GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Intrusion Detection In-Depth (Security 503)"
at http://www.giac.org/registration/gcia

Practical Assignment for SANS Security DC 2000

GIAC Intrusion Detection Certification

By

Ken Wellmaker

Sunday, August 06, 2000

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Assignment #1 – Network Detects

Five network detects with analysis - Each of the detects must be different. The first two detects must be related to an attack listed in the top ten list.

Detect 1

19-May-00 17:31:59 drop inbound udp scan.wins.bad.guy MY.NET.29.8 netbios-ns netbios-ns 78
19-May-00 17:32:09 drop inbound udp scan.wins.bad.guy MY.NET.29.9 netbios-ns netbios-ns 78
19-May-00 17:32:20 drop inbound udp scan.wins.bad.guy MY.NET.29.10 netbios-ns netbios-ns 78
------snipped-----
19-May-00 18:15:18 drop inbound udp scan.wins.bad.guy MY.NET.29.252 netbios-ns netbios-ns 78
19-May-00 18:15:29 drop inbound udp scan.wins.bad.guy MY.NET.29.253 netbios-ns netbios-ns 78
19-May-00 18:15:39 drop inbound udp scan.wins.bad.guy MY.NET.29.254 netbios-ns netbios-ns 78

1. Source of trace

My network

2. Detect was generated by:

Checkpoint Firewall One – Firewall logs are loaded on a SQL database that can later be queried as needed. This data is actually from a SQL query for a subset of data. The format for the data is – Date, Time, Action, Direction, Protocol, Source Address, Destination Address, **Destination Port, Source Port**, and Length. Bolded for emphasis (order of Destination port and Source Port may be confusing).

3. Probability the source address was spoofed

Low – The attacker is attempting to gather information about my network and is relying on response (or the lack of a response).

4. Description of attack:

This is a scan of virtually an entire Class C address space. The scan did not cover addresses 1-7 and roughly 10 seconds expires between packets. This is likely a script running that waits for a response and will possibly try a connection if successful in locating the service.

5. Attack mechanism:

Port 137 can be the source of troubles for servers running WINS. Known DOS attacks exist for these services and significant compromise of reconnaissance information can result from an improperly configured WINS server. If the attacker had found active ports, it would be likely that additional malicious activity would result.

6. Correlations:

© SANS Institute 2000 - 2002, Author retains full rights.

This scan relates to "The Ten Most Critical Internet Security Threats" #7 – Global file sharing and inappropriate information sharing via NETBIOS and Windows NT ports 135 – 139.

A search of our records produced no results for related activity from this host.

CVE-1999-0288 - Denial of service in WINS with malformed data to port 137 (NETBIOS Name Service).

CVE-1999-0294 - All records in a WINS database can be deleted through SNMP for a denial of service.

7. Evidence of active targeting:

There is no evidence of active targeting by this host.

8. Severity:

(criticality + lethality) - (system + network) = severity

(2 + 2) – (3 + 5) = -4

9. Defensive recommendation:

Defenses are fine. Scan is successfully blocked at perimeter by the firewall.

10. Multiple choice test question

Which is true for the scan above?

a) The network is congested

b) The scan was stealth

c) The scan was directed to port 137

d) Typical NETBIOS traffic is TCP

Answer: c

Detect 2

```
24-Jun-00 8:10:56 drop inbound udp scan.snmp.bad.guy MY.NET.28.255 snmp cadis-2 70
24-Jun-00 8:10:56 drop inbound udp scan.snmp.bad.guy MY.NET.29.255 snmp ies-lm 70
24-Jun-00 8:10:56 drop inbound udp scan.snmp.bad.guy MY.NET.30.255 snmp marcam-lm 70
24-Jun-00 8:10:56 drop inbound udp scan.snmp.bad.guy MY.NET.31.255 snmp proxima-lm 70
24-Jun-00 8:11:26 drop inbound udp scan.snmp.bad.guy MY.NET.28.255 snmp 2293 70
24-Jun-00 8:11:26 drop inbound udp scan.snmp.bad.guy MY.NET.29.255 snmp 2294 70
24-Jun-00 8:11:26 drop inbound udp scan.snmp.bad.guy MY.NET.31.255 snmp 2296 70
24-Jun-00 8:11:26 drop inbound udp scan.snmp.bad.guy MY.NET.30.255 snmp 2295 70
24-Jun-00 8:11:56 drop inbound udp scan.snmp.bad.guy MY.NET.28.255 snmp 3000 70
24-Jun-00 8:11:56 drop inbound udp scan.snmp.bad.guy MY.NET.30.255 snmp 3002 70
24-Jun-00 8:11:56 drop inbound udp scan.snmp.bad.guy MY.NET.31.255 snmp 3021 70
```

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

24-Jun-00 8:11:57 drop inbound udp scan.snmp.bad.guy MY.NET.29.255 snmp 3028 70

1. Source of trace

My network

2. Detect was generated by:

Checkpoint Firewall One – Firewall logs are loaded on a SQL database that can later be queried as needed. This data is actually from a SQL query for a subset of data. The format for the data is – Date, Time, Action, Direction, Protocol, Source Address, Destination Address, **Destination Port, Source Port**, and Length. Bolded for emphasis (order of Destination port and Source Port may be confusing).

3. Probability the source address was spoofed

Low – The attacker is attempting to gather information about my network and is relying on response (or the lack of a response).

4. Description of attack:

The attacker is using a broadcast scan with sequential port numbers to look for machines that respond to probes directed to port 161. The UDP requests are retried to verify results. This is an effective way to scan all hosts on a network and is likely part of a larger scan of address space.

5. Attack mechanism:

A variety of known attacks are available for SNMP services ranging from DOS to root compromise. These vulnerabilities range across many devices including routers, printers, firewalls as well as servers and hosts. These known vulnerabilities also affect a wide range of operating systems. In addition, many SNMP community strings are improperly configured and give ready access by the default public/private "passwords". Significant reconnaissance can also be accomplished using SNMP access. If the attacker had found active ports, it would be likely that additional malicious activity would result.

6. Correlations:

This scan relates to "The Ten Most Critical Internet Security Threats" #10 – Default SNMP community strings set to 'public' and 'private'.

A search of our records produced no results for related activity from this host.

CVE - There are 13 records and candidates associated with SNMP services listed at http://www.cve.mitre.org

7. Evidence of active targeting:

There is no evidence of active targeting by this host.

8. Severity:

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

(criticality + lethality) - (system + network) = severity

(2 + 2) – (3 + 5) = -4

9. Defensive recommendation:

Defenses are fine. Scan is successfully blocked at perimeter by the firewall.

10. Multiple choice test question

Which is true about the logs shown above?

a) Typical SNMP traffic is UDP

b) The address is spoofed

c) The attacker is looking for Windows machines

d) None of the above

Answer: a

Detect 3

26-Jun-00 21:34:48 drop inbound tcp scan.pop.bad.guy MY.NET.28.1 pop2 pop2 40
26-Jun-00 21:34:48 drop inbound tcp scan.pop.bad.guy MY.NET.28.1 pop3 pop3 40
26-Jun-00 21:34:48 drop inbound tcp scan.pop.bad.guy MY.NET.28.2 pop2 pop2 40
26-Jun-00 21:34:48 drop inbound tcp scan.pop.bad.guy MY.NET.28.2 pop3 pop3 40
-----snipped-----
26-Jun-00 21:34:58 drop inbound tcp scan.pop.bad.guy MY.NET.28.254 pop2 pop2 40
26-Jun-00 21:34:58 drop inbound tcp scan.pop.bad.guy MY.NET.28.254 pop3 pop3 40
26-Jun-00 21:34:58 drop inbound tcp scan.pop.bad.guy MY.NET.28.255 pop2 pop2 40
26-Jun-00 21:34:58 drop inbound tcp scan.pop.bad.guy MY.NET.28.255 pop3 pop3 40
26-Jun-00 21:34:58 drop inbound tcp scan.pop.bad.guy MY.NET.29.1 pop2 pop2 40
26-Jun-00 21:34:58 drop inbound tcp scan.pop.bad.guy MY.NET.29.1 pop3 pop3 40
26-Jun-00 21:34:58 drop inbound tcp scan.pop.bad.guy MY.NET.29.2 pop2 pop2 40
26-Jun-00 21:34:58 drop inbound tcp scan.pop.bad.guy MY.NET.29.2 pop3 pop3 40
-----snipped-----
26-Jun-00 21:35:08 drop inbound tcp scan.pop.bad.guy MY.NET.29.254 pop2 pop2 40
26-Jun-00 21:35:08 drop inbound tcp scan.pop.bad.guy MY.NET.29.254 pop3 pop3 40
26-Jun-00 21:35:08 drop inbound tcp scan.pop.bad.guy MY.NET.29.255 pop2 pop2 40
26-Jun-00 21:35:08 drop inbound tcp scan.pop.bad.guy MY.NET.29.255 pop3 pop3 40
26-Jun-00 21:35:08 drop inbound tcp scan.pop.bad.guy MY.NET.30.1 pop2 pop2 40
26-Jun-00 21:35:08 drop inbound tcp scan.pop.bad.guy MY.NET.30.1 pop3 pop3 40
26-Jun-00 21:35:08 drop inbound tcp scan.pop.bad.guy MY.NET.30.2 pop2 pop2 40
26-Jun-00 21:35:08 drop inbound tcp scan.pop.bad.guy MY.NET.30.2 pop3 pop3 40
-----snipped-----
26-Jun-00 21:35:19 drop inbound tcp scan.pop.bad.guy MY.NET.30.254 pop2 pop2 40
26-Jun-00 21:35:19 drop inbound tcp scan.pop.bad.guy MY.NET.30.254 pop3 pop3 40
26-Jun-00 21:35:19 drop inbound tcp scan.pop.bad.guy MY.NET.30.255 pop2 pop2 40
26-Jun-00 21:35:19 drop inbound tcp scan.pop.bad.guy MY.NET.30.255 pop3 pop3 40
26-Jun-00 21:35:19 drop inbound tcp scan.pop.bad.guy MY.NET.31.1 pop2 pop2 40
26-Jun-00 21:35:19 drop inbound tcp scan.pop.bad.guy MY.NET.31.1 pop3 pop3 40

© SANS Institute 2000 - 2002, Author retains full rights.

26-Jun-00 21:35:19 drop inbound tcp scan.pop.bad.guy MY.NET.31.2 pop2 pop2 40
26-Jun-00 21:35:19 drop inbound tcp scan.pop.bad.guy MY.NET.31.2 pop3 pop3 40
-----snipped-----
26-Jun-00 21:35:29 drop inbound tcp scan.pop.bad.guy MY.NET.31.254 pop2 pop2 40
26-Jun-00 21:35:29 drop inbound tcp scan.pop.bad.guy MY.NET.31.254 pop3 pop3 40
26-Jun-00 21:35:29 drop inbound tcp scan.pop.bad.guy MY.NET.31.255 pop2 pop2 40
26-Jun-00 21:35:29 drop inbound tcp scan.pop.bad.guy MY.NET.31.255 pop3 pop3 40

1. Source of trace

My network

2. Detect was generated by:

Checkpoint Firewall One – Firewall logs are loaded on a SQL database that can later be queried as needed. This data is actually from a SQL query for a subset of data. The format for the data is – Date, Time, Action, Direction, Protocol, Source Address, Destination Address, **Destination Port, Source Port**, and Length. Bolded for emphasis (order of Destination port and Source Port may be confusing).

3. Probability the source address was spoofed

Low – The attacker is attempting to gather information about my network and is relying on response (or the lack of a response).

4. Description of attack:

This scan looks for responses to TCP ports 109 and 110 alternately and marched through the entire address space for my four Class C addresses. The automated scan is likely part of a larger scan that includes other address space. The tool also uses source port 109 for active POP-2 services and source port 110 for active POP-3 services.

5. Attack mechanism:

There is a wide variety of know problems associated with POP services. These compromises range from DOS to root level control and also include compromise of the mail content as well. Vulnerabilities cover a wide range of operating systems and vendors making this a good choice if you are looking to "get your foot in the door"! If the attacker had found active ports, it would be likely that additional malicious activity would result.

6. Correlations:

This scan relates to "The Ten Most Critical Internet Security Threats" #9 – IMAP and POP buffer overflow vulnerabilities or incorrect configuration.

A search of our records produced no results for related activity from this host.

CVE - There are 25 records and candidates associated with POP-2 and POP3 services listed at http://www.cve.mitre.org

7. Evidence of active targeting:

© SANS Institute 2000 - 2002 Author retains full rights.

There is no evidence of active targeting by this host.

8. Severity:

(criticality + lethality) - (system + network) = severity

(3 + 2) – (4 + 5) = -4

9. Defensive recommendation:

Defenses are fine. Scan is successfully blocked at perimeter by the firewall.

10. Multiple choice test question

Which is true concerning the log above?

a) POP-2 and POP-3 represent ports 109 and 110 respectively

b) POP services can be used to cause DOS

c) POP traffic normally uses TCP as the protocol

d) All of the above

Answer: d

Detect 4

```
26-May-00 16:06:07 drop inbound tcp scan.sub7.bad.guy MY.NET.28.1 27374 4256 48
26-May-00 16:06:07 drop inbound tcp scan.sub7.bad.guy MY.NET.28.2 27374 4257 48
-----snipped-----
26-May-00 16:06:21 drop inbound tcp scan.sub7.bad.guy MY.NET.28.253 27374 4508 48
26-May-00 16:06:21 drop inbound tcp scan.sub7.bad.guy MY.NET.28.254 27374 4509 48
26-May-00 16:06:24 drop inbound tcp scan.sub7.bad.guy MY.NET.29.1 27374 4510 48
26-May-00 16:06:24 drop inbound tcp scan.sub7.bad.guy MY.NET.29.2 27374 4511 48
-----snipped-----
26-May-00 16:06:41 drop inbound tcp scan.sub7.bad.guy MY.NET.29.253 27374 4762 48
26-May-00 16:06:41 drop inbound tcp scan.sub7.bad.guy MY.NET.29.254 27374 4763 48
26-May-00 16:06:45 drop inbound tcp scan.sub7.bad.guy MY.NET.30.1 27374 4764 48
26-May-00 16:06:45 drop inbound tcp scan.sub7.bad.guy MY.NET.30.2 27374 4765 48
-----snipped-----
26-May-00 16:07:01 drop inbound tcp scan.sub7.bad.guy MY.NET.30.253 27374 1040 48
26-May-00 16:07:01 drop inbound tcp scan.sub7.bad.guy MY.NET.30.254 27374 1041 48
26-May-00 16:07:05 drop inbound tcp scan.sub7.bad.guy MY.NET.31.1 27374 1042 48
26-May-00 16:07:05 drop inbound tcp scan.sub7.bad.guy MY.NET.31.2 27374 1043 48
-----snipped-----
26-May-00 16:07:21 drop inbound tcp scan.sub7.bad.guy MY.NET.31.253 27374 1302 48
26-May-00 16:07:21 drop inbound tcp scan.sub7.bad.guy MY.NET.31.254 27374 1303 48
```

1. Source of trace

© SANS Institute 2000 - 2002, Author retains full rights.

My network

2. Detect was generated by:

Checkpoint Firewall One – Firewall logs are loaded on a SQL database that can later be queried as needed. This data is actually from a SQL query for a subset of data. The format for the data is – Date, Time, Action, Direction, Protocol, Source Address, Destination Address, **Destination Port, Source Port**, and Length. Bolded for emphasis (order of Destination port and Source Port may be confusing).

3. Probability the source address was spoofed

Low – The attacker is attempting to gather information about my network and is relying on response (or the lack of a response).

4. Description of attack:

This scan looks for hosts that respond to probes for TCP port 27374. The tool uses sequential port numbers as the source port for the scan and is likely part of a larger scan of address space. This scam covered the entire range of my four Class C address space. There is also about a three second pause between Class Cs which may be useful in fingerprinting this tool.

5. Attack mechanism:

This particular scan is looking for Sub7 2.1 (port 27374). Other common ports associated with Sub7 are 1243, 6711, 6712, 6713, and 6776. Sub7 is a two part (client/server) Trojan for the Windows platform. The Trojan is configurable to make detection more difficult and also has the capability to notify the attacker when the machine is online. Once the Trojan has been successfully loaded on the target, the hacker has full control of the machine. If the attacker had found active ports, it would be almost certain that additional malicious activity would result.

6. Correlations:

A search of our records produced no results for related activity from this host.

There is additional information about Sub7 available at http://www.sans.org/y2k/subseven.htm.

CVE - ** CANDIDATE (under review) ** A hacker utility or Trojan Horse is installed on a system, e.g. NetBus, Back Orifice, Rootkit, etc.

7. Evidence of active targeting:

There is no evidence of active targeting by this host.

8. Severity:

(criticality + lethality) - (system + network) = severity

(2 + 2) – (3 + 5) = -4

9. Defensive recommendation:

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Defenses are fine. Scan is successfully blocked at perimeter by the firewall.

10. Multiple choice test question

Which is true concerning the scan above?

a) The scanner uses sequential port numbers

b) The address is spoofed

c) The scan was aborted

d) None of the above

Answer: a

Detect 5

17-May-00 4:34:38 drop inbound tcp scan.napster.bad.guy MY.NET.30.100 6670 4747 48
17-May-00 4:34:38 drop inbound tcp scan.napster.bad.guy MY.NET.30.101 6670 4748 48
17-May-00 4:34:38 drop inbound tcp scan.napster.bad.guy MY.NET.30.102 6670 4749 48
-----snipped-----
17-May-00 4:34:46 drop inbound tcp scan.napster.bad.guy MY.NET.30.252 6670 4899 48
17-May-00 4:34:46 drop inbound tcp scan.napster.bad.guy MY.NET.30.253 6670 4900 48
17-May-00 4:34:46 drop inbound tcp scan.napster.bad.guy MY.NET.30.254 6670 4901 48

1. Source of trace

My network

2. Detect was generated by:

Checkpoint Firewall One – Firewall logs are loaded on a SQL database that can later be queried as needed. This data is actually from a SQL query for a subset of data. The format for the data is – Date, Time, Action, Direction, Protocol, Source Address, Destination Address, **Destination Port, Source Port**, and Length. Bolded for emphasis (order of Destination port and Source Port may be confusing).

3. Probability the source address was spoofed

Low – The attacker is attempting to gather information about my network and is relying on response (or the lack of a response).

4. Description of attack:

This scan starts at address 100 of my Class C network since many host machines that will be likely candidates for Napster usually reside at the higher address space. The scanning tool used uses TCP and sequential port numbers to look for responses to port 6670.

5. Attack mechanism:

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Napster commonly uses port 6670 and is vulnerable to DOS attacks and compromise of files on the client machine. Aside from these major concerns, Napster's intended use has implications such as possible violation of usage policies in some business networks and possible network congestion on small internet connections. Given the fact that the scanner was looking for well know Trojan ports in addition to this scan, I conclude the intent was likely malicious rather that looking for MP3 files!

6. Correlations:

A search of our records produced additional data indicating scans by this same host for ports 1243 (BackDoor-G, SubSeven, SubSeven Apocalypse, Tiles), 20034 (NetBus 2 Pro, NetRex, Whack Job), and 12346 (GabanBus, NetBus, X-bill) on the same day.

CVE - CAN-2000-0281 ** CANDIDATE (under review) ** Buffer overflow in the Napster client beta 5 allows remote attackers to cause a denial of service via a long message

CVE – CAN-2000-0412 ** CANDIDATE (under review) ** The gnapster and knapster clients for Napster do not properly restrict access only to MP3 files, which allows remote attackers to read arbitrary files from the client by specifying the full pathname for the file.

7. Evidence of active targeting:

There is no evidence of active targeting by this host.

8. Severity:

(criticality + lethality) - (system + network) = severity

(1 + 1) – (1 + 5) = -4

9. Defensive recommendation:

Defenses are fine. Scan is successfully blocked at perimeter by the firewall. Since other scans for well-known trojans have performed by the same host, it would be prudent to note the source of the scan for future reference.

10. Multiple choice test question

Which is true concerning Napster?

a) The clients for Napster can be used for DOS attacks

b) The clients for Napster can be used to read files other than MP3 files

c) Napster traffic can cause a significant drain on network resources

d) All of the above

Answer: d

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Assignment 2 – Evaluate an Attack

1. Give the URL, location, or command that you acquired the attack from

http://hackersclub.com/km/files/hfiles/cg_oob.zip

2. Describe the attack including how it works

By using a special program, malicious people can crash any Windows 3.11/95/NT machine without a fix. It is done by sending OOB [Out Of Band] data to an established connection with a Windows user. Systems that are affected are Windows 3.11, Windows 95, Windows NT 3.51, Windows NT 4.0.

WinNuke sends a string (in the original source code the string is "bye") to your NETBIOS port (139) using OOB (Out Of Band data). The port is open by default on most Windows machines and is used for networking over TCP/IP. The problem is that Windows, although it supports OOB's, doesn't know what to do with them all the time. Windows 95 goes for the exception handler, and fails, leaving most users with a blue screen. NetBIOS [139] seems to be the most effective since this is a part of Windows, but any port that listens for data can be attacked, like Identd [113].

CVE-1999-0153 - Windows 95/NT out of band (OOB) data denial of service through NETBIOS port, aka WinNuke.

3. Provide an annotated network trace of the attack in action

This was a successful attack against a Windows NT Server with service pack 1 installed in a lab environment.

The first three packets are the three-way handshake.

SYN

17:07:54.467876 eth0 P 172.16.20.211.1170 > 172.16.10.64.netbios-ssn: S 345133:345133(0) win 8192 <mss 1460> (DF)

SYN/ACK

17:07:54.467967 eth0 P 172.16.10.64.netbios-ssn > 172.16.20.211.1170: S 4186078:4186078(0) ack 345134 win 8760 <mss 1460> (DF)

ACK

17:07:54.468407 eth0 P 172.16.20.211.1170 > 172.16.10.64.netbios-ssn: . 1:1(0) ack 1 win 8760 (DF)

The next three packets are OOB Packets with the URG bit set

17:07:55.503007 eth0 P 172.16.20.211.1170 > 172.16.10.64.netbios-ssn: P 1:4(3) ack 1 win 8760 urg 3>>> NBT (DF)

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

17:07:55.503127 eth0 P 172.16.20.211.1170 > 172.16.10.64.netbios-ssn: F 4:4(0) ack 1 win 8760 (DF)

17:07:58.492739 eth0 P 172.16.20.211.1170 > 172.16.10.64.netbios-ssn: FP 1:4(3) ack 1 win 8760 urg 3>>> NBT (DF)

© SANS Institute 2000 - 2002, Author retains full rights.

Assignment 3 – Analyze This

Intent of Report

The intent of this report is to identify representative data associated with the Scan logs and Alert logs produced by Snort. This report is not intended to encompass all activity logged by the sensor; rather it is intended to illustrate different techniques used by attackers as well as other areas that may be of concern.

Executive Summary

A sensor was placed on the network with a standard filter to collect traffic. Collectively, these logs contain 539,337 records from the network deserving analysis. Some problems associated with the data collection were identified and as a result, these logs do not contain all records for the time they were in place.

Concerns associated with the collected data range from reconnaissance to compromised systems. The following detail, while not all-inclusive, will illustrate areas of concern and techniques used by the attackers.

The report begins by illustrating different techniques used by attackers to gain information about the design of the network. Examples are then shown that illustrate how hosts are targeted by the attacker to gain additional information about the function the machine provides or compromises that have been loaded on the host. These targeted searches may give the attacker the specific information required to compromise the host.

Next evidence is shown that illustrates attackers have identified certain hosts on the network and identified some of the services running on those machines. Then I will look at examples of "Unwelcome" traffic and compromised hosts that have been identified on the network.

Finally, recommendations are covered in greater detail at the end of the report but the primary recommendation is that qualified personnel should be retained to secure the perimeter of the network, properly set up intrusion detection, and further investigate the hosts on the network for compromised systems.

Network mapping

The following data shows a SYN/FIN scan that looks across the entire Class B address space for hosts running DNS services. Notice also that the source port for the scan is port 53 as well. Many times the attackers will use ports that may be passed through firewalls or other perimeter devices. Hosts running DNS services are one of the most sought after types of hosts since they contain crucial information about the networks they service. In addition, there is a wide range of vulnerabilities for DNS services regardless of platform, OS, or vendor.

Scan Date	Origin	SP	Destination	DP	State	Flag	RBits
6/4/2000 2:07:52 AM	203.233.103.188	53	MY.NET.10.102	53	SYNFIN	**SF****	

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Scan Date	Origin	SP	Destination	DP	State	Flag	RBits
6/4/2000 2:07:52 AM	203.233.103.188	53	MY.NET.10.103	53	SYNFIN	**SF****	
6/4/2000 2:07:52 AM	203.233.103.188	53	MY.NET.10.104	53	SYNFIN	**SF****	
6/4/2000 2:07:52 AM	203.233.103.188	53	MY.NET.10.105	53	SYNFIN	**SF****	
6/4/2000 2:07:52 AM	203.233.103.188	53	MY.NET.10.106	53	SYNFIN	**SF****	
snipped							
6/4/2000 2:28:36 AM	203.233.103.188	53	MY.NET.254.94	53	SYNFIN	**SF****	
6/4/2000 2:28:36 AM	203.233.103.188	53	MY.NET.254.95	53	SYNFIN	**SF****	
6/4/2000 2:28:36 AM	203.233.103.188	53	MY.NET.254.96	53	SYNFIN	**SF****	
6/4/2000 2:28:36 AM	203.233.103.188	53	MY.NET.254.97	53	SYNFIN	**SF****	
6/4/2000 2:28:36 AM	203.233.103.188	53	MY.NET.254.98	53	SYNFIN	**SF****	
6/4/2000 2:28:36 AM	203.233.103.188	53	MY.NET.254.99	53	SYNFIN	**SF****	

The dates in the scan logs do not provide the significant digits in the date/time field so order of packets may be off. The intent of the data is the same. We see below that this attacker is scanning most of the address space for the Class B network looking for the Sub7 Trojan. As you can see near the bottom of the scan, the host addresses are repeated with the same source port number. In addition, this attacker ran another scan on 6/1 that covered some of the address space missed by this scan and also used the same range of source port numbers.

This particular scan is looking for Sub7 2.1 (port 27374). Other common ports associated with Sub7 are 1243, 6711, 6712, 6713, and 6776. Sub7 is a two-part (client/server) Trojan for the Windows platform. The Trojan is configurable to make detection more difficult and also has the capability to notify the attacker when the machine is online. Once the Trojan has been successfully loaded on the target, the hacker has full control of the machine. If the attacker has found active ports, it is almost certain that additional malicious activity will result.

Scan Date	Origin	SP	Destination	DP	State	Flag	RBits
5/26/2000 9:04:24 PM	24.2.169.101	1580	MY.NET.60.41	27374	SYN	**S*****	
5/26/2000 9:04:24 PM	24.2.169.101	1568	MY.NET.60.29	27374	SYN	**S*****	
5/26/2000 9:04:24 PM	24.2.169.101	1565	MY.NET.60.26	27374	SYN	**S*****	
5/26/2000 9:04:24 PM	24.2.169.101	1563	MY.NET.60.24	27374	SYN	**S*****	
*****snipped*****							
5/26/2000 9:43:04 PM	24.2.169.101	1906	MY.NET.232.246	27374	SYN	**S*****	
5/26/2000 9:43:04 PM	24.2.169.101	1908	MY.NET.232.248	27374	SYN	**S*****	
5/26/2000 9:43:04 PM	24.2.169.101	1909	MY.NET.232.249	27374	SYN	**S*****	
5/26/2000 9:43:04 PM	24.2.169.101	1905	MY.NET.232.245	27374	SYN	**S*****	
5/26/2000 9:43:04 PM	24.2.169.101	1910	MY.NET.232.250	27374	SYN	**S*****	
5/26/2000 9:43:04 PM	24.2.169.101	1907	MY.NET.232.247	27374	SYN	**S*****	
5/26/2000 9:43:04 PM	24.2.169.101	1906	MY.NET.232.246	27374	SYN	**S*****	

The scan log produced this scan of the MY.NET.97 Class C for UDP port 44767. Port 44767 is no stranger to persons looking at scans but I have been unsuccessful in finding a definitive answer about what the port is used for. The most common belief is that since many Trojans are configurable, this is a search for Trojans.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Scan Date	Origin	SP	Destination	DP	State	Flag	RBits
6/22/2000 10:50:53 AM	212.133.136.96	1414	MY.NET.97.1	44767	UDP		
*****snipped*****							
6/22/2000 10:50:56 AM	212.133.136.96	1661	MY.NET.97.248	44767	UDP		

By filtering the scan log and looking for distinct records in the origin field, we find that three other scans were launched looking for the port 44767 on the same Class C. In fact, the last three scans were sourced from the same Class C network! This is likely the same attacker using different addresses.

Scan Date	Origin	SP	Destination	DP	State	Flag	RBits
6/16/2000 1:02:32 PM	212.29.82.197	4816	MY.NET.97.244	44767	UDP		
6/22/2000 9:33:29 AM	212.133.136.86	1698	MY.NET.97.33	44767	UDP		
6/22/2000 10:50:56 AM	212.133.136.96	1658	MY.NET.97.245	44767	UDP		
6/22/2000 2:41:53 PM	212.133.136.61	3592	MY.NET.97.35	44767	UDP		

Below is a random scan looking for linuxconf. With the growing popularity of Linux and the use of Linux for servers (especially web servers), this scan is common.

Scan Date	Origin	SP	Destination	DP	State	Flag	RBits
6/2/2000 8:42:40 PM	203.197.234.162	2902	MY.NET.1.62	98	SYN	**S*****	
6/2/2000 8:42:40 PM	203.197.234.162	2955	MY.NET.1.115	98	SYN	**S*****	
6/2/2000 8:42:40 PM	203.197.234.162	2973	MY.NET.1.133	98	SYN	**S*****	
6/2/2000 8:42:40 PM	203.197.234.162	3028	MY.NET.1.188	98	SYN	**S*****	
*****snipped*****							

Below you will see a random SYN scan looking for SMTP. This is a slow scan to a degree and randomizes not only the hosts on the network being scanned, but the networks as well. There are quite a few exploits for machines and services running port 25. These include buffer overflow, majordomo, root level compromise, etc. Some sendmail configurations include an alias called 'decode' that pipes mail through the uudecode program. By creating and sending uuencoded data to the 'decode' alias, an attacker could for example place an arbitrary .rhosts file onto your system.

Scan Date	Origin	SP	Destination	DP	State	Flag	RBits
*****snipped*****							
6/1/2000 6:29:20 PM	216.41.50.212	1724	MY.NET.145.160	25	SYN	**S*****	
6/1/2000 6:29:20 PM	216.41.50.212	1725	MY.NET.145.54	25	SYN	**S*****	
6/1/2000 6:29:21 PM	216.41.50.212	1727	MY.NET.145.71	25	SYN	**S*****	
6/1/2000 6:29:21 PM	216.41.50.212	1728	MY.NET.145.72	25	SYN	**S*****	
6/1/2000 6:29:21 PM	216.41.50.212	1721	MY.NET.111.125	25	SYN	**S*****	
6/1/2000 6:29:22 PM	216.41.50.212	1729	MY.NET.111.41	25	SYN	**S*****	
*****snipped*****							

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

This scan is looking for Solaris RPC ports. It is a random SYN scan from cable modem land. The attacker also scanned for DNS services immediately prior to this scan.

Scan Date	Origin	SP	Destination	DP	State	Flag	RBits
6/12/2000 12:57:43 PM	24.3.234.246	4872	MY.NET.99.67	32772	SYN	**S*****	
6/12/2000 12:57:43 PM	24.3.234.246	4882	MY.NET.99.77	32772	SYN	**S*****	
6/12/2000 12:57:43 PM	24.3.234.246	4880	MY.NET.99.75	32772	SYN	**S*****	
6/12/2000 12:57:43 PM	24.3.234.246	4873	MY.NET.99.68	32772	SYN	**S*****	
*****snipped*****							

One type of scan that is extremely efficient is a broadcast scan. Shown below we see the attacker looking for POP-2 servers and scans the entire Class B in a matter of a few minutes. There is a wide variety of know problems associated with POP services. These compromises range from DOS to root level control and also include compromise of the mail content as well. Vulnerabilities cover a wide range of operating systems and vendors, making this a good choice if you are looking to "get your foot in the door"!

Scan Date	Origin	SP	Destination	DP	State	Flag	RBits
6/4/2000 6:52:19 PM	210.97.12.129	109	MY.NET.1.255	109	SYNFIN	**SF****	
*****snipped*****							
6/4/2000 7:13:53 PM	210.97.12.129	109	MY.NET.254.255	109	SYNFIN	**SF****	

Shown here is the beginning of a broadcast scan using the .0 broadcast. This attacker from cable modem land is looking for DNS services and covers a lot of networks in a short period of time. The missing MY.NET.3.0 may indicate that we are missing packets. Furthermore, the port numbers and timing together may indicate this is part of a larger scan.

Scan Date	Origin	SP	Destination	DP	State	Flag	RBits
6/4/2000 4:19:13 PM	24.13.87.239	1905	MY.NET.1.0	53	SYN	**S*****	
6/4/2000 4:19:17 PM	24.13.87.239	2160	MY.NET.2.0	53	SYN	**S*****	
6/4/2000 4:19:28 PM	24.13.87.239	2670	MY.NET.4.0	53	SYN	**S*****	
6/4/2000 4:19:33 PM	24.13.87.239	2925	MY.NET.5.0	53	SYN	**S*****	
*****snipped*****							

Port mapping

The table below shows a sequential portscan of a host. We can see by the sequential source ports that the destination port of 26601 was skipped. This is a partial scan and the attacker may be working from different sources or may be doing limited scanning on different days to try avoid detection.

Scan Date	Origin	SP	Destination	DP	State	Flag	RBits

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Scan Date	Origin	SP	Destination	DP	State	Flag	RBits
5/25/2000 5:12:28 PM	24.3.29.25	1369	MY.NET.60.11	26600	SYN	**S*****	
5/25/2000 5:12:28 PM	24.3.29.25	1370	MY.NET.60.11	26602	SYN	**S*****	
5/25/2000 5:12:29 PM	24.3.29.25	1371	MY.NET.60.11	26603	SYN	**S*****	
5/25/2000 5:12:29 PM	24.3.29.25	1372	MY.NET.60.11	26604	SYN	**S*****	
*****snipped*****							

At first glance this looks like a typical random scan for telnet. Some attackers will randomize their scans to make it harder for the analyst to spot the scan and in some cases make it harder to identify the total scope. See the trace following this one to see what I mean!

Scan Date	Origin	SP	Destination	DP	State	Flag	RBits
6/22/2000 8:57:48 PM	212.25.68.195	1709	MY.NET.140.123	23	SYN	**S*****	
6/22/2000 8:57:48 PM	212.25.68.195	1690	MY.NET.157.71	23	SYN	**S*****	
6/22/2000 8:57:48 PM	212.25.68.195	1688	MY.NET.142.42	23	SYN	**S*****	
6/22/2000 8:57:48 PM	212.25.68.195	1748	MY.NET.140.31	23	SYN	**S*****	
6/22/2000 8:57:48 PM	212.25.68.195	1625	MY.NET.179.37	23	SYN	**S*****	
*****snipped*****							

Upon closer analysis and sorting by Destination address, we can clearly see that the attacker is looking for POP3, telnet, the original version of Sub7, and FTP.

Scan Date	Origin	SP	Destination	DP	State	Flag	RBits
*****snipped*****							
6/22/2000 8:59:03 PM	212.25.68.195	2581	MY.NET.1.14	110	SYN	**S*****	
6/22/2000 8:57:51 PM	212.25.68.195	1624	MY.NET.1.14	23	SYN	**S*****	
6/22/2000 8:58:33 PM	212.25.68.195	1624	MY.NET.1.14	23	SYN	**S*****	
6/22/2000 8:58:07 PM	212.25.68.195	1948	MY.NET.1.14	21	SYN	**S*****	
6/22/2000 8:58:53 PM	212.25.68.195	2289	MY.NET.1.14	143	SYN	**S*****	
6/22/2000 8:57:48 PM	212.25.68.195	1624	MY.NET.1.14	23	SYN	**S*****	
6/22/2000 8:58:09 PM	212.25.68.195	1640	MY.NET.10.101	23	SYN	**S*****	
6/22/2000 8:58:07 PM	212.25.68.195	1953	MY.NET.10.101	21	SYN	**S*****	
6/22/2000 8:58:01 PM	212.25.68.195	1953	MY.NET.10.101	21	SYN	**S*****	
6/22/2000 8:58:08 PM	212.25.68.195	2302	MY.NET.10.101	143	SYN	**S*****	
*****snipped*****							

In the trace below, we see that the attacker is port scanning the host in sequential order. I also note that the scanner is using sequential source port numbers for the scan. This is only a partial scan, which is the reason it was selected. Only 31 packets were captured from this attacker. Since this was near the end of the time frame that we captured packets on the network, it is likely

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

that he came back to finish the scan later or he may be working in conjunction with other attackers or hosts.

Scan Date	Origin	SP	Destination	DP	State	Flag	RBits
6/2/2000 4:49:50 PM	216.234.231.190	64596	MY.NET.180.26	3136	SYN	**S*****	
6/2/2000 4:49:50 PM	216.234.231.190	64597	MY.NET.180.26	3137	SYN	**S*****	
6/2/2000 4:49:50 PM	216.234.231.190	64599	MY.NET.180.26	3138	SYN	**S*****	
*****snipped*****							

In the scan below, I searched for the source address 169.226.248.62 and found that he was scanning a host for several ports on 6/4 and then resumed on 6/6 and again on 6/15.

Scan Date	Origin	SP	Destination	DP	State	Flag	RBits
*****snipped*****							
6/4/2000 11:50:14 PM	169.226.248.62	1563	MY.NET.217.74	1180	SYN	**S*****	
6/4/2000 11:50:14 PM	169.226.248.62	1568	MY.NET.217.74	1187	SYN	**S*****	
6/4/2000 11:50:14 PM	169.226.248.62	1566	MY.NET.217.74	1183	SYN	**S*****	
6/6/2000 12:12:33 AM	169.226.248.62	3036	MY.NET.217.74	3600	SYN	**S*****	
6/6/2000 12:12:33 AM	169.226.248.62	3033	MY.NET.217.74	3596	SYN	**S*****	
6/6/2000 12:12:33 AM	169.226.248.62	3031	MY.NET.217.74	3594	SYN	**S*****	
*****snipped*****							
6/6/2000 12:12:37 AM	169.226.248.62	3032	MY.NET.217.74	3595	SYN	**S*****	
6/6/2000 12:12:39 AM	169.226.248.62	3030	MY.NET.217.74	3593	SYN	**S*****	
6/6/2000 12:12:40 AM	169.226.248.62	3030	MY.NET.217.74	3593	SYN	**S*****	
6/15/2000 10:03:46 PM	169.226.248.62	4083	MY.NET.217.14	4933	SYN	**S*****	
6/15/2000 10:03:46 PM	169.226.248.62	4086	MY.NET.217.14	4936	SYN	**S*****	
6/15/2000 10:03:47 PM	169.226.248.62	4085	MY.NET.217.14	4935	SYN	**S*****	
*****snipped*****							

Scanning for port 443 is looking for HTTPS and there might be value in launching an application level attack on your http server. Https only serves to encrypt end to end. You could still be vulnerable to CGI-based attacks. The attacker is captured targeting two hosts for that service.

Scan Date	Origin	SP	Destination	DP	State	Flag	RBits
6/5/2000 10:27:33 AM	200.47.1.58	1189	MY.NET.253.112	443	NULL	********	
6/5/2000 10:27:33 AM	200.47.1.58	1187	MY.NET.253.112	443	SYN	**S*****	
6/5/2000 10:34:20 AM	200.47.1.58	1236	MY.NET.5.29	443	NULL	********	
6/5/2000 10:34:20 AM	200.47.1.58	1233	MY.NET.5.29	443	SYN	**S*****	

The scan listed below illustrates an attacker targeting a host and looking only for specific ports that are known to be home to Trojan activity. This is the entire scan that the attacker performed on this host and is a common scan used by attackers. Packets may have arrived out of order but I would conclude that sequential source ports were used. Also notice the time jump and port number jump between 12:06 and 12:16. The scanner is also probably scanning others not on our network as part of this scan.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Scan Date	Origin	SP	Destination	DP	State	Flag	RBits
6/4/2000 12:06:15 AM	203.94.224.241	3283	MY.NET.60.11	456	SYN	**S*****	
6/4/2000 12:06:16 AM	203.94.224.241	3277	MY.NET.60.11	1243	SYN	**S*****	
6/4/2000 12:06:16 AM	203.94.224.241	3275	MY.NET.60.11	20034	SYN	**S*****	
6/4/2000 12:06:16 AM	203.94.224.241	3273	MY.NET.60.11	12345	SYN	**S*****	
6/4/2000 12:06:17 AM	203.94.224.241	3278	MY.NET.60.11	27374	SYN	**S*****	
6/4/2000 12:06:17 AM	203.94.224.241	3280	MY.NET.60.11	6671	SYN	**S*****	
6/4/2000 12:06:18 AM	203.94.224.241	3279	MY.NET.60.11	6670	SYN	**S*****	
6/4/2000 12:06:18 AM	203.94.224.241	3281	MY.NET.60.11	21554	SYN	**S*****	
6/4/2000 12:06:18 AM	203.94.224.241	3274	MY.NET.60.11	1080	SYN	**S*****	
6/4/2000 12:06:18 AM	203.94.224.241	3282	MY.NET.60.11	9400	SYN	**S*****	
6/4/2000 12:06:18 AM	203.94.224.241	3276	MY.NET.60.11	31377	SYN	**S*****	
6/4/2000 12:16:51 AM	203.94.224.241	4943	MY.NET.60.11	9400	SYN	**S*****	
6/4/2000 12:16:51 AM	203.94.224.241	4942	MY.NET.60.11	21554	SYN	**S*****	
6/4/2000 12:16:51 AM	203.94.224.241	4938	MY.NET.60.11	1243	SYN	**S*****	
6/4/2000 12:16:51 AM	203.94.224.241	4940	MY.NET.60.11	6670	SYN	**S*****	
6/4/2000 12:16:51 AM	203.94.224.241	4937	MY.NET.60.11	31377	SYN	**S*****	
6/4/2000 12:16:51 AM	203.94.224.241	4939	MY.NET.60.11	27374	SYN	**S*****	
6/4/2000 12:16:51 AM	203.94.224.241	4936	MY.NET.60.11	20034	SYN	**S*****	
6/4/2000 12:16:52 AM	203.94.224.241	4941	MY.NET.60.11	6671	SYN	**S*****	
6/4/2000 12:16:52 AM	203.94.224.241	4944	MY.NET.60.11	456	SYN	**S*****	
6/4/2000 12:16:54 AM	203.94.224.241	4943	MY.NET.60.11	9400	SYN	**S*****	
6/4/2000 12:16:54 AM	203.94.224.241	4937	MY.NET.60.11	31377	SYN	**S*****	
6/4/2000 12:16:54 AM	203.94.224.241	4939	MY.NET.60.11	27374	SYN	**S*****	
6/4/2000 12:16:54 AM	203.94.224.241	4942	MY.NET.60.11	21554	SYN	**S*****	
6/4/2000 12:16:54 AM	203.94.224.241	4940	MY.NET.60.11	6670	SYN	**S*****	
6/4/2000 12:16:54 AM	203.94.224.241	4938	MY.NET.60.11	1243	SYN	**S*****	
6/4/2000 12:16:56 AM	203.94.224.241	4935	MY.NET.60.11	1080	SYN	**S*****	
6/4/2000 12:16:56 AM	203.94.224.241	4934	MY.NET.60.11	12345	SYN	**S*****	

Tools

The trace below illustrates a targeted host being scanned by an attacker that is using a tool to craft packets and has the option to slow down the scan. The trace also shows the attacker revisited the host about the same time the next morning. Other evidence reveals that this host may be a mail server so this type of activity would be typical of an attacker trying to fingerprint the machine. The attacker in this case is on cable modem address space.

Scan Date	Origin	SP	Destination	DP	State	Flag	RBits
6/6/2000 7:05:32 AM	24.23.45.19	1490	MY.NET.6.7	8554	NOACK	2**FR***	RESERVEDBITS
6/6/2000 7:05:34 AM	24.23.45.19	195	MY.NET.6.7	1490	NOACK	2**FR***	RESERVEDBITS
*****snipped*****							
6/7/2000 7:03:58 AM	24.23.45.19	1156	MY.NET.6.7	4664	SYNFIN	21SF****	RESERVEDBITS
6/7/2000 7:04:06 AM	24.23.45.19	212	MY.NET.6.7	1156	FULLXMAS	*1SFRPAU	RESERVEDBITS

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Scan Date	Origin	SP	Destination	DP	State	Flag	RBits
6/7/2000 7:04:06 AM	24.23.45.19	1156	MY.NET.6.7	4664	FULLXMAS	*1SFRPAU	RESERVEDBITS

The capture below indicates the attacker is using NMAP in an attempt to determine the host's operating system. NMAP is a scanning tool that provides a reliable fingerprint making it relatively easy to detect. Notice the source port of 0 and the source port and destination port of 6688. Snort of course makes it easy for us by indicating NMAPID in the State field!

Scan Date	Origin	SP	Destination	DP	State	Flag	RBits
5/26/2000 2:17:58 AM	169.237.30.234	6688	MY.NET.201.6	1040	NULL	********	
5/26/2000 2:17:58 AM	169.237.30.234	6688	MY.NET.201.6	1040	NULL	********	
5/26/2000 2:18:38 AM	169.237.30.234	0	MY.NET.201.6	6688	NMAPID	**SF*P*U	
5/26/2000 2:18:38 AM	169.237.30.234	0	MY.NET.201.6	6688	NMAPID	**SF*P*U	
5/26/2000 2:19:07 AM	169.237.30.234	6688	MY.NET.201.6	1041	NMAPID	**SF*P*U	
5/26/2000 2:19:07 AM	169.237.30.234	6688	MY.NET.201.6	1041	NMAPID	**SF*P*U	
5/26/2000 2:19:38 AM	169.237.30.234	16	MY.NET.201.6	6688	NMAPID	**SF*P*U	
5/26/2000 2:19:38 AM	169.237.30.234	16	MY.NET.201.6	6688	NMAPID	**SF*P*U	
5/26/2000 2:20:29 AM	169.237.30.234	6688	MY.NET.201.6	1041	NMAPID	**SF*P*U	
5/26/2000 2:20:29 AM	169.237.30.234	6688	MY.NET.201.6	1041	NMAPID	**SF*P*U	
5/26/2000 2:21:03 AM	169.237.30.234	6688	MY.NET.201.6	1045	NOACK	2*SFR**U	RESERVEDBITS
5/26/2000 2:21:03 AM	169.237.30.234	6688	MY.NET.201.6	1045	NOACK	2*SFR**U	RESERVEDBITS
5/26/2000 2:21:09 AM	169.237.30.234	6688	MY.NET.201.6	1045	INVALIDACK	*1S*R*AU	RESERVEDBITS
5/26/2000	169.237.30.234	6688	MY.NET.201.6	1045	INVALIDACK	*1S*R*AU	RESERVEDBITS

© SANS Institute 2000 - 2002, Author retains full rights.

Scan Date	Origin	SP	Destination	DP	State	Flag	RBits
2:21:09 AM							

Other attackers running NMAP include those listed below. One of particular interest is the internal host.

Alert Date	Message	Origin	SP	Destination	DP
05/27-02:04:27.903992	[**] NMAP TCP ping! [**]	141.223.180.1	80	MY.NET.6.7	80
05/24-07:26:32.134443	[**] Probable NMAP fingerprint attempt [**]	147.32.141.190	6699	MY.NET.203.134	2857
05/26-02:19:38.289469	[**] Probable NMAP fingerprint attempt [**]	169.237.30.234	16	MY.NET.201.6	6688
06/13-11:59:38.464507	[**] NMAP TCP ping! [**]	194.217.242.41	9000	MY.NET.1.2	9004
05/31-21:38:45.656482	[**] Probable NMAP fingerprint attempt [**]	195.11.212.36	27045	MY.NET.20.10	27005
06/18-15:18:36.224162	[**] NMAP TCP ping! [**]	195.54.105.6	80	MY.NET.1.8	53
06/13-00:23:58.957477	[**] Probable NMAP fingerprint attempt [**]	200.53.242.138	6699	MY.NET.181.87	2696
06/20-06:21:41.960912	[**] NMAP TCP ping! [**]	209.218.228.201	80	MY.NET.1.8	53
06/16-02:06:03.597988	[**] NMAP TCP ping! [**]	209.218.228.46	80	MY.NET.1.8	53
05/28-00:24:01.616581	[**] NMAP TCP ping! [**]	216.204.66.115	46530	MY.NET.20.10	38815
06/01-01:32:30.868976	[**] NMAP TCP ping! [**]	MY.NET.253.12	43758	MY.NET.101.161	36834

Services located

The following services were located by the scans performed.

DNS Servers located are:	Mail Servers located are:
MY.NET.1.3	MY.NET.1.2
MY.NET.1.4	MY.NET.110.108
MY.NET.1.5	MY.NET.110.109
MY.NET.1.9	MY.NET.110.150
MY.NET.109.38	MY.NET.110.39
MY.NET.109.40	MY.NET.110.82
MY.NET.109.41	MY.NET.130.81
MY.NET.110.100	MY.NET.140.253
MY.NET.110.104	MY.NET.145.54
MY.NET.110.110	MY.NET.145.76
MY.NET.110.131	MY.NET.145.9
MY.NET.110.16	MY.NET.162.80

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

MY.NET.130.122 MY.NET.140.16 MY.NET.140.17 MY.NET.5.117 MY.NET.75.1 MY.NET.76.11 MY.NET.100.230 (Mail & DNS Server)	MY.NET.253.41 MY.NET.253.42 MY.NET.253.43 MY.NET.6.34 MY.NET.6.34 MY.NET.6.35 MY.NET.6.47 MY.NET.6.7 MY.NET.60.17 MY.NET.100.230 (Mail & DNS Server)

The following is one example that illustrates how the scanner identifies the services. This particular scan covered the majority of the Class B address space and when a response is received from the SYN/FIN packet, the attacker sends both a UDP packet and a SYN request to the responding host.

Scan Date	Origin	SP	Destination	DP	State	Flag
6/5/00 1:43 AM	208.220.120.13	53	MY.NET.75.1	53	SYNFIN	**SF****
6/5/00 1:43 AM	208.220.120.13	53	MY.NET.75.2	53	SYNFIN	**SF****
6/5/00 1:43 AM	208.220.120.13	53	MY.NET.75.3	53	SYNFIN	**SF****
6/5/00 1:43 AM	208.220.120.13	53	MY.NET.75.4	53	SYNFIN	**SF****
6/5/00 1:43 AM	208.220.120.13	53	MY.NET.75.5	53	SYNFIN	**SF****
6/5/00 1:43 AM	208.220.120.13	53	MY.NET.75.6	53	SYNFIN	**SF****
6/5/00 1:43 AM	208.220.120.13	4805	MY.NET.75.1	53	UDP	
6/5/00 1:43 AM	208.220.120.13	53	MY.NET.75.8	53	SYNFIN	**SF****
6/5/00 1:43 AM	208.220.120.13	4179	MY.NET.75.1	53	SYN	**S*****
6/5/00 1:43 AM	208.220.120.13	53	MY.NET.75.9	53	SYNFIN	**SF****
6/5/00 1:43 AM	208.220.120.13	53	MY.NET.75.10	53	SYNFIN	**SF****
6/5/00 1:43 AM	208.220.120.13	53	MY.NET.75.11	53	SYNFIN	**SF****

It would be safe to assume that the attackers below have gathered enough information to be considered dangerous. While this list was obtained from analysis of the data recorded, it is not intended to be an all-inclusive list of attackers that have knowledge of the network. It is meant to illustrate that specific attackers have gained significant reconnaissance information about the hosts.

208.220.120.13
209.185.131.81
209.209.12.133
216.32.241.15
63.166.66.22
63.170.203.133
63.92.26.236
63.92.26.236
64.4.9.13

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Concerns

This hacker sent fragmented traffic to the host shown below. Although fragmentation is normal, fragmentation can be used to facilitate hostile activity. Most networks pass traffic without requiring fragmentation.

Alert Date	Message	Origin	SP	Destination	DP
06/18-01:21:49.368962	[**] Tiny Fragments - Possible Hostile Activity [**]	63.236.34.174		MY.NET.1.8	
06/18-01:10:01.394944	[**] Tiny Fragments - Possible Hostile Activity [**]	63.236.34.174		MY.NET.1.8	
06/18-01:10:01.394862	[**] Tiny Fragments - Possible Hostile Activity [**]	63.236.34.174		MY.NET.1.8	
06/18-01:21:49.369093	[**] Tiny Fragments - Possible Hostile Activity [**]	63.236.34.174		MY.NET.1.8	
06/18-01:10:01.395084	[**] Tiny Fragments - Possible Hostile Activity [**]	63.236.34.174		MY.NET.1.8	
06/18-01:21:49.369226	[**] Tiny Fragments - Possible Hostile Activity [**]	63.236.34.174		MY.NET.1.8	

Here I show that our filter alerted on a known virus signature. What a way to locate mail servers!

Alert Date	Message	Origin	SP	Destination	DP
05/25-09:53:44.364111	[**] Happy 99 Virus [**]	207.172.145.30	1294	MY.NET.253.51	25
05/25-09:53:44.364111	[**] Happy 99 Virus [**]	207.172.145.30	1294	MY.NET.253.51	25
06/13-10:26:37.292191	[**] Happy 99 Virus [**]	207.172.132.67	1038	MY.NET.253.52	25

This activity triggered our SMTP source port filter for source and destination ports 25. Source port 25 is passed through many perimeter devices such as firewalls and filtering routers.

Alert Date	Message	Origin	SP	Destination	DP
05/27-17:39:47.392166	[**] TCP SMTP Source Port traffic [**]	212.209.122.1	25	MY.NET.253.105	25
05/27-17:39:47.392166	[**] TCP SMTP Source Port traffic [**]	212.209.122.1	25	MY.NET.253.105	25
06/12-05:51:09.312644	[**] TCP SMTP Source Port traffic [**]	148.204.183.85	25	MY.NET.60.14	25
06/12-05:51:09.312644	[**] TCP SMTP Source Port traffic [**]	148.204.183.85	25	MY.NET.60.14	25

Attackers and spammers will use improperly configured WinGates (read default settings) to bounce through and hide their real source location. There are 22,111 alerts in the logs concerning traffic destined for MY.NET.253.105. In addition, MY.NET.253.12 who we know to be compromised is the source of much WinGate traffic. It is safe to assume there is a problem that should be addressed on the network.

Alert Date	Message	Origin	SP	Destination	DP
05/16-	[**] WinGate 8080 Attempt	216.164.224.7	1333	MY.NET.253.105	8080

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Alert Date	Message	Origin	SP	Destination	DP
00:00:07.913027	[**]				
05/16-00:00:53.854387	[**] WinGate 8080 Attempt [**]	216.164.224.7	1338	MY.NET.253.105	8080
05/16-00:44:19.666218	[**] WinGate 8080 Attempt [**]	172.153.82.138	3618	MY.NET.253.105	8080
05/16-02:06:28.572210	[**] WinGate 8080 Attempt [**]	216.70.70.51	1076	MY.NET.253.105	8080
*****snipped*****					

These records indicate that internal hosts on the network have file sharing set up improperly on their Windows machines and the listed attackers have found the shares.

Alert Date	Message	Origin	SP	Destination	DP
05/24-20:52:48.660568	[**] SMB Name Wildcard [**]	166.90.30.149	137	MY.NET.100.130	137
06/01-09:41:23.949733	[**] SMB Name Wildcard [**]	192.168.7.2	137	MY.NET.14.1	137
05/22-22:13:23.799380	[**] SMB Name Wildcard [**]	63.208.201.185	137	MY.NET.100.130	137
05/22-12:24:00.842981	[**] SMB Name Wildcard [**]	63.208.203.51	137	MY.NET.100.130	137
05/22-20:03:20.508026	[**] SMB Name Wildcard [**]	63.208.207.98	137	MY.NET.100.130	137
05/16-19:54:37.372961	[**] SMB Name Wildcard [**]	63.208.29.210	137	MY.NET.100.130	137
05/22-15:30:13.239348	[**] SMB Name Wildcard [**]	63.208.31.202	137	MY.NET.100.130	137

A variety of known attacks are available for SNMP services ranging from DOS to root compromise. These vulnerabilities range across many devices including routers, printers, firewalls as well as servers and hosts. These known vulnerabilities also affect a wide range of operating systems. In addition, many SNMP community strings are improperly configured and give ready access by the default public/private "passwords". Significant reconnaissance can also be accomplished using SNMP access. There are 2,062 records that triggered alerts all from internal addresses and all to the same host. Although this does not necessarily mean that the host has been compromised, it does indicate there is a vulnerability that should be corrected. Three examples follow.

Alert Date	Message	Origin	SP	Destination	DP
05/23-09:32:38	[**] SNMP public access [**]	MY.NET.97.129	1056	MY.NET.101.192	161
05/23-14:06:46	[**] SNMP public access [**]	MY.NET.97.133	1208	MY.NET.101.192	161
05/23-10:44:29	[**] SNMP public access [**]	MY.NET.97.87	1252	MY.NET.101.192	161

© SANS Institute 2000 - 2002, Author retains full rights.

This questionable activity fell out of the filter. There were a total of 38 packets that triggered alerts and all but the first two were directed at MY.NET.179.77. A search for the answer produced only the fact that other administrators are reporting traffic that triggers this filter.

Alert Date	Message	Origin	SP	Destination	DP
05/25-05:18:02.966270	[**] GIAC 08-feb-2000 [**]	195.11.50.204	4910	MY.NET.100.165	53
05/25-05:18:02.966270	[**] GIAC 08-feb-2000 [**]	195.11.50.204	4910	MY.NET.100.165	53
05/28-06:15:59.482947	[**] GIAC 08-feb-2000 [**]	195.11.50.204	61160	MY.NET.179.77	554
05/28-06:15:59.482947	[**] GIAC 08-feb-2000 [**]	195.11.50.204	61160	MY.NET.179.77	554
05/28-06:15:59.482947	[**] GIAC 08-feb-2000 [**]	195.11.50.204	61160	MY.NET.179.77	554
*****snipped*****					

There are 22,715 alerts in the alert log associated with Watchlist traffic. I will only look at one set of questionable traffic below. Here you see the attacker from the 159.226 Class B send a packet to port 25 of a host on the network. Then a connection is made from the telnet port to port 2055. The pattern is repeated over and over and is shown a second time below. This time the packet goes to port 25 and another host makes a connection to another host.

Alert Date	Message	Origin	SP	Destination	DP
05/22-15:06:18.976327	[**] Watchlist 000222 NET-NCFC [**]	159.226.45.3	1086	MY.NET.253.41	25
05/22-15:12:19.623379	[**] Watchlist 000222 NET-NCFC [**]	159.226.45.3	23	MY.NET.162.121	2055
05/22-15:12:46.488485	[**] Watchlist 000222 NET-NCFC [**]	159.226.45.3	23	MY.NET.162.121	2055
05/22-15:12:47.920323	[**] Watchlist 000222 NET-NCFC [**]	159.226.45.3	23	MY.NET.162.121	2055
05/22-15:12:54.270086	[**] Watchlist 000222 NET-NCFC [**]	159.226.45.3	23	MY.NET.162.121	2055
05/22-15:12:56.700514	[**] Watchlist 000222 NET-NCFC [**]	159.226.45.3	23	MY.NET.162.121	2055
05/22-15:15:06.230462	[**] Watchlist 000222 NET-NCFC [**]	159.226.45.3	23	MY.NET.162.121	2055
05/22-15:15:36.605281	[**] Watchlist 000222 NET-NCFC [**]	159.226.45.3	23	MY.NET.162.121	2055
05/22-22:24:33.063396	[**] Watchlist 000222 NET-NCFC [**]	159.226.120.19	64868	MY.NET.253.41	25
05/23-00:02:56.631299	[**] Watchlist 000222 NET-NCFC [**]	159.226.133.85	25	MY.NET.100.230	46552
05/23-00:02:56.631299	[**] Watchlist 000222 NET-NCFC [**]	159.226.133.85	25	MY.NET.100.230	46552
05/23-00:03:10.456832	[**] Watchlist 000222 NET-NCFC [**]	159.226.133.85	25	MY.NET.100.230	46552
05/23-00:03:10.456832	[**] Watchlist 000222 NET-NCFC [**]	159.226.133.85	25	MY.NET.100.230	46552
*****snipped*****					

© SANS Institute 2000 - 2002, Author retains full rights.

Ports shown below are associated with Trinoo (trin00), a distributed network denial of service tool. The master will have many clients reporting to it and can direct the clients to attack a specific host. Based on the 401 alerts recorded, it is likely that trinoo is on the network.

Alert Date	Message	Origin	SP	Destination	DP
05/16-00:15:24.758792	[**] GIAC 000218 VA-CIRT port 35555 [**]	209.25.8.7	25	MY.NET.253.52	35555
05/16-00:15:30.283879	[**] GIAC 000218 VA-CIRT port 35555 [**]	209.25.8.7	25	MY.NET.253.52	35555
05/16-02:07:34.730600	[**] GIAC 000218 VA-CIRT port 34555 [**]	155.207.19.1	25	MY.NET.100.230	34555
05/16-02:07:38.355649	[**] GIAC 000218 VA-CIRT port 34555 [**]	155.207.19.1	25	MY.NET.100.230	34555

Compromised hosts

This table of data shows the attackers that have successfully connected to port 32771 (SUNRPC). This indicates these hosts have been compromised. In addition, MY.NET.253.12 is listed as a source indicating that he has been compromised as well. MY.NET.253.12 has triggered 4,225 SUNRPC highport alerts indicating he may have compromised other hosts on the 101, 102, 16 and 19 networks. In addition to this activity, there are 6,849 "attempted" alerts in the logs from various attackers.

Alert Date	Message	Origin	SP	Destination	DP
05/24-14:18:05.175232	[**] SUNRPC highport access! [**]	128.8.10.141	23	MY.NET.2.203	32771
05/16-14:34:23.706666	[**] SUNRPC highport access! [**]	132.241.252.14	43345	MY.NET.253.24	32771
06/20-17:04:50.450108	[**] SUNRPC highport access! [**]	192.102.249.3	25	MY.NET.130.94	32771
05/27-22:47:39.173725	[**] SUNRPC highport access! [**]	199.60.228.130	7000	MY.NET.97.106	32771
06/22-13:49:37.272815	[**] SUNRPC highport access! [**]	200.223.1.120	42455	MY.NET.12.53	32771
06/19-00:23:15.811327	[**] SUNRPC highport access! [**]	205.188.4.134	5190	MY.NET.97.119	32771
06/12-16:59:25.978455	[**] SUNRPC highport access! [**]	207.25.253.26	20	MY.NET.70.127	32771
06/16-09:51:34.786129	[**] SUNRPC highport access! [**]	208.226.167.19	21	MY.NET.143.87	32771
06/12-21:42:56.272373	[**] SUNRPC highport access! [**]	24.13.123.8	3708	MY.NET.179.78	32771
06/13-18:22:46.343232	[**] SUNRPC highport access! [**]	24.18.90.197	2468	MY.NET.179.78	32771
06/23-15:42:32.969528	[**] SUNRPC highport access! [**]	24.3.28.220	6000	MY.NET.99.51	32771
05/29-01:50:19.949231	[**] SUNRPC highport access! [**]	MY.NET.253.12	43749	MY.NET.16.195	32771

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Here the internal host is shown SYN scanning another internal host. This traffic is concerning because the activity is not normal traffic and the source is internal.

Scan Date	Origin	SP	Destination	DP	State	Flag	RBits
5/27/2000 11:44:42 PM	MY.NET.253.12	43746	MY.NET.14.1	797	SYN	**S*****	
5/27/2000 11:44:42 PM	MY.NET.253.12	43746	MY.NET.14.1	983	SYN	**S*****	
5/27/2000 11:44:42 PM	MY.NET.253.12	43746	MY.NET.14.1	667	SYN	**S*****	
*****snipped*****							

Here the same internal host is going through hosts looking for specific services. This is part of a much larger scan. The attacker repeats these ports on the same hosts and then marches on sequentially through many networks.

Alert Date	Message	Origin	SP	Destination	DP
05/28-14:33:41.408218	[**] WinGate 1080 Attempt [**]	MY.NET.253.12	43746	MY.NET.16.3	1080
*****snipped*****					
05/28-14:34:03.399053	[**] WinGate 8080 Attempt [**]	MY.NET.253.12	43747	MY.NET.16.3	8080
*****snipped*****					
05/28-14:34:34.562778	[**] SUNRPC highport access! [**]	MY.NET.253.12	43746	MY.NET.16.3	32771
*****snipped*****					
05/28-14:36:19.467825	[**] NMAP TCP ping! [**]	MY.NET.253.12	43758	MY.NET.16.3	36384
*****snipped*****					
05/28-14:36:27.126701	[**] NMAP TCP ping! [**]	MY.NET.253.12	43758	MY.NET.16.3	40341
*****snipped*****					
05/28-14:36:33.568525	[**] NMAP TCP ping! [**]	MY.NET.253.12	43758	MY.NET.16.3	36650
*****snipped*****					

The data below shows that our internal scanner has been the host for some scans as well. We may be dealing with a compromised system or an internal threat.

Scan Date	Origin	SP	Destination	DP	State	Flag	RBits
6/1/2000 2:38:10 AM	202.38.128.188	1904	MY.NET.253.12	8080	SYN	**S*****	
6/4/2000 2:28:29 AM	203.233.103.188	53	MY.NET.253.12	53	SYNFIN	**SF****	
6/4/2000 4:39:16 PM	24.13.87.239	2561	MY.NET.253.12	53	SYN	**S*****	
6/4/2000 7:13:43 PM	210.97.12.129	109	MY.NET.253.12	109	SYNFIN	**SF****	
6/5/2000 1:58:49 AM	208.220.120.13	53	MY.NET.253.12	53	SYNFIN	**SF****	
6/7/2000 11:36:51 PM	195.76.27.44	65535	MY.NET.253.12	53	SYN	**S*****	
6/11/2000 11:56:54 PM	24.27.187.245	53	MY.NET.253.12	53	SYNFIN	**SF****	
6/15/2000 6:45:40 PM	194.179.163.253	53	MY.NET.253.12	53	SYNFIN	**SF****	
6/20/2000 6:07:13 PM	211.53.209.109	2666	MY.NET.253.12	27374	SYN	**S*****	

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

These records were copied from the alert logs and are not intended to show any traffic in particular. The intent is to illustrate that other internal hosts are involved in questionable activity. Note that MY.NET.1.3 and MY.NET.1.4 are suspected to be running DNS services.

Alert Date	Message	Origin	SP	Destination	DP
05/26-17:31:07.358910	[**] spp_portscan: End of portscan from MY.NET.1.3 (TOTAL HOSTS:3 TCP:0 UDP:11) [**]				
06/20-11:23:28.124888	[**] spp_portscan: End of portscan from MY.NET.1.4 (TOTAL HOSTS:1 TCP:0 UDP:12) [**]				
06/16-15:06:24.676948	[**] spp_portscan: End of portscan from MY.NET.100.164 (TOTAL HOSTS:1 TCP:0 UDP:8) [**]				
05/31-15:03:59.573846	[**] spp_portscan: End of portscan from MY.NET.101.1 (TOTAL HOSTS:1 TCP:1 UDP:0) [**]				
05/28-16:20:31.869303	[**] spp_portscan: End of portscan from MY.NET.101.192 (TOTAL HOSTS:1 TCP:0 UDP:10) [**]				
05/29-07:46:49.152997	[**] spp_portscan: End of portscan from MY.NET.19.10 (TOTAL HOSTS:1 TCP:1 UDP:0) [**]				
05/29-20:05:00.255467	[**] spp_portscan: End of portscan from MY.NET.253.12 (TOTAL HOSTS:2 TCP:9616 UDP:16) [**]				
05/28-15:47:06.274373	[**] spp_portscan: End of portscan from MY.NET.70.234 (TOTAL HOSTS:210 TCP:214 UDP:0) [**]				

Network concerns

The network is believed to be switched and the configuration and/or sensor placement is preventing capture of all traffic. In many cases throughout the analysis, having the packets that were sent in response to the suspect packets would have been of great help.

There are also data missing during the collection period. These could be the result of hardware/software problems, power outages, etc.

Our sensor is probably dropping packets as illustrated by the capture below. In addition to the problem of not having the time recorded to the millisecond, we can determine that this scan is using sequential port numbers to scan sequential hosts. We miss packets between MY.NET.97.116 and MY.NET.97.138 and then the sequence continues.

Scan Date	Origin	SP	Destination	DP	State	Flag	RBits
6/22/2000 10:50:55 AM	212.133.136.96	1528	MY.NET.97.115	44767	UDP		
6/22/2000 10:50:55 AM	212.133.136.96	1529	MY.NET.97.116	44767	UDP		
6/22/2000 10:50:55 AM	212.133.136.96	1551	MY.NET.97.138	44767	UDP		

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Scan Date	Origin	SP	Destination	DP	State	Flag	RBits
6/22/2000 10:50:55 AM	212.133.136.96	1552	MY.NET.97.139	44767	UDP		
6/22/2000 10:50:55 AM	212.133.136.96	1553	MY.NET.97.140	44767	UDP		

Recommendations

Qualified staff should be retained to secure and monitor the network. Perimeter defenses should be deployed and/or strengthened and intrusion detection should be properly set up and "tuned" for the network to reduce false alarms. The qualified staff will address the issues listed above under "Network Concerns".

Finally, since there are compromised hosts on the network, all of the hosts on the network need to be scanned for vulnerabilities and cleaned as appropriate. There may also be other issues needing attention such as "Inappropriate Use".

© SANS Institute 2000 - 2002, Author retains full rights.

Last Updated: May 23rd, 2017

Upcoming Training

Mentor Session - SEC503	Oceanside, CA	May 29, 2017 - Jun 29, 2017	Mentor
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANSFIRE 2017 - SEC503: Intrusion Detection In-Depth	Washington, DC	Jul 24, 2017 - Jul 29, 2017	vLive
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
SANS vLive - SEC503: Intrusion Detection In-Depth	SEC503 - 201709,	Sep 11, 2017 - Oct 18, 2017	vLive
Baltimore September 2017 - SEC503: Intrusion Detection In-Depth	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Scottsdale SEC503	Scottsdale, AZ	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS October Singapore 2017	Singapore, Singapore	Oct 09, 2017 - Oct 28, 2017	Live Event
Community SANS Ottawa SEC503	Ottawa, ON	Oct 16, 2017 - Oct 21, 2017	Community SANS
SANS San Diego 2017	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	Live Event
San Diego Fall 2017 - SEC503: Intrusion Detection In-Depth	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	vLive
SANS Seattle 2017	Seattle, WA	Oct 30, 2017 - Nov 04, 2017	Live Event
SIEM & Tactical Analytics Summit & Training	Scottsdale, AZ	Nov 28, 2017 - Dec 05, 2017	Live Event
SANS OnDemand	Online	Anytime	Self Paced
SANS SelfStudy	Books & MP3s Only	Anytime	Self Paced