TCP and UDP, however all documentation regarding the Adore worm indicates that it uses TCP only[8], so it is likely that the following reconstructed Snort signature is likely similar to the signature used by the UNWT Snort IDS.

```
alert tcp $EXTERNAL_NET any <> $HOME_NET 65535 (msg: " High port 65535 \ tcp
– possible Red Worm – traffic";
```

This signature will alert on traffic to or from TCP port 65535 in any direction between the UNWT network and any external network and will log the message "High port 65535 tcp – possible Red Worm – traffic". The alerts are logged in Snort's Fast Mode and contain minimal information such as timestamp, signature, source host/port and destination host/port. The following is an example of the Adore/Red Worm alerts that were generated.

```
04/22-01:37:03.210282  [**] High port 65535 tcp - possible Red Worm - traffic [**]
MY.NET.43.8:3883 -> 64.12.24.35:65535
04/22-01:37:03.538440  [**] High port 65535 tcp - possible Red Worm - traffic [**]
MY.NET.43.8:3883 -> 64.12.24.35:65535
04/22-01:37:05.943031  [**] High port 65535 tcp - possible Red Worm - traffic [**]
MY.NET.43.8:3883 -> 64.12.24.35:65535
```

[8] http://isc.sans.org/port_details.php?port=65535

04/22-01:37:09.147722 [**] High port 65535 tcp - possible Red Worm - traffic [**] MY.NET.43.8:3883 -> 64.12.24.35:65535

- Probability the source address was spoofed

The source addresses in these alerts were probably not spoofed given the requirement of the TCP three-way handshake. Several of these alerts were generated by hosts within the UNWT network are almost certainly not spoofed given that these hosts belong to the UNWT, but firewall and router logs should be used to further corroborate this. Source hosts external to the UNWT network probably are not even aware that they have been compromised by the Adore/Red Worm and would therefore not purposely spoof their addresses.

- Attack mechanism

This compromise was successful because the worm scans random Class B networks looking for vulnerable systems to attack. The UNWT is not doing sufficient traffic management at the network borders and any Linux hosts on the UNWT network that were vulnerable to the Adore worm would have been compromised. When the worm was first discovered, most of the affected Linux systems were Red Hat 7 systems that were configured with the default configuration.

- Correlations

The Adore/Red Worm was originally discovered as a variant of other Linux worms as detailed on the following site: https://ucsb.edu/pipermail/security-linux/2001-April/000121.html

There is no specific CVE for the Adore/Red Worm, but the CVE entries for the Linux vulnerabilities that Adore attacks are as follows[9]:

CVE-2000-0666: rpc.statd - http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2000-0666
CVE-2000-0917: LPRng - http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2000-917
CVE-2001-0010: BIND 8 - http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2001-0010
CVE-2001-0011: BIND 4 - http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2001-0011
CVE-2000-0573: wu-ftpd - http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2000-0573

- Evidence of active targeting

[9] Credit to Brett Hutley, http://www.giac.org/certified_professionals/practicals/gcia/0775.php

There is no evidence of the active targeting of hosts on the UNWT network because the Adore/Red Worm propagates itself by scanning random Class B networks looking for vulnerable hosts to attack[10].

- Severity

The following formula is used to calculate the severity of this detect in relation to the UNWT network:

Severity = (criticality + lethality) – (system countermeasures + network countermeasures)

Severity = (4 + 4) – (0 + 1)

On a scale of 1 – 10, this alert rates a 7. The criticality is scored at 4 because no core systems appear to be compromised yet, but the bandwidth is a core resource and is likely suffering because of the traffic. The lethality is scored at 4 because this worm has successfully propagated to the UNWT network, but there are patches and other countermeasures available to correct this. System countermeasures scored 0 because these hosts apparently are not patched and are not running personal firewalls. Network countermeasures scored 1 because even though no countermeasures have been taken, it is easy to block this traffic with ingress or egress filtering.

3.2.2 – Detect 2: Tiny Fragments – Possible Hostile Activity

- Description of detect

The "Tiny Fragments" attack or scan occurs when an attacker sends fragmented packets to a host for the purpose of evading firewalls or intrusion detection systems. This works because many IDS' and firewalls have known issues with reassembling fragmented IP datagrams and can be tricked into missing this type of attack or scan[11]. Fragmentation attacks are usually for the purpose of denial of service and there are many tools available such as nmap and fragrouter that can craft fragmented IP packets.

- Reason this detect was selected

This detect was selected because SANS instructs analysts to treat any incoming fragmentation as suspicious, and the MTU on the UNWT backbone should be large enough that fragmentation would not be required. This would make any ingress fragmentation suspicious by default[12]. However, the main reason that this detect was selected was because host MY.NET.12.6 was one of the targets, and this host is one of the UNWT mail servers, which is obviously one of the UNWT critical systems.

[10] http://www.europe.f-secure.com/v-descs/adore.shtml
[11] http://www.snort.org/snort-db/sid.html?sid=522
[12] http://marc.theaimsgroup.com/?l=snort-users&m=97089915603238&w=2

© SANS Institute 2000 - 2005 Author retains full rights.

4,384 alerts were generated by 3 external hosts to 14 UNWT destination hosts.

- Detect was generated by

This detect was generated by a customized version of Snort signature 522[13].

```
alert ip $EXTERNAL_NET any -> $HOME_NET any (msg:"Tiny Fragments \
Possible Hostile Activity"; dsize:< 25; fragbits:M;)
```

This signature will alert on any IP traffic from an external network on any port to the UNWT network on any port with a datagram size of less than 25 bytes and the more fragments bit set.

The alerts are logged in Snort's Fast Mode and contain minimal information such as timestamp, signature, source host/port and destination host/port. The following is an example of the Tiny Fragments alerts that were generated.

```
04/20-21:50:57.034752  [**] Tiny Fragments - Possible Hostile Activity [**]
61.216.77.135 -> MY.NET.12.6
04/20-21:50:57.074890  [**] Tiny Fragments - Possible Hostile Activity [**]
61.216.77.135 -> MY.NET.12.6
04/20-21:50:57.351302  [**] Tiny Fragments - Possible Hostile Activity [**]
61.216.77.135 -> MY.NET.12.6
04/20-21:50:57.848646  [**] Tiny Fragments - Possible Hostile Activity [**]
61.216.77.135 -> MY.NET.12.6
```

- Probability the source address was spoofed

Whether the source address in these attacks is spoofed or not depends entirely on the purpose of the attacker. Typically if the attacker were to scan a host, the attacker would require a valid IP address to receive the responses; however this isn't necessarily true anymore, as the FTP bounce scan proves.

If the purpose of the Tiny Fragments attack is denial of service, using a valid IP address is not necessary and possibly irrelevant. However, it is also possible that the source host has been compromised and is being used to attack other hosts, and in that case the source IP would be valid depending on the context of source.

- Attack mechanism

This attack succeeded because it is extremely easy to craft fragmented IP datagrams and the UNWT is not doing sufficient traffic management at the Internet borders. If the operating system on the mail server is susceptible to fragment attacks such as the

[13] http://www.snort.org/snort-db/sid.html?sid=522

Teardrop attack, denial of service or worse is possible.

The following paragraph is taken from http://www.insecure.org/nmap/nmap_doc.html#frag and is the author of nmap's description of fragmentation scanning.

> *"Fragmentation scanning : This is not a new scanning method in and of itself, but a modification of other techniques. Instead of just sending the probe packet, you break it into a couple of small IP fragments. You are splitting up the TCP header over several packets to make it harder for packet filters and so forth to detect what you are doing. Be careful with this! Some programs have trouble handling these tiny packets."* – Fyodor, www.insecure.org

- Correlations

Doing a search for fragments on http://www.cve.mitre.org returns several entries for systems that are susceptible to fragment scanning or attacks. 3 entries that deal with Unix hosts, Cisco routers and Linux firewalls have been chosen as examples.

CVE-2001-0710: NetBSD/FreeBSD - http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-0710
CVE-2001-0867: Cisco - http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-0867
CAN-1999-1018: IPChains - http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-1999-1018

- Evidence of active targeting

In addition to the Tiny Fragments scan, host 61.216.77.135 sent several NULL and INVALIDACK scans to host MY.NET.12.6 between 21:38 and 21:50 on 04/20. Host 61.216.77.135 did not communicate with any other UNWT hosts during these three days monitored. It is unclear what host 61.216.77.135 was looking for, but this could be the early warning signs of an attack yet to come because of the location of the source IP and the fact that the destination host is a critical network host.

- Severity

The following formula is used to calculate the severity of this detect in relation to the UNWT network:

> *Severity = (criticality + lethality) – (system countermeasures + network countermeasures)*

Severity = (5 + 4) – (3 + 1)

On a scale of 1 – 10, this alert rates a 5. The criticality is scored at 5 because the mail

servers are critical components to the UNWT, and a compromise of the host would be devastating. The lethality is scored a 4 because it only appears that this traffic is mostly reconnaissance, but denial of service is entirely possible when using crafted packets. System countermeasures are scored at 3 because there is no evidence that this system is not vulnerable to denial of service, but given that other UNWT hosts have been compromised by other worms, it is possible that this host is not patched. Network countermeasures are scored at 1 because there is insufficient ingress filtering being utilized at the UNWT border, but this is easy to rectify.

3.2.3 – Detect 3: FTP DoS ftpd globbing

- Description of detect

The FTP DoS ftpd globbing attack targets FTP servers that have vulnerabilities associated with the glob function.

> *"The glob( ) function searches for all the pathnames matching pattern according to the rules used by the shell."* – Linux Programmer's Manual ($man glob)

This particular attack targets FTP servers running Washington Universities FTP Daemon (wu-ftpd), which is a widely deployed FTP server that runs on Unix and Linux systems. According to this CERT Advisory http://www.cert.org/advisories/CA-2001-33.html there are two remote code execution vulnerabilities that allow attackers to run commands as root on vulnerable WU-FTP servers.

CERT Advisory: CA-2001-33 - http://www.cert.org/advisories/CA-2001-33.html
CERT Advisory: CA-2001-07 - http://www.cert.org/advisories/CA-2001-07.html
US-CERT Vulnerability Note: VU#886083 - http://www.kb.cert.org/vuls/id/886083

- Reason this detect was selected

There were 15 alerts generated by host 221.132.60.134 to host MY.NET.24.27 between 02:05 and 02:13 on 04/21. This external host did not generate any events in the scan or OOS logs and there were curiously no scan events against host MY.NET.24.27 between 21:36 on 04/20 and 04:44 on 04/21. Also interesting is that the external host generated the alerts at two different times. The attacker went away for about 6 minutes then returned and ran the same attack against host MY.NET.24.27. It should be noted that the external host's source port had incremented indicating other traffic to other networks, but perhaps something about host MY.NET.24.27 triggered the attacker's curiosity, thus prompting the return visit.

This particular attack would indicate that the UNWT is probably running WU-FTP servers. This is concerning because the wuftpd service was one of the processes that is vulnerable to the Adore/Red Worm attack. If this host is running a vulnerable wuftpd process, the chances of this host running some of the other vulnerable processes is very

high.

- Detect was generated by

This detect was generated by a custom Snort signature[14].

```
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg: FTP DoS \
ftpd globbing"; flags:A+; content:"~"; content:"{"; content:!"}";)
```

This alert will trigger on any traffic from any external network with any source port to the internal network on TCP port 21 with the ACK bit set, a tilde ~ and an open curly brace { in the request, but not the closing curly brace }. According to Jennifer Allen's description, this will allow most legitimate requests, but requests such as }{ could evade detection.

The alerts are logged in Snort's Fast Mode and contain minimal information such as timestamp, signature, source host/port and destination host/port. The following is an example of the FTP DoS ftpd globbing alerts that were generated.

```
04/21-02:05:51.647333  [**] FTP DoS ftpd globbing [**] 221.132.60.134:19568 ->
MY.NET.24.27:21
04/21-02:05:57.681685  [**] FTP DoS ftpd globbing [**] 221.132.60.134:19568 ->
MY.NET.24.27:21
04/21-02:12:05.234909  [**] FTP DoS ftpd globbing [**] 221.132.60.134:20022 ->
MY.NET.24.27:21
04/21-02:12:08.284460  [**] FTP DoS ftpd globbing [**] 221.132.60.134:20022 ->
MY.NET.24.27:21
```

- Probability the source address was spoofed

The source addresses in these alerts were probably not spoofed given the requirement of the TCP three-way handshake. It should also be noted that the external host's source port had incremented when the attacker returned the second time, indicating a live host that is passing active IP traffic. Given that the external host's source port had not incremented by too much, and only six minutes had passed between connections, it is possible that the attacker was doing something like passing HTTP traffic at the same time, perhaps looking up information on other UNWT systems.

- Attack mechanism

This attack is successful when a user is able to log onto a vulnerable FTP server, including anonymously, and inputs addresses and shellcode using FTP commands. If the attack is successful, the attacker can get the FTP server to execute arbitrary commands with the

[14] Credit to Jennifer Allen, http://www.giac.org/practical/Jenn_Allen_GCIH.doc

© SANS Institute 2000 - 2005 Author retains full rights.

permissions of the wuftpd, usually root. If the attack is unsuccessful the request will fail but the wuftpd service will continue to run, giving the attacker ample opportunity to get the syntax right. See http://www.cert.org/advisories/CA-2001-33.html for more specific information.

- Correlations

There is plenty of information available regarding multiple vulnerabilities with several FTP servers.

CERT Advisory: CA-2001-33 - http://www.cert.org/advisories/CA-2001-33.html
CERT Advisory: CA-2001-07 - http://www.cert.org/advisories/CA-2001-07.html
US-CERT Vulnerability Note: VU#886083 - http://www.kb.cert.org/vuls/id/886083
Solaris Security Digest:
http://www.boran.com/solarisdigest/2001/solaris20010416.html#solaris
Jennifer Allen: GCIH Paper - http://www.giac.org/practical/Jenn_Allen_GCIH.doc
Snort Signature Database: 345 - http://www.snort.org/snort-db/sid.html?sid=345
Network World Fusion - http://www.nwfusion.com/news/2001/1129linftp.html
Covert Labs Security Advisory: COVERT-2001-02 - http://cert.uni-stuttgart.de/archive/bugtraq/2001/04/msg00165.html

- Evidence of active targeting

Prior to the first alert at 02:05 on 04/21, there were no port scans, hosts scans or OOS entries. After the last alert on 02:13 on 04/21 there are no other alerts from host 221.132.60.134. This does not mean that scanning did not occur prior to 04/21 or after 04/22, it just means that within the logs that were made available by the UNWT there is no other activity.

It should be noted that the external host went away for approximately six minutes and then returned for another try at the FTP server on MY.NET.24.27. This is alarming because it can be indicative of the attacker being persistently interested in host MY.NET.24.27.

- Severity

The following formula is used to calculate the severity of this detect in relation to the UNWT network:

Severity = (criticality + lethality) – (system countermeasures + network countermeasures)

Severity = (4 + 4) – (0 + 1)

On a scale of 1 – 10, this alert rates a 7. The criticality is scored at 4 because this host is

not a mission critical system, but if compromised can be used to attack core hosts on the UNWT network. The lethality is scored at 4 because the wuftpd process is likely running as root and this would make further attacks against UNWT hosts damaging if an attacker had root on one of the UNWT's own servers. System countermeasures scored a 0 because this system is likely not patched because the UNWT appears to be behind with patch management. It is also important to note that the Adore/Red Worm attacks vulnerable wuftpd processes, and if those hosts are vulnerable to Adore, they are also likely vulnerable to globbing attacks. Network countermeasures scored at 1 because there appears to be no ingress filtering, but it is easy to implement.

4.1 – Network Statistics

4.1.1 – Top Talkers

- Alerts

Table 4.1.1.1 details the top 5 source IP addresses that were in the alert log files.

Table 4.1.1.1

Alerts	IP	Signatures	Destinations
21788	134.192.42.11	10 signatures	MY.NET.30.4
4742	209.164.32.205	3 signatures	10 destination IP's
3730	68.55.155.26	1 signature	MY.NET.30.4
3243	131.92.177.18	1 signature	MY.NET.30.3
3230	MY.NET.43.8	1 signature	7 destination IP's

It should be noted that 3 of the Top 5 source IP addresses had MY.NET.30.4 and MY.NET.30.3 as the only destination IP address. These two hosts are believed to be some type of Novell file servers and the Snort rule appears to trigger alerts on any traffic to these hosts which is generating a considerable amount of false positives.

Table 4.1.1.2 details the top 5 destination IP addresses that were in the alert log files.

Table 4.1.1.2

Alerts	IP	Signatures	Originating sources
30843	MY.NET.30.4	11 signatures	208 source IP's
9271	MY.NET.30.3	3 signatures	117 source IP's
3430	MY.NET.43.8	2 signatures	7 source IP's
3067	64.12.24.34	1 signature	3 source IP's
2989	67.167.3.240	1 signature	MY.NET.69.232

It should be noted that 2 of the top 5 destination IP addresses were the two Novell file servers that also appear as destination hosts in Table 4.1.1.1. It is very probable that a

high number of these alerts are false positives.

- Scans

Table 4.1.1.3 details the top 5 source IP addresses that were in the scan log files.

Table 4.1.1.3

Scans	IP
2536677	MY.NET.1.3
1179156	MY.NET.17.45
747940	MY.NET.1.4
713579	MY.NET.112.189
694877	MY.NET.81.39

It should be noted that hosts MY.NET.1.3 and MY.NET.1.4 are the UNWT DNS servers and the traffic recorded in the scan logs is most likely valid DNS traffic, and the remaining 3 host's scans contained characteristics of Trojan/worm propagation.

Table 4.1.1.4 details the top 5 destination IP addresses that were in the scan log files.

Table 4.1.1.4

Scans	Host
61275	128.8.10.90
50480	192.26.92.30
50480	128.63.2.53
44901	69.6.25.84
42059	198.41.0.4

It should be noted that all 5 destination IP addresses were hosts that the two DNS servers communicated with, so this is all likely valid DNS traffic and therefore probably all false positives.

- OOS

Table 4.1.1.5 details the top 5 source IP addresses that were in the OOS files.

Table 4.1.1.5

OOS	IP
931	68.54.84.49
133	66.225.198.20
89	128.59.22.253

88	195.38.115.167
82	141.152.34.103

Table 4.1.1.6 details the top 5 destination IP addresses that were in the OOS files.

Table 4.1.1.6

OOS	IP
1001	MY.NET.6.7
944	MY.NET.12.6
137	MY.NET.24.44
126	MY.NET.71.246
117	MY.NET.5.67

It should be noted that top 2 source IP addresses also directly correlate with the top 2 destination IP addresses and the traffic appears to POP3 and SMTP.

4.1.2 – Targeted Services/Ports

Table 4.1.2.1 details the top 5 targeted services/ports on destination hosts in the UNWT network that were in the alert log files.
Table 4.1.2.1

Alerts	Port	Common Service
25477	51443	Novell iFolder
12184	80	HTTP
9023	524	NCP
3783	8009	Novell iMonitor[15]
2256	1971	NetOP School

It should be noted that 3 of the top 5 destination ports were associated with hosts MY.NET.30.4 and MY.NET.30.3. These two hosts are most likely Novell file servers and because of the way the Snort rule is written, most of these alerts are most likely false positives.

Table 4.1.2.2 details the top 5 targeted services/ports on destination hosts in the UNWT network that were in the scan log files.

Table 4.1.2.2

Scans	Port	Common Service
99448	443	HTTPS
90986	6129	DameWare
59609	80	HTTP
55722	4899	Radmin

[15] http://www.novell.com/coolsolutions/appnote/7993.html

41013	20168	Lovegate Trojan

Table 4.1.2.3 details the top 5 targeted services/ports on destination hosts in the UNWT network that were in the OOS log files.

Table 4.1.2.3

OOS	Port	Common Service
1007	25	SMTP
976	110	POP3
376	80	HTTP
169	6881	BitTorrent
122	8080	HTTP-ALT

4.1.3 – Suspicious External Addresses

4.1.3.1 – Suspicious IP Number 1

The first external IP address that should be flagged for further investigation is 221.132.60.134. This host triggered 15 FTP DoS ftpd globbing alerts against host MY.NET.24.27 between 02:05 and 02:13 on 04/21. This IP address is registered to a network in Vietnam and the time of the attacks and the fact that the attacker returned several minutes later for another try is very suspicious. This host is not listed in the DSHIELD most wanted or hosts to block lists.

- Registration Information – See Appendix A

4.1.3.2 – Suspicious IP Number 2

The second external IP address that should be flagged for further investigation is 61.216.77.135. This host triggered 41 Tiny Fragments – Possible Hostile Activity alerts against host MY.NET.12.6 between 21:38 and 21:50 on 04/20. This IP address is registered to a network in Taiwan and all fragmented traffic should be treated as suspect, especially when the target host is one of the UNWT mail servers. This host is not listed in the DSHIELD most wanted or hosts to block lists.

- Registration Info – See Appendix A

4.1.3.3 – Suspicious IP Number 3

The third external IP address that should be flagged for further investigation is 207.3.145.130. This host triggered 9 External RPC call alerts, 1 MY.NET.30.3 activity alert and 3 External FTP to HelpDesk MY.NET.x.x alerts between 22:59 and 23:13 on 04/21. This host also generated 18,380 scan alerts during the same time period. Since the HelpDesk systems probably contain information about other UNWT systems, anytime

they are scanned should be reason for concern. This host is not on the DSHIELD most wanted or hosts to block lists.

- Registration Information – See Appendix A

5.1 – Correlations with previous practicals

The following practicals were reviewed for correlation on the writing of this paper.

- Mike Poor - http://www.giac.org/certified_professionals/practicals/gcia/0444.php
- Patrik Sternudd - http://www.giac.org/certified_professionals/practicals/gcia/0731.php
- Stephen Hall - http://www.giac.org/certified_professionals/practicals/gcia/0703.php
- Jan Stodola - http://www.giac.org/certified_professionals/practicals/gcia/0754.php
- Brett Hutley - http://www.giac.org/certified_professionals/practicals/gcia/0775.php
- Jorge Ortiz - http://www.giac.org/certified_professionals/practicals/gcia/0769.php

The following non-GCIA practical was reviewed for information on WU-FTPD globbing

- Jennifer Allen - http://www.giac.org/certified_professionals/practicals/gcih/0265.php

6.1 – Insights into compromise

Based on the three highlighted attacks, the Adore/Red Worm has almost certainly compromised many systems on the UNWT network. These hosts should be disconnected from the network until they have been patched from this vulnerability because they are attempting to compromise other hosts and it's only a matter of time before one of the core systems gets compromised, or the network bandwidth gets throttled down to unacceptable level.

The Tiny Fragments could have been just a scan, but these types of scans have been know to have negative affects on the target hosts during reassembly and the fact that one of the mail servers was targeted is reason for alarm.

The ftpd globbing attack is also alarming because the UNWT seems to be behind several patches and the wuftpd service was also vulnerable to the Adore/Red Worm, so the UNWT FTP servers are at twice the risk of compromise and can be used as a stepping stone to attack other core UNWT systems.

7.1 – Defensive recommendations

In respect of the UNWT's open policy on network traffic, the UNWT network

administrators should take some measures to enhance the overall security of the UNWT network and make the job detecting intrusions and attacks easier to manage.

- Some ingress and egress filtering should be considered for the network borders. This does not have to be a DENY ALL policy as this is adverse to the UNWT open philosophy, but blocking known bad traffic such as the SANS Top 20 list is a good start.
- Core systems need to be patched regularly and swiftly when vulnerabilities are discovered.
- The Snort IDS should be upgraded to the current version and the rule set needs to be tuned to cut down on the enormous amount of false positives. For example 2 custom signatures regarding hosts MY.NET.30.4 and MY.NET.30.3 generated so many alerts it would be very easy to miss any attacks. The DNS and SMTP traffic also generated many false positives. The *snort.conf file* should be configured to ignore some of these known false positives.
- Access to firewall, router, web and mail logs would have been beneficial in augmenting the Snort logs and would be very helpful in determining the severity of an attack.
- Staff and especially students need to be encouraged to be good Internet citizens by keeping their systems patched and use personal firewalls and anti-virus products. The UNWT should not want to be another contributor to the already volatile Internet.

Part III – Analysis Process

The analysis process of the log files was performed on an IBM NetVista PC running the Fedora Core 2 Linux operating system. A Compaq Evo N600 laptop with Windows 2000 and Microsoft Office 2000 was used to write this practical. The link graph was composed with Microsoft Visio 2002.

Processing the data

Standard Linux tools such as egrep, grep, awk, sed, sort and uniq were mostly used to parse the log files into manageable files. Extensive use of the man pages and Google was used to get a better handle on regular expressions and their use with this type of data. More importantly, new skills with the Linux command line were learned that I will be able to make use of on the job.

Visualizing the data

Snortsnarf was used to get a somewhat graphical view of the data. Another tool that I used in the beginning was snort_sort.pl with the HTML output option, but in the end decided to stick with Snortsnarf. The only problem with Snortsnarf was when it came time to process the scan logs. The application kept running out of memory and I ran out

of patience and elected to use command line tools and Excel to parse this data.

Maintaining sanity

To keep my sanity and stamina for processing this data and sitting down to write, I resorted to drinking lots of coffee and listening to lots of Johnny Cash on the iPod.

References

- The complete SANS Track 3 – Intrusion Detection In-Depth course materials
- Snort 2.1 Intrusion Detection 2nd Edition
- Mike Poor - http://www.giac.org/certified_professionals/practicals/gcia/0444.php
- Patrik Sternudd - http://www.giac.org/certified_professionals/practicals/gcia/0731.php
- Stephen Hall - http://www.giac.org/certified_professionals/practicals/gcia/0703.php
- Jan Stodola - http://www.giac.org/certified_professionals/practicals/gcia/0754.php
- Brett Hutley - http://www.giac.org/certified_professionals/practicals/gcia/0775.php
- Jorge Ortiz - http://www.giac.org/certified_professionals/practicals/gcia/0769.php
- Jennifer Allen - http://www.giac.org/certified_professionals/practicals/gcih/0265.php
- Chris Baker - http://www.giac.org/certified_professionals/practicals/gcia/0371.php
- SANS Website – http://ww.sans.org
- Snort Website – http://www.snort.org
- The Internet Ports Database – http://www.portsdb.org
- The Internet Storm Center – http://isc.sans.org
- DSHIELD – http://www.dshield.org
- Common Vulnerabilities and Exposures – http://www.cve.mitre.org
- CERT CC – http://www.cert.org
- US-CERT – http://www.us-cert.gov
- Google – http://www.google.ca
- ARIN – http://www.arin.net
- APNIC – http://www.apnic.org
- Novell - http://www.novell.com/coolsolutions/qna/8443.html
- http://linux0.cs.uaf.edu/archive31Jul01/msg00102.html
- http://wiki.ethereal.com/APIPA
- https://ucsb.edu/pipermail/security-linux/2001-April/000121.html
- http://www.europe.f-secure.com/v-descs/adore.shtml
- http://marc.theaimsgroup.com/?l=snort-users&m=97089915603238&w=2
- INSECURE.ORG – http://www.insecure.org
- Solaris Security Digest – http://www.boran.com/solarisdigest/2001/solaris20010416.html#solaris
- Covert Labs Security Advisory - http://cert.uni-stuttgart.de/archive/bugtraq/2001/04/msg00165.html
- http://www.novell.com/coolsolutions/appnote/7993.html

Appendix A

Registration Information

- **Suspicious IP Number 1**

% Whois data copyright terms http://www.apnic.net/db/dbcopyright.html

inetnum: 221.132.0.0 - 221.132.63.255
netname: VNPT-VNNIC-VN
country: VN
descr: Vietnam Posts and Telecommunications (VNPT)
descr: 23 Phan Chu Trinh st., Hanoi capital, Vietnam
admin-c: NXC1-AP
tech-c: KNH1-AP
status: ALLOCATED PORTABLE
changed: hm-changed@vnnic.net.vn 20041011
mnt-by: MAINT-VN-VNNIC
mnt-lower: MAINT-VN-VNPT
source: APNIC

person: Nguyen Xuan Cuong
nic-hdl: NXC1-AP
e-mail: cuong.ng@vnn.vn
address: Vietnam Posts and Telecommunications (VNPT)
address: 18 Nguyen Du street, Hanoi capital, Vietnam
phone: +84-4-9430427
fax-no: +84-4-8226861
country: VN
changed: hm-changed@vnnic.net.vn 20040527
mnt-by: VNPT
source: APNIC

person: Khanh Nguyen Hien
address: Vietnam Datacommunications Company (VDC)
address: 258 Ba Trieu street, Hanoi capital, Vietnam
country: VN
phone: +84-4-8212680
fax-no: +84-4-9760397
e-mail: pbthuy29@vnn.vn
nic-hdl: KNH1-AP
remarks: Contact: pbthuy29@vnn.vn
mnt-by: VNPT

changed: admin.vnn@vnnic.net.vn 20020604
source: APNIC

- **Suspicious IP Number 2**

```
% Whois data copyright terms
http://www.apnic.net/db/dbcopyright.html
inetnum:        61.216.0.0 - 61.219.255.255
netname:        HINET-TW
descr:          CHTD, Chunghwa Telecom Co.,Ltd.
descr:          Data-Bldg.6F, No.21, Sec.21, Hsin-Yi Rd.
descr:          Taipei Taiwan 100
country:        TW
admin-c:        HN27-AP
tech-c:         HN28-AP
remarks:        Delegated to HiNet for ADSL subscriber.
remarks:        This information has been partially mirrored by
APNIC from
remarks:        TWNIC. To obtain more specific information, please
use the
remarks:        TWNIC whois server at whois.twnic.net.
mnt-by:         MAINT-TW-TWNIC
changed:        hostmaster@twnic.net 20010117
status:         ALLOCATED PORTABLE
source:         APNIC
person:         HINET Network-Adm
address:        CHTD, Chunghwa Telecom Co., Ltd.
address:        Data-Bldg. 6F,  No. 21, Sec. 21, Hsin-Yi Rd.,
address:        Taipei Taiwan 100
country:        TW
phone:          +886 2 2322 3495
phone:          +886 2 2322 3442
phone:          +886 2 2344 3007
fax-no:         +886 2 2344 2513
fax-no:         +886 2 2395 5671
e-mail:         network-adm@hinet.net
nic-hdl:        HN27-AP
remarks:        same as TWNIC nic-handle HN184-TW
mnt-by:         MAINT-TW-TWNIC
changed:        hostmaster@twnic.net 20000721
source:         APNIC
person:         HINET Network-Center
address:        CHTD, Chunghwa Telecom Co., Ltd.
address:        Data-Bldg. 6F,  No. 21, Sec. 21, Hsin-Yi Rd.,
address:        Taipei Taiwan 100
country:        TW
phone:          +886 2 2322 3495
phone:          +886 2 2322 3442
phone:          +886 2 2344 3007
fax-no:         +886 2 2344 2513
fax-no:         +886 2 2395 5671
e-mail:         network-center@hinet.net
nic-hdl:        HN28-AP
remarks:        same as TWNIC nic-handle HN185-TW
mnt-by:         MAINT-TW-TWNIC
changed:        hostmaster@twnic.net 20000721
source:         APNIC
```

```
inetnum:        61.216.0.0 - 61.216.255.255
netname:        HINET-NET
descr:          CHTD, Chunghwa Telecom Co., Ltd.
descr:          Data-Bldg. 6F,  No. 21, Sec. 21, Hsin-Yi Rd.,
descr:          Taipei Taiwan
country:        TW
admin-c:        CYK-TW
tech-c:         CYK-TW
mnt-by:         MAINT-TW-TWNIC
remarks:        This information has been partially mirrored by
APNIC from
remarks:        TWNIC. To obtain more specific information, please
use the
remarks:        TWNIC whois server at whois.twnic.net.
changed:        fkchung@ms1.hinet.net 20010117
status:         ASSIGNED NON-PORTABLE
source:         TWNIC
person:         Chung Yung Kang
address:        Chunghwa Telecom Data communication Business Group
address:        No.21, Hsin-Yi Rd., sec. 1
address:        Taipei Taiwan
country:        TW
phone:          +886-2-2322-3442
fax-no:         +886-2-2344-2513
e-mail:         cykang@ms1.hinet.net
nic-hdl:        CYK-TW
remarks:        This information has been partially mirrored by
APNIC from
remarks:        TWNIC. To obtain more specific information, please
use the
remarks:        TWNIC whois server at whois.twnic.net.
changed:        hostmaster@twnic.net 19990924
source:         TWNIC
```

- **Suspicious IP Number 3**

```
OrgName:    WorldPath Internet Services
OrgID:      WPIS
Address:    11 Manchester Square
City:       Portsmouth
StateProv:  NH
PostalCode: 03801
Country:    US

NetRange:   207.3.144.0 - 207.3.151.255
CIDR:       207.3.144.0/21
NetName:    CW-207-3-144-A
NetHandle:  NET-207-3-144-0-1
Parent:     NET-207-2-128-0-1
NetType:    Reallocated
Comment:
RegDate:    2004-07-21
Updated:    2004-11-15

TechHandle: NOC1427-ARIN
TechName:   Network Operations Center
TechPhone:  +1-603-766-3444
```

```
TechEmail:  noc@worldpath.net

OrgAbuseHandle: NAD18-ARIN
OrgAbuseName:   Network Abuse Department
OrgAbusePhone:  +1-603-859-5000
OrgAbuseEmail:  abuse@worldpath.net

OrgTechHandle: NOC1427-ARIN
OrgTechName:   Network Operations Center
OrgTechPhone:  +1-603-766-3444
OrgTechEmail:  noc@worldpath.net
```