Global Information Assurance Certification Paper

Dwayne E. Spriggs

Version 2.9

The GCIA Practical

Assignment 1-Network Detects
- Trace Analysis 1
- Trace Analysis 2
- Trace Analysis 3
- Trace Analysis 4
- Trace Analysis 5

Assignment 2
- Research Paper "HIDS Vs. NIDS"

Assignment 3 "Analyze This"
- Overview
- Alert Logs
- OSS (Out of Spec) Analysis
- Scan Logs Analysis
- Analysis Summary
- Analysis Process
- References and Resources

Assignment 1

Trace Analysis 1

1. Source of Trace

WWW.SANS.ORG/Y2K/040901-1500.HTM

```
Apr  3 16:50:58 hostka portsentry[430]: attackalert: Connect from host:
  pc129-lut21.cable.ntl.com/213.107.39.129 to TCP port: 1080
Apr  3 16:51:02 hosth portsentry[382]: attackalert: Connect from host:
  pc129-lut21.cable.ntl.com/213.107.39.129 to TCP port: 1080
Apr  3 16:51:09 hostman portsentry[186]: attackalert: Connect from
host:
  pc129-lut21.cable.ntl.com/213.107.39.129 to TCP port: 1080
Apr  3 16:51:09 hostl portsentry[386]: [ID 702911 daemon.notice]
attackalert:
  Connect from host: pc129-lut21.cable.ntl.com/213.107.39.129 to TCP
port: 1080
Apr  3 16:51:09 hostl portsentry[386]: [ID 702911 daemon.notice]
attackalert:
  Connect from host: pc129-lut21.cable.ntl.com/213.107.39.129 to TCP
port: 1080
Apr  3 16:51:10 hostci portsentry[556]: attackalert: Connect from host:
  pc129-lut21.cable.ntl.com/213.107.39.129 to TCP port: 1080
Apr  3 16:51:10 hostt portsentry[653]: attackalert: Connect from host:
  pc129-lut21.cable.ntl.com/213.107.39.129 to TCP port: 1080
Apr  3 16:51:10 hostt portsentry[653]: attackalert: Connect from host:
  pc129-lut21.cable.ntl.com/213.107.39.129 to TCP port: 1080

Apr  3 16:50:57 hostka snort: SCAN wingate attempt: 213.107.39.129:4488
```

```
->
  a.b.c.225:1080
Apr  3 16:54:04 hostka snort: SCAN wingate attempt: 213.107.39.129:1894
->
  a.b.c.225:1080
```

2. Detection was generated by:

Port Sentry Scan monitor

3. Probability the source address was spoofed

This log was created by Port Sentry, which by design recognizes ports scans. Although the source port can be spoofed in order to be affective port scans require an un-spoofed addressed. This allows the attacker to gather the data created by the port scan for future attack targets.

4. Description of Attack

This type of scan is focus on the same port (1080) on multiple host.

5. Attack Mechanism

This port scan is looking for host with an open port 1080, which is the port for a SOCK connection. SOCK connections allow a client to access the Internet through a SOCK server. The client assumes the SOCKS servers IP address. Attackers use SOCK servers as proxies to hide their source address on the Internet. The snort logs show this as a Wingate scans. Wingate is a popular SOCKS server application. www.wingate.com

This is a typical reconnaissance tactic for finding proxies server on the Internet for potential use during future attacks.

6. Correlations

WWW.Incidents.org has an extensive list of detects that correlate to this type of scan. Below is a sample list of these correlations.

http://www.incidents.org/archives/y2k/100600.htm
http://www.incidents.org/archives/intrusions/msg01122.html

7. Evidence of active targeting

This port scan could potentially cover multiple subnets and in this class C network. The scan is most effective it covers multiple host.

8. Severity

Severity is determined using the following formula

(Critical + Lethal)-(System + Net Countermeasures) = Severity

Critical = 3: The system does not appear to be critical system but could be so a neutral is assigned.

Lethal = 1: At this point the attack is in the reconnaissance phase the attacker is checking multiple host for this port. No evidence of data exchange.

System Countermeasures = 4: The system is running port sentry.

Network Countermeasures = 4: The network is running snort.

(3 + 1) – (4+4) = 4 – 8 = 4

9. Defensive Recommendation:

Port Sentry alerted on this attack. Port Sentry has the ability to stop this connection by sending a reject packet to the attackers host. This feature was not enabled for this type of attack. Instead port Sentry sent an alert using the "daemon.notice". If this notice is not received in real time it is too late to act. Port Sentry should be configured to reject attempted connections to port 1080 on this network.

10. Multiple choice test question.

Which service uses port 1080?

A. Back Orifice
B. SMTP
C. Telnet
D. SOCK

Trace Analysis 2

1. Source of Trace

www.sans.org/y2k/040901-1500.hm

```
Server used for this query: [ whois.ripe.net ]
        inetnum:     213.156.192.0 - 213.156.194.191
```

```
        netname:     KRAFT-S
        descr:       Kraft-s joint stock company
        descr:       Computer trading and ISP
        country:     RU

Apr  3 18:59:30 hostmau portsentry[155]: attackalert: Connect from
host:
  igostest.kraft-s.ru/213.156.193.17 to TCP port: 111
Apr  3 19:09:54 hostmau portsentry[2615]: attackalert: Connect from
host:
  igostest.kraft-s.ru/213.156.193.17 to UDP port: 111
Apr  3 19:39:18 hostmau portsentry[2615]: attackalert: Connect from
host:
  igostest.kraft-s.ru/213.156.193.17 to UDP port: 111

Apr  3 19:01:22 hostbe rpcbind: refused connect from 213.156.193.17 to
getport(status)
Apr  3 19:30:46 hostre rpcbind: refused connect from 213.156.193.17 to
getport(status)
Apr  3 19:30:46 hostbe rpcbind: refused connect from 213.156.193.17 to
getport(status)
Apr  3 19:30:51 hostbe rpcbind: refused connect from 213.156.193.17 to
getport(status)
```

2. Detection was generated by:

Port Sentry Scan monitor

3. Probability the source address was spoofed

This type of attack would require an un-spoofed address make use of the information returned by the attack.

4. Description of Attack

This attack queries port 111 on multiple hosts.

5. Attack Mechanism

This port 111 is used for RPC bind or portmapper on SUN Solaris systems. Portmapper maps programs running on the system to TCP\UDP ports. This allows programs to run remotely using RPC. The attacker uses getport (status) to get this information. Querying the status of portmapper can provide information to an attacker on what type of programs are running on the host. This attack can have multiple end results ranging from root access to a DOS attack.

6. Correlations

http://www.incidents.org/archives/intrusions/msg00621.html

http://www.incidents.org/archives/y2k/022801.htm

7. Evidence of active targeting

The attack targets a few host. This could be the follow up of earlier reconnaissance scan. Which narrowed the list of target potential targets.

8. Severity

Severity is determined using the following formula

(Critical + Lethal)-(System + Net Countermeasures) = Severity

Critical = 3: Unable to determine the criticality of the targeted hosts. The type of attack can make the host the starting point for others attacks.

Lethal = 5: The attack can lead to several types of exploits.

System Countermeasures = 2: The hosts are running port sentry and the connections were refused in some cases. I am unsure of the security patch level on the host.

Network Countermeasures = 3: Unsure

(4 + 5) – (2+3) = 9 – 5 = 4

9. Defensive Recommendation:

Port Sentry refuses this connection on some hosts. This attack is targeted for SUN systems a firewall should be used to prevent these types of connections from external sources.

10. Sample test question:

What is portmapper used for?

A. Connecting Share Drives
B. Connecting Printers
C. Mapping RPC services
D. Mapping the way to work

Trace Analysis 3

1. Source of Trace

www.sans.org/y2k/040901-1500.hm

```
        Server used for this query: [ whois.ripe.net ]
        inetnum:     213.224.128.0 - 213.224.223.255
        netname:     TELENET
        descr:       Telenet Operaties N.V.
        country:     BE

Apr  3 20:18:26 213.224.200.131:1718 -> a.b.c.9:21 SYN ******S*
Apr  3 20:18:23 213.224.200.131:1739 -> a.b.c.30:21 SYN ******S*
Apr  3 20:18:23 213.224.200.131:1742 -> a.b.c.33:21 SYN ******S*
Apr  3 20:18:23 213.224.200.131:1760 -> a.b.c.51:21 SYN ******S*
Apr  3 20:18:23 213.224.200.131:1781 -> a.b.c.72:21 SYN ******S*
Apr  3 20:18:23 213.224.200.131:1780 -> a.b.c.71:21 SYN ******S*
Apr  3 20:18:23 213.224.200.131:1789 -> a.b.c.80:21 SYN ******S*
Apr  3 20:18:26 213.224.200.131:1790 -> a.b.c.81:21 SYN ******S*
Apr  3 20:18:41 213.224.200.131:2252 -> a.b.e.34:21 SYN ******S*
Apr  3 20:18:41 213.224.200.131:2260 -> a.b.e.42:21 SYN ******S*
Apr  3 20:18:41 213.224.200.131:2270 -> a.b.e.52:21 SYN ******S*

Apr 03 20:18:40 hostl proftpd[7257] hostl (D5E0C883.kabel.telenet.be
  [213.224.200.131]): connected - local  : a.b.c.57:21
Apr 03 20:18:40 hostl proftpd[7257] hostl (D5E0C883.kabel.telenet.be
  [213.224.200.131]): connected - remote : 213.224.200.131:1766
Apr 03 20:18:40 hostl proftpd[7257] hostl (D5E0C883.kabel.telenet.be
  [213.224.200.131]): FTP session opened.
Apr 03 20:18:40 hostl proftpd[7257] hostl (D5E0C883.kabel.telenet.be
  [213.224.200.131]): received: USER anonymous
Apr 03 20:18:40 hostl proftpd[7257] hostl (D5E0C883.kabel.telenet.be
  [213.224.200.131]): received: PASS (hidden)
Apr 03 20:18:40 hostl proftpd[7257] hostl (D5E0C883.kabel.telenet.be
  [213.224.200.131]): ANON anonymous: Login successful.
Apr 03 20:18:40 hostl proftpd[7257] hostl (D5E0C883.kabel.telenet.be
  [213.224.200.131]): Preparing to chroot() the environment, path =
'/var/local/ftp'
Apr 03 20:18:40 hostl proftpd[7257] hostl (D5E0C883.kabel.telenet.be
  [213.224.200.131]): Environment successfully chroot()ed.
Apr 03 20:18:41 hostl proftpd[7257] hostl (D5E0C883.kabel.telenet.be
  [213.224.200.131]): received: CWD /pub/
Apr 03 20:18:41 hostl proftpd[7257] hostl (D5E0C883.kabel.telenet.be
  [213.224.200.131]): received: MKD 010404021720p
```

2. Detection was generated by:

Possibly TCP-DUMP

3. Probability the source address was spoofed

The probability of a spoofed address is low. Both phases of this attack require return packets to be successful.

4. Description of Attack

A port scan is used to identify FTP host on a network.
Once a host with an open FTP port is located the attack is launched

5. Attack Mechanism

The attack starts off with a scan using syn packets searching for open port 21 (FTP) on multiple hosts. The information gathered during the port scan is later used in the attack establishing an FTP session with a host. The attacker successfully logs on as an anonymous user. The attacker then issues the chroot() function call. The chroot() function is used to establish a new root path for a particular process. It reassigns the "/" to pathname used in the chroot() function. This allows processes to run and only have access to the path define in the chroot() function. In this case the chroot() function could have been used to establish a new root for the FTP process on the server. When the attacker issues the chroot() function with no path the root is set back to the default root of the server. The attacker then changes to the /pub/ directory and creates a new directory. From this point the attacker can create directories and files at will. The attacker creates a directory with a long name. This could be an attempt to exploit a potential "FTP Long Path Buffer Overflow Vulnerability" on the FTP server.
www.securityfocus.com/bid/2242

6. Correlations

The pre-attack measure of scanning multiple hosts for FTP connections directly correlates with the attack later using the FTP port.

Similar patterns can also be found at:
http://www.incidents.org/archives/intrusions/msg00851.html

http://www.incidents.org/archives/intrusions/msg00713.html

7. Evidence of active targeting

The pre-attack is not targeted for a specific host. The pre-attack may be targeted for a specific network however. The actual attack is targeted to an FTP server most likely identified by the pre-attack scan.

8. Severity

Severity is determined using the following formula

(Critical + Lethal)-(System + Net Countermeasures) = Severity

Critical = 3: Unable to determine the criticality of the targeted hosts. The host is running FTP services.

Lethal = 5: Once the attacker has changed the chroot() environment they could get access to the other files.

System Countermeasures = 1: The host is compromised due to an vulnerable implementation of chroot() and anonymous access is allowed.

Network Countermeasures = 1: I firewall or IDS would do little in preventing this attack, especially if FTP is allowed from external sources to this host.

(3+ 5) – (1+1) = 8 – 2 = 6

9. Defensive Recommendation:

Tighten security of the FTP server. If anonymous access is not necessary it should not be allowed. Configure the FTP service to run at a non-root level.

This link gives examples of how to correctly implement chroot()

http://www.incidents.org/protect/borland.php

10. Sample test question:

What is a SYN packet?

A. The last packet in a three way handshake
B. The first packed in a three way handshake
C. A whois query packet
D. A DNS lookup packet

Trace Analysis 4

1. Source of Trace

www.sans.org/y2k/042401.htm

```
Server used for this query: [ whois.arin.net ]
California Regional Internet, Inc. (NETBLK-CARI)
8929A COMPLEX DRIVE SAN DIEGO, CA 92123 US
Netname: CARI
```

```
        Netblock: 209.126.128.0 - 209.126.175.255
        Maintainer: CALI

Apr 13 11:48:25 209.126.168.231:4504 -> a.b.c.114:53 SYN ******S*
Apr 13 11:48:25 209.126.168.231:4597 -> a.b.c.207:53 SYN ******S*
Apr 13 11:48:28 209.126.168.231:4420 -> a.b.c.30:53 SYN ******S*
Apr 13 11:48:28 209.126.168.231:4441 -> a.b.c.51:53 SYN ******S*
Apr 13 11:48:28 209.126.168.231:4461 -> a.b.c.71:53 SYN ******S*
Apr 13 11:48:28 209.126.168.231:4472 -> a.b.c.82:53 SYN ******S*
Apr 13 11:48:28 209.126.168.231:4557 -> a.b.c.167:53 SYN ******S*
Apr 13 11:48:28 209.126.168.231:1388 -> a.b.c.225:53 SYN ******S*
Apr 13 11:48:28 209.126.168.231:1107 -> a.b.c.225:53 UDP
Apr 13 11:48:28 209.126.168.231:1407 -> a.b.c.244:53 SYN ******S*
Apr 13 11:48:31 209.126.168.231:1528 -> a.b.d.52:53 SYN ******S*
Apr 13 11:48:31 209.126.168.231:1678 -> a.b.d.202:53 SYN ******S*
Apr 13 11:48:31 209.126.168.231:1928 -> a.b.e.195:53 SYN ******S*
Apr 13 11:48:31 209.126.168.231:1947 -> a.b.e.214:53 SYN ******S*
Apr 13 11:48:32 209.126.168.231:1952 -> a.b.e.219:53 SYN ******S*
Apr 13 11:48:35 209.126.168.231:1971 -> a.b.e.238:53 SYN ******S*
Apr 13 11:48:37 209.126.168.231:2938 -> a.b.f.145:53 SYN ******S*
Apr 13 11:48:40 209.126.168.231:2941 -> a.b.f.148:53 SYN ******S*
Apr 13 11:48:37 209.126.168.231:2942 -> a.b.f.149:53 SYN ******S*
Apr 13 11:48:40 209.126.168.231:2947 -> a.b.f.154:53 SYN ******S*
Apr 13 11:48:37 209.126.168.231:2957 -> a.b.f.164:53 SYN ******S*
Apr 13 11:48:37 209.126.168.231:2959 -> a.b.f.166:53 SYN ******S*
Apr 13 11:48:37 209.126.168.231:2974 -> a.b.f.181:53 SYN ******S*
Apr 13 11:48:37 209.126.168.231:2976 -> a.b.f.183:53 SYN ******S*
Apr 13 11:48:40 209.126.168.231:2985 -> a.b.f.192:53 SYN ******S*
Apr 13 11:48:40 209.126.168.231:3041 -> a.b.f.246:53 SYN ******S*
Apr 13 11:48:40 209.126.168.231:1713 -> a.b.d.237:53 SYN ******S*
Apr 13 11:48:40 209.126.168.231:1947 -> a.b.e.214:53 SYN ******S*
Apr 13 11:48:41 209.126.168.231:1971 -> a.b.e.238:53 SYN ******S*
Apr 13 11:48:41 209.126.168.231:2340 -> a.b.f.18:53 SYN ******S*

Apr 13 11:48:28 hostka named[17373]: security: notice: denied query
from
  [209.126.168.231].1107 for "version.bind"
Apr 13 11:47:52 hosth /kernel: Connection attempt to TCP a.b.c.62:53
from
  209.126.168.231:4452
Apr 13 11:48:28 hostka named[17373]: security: notice: denied query
from
  [209.126.168.231].1107 for "version.bind"
Apr 13 11:48:54 hostmf /kernel: Connection attempt to TCP a.b.f.167:53
from
  209.126.168.231:2960
Apr 13 11:48:28 hostka snort: DNS named version attempt:
209.126.168.231:1107
  -> a.b.c.225:53
Apr 13 11:48:28 hostka snort: DNS named version attempt:
209.126.168.231:1107
  -> a.b.c.225:53
```

2. Detection was generated by:

TCP Dump and Snort

3. Probability the source address was spoofed

Low, the attacker is attempting to establish a connection to send to and receive packets.

4. Description of Attack

The attack starts with a port scan target for port 53 on multiple systems. Once the attacker identifies an active host a connection is established.

5. Attack Mechanism

Port 53 is the port for DNS query. Most firewalls have this port open to allow DNS servers to communicate with the Internet. The software that runs DNS is called BIND. Several versions of BIND have security flaws that can lead to exploits such as root access or DNS spoofing. Once the attacker has identified an active host the attacker queries the host for BIND Version. This information can provide the attacker the types of vulnerabilities exist on the DNS servers. The attacker tries several query tactics to get the version of DNS BIND being used.

6. Correlations

http://www.incidents.org/archives/intrusions/msg00215.html

http://www.securityfocus.com/bid/2302

7. Evidence of active targeting

Pre-Attack is not targeted but the actual attack is target for a discovered active DNS server.

8. **Severity**

Severity is determined using the following formula

(Critical + Lethal)-(System + Net Countermeasures) = Severity

Critical = 5: The targeted host is a DNS server. A compromise of this server can disrupt several other network servers.

Lethal = 5: There are several exploits associated with DNS.

System Countermeasures = 5: The host rejects the query of the DNS version providing evidence that patches are in place preventing this type of query.

Network Countermeasures = 5: Snort is installed on the network.

(5+ 5) – (5+5) = 10 – 10 = 0

9. Defensive Recommendation:

The attack appears to be unsuccessful. It is difficult to determine from the logs if the DNS servers provide the attacker with the BIND version information. None the less BIND should be updated to latest version which has been patched to ignore this type of query.

10. Test Question

When does DNS use a TCP connection instead of a UDP connection?

a. During a zone transfer
b. Queries
c. Large Queries and Response
d. A and C
e. B and C
f. None of the above

Trace Analysis 5

1. Source of Trace

www.sans.org/y2k/040901-1500.hm

```
Server used for this query: [ whois.arin.net ]
        Colgate University (NET-COLGATE-)
        Computer Center 13 Oak Drive Hamilton, NY 13346 US
        Netname: COLGATE-1
        Netblock: 149.43.0.0 - 149.43.255.255

Apr  5 03:12:55 hostmau portsentry[155]: attackalert: Connect from
host:
  netmon.colgate.edu/149.43.160.160 to TCP port: 515
Apr  5 03:14:57 hostmau portsentry[155]: attackalert: Connect from
host:
  netmon.colgate.edu/149.43.160.160 to TCP port: 515
Apr  5 03:14:58 hostmau portsentry[155]: attackalert: Connect from
host:
  netmon.colgate.edu/149.43.160.160 to TCP port: 515
Apr  5 03:14:58 hostmau portsentry[155]: attackalert: Connect from
host:
  netmon.colgate.edu/149.43.160.160 to TCP port: 515
```

```
Apr  5 03:15:04 hostmau portsentry[155]: attackalert: Connect from
host:
  netmon.colgate.edu/149.43.160.160 to TCP port: 515
Apr  5 03:15:04 hostmau portsentry[155]: attackalert: Connect from
host:
  netmon.colgate.edu/149.43.160.160 to TCP port: 515
Apr  5 03:15:06 hostmau portsentry[155]: attackalert: Connect from
host:
  netmon.colgate.edu/149.43.160.160 to TCP port: 515
Apr  5 03:15:06 hostmau portsentry[155]: attackalert: Connect from
host:
  netmon.colgate.edu/149.43.160.160 to TCP port: 515
Apr  5 03:15:06 hostmau portsentry[155]: attackalert: Connect from
host:
  netmon.colgate.edu/149.43.160.160 to TCP port: 515
Apr  5 03:15:07 hostmau portsentry[155]: attackalert: Connect from
host:
  netmon.colgate.edu/149.43.160.160 to TCP port: 515
Apr  5 03:15:08 hostmau portsentry[155]: attackalert: Connect from
host:
  netmon.colgate.edu/149.43.160.160 to TCP port: 515
Apr  5 03:15:08 hostmau portsentry[155]: attackalert: Connect from
host:
  netmon.colgate.edu/149.43.160.160 to TCP port: 515
Apr  5 03:15:08 hostmau portsentry[155]: attackalert: Connect from
host:
  netmon.colgate.edu/149.43.160.160 to TCP port: 515
Apr  5 03:15:09 hostmau portsentry[155]: attackalert: Connect from
host:
  netmon.colgate.edu/149.43.160.160 to TCP port: 515

Apr  5 03:14:57 hostmau Connection attempt to TCP z.y.x.28:3879 from
  149.43.160.160:2040
Apr  5 03:14:58 hostmau Connection attempt to TCP z.y.x.28:3879 from
  149.43.160.160:2388
Apr  5 03:14:59 hostmau Connection attempt to TCP z.y.x.28:3879 from
  149.43.160.160:2725
Apr  5 03:15:02 hostmau Connection attempt to TCP z.y.x.28:3879 from
  149.43.160.160:4443
Apr  5 03:15:03 hostmau Connection attempt to TCP z.y.x.28:3879 from
  149.43.160.160:4791
Apr  5 03:15:04 hostmau Connection attempt to TCP z.y.x.28:3879 from
  149.43.160.160:1141
Apr  5 03:15:04 hostmau Connection attempt to TCP z.y.x.28:3879 from
  149.43.160.160:1453
Apr  5 03:15:05 hostmau Connection attempt to TCP z.y.x.28:3879 from
  149.43.160.160:1889
Apr  5 03:15:06 hostmau Connection attempt to TCP z.y.x.28:3879 from
  149.43.160.160:2308
```

2. Detection was generated by:

Port Sentry

3. Probability the source address was spoofed

There is a high probability the source addressed was not spoofed. This attack does not have the characteristic of a port scan since the targeted host and port are constant. There is no evidence of a requirement for the attacker to view the return packet. However the type of exploits sought after in this attack would be difficult to accomplish without seeing return packets.

4. Description of Attack

The attacker sends packets to port 515 on a particular host. The attacker then sends packets to port 3879 on the same host.

5. Attack Mechanism

The attacker connects to port 515 on a host. This can either be an attempt at a Dos attack on the lpd printer port of a windows system (www.securityfocus.com/bid/1082) or an attempt to execute arbitrary code on the same port using a buffer overflow (www.securityfocus.com/bid/2894) on a Unix system. The latter of the two is more likely since the attacker later tries to connect to port 3879 and exploit and vulnerability know as "GNOME gdm XCDMCP buffer Overflow Vulnerability" (www.securityfocus.com/bid/1233.html) to once again execute arbitrary code. This vulnerability maps a root shell to port 3879 to allow the attacker to execute code at the root level. (www.netice.com/advice/exploits/ports/3879/default.htm).

6. Correlations

http://www.incidents.org/archives/y2k/040401.htm
http://www.incidents.org/archives/y2k/040401-1145.htm

7. Evidence of active targeting

The attacked is focused on one port and one host. In addition multiple exploits were attempted on the same host. This reduces the chance of this being a random host or part of a larger group of targeted host.

8. Severity

Severity is determined using the following formula

(Critical + Lethal)-(System + Net Countermeasures) = Severity

Critical = 3: Unable to determine the criticality of the targeted hosts.

Lethal = 5: Either a DoS or root access will be result of this attack if successful.

System Countermeasures = 3: Port Sentry is in place on the on the host but, packets wer not rejected.

Network Countermeasures = 3: Unknown. .

(3+5) – (3+3) = 8 – 6 = 2

9. Defensive Recommendation:

Both vulnerabilities targeted here are products of older software. The best way to eliminate this vulnerability is to update the software to latest version.

10. Test Question

What type of vulnerabilities is exploited during this attack?

a. TCP\IP
b. UDP\IP
c. OS
d. Hardware

Assignment 2

Host-Base (HIDS) VS Network Based (NIDS)

Just like a router, firewall or switch, the Intrusion Detection System (IDS) has become a standard part of any network. Although you won't find much argument on the importance of IDS you will find different opinions on where they should be used. There are two basic types of IDS, Network-based and Host-based. This research paper will discuss some of the common points on making a decision on the type of IDS you should use.

What are the Differences?

Host-based IDS (HIDS) are installed on the host and monitor systems for changes and other events. Like the Anti-Virus software HIDS use signatures to detect malicious intent. HIDS can also monitor the communication ports on a system for malicious connection attempts. Most HIDS can take multiple actions once an attack is detected.

Network-based IDS (NIDS) are installed on a host and monitor network traffic. These hosts have a network card configured into promiscuous mode to capture packets on the network. The network traffic is then compared against attack signatures. NIDS are not host specific and run on separate OS platforms. NIDS can also take multiple actions in real time if an attack is detected.

Platform Support

Although the list of support platforms for HIDS is extensive it is not complete. Even the leading providers of HIDS do not support every platform and every version of every platform. Making the ability to fully deploy a HIDS in a large enterprise difficult when multiple platforms are used.

In detecting attacks on systems NIDS are platform independent. Platforms become a factor with the platform the NIDS host is using. This may force you to support a platform that you previously chose not to, just for the implementation of the NIDS. No matter what the platform of the NIDS host it will still detect attacks regardless of the targeted platform.

Effectiveness

HIDS rely on system changes and log entries to determine an attack. In some situations this is too late to be effective. If the attack has already occurred the damage is already done. For instance a DoS attack could crash the system before the HIDS got a chance to act on the attack. If the host running the HIDS crashes then so does the HIDS. The action the HIDS is configured to take during an attack (for example send an alert to the system administrator) may never be performed. Using HIDS that control on monitor connections to the host ports can reduce this risk.

Some HIDS have the ability to monitor connection attempts to communications ports. This would be fine on host that does not expect connection attempts such as a home pc. A HIDS on host that expects connections attempts such as a web server may not be able to determine the difference between a legitimate HTTP connection and a malicious one.

NIDS rely on network traffic to determine attacks. Some NIDS (ISS Real Secure for example) can intercept connection attempts by sending reject packets to the attacker closing their connection. Even if the targeted host falls victim to the attack the NIDS can still act on the attack.

Since NIDS rely on network traffic patterns an attacker can generate traffic to flood the NIDS with information causing the NIDS to miss packets or even become overwhelmed to the point that it is in effective (the STICK exploit does this).

In addition NIDS can be prone to false positives. False positives occur when network activity resembles and attack but in fact it is normal acceptable behavior. For example most network monitor software use pings to detect if a host is active. If the software does

not get a response from the pinged host it sends out an alert that the host is down. If a NIDS captures this kind of activity it could act as if the host pinged is under a ping flood attack instead of being network monitored. To avoid this type of false positive reporting the NIDS has to be fine tuned to ignore this type of behavior from the network management system. It can take some time to completely fine tune a NIDS to illuminate all false positives.

HIDS are more accurate in its attack recognition. If a file is change or a log entry is made there is no mistaking that it actually occurred and the alerts are not "False Positives".

Performance

HIDS are installed on the host so naturally they rely on the host's processor and memory as resources to function. If the host does not have enough resources then the performance of the HIDS will suffer. Its is hard to determine the amount of resources that will be required to successfully run the HIDS and any other functions the host performs. HIDS vendors do provide estimates but there at too many factors to predetermine how a HIDS will perform in your environment.

The resource of the network host does not matter to the NIDS. On the NIDS host itself vendors recommend that no other programs are running to minimize resource use. The performance issue on the NIDS comes into to play with the amount of network traffic the NIDS has to process. The more network traffic you have the more resources your NIDS will need. NIDS vendor do provide estimates, base on network loads of the resources a NIDS will need.

Network speeds can also play a factor in your NIDS performance. NIDS have a hard enough time keeping up with megabits network speeds. With the increase use of gigabits network speeds NIDS host are forced to be faster and more stream line.

Scalability

A single HIDS can only protect a single host. Therefore each host must have it own HIDS. In a large enterprise this can be costly and difficult to scale. This can be even more costly if the HIDS vendor not only charges per host but per platform used on your network.

A single NIDS can protect multiple hosts. A properly placed NIDS can monitor all hosts on a network. As the number of host grows the number of NIDS does not have to increase. However, if the amount of traffic grows the resources of the host running the NIDS much increase.

Summary

Intrusion Detection will continue to change as IDS technology continues to grow. HIDS have found a strong holding in the home computing environment. Several vendors have geared their HIDS to home use and continue to improve in those areas. All the shortcomings of HIDS do not play as much of a factor in the home pc environment.

NIDS have established themselves in the professional networking environment. The effectiveness and scalability have made them more common than HIDS. To address some the resource shortcoming of NIDS with network speeds and traffic loads, vendors have now developed appliance NIDS. An appliance NIDS is a device with sole purpose is intrusion detection. On a traditional NIDS resources are wasted on running the PC OS and hardware. Appliance NIDS resources are completely dedicated to intrusion detection. This has made the NIDS even more platform independent and streamline.

Major Intrusion detection vendors have begun to integrate both HIDS and NIDS into their Intrusion Detection solutions. Vendors are recommending the use of both, arguing that both play a key role and the weakness of one are the strengths of the other. This new trend proves that you can never have to many methods for protecting your information.

References:

http://www.tripwire.com/products/servers/platforms.cfml
http://www.networkcomputing.com/1023/1023f1.html
http://enterprisesecurity.symantec.com/products/products.cfm?ProductID=48&PID=7715670
http://www.gocsi.com/roundtable.htm
http://www.linux.ie/articles/portsentryandsnortcompared.php

Assignment 3 "Analyze This"

Overview

This security audit provides a list of detects prioritized by occurrences and a brief description of them including information about the external source (if available). The audit provides insight on potential system compromise or any other dangerous activity discovered during the audit. Recommendations will be made on how best to prevent to mitigate the risk of these attacks.

This security audit covers five days of network traffic generated by Snort with a standard rule base. The files used for this audit are as follows:

Name	File Size

Alert-02-Apr	126kb
Alert-02-Apr	1033kb
Alert-03-Apr	1033kb
Alert-23-Mar	1346kb
Alert-26-Mar	1634kb
Alert-27-Mar	1954kb
OOS-APR.02	26kb
OOS-Mar.08.2000.packets.de0	256kb
OOS-Mar.11.2001.packets.de0	27kb
OOS-Mar.12.2001.packets.de0	21kb
OOS-Mar.15.2001.packets.de0	127Kb
OOS-Mar.19.2001.packets.de0	12Kb
ScanSummary01-Apr	11Kb
ScanSummary02-Apr	13Kb
ScanSummary19-Mar	12Kb
ScanSummary22-Mar	8Kb
ScanSummary23-March	10Kb

Analysis of Alert Logs

RPC connection attempt to High Ports

This alert was triggered most frequently in the log files analyzed. This type off connection is targeted to the RPC bind service (also know as portmapper). RPC bind is a service that allows program to request a service from another computer. Vulnerabilities in RPC allows an attacker to remotely remove or add programs at will. This could allow the attacker to gain root access to a system by running an arbitrary program. A DoS attack can also be launched if the attacker removes a program running on the machine. The port used for this attack is 32771.

Sample of RPC logs

Host	Target	Connection	Source Host Info
205.188.153.101	MY.NET.228.90	2	Aol Account
209.150.227.153	MY.NET.224.2	904	New York Based ISP
63.121.232.165	MY.NET.224.2	2906	Indiana Based ISP
63.121.232.165	MY.NET.221.198	8926	" "
216.136.171.195	MY.NET.100.25	10	Sourceforge.net

This connection was attempted 12,748 times with 10 successful connections. There is evidence of active targeting. This is evident since the source host concentrated on very few targets with a large amount of connections. The 10 connections came from Sourceforge.net. This is an open source development website that allows account holders to test code on the website servers. Attackers use these types of sites to develop and test

attack code. This could be an approved connection for testing purposes, however since it was a successful connection it should be investigated further.

Defensive Measures

A firewall with a rule to prevent this type of connection externally or from an un-trusted host should be established. If this functionality is not required it should be removed from any server that does not require it. Not all Unix systems are vulnerable to this type of connection. The proper patches should be installed to fix any remaining vulnerabilities to this type of an attack.

Watchlist

This alert was triggered by connections from Israeli and Amsterdam ISPs. It is difficult to determine if these connections are stimulus or response from a stimulus. Some of the ports connected to are used by Napster. Since Napster allows you to change the default Napster ports, it is possible host are using non-standard host for Napster. Another possibility is that is traffic could be the result of "Stock Monitoring" software running on the host. "Watchlist" are list of stocks that a user of stock monitoring software chooses to monitor and receive real time updates on their status.

Sample of Watchlist Alerts

Host Source	Target	Connections	Source Host Info
212.179.4.50	MY.NET.222.154	6473	Israeli ISP
212.179.72.226	MY.NET.201.238	2164	Israeli ISP
212.179.127.41	MY.NET.156.55	2160	Israeli ISP
212.179.28.66	MY.NET.219.14	831	Israeli ISP
212.179.5.87	MY.NET.219.38	146	Israeli ISP
159.226.92.9	MY.NET.144.54	96	Amsterdam ISP*
212.179.27.6	MY.NET.222.154	80	Israeli ISP
212.179.83.143	MY.NET.219.18	69	Israeli ISP
212.179.95.5	MY.NET.207.210	48	Israeli ISP
212.179.7.182	MY.NET.202.10	44	Israeli ISP

* These hosts did not return an nslookup response. Tracert was used to determine a possible host. The closet resolvable IP belonged to an Amsterdam ISP Network.

This alert was triggered a total of 12,235 times, making it the second highest alert in the log analysis. The host targeted in these connections should be examined to determine which programs (if any) are using these ports

Defensive Measures

A firewall can be used to block these kinds of connections. The host targeted in these connections needs to be examined to determine if these types of connections should be allowed.

Source and Destination Outside Network

This alert was triggered because neither the source nor destinations are part of the network where Snort is running. This could be due to a broadcast packet that has traversed subnets. An analysis of the ports used in these connections reveals that most connections are of a broadcast nature. Below is a summary of the most frequent ports used in connections that generated this alert.

Service	Port No.	Description
BootP	67	Protocol used to configure IP settings on host dynamically. Host will broadcast to find BootP servers if one is not found on the subnet. This is more commonly seen in the use of DHCP to configure Windows host
Netbious-NS	137&138	Protocol used by windows host to resolve name to IP addresses. This is most likely associated to a WINS. However web host using Windows may generate or respond to this type of traffic as well. The Windows host can be configured to broadcast for a Netbios name if one cannot be located on the subnet. An attacker can use port 138 to make a web server believe that packets are local. This can be used to bypass Windows security features that differentiate between local and remote host.
DNS	53	Used to resolve names to IP address.
AIM	5190	Used for file transfer with AOL instant messenger.

Sample of Unkown Source and Destination Logs

Source	Target	Connections
10.0.0.1	10.255.255.255	1502
129.2.225.92	128.183.7.7	502
192.168.0.2	192.168.0.255	383
192.168.0.13	199.45.32.38	55
192.168.0.13	199.45.32.43	46
134.192.134.112	134.192.148.14	44
65.9.246.190	172.173.102.93	40
169.254.77.98	169.254.255.255	33
204.62.41.254	204.62.32.194	32
23.8.3.1	23.8.3.255	32

The Source of some of these connections belongs to a reserved address space. This indicates that there maybe NAT taken place on the network. The use of the "255" address supports the idea of these packets being the result of a broadcast.

Defensive Measures

This traffic poses a minimal threat additional analysis would be needed to determine cause of traffic.

External RPC Call

This traffic triggered and alert because an external host tried to connect using port 111. The same vulnerabilities as motioned above for " **RPC connection attempt to High Ports"** apply to this kind of attack. Port 111 is the default port for RPC connections and the above-mentioned port 32771 is the alternative.

Sample of External RPC Call Logs

This chart shows all the sources and three targets of their connections. The list of different targets is too extensive to include in this document.

Source	Target	Connections	Source Host Info
63.109.70.97	MY.NET.132.209	4	UUNET ISP address assigned to Lima, Peru
63.109.70.97	MY.NET.132.59	4	UUNET ISP address assigned to Lima, Peru
63.109.70.97	MY.NET.135.201	4	UUNET ISP address assigned to Lima, Peru
209.189.124.214	MY.NET.132.194	2	ISP Verio.NET IP range
209.189.124.214	MY.NET.132.203	2	ISP Verio.NET IP range
209.189.124.214	MY.NET.132.238	2	ISP Verio.NET IP range
209.217.53.190	MY.NET.132.1	2	Catalog.com hosting site
209.217.53.190	MY.NET.132.100	2	Catalog.com hosting site
209.217.53.190	MY.NET.132.108	2	Catalog.com hosting site
38.162.57.27	MY.NET.132.1	2	Wnec.edu
38.162.57.27	MY.NET.132.120	2	Wnec.edu
38.162.57.27	MY.NET.132.124	2	Wnec.edu
61.129.39.161	MY.NET.100.130	2	Shanghai Tricon Consult Co.
61.129.39.161	MY.NET.132.101	2	Shanghai Tricon Consult Co
61.129.39.161	MY.NET.132.109	2	Shanghai Tricon Consult Co
63.109.70.97	MY.NET.132.208	2	UUNET ISP address assigned to Lima, Peru
63.109.70.97	MY.NET.132.211	2	UUNET ISP address assigned to Lima, Peru
63.109.70.97	MY.NET.132.219	2	UUNET ISP address assigned to Lima, Peru
209.70.72.22	MY.NET.132.108	1	ISP Verio.NET IP range
209.70.72.22	MY.NET.132.129	1	ISP Verio.NET IP range
209.70.72.22	MY.NET.132.137	1	ISP Verio.NET IP range
61.129.39.161	MY.NET.132.0	1	Shanghai Tricon Consult Co
61.129.39.161	MY.NET.132.10	1	Shanghai Tricon Consult Co

61.129.39.161	MY.NET.132.102	1	Shanghai Tricon Consult Co

The important thing to note here is not the amount of connections per source but the number of different targets involved. This is a well know exploit and attackers spread there searches for across multiple host looking for a vulnerable system. This connection was attempted 294 times. Even though this traffic was similar to the " **RPC connection attempt to High Ports"** traffic these targets were not actively targeted. The wide range of targets covered by each host is evidence of some type of reconnaissance being performed by the source.

Defensive Measures

A firewall with a rule to prevent this type of connection externally or from an un-trusted host should be established. If this functionality is not required it should be removed from any server that does not require it. If the service is required then the security patches addressing this vulnerability must be applied.

Connect to 515 from outside source

These connections are to port 515, which is a "line printer" port used for remote printing. There multiple vulnerabilities associated with this port. They range from DoS to gaining root access to the system. On Sun systems gaining root access can be accomplished by sending arbitrary code to this port. The vulnerability is documented explained at www.securityfocus.com/bid/2894.

Sample Connect to 515 from outside source Logs

This chart shows all the sources and a sample of the targets in the connection.

Source	Target	Connection	Source Host Info
MY.NET.179.78	24.13.123.8	2	Internal Host
63.123.106.6	MY.NET.132.108	2	UUNET ISP Address
63.123.106.6	MY.NET.132.121	2	UUNET ISP Address
63.123.106.6	MY.NET.132.126	2	UUNET ISP Address
24.91.8.50	MY.NET.133.156	2	MediaOne Net
24.91.8.50	MY.NET.135.175	2	MediaOne Net
24.91.8.50	MY.NET.135.48	2	MediaOne Net
216.162.44.140	MY.NET.132.1	1	Inet-Sys
216.162.44.140	MY.NET.132.11	1	Inet-Sys
216.162.44.140	MY.NET.132.12	1	Inet-Sys
212.125.177.199	MY.NET.132.130	2	Telenostra.com
212.125.177.199	MY.NET.132.160	2	Telenostra.com
212.125.177.199	MY.NET.132.243	2	Telnenostra.com
205.238.235.88	MY.NET.133.170	2	Dallas, Texas ISP
205.238.235.88	MY.NET.133.192	2	Dallas, Texas ISP
205.238.235.88	MY.NET.133.196	2	Dallas, Texas ISP
171.64.67.106	MY.NET.134.0	2	Stanford University
171.64.67.106	MY.NET.134.1	2	Stanford University
171.64.67.106	MY.NET.134.16	2	Stanford University

This can also be viewed as a reconnaissance tactic to find available open 515 connections. A total of 362 alerts were triggered by this type of traffic.

Defensive Measures

A firewall with a rule to prevent this type of connection externally or from an un-trusted host should be established. If this functionality is not required it should be removed from any server that does not require it. There are software patches for this vulnerability as well.

Ramen Server Activity

Ramen is an Internet worm that attacks FTP, RPC and Print vulnerabilities. Once the worm affects a host. It changes its default web page to an advertisement for Ramen Noodles (Hence the name). It also scans the network for other vulnerable servers to infect. The scanning process can be bandwidth intensive.

Sample of Ramen Server Activity Logs

This is an example of the type of traffic that will trigger this response.

Source IP	Source Port	Target IP	Target Port
195.163.231.15	2742	MY.NET.219.178	27374
MY.NET.219.178	27374	148.223.158.176	2992
MY.NET.219.178	27374	212.217.49.103	2469
MY.NET.219.178	27374	212.12.228.54	2432
MY.NET.219.178	27374	212.12.228.54	2432
MY.NET.219.178	27374	212.12.228.54	2432

In this sample the external source "195.163.231.15" connects to internal "MY.NET.219.178" using port 2734. This port is known to be used to spread worms and Trojans like SubSeven. "MY.NET.219.178" then tries to connect to other targets using port 2734. This type of traffic triggered 285 alerts.

Defensive Measures

The patches for the RAMEN worm are available and should be applied to all servers that have not had it applied it yet. Preventing port 27374 from entering or exiting network would also help to prevent the spread of this worm

SMB Wildcard

SMB is used by Windows to map network drives or log into a NT domain. Alert logs captured connections from external host connecting to internal host using port 137. When

the source and destination ports are both 137 this can be considered benign behavior, as this is the nature of Windows to broadcast for SMB host. However, when the source port is not 137 or used in conjunction with another port (usually 138 or 139), can constitute a probe looking for shared resources on a host.

Sample of SMB Wildcard Logs

Source	Source Port	Target Host	Target Port	Source Info
200.193.160.225	1044	MY.NET.135.25	137	Brazil ISP
200.193.160.225	1027	MY.NET.135.25	137	Brazil ISP
200.193.160.225	1044	MY.NET.135.25	137	Brazil ISP
211.74.120.128	1044	MY.NET.133.228	137	Taiwan ISP
211.74.120.128	1044	MY.NET.133.228	137	Taiwan ISP
211.74.120.128	1044	MY.NET.133.228	137	Taiwan ISP
211.74.120.128	1044	MY.NET.133.228	137	Taiwan ISP
24.170.22.97	1025	MY.NET.134.74	137	Virginia ISP
24.170.22.97	1025	MY.NET.134.74	137	Virginia ISP
24.201.212.57	1025	MY.NET.134.134	137	Candia ISP
24.201.212.57	1025	MY.NET.134.134	137	Candia ISP
24.201.212.57	1025	MY.NET.134.134	137	Candia ISP

Notice the source port on these connections. This alert was triggered 248 times. The 12 triggers listed above should be considered the potentially malicious.

Defense Measures

These hosts should be investigated further to determine vulnerabilities. A firewall can also be used to protect these hosts for external connections.

Wingate

Wingate is an application that uses the SOCKS port to allow proxy connection. Using a proxy is a method used by attackers to hide their identity and remain anonymous on the Internet. Reconnaissance scans are used to identify host with this type of ports open for proxy. Attackers can used this information to launch future attacks through these servers.

Sample of Wingate Logs

This shows the reconnaissance pattern of a single source to multiple targets.

Source	Target	Connection Count	Source Info
64.154.61.232	MY.NET.219.94	1	Level3.net Colorado ISP
64.154.61.232	MY.NET.60.8	1	Level3.net Colorado ISP
64.154.61.232	MY.NET.97.97	1	Level3.net Colorado ISP
64.154.61.232	MY.NET.98.45	1	Level3.net Colorado ISP

63.102.227.48	MY.NET.98.114	3	Uunet World Wide ISP
63.102.227.48	MY.NET.98.151	3	Uunet World Wide ISP
63.102.227.48	MY.NET.98.187	2	Uunet World Wide ISP
217.10.143.59	MY.NET.205.126	2	OH.SOD.IT (Italian Tiles and Ceramics)
217.10.143.59	MY.NET.222.222	2	OH.SOD.IT (Italian Tiles and Ceramics)
216.54.223.198	MY.NET.222.202	3	OZONA Online, Florida ISP
216.54.223.198	MY.NET.225.170	2	OZONA Online, Florida ISP
216.234.161.197	MY.NET.153.168	2	Tera-Byte Online Services, Alabama ISP
216.234.161.197	MY.NET.218.2	2	Tera-Byte Online Services, Alabama ISP
216.198.192.197	MY.NET.219.10	1	Cybercon St. Louis ISP
216.198.192.197	MY.NET.98.146	1	Cybercon St. Louis ISP
216.152.64.211	MY.NET.218.102	2	Webmaster, Ca ISP
216.152.64.211	MY.NET.220.142	1	Webmaster, Ca ISP

This alert is triggered 118 times the list above shows the most frequent connections.

Defense Measures

If Wingate or (Socks) are used on this network. The host should be configured to require authentication for use of its Wingate features. A firewall should be used to prevent these types of scans.

Queso Fingerprinting

Queso is a reconnaissance tool used to provide information about a host. Queso has a very distinctive signature. The response from the Queso packets can tell Queso what kind of OS the host is using. This is known as OS fingerprinting. This could allow an attacker to build a list of vulnerabilities to exploit on hosts on a network. The source address can be spoofed but this is not likely because the attacker would want a response to get the information. Queso chooses random source ports to perform scans.

Sample of Queso Fingerprint Logs

Source	Target	Connection Count	Source Info
129.206.170.20	MY.NET.202.54	98	University of Heidelberg
24.50.80.131	MY.NET.229.38	6	Adelphenia Cable Comm
213.64.149.61	MY.NET.219.14	5	Telina Network, Sweden
158.75.57.4	MY.NET.219.14	3	Nicolaus Copernicus University, Poland
130.233.26.197	MY.NET.219.134	3	Helsinki University of Technology

Source 129.206.170.20 was most active in this scan of the network. This source is responsible for 71% out of a total of 138 alerts.

Defense Measures

We have to look at what makes Queso affective to develop a defense. The attacker must know which ports are open to determine which ports Queso should use. The attacker also has to know if the system exists. Preventing this type of information from leaving the network is the first step to preventing this type of scan. Restricting responses to "active host" scans from exiting the network can do this. For example active host scan will ping a range of host on the network. The systems that respond to the pings can later be targeted for a Queso scan. Preventing the ping response from exiting the network can prevent an attempt to identify active host for a more detailed scan like Queso fingerprinting.

Back Orifice

Back Orifice is Trojan program that can give an attacker remote access to a host. Back Orifice operates in a client server mode where the server is the target host. Once the Back Orifice Server has been installed on a host, a client can connect and remotely control the host. Back Orifice comes with some basic tools like:

Screen Capture
Key Logger
Remote Networking
Drive Mapper

Back Orifice has many built in functionalities to be used by the attacker. Additional functionality known as "Butt Plugs", which are plug-in for Back Orifice can be added later. The Trojan can be spread the same way as a virus. Once the server portion is installed on a host it can run in stealth mode awaiting a client connection. Attackers will scan network looking for Back Orifice servers by attempting connections to the default Back Orifice port 31337.

Sample Back Orifice Logs

Source	Target	Source Info
24.162.245.198	MY.NET.1.113	Road Runner, VA ISP
24.162.245.198	MY.NET.1.127	" "
24.162.245.198	MY.NET.1.161	" "
24.162.245.198	MY.NET.1.167	" "
24.162.245.198	MY.NET.10.125	" "
24.162.245.198	MY.NET.10.166	" "
24.162.245.198	MY.NET.10.57	" "
24.162.245.198	MY.NET.11.24	" "
24.162.245.198	MY.NET.11.28	" "
24.162.245.198	MY.NET.12.114	" "

This is a sample of the alerts generated by this scan. The alerts show 109 attempts by the same Source to connect to a Back Orifice Server.

Defensive Measures

A firewall can be used to block the default Back Orifice port. This will prevent clients for connecting externally. Most anti-virus software can detect and/or inoculate the Back Orifice Trojan. This requires ensuring that all host on the network have the latest virus protection.

Russian Dynamo

This is a custom snort rule inserted to detect this abnormal behavior. Total of three-host repeatedly connecting to port 317 on the same host generated this trigger. Only one connection was targeted to a different port (6346).

The alert was trigger 46 times with two different target host.

Null Scan

Null Scan is another reconnaissance tactic used to gather information from a host. A null scan works by sending a packet with no flags set to a port on a host. If the port is open then the host will discard the packet. If the port is closed then hose will respond with a RST packet. Sending numerous packets to numerous hosts can tell an attacker which ports are active.

Source	Source Port	Target	Target Source	Source Info
24.108.215.109	1	MY.NET.220.38	3575	California ISP
24.108.215.109	1	MY.NET.220.38	3575	" "
24.108.215.109	197	MY.NET.220.38	4857	" "
24.108.215.109	0	MY.NET.220.38	1231	" "
24.108.215.109	165	MY.NET.220.38	2105	" "
24.108.215.109	197	MY.NET.220.38	2070	" "

This is a sample of the traffic generated by the most active host causing this alert. Port numbers used in this scan are out of the ordinary. Normally the attacker would try ports below 1024 on the host to get a response. A search on www.incidents.org shows the ports null scans with these ports (3575 and 4875) being the source ports rather that the target

ports as seen here. At first this appeared to be a possible stimulus to null scan originating from an internal host. However, the logs do not support or reject this theory. This could be a result of an inexperienced attacker mis-configuring a null scan tool as well. This alert was trigger 28 times.

Nmap Ping

Nmap is a tool like the above mention Queso. However, NMAP is more robust in that it provides more functionality than just OS fingerprinting. Its artillery includes tools to perform several different types of scans. The traffic captured in the alert logs is the result of a "NMAP ping" scans, which simply identifies active host on the network. This can be a precursor to many things such as addition reconnaissance like OS fingerprinting or an actual attack.

Since this is a reconnaissance tool the attacker would need to see the response reducing the likelihood that the source is spoofed. NMAP does have a decoy option that sends packet with spoofed source addresses in addition to packets with the real source address. This makes it difficult to determine the real source of the scan. The date and times stamps on the alerts vary enough to support the theory that the decoy method was not used.

Sample of NMAP Ping Logs

Source	Target	Connection Count	Target Port	Source Info
192.102.197.234	MY.NET.1.8	7	53	Intel Corp
195.25.86.2	MY.NET.60.14	2	80	Oleane, France ISP
63.119.91.2	MY.NET.110.39	1	25	Uunet Technologies
63.67.116.15	MY.NET.98.184	1	1303	Uunet Technologies

The log analysis shows multiple hosts looking for DNS, HTTP, SMTP and 1303 open ports. WWW.incidents.org show 1303 to be related to DNS version query. Previous connections to port 53 (DNS) in the same log file support this theory. This alert was generated 26 times.

NMAP uses multiple techniques to determine active host and available ports. These techniques include using ACK packets instead of the traditional ping (echo request or reply) packets. This allows NMAP to scan networks that use firewalls that prevent ping packets for accessing the network. NMAP is even advanced enough to use the same ACK packet technique to determine if a network is protected by a stateful inspection or packet filtering firewall. Most stateful connection firewalls will prevent connections starting with an ACK packet.

Defense Measures

NMAP like Queso is a reconnaissance tool and its function is to provide information that can be used later for an attack. NMAP is more advanced than Queso because it has the

ability to do both scans of active host and OS fingerprinting. As in Queoso preventing host from responding to ping packets is a method of preventing certain scans. In addition implementing stateful firewalls that prevent scans using ACK packets. Monitoring logs that are generated by firewalls and Intrusion Detection Systems can also provide information on which host and ports are targeted for future attacks. .

"Myserver"

"Myserver" is a Distributed Denial of Service (DDoS) Agent Trojan. A DDoS uses multiple hosts to launch a Denial of Service attack on a single host or a smaller group of host. To accomplish this a Trojan is installed on the compromised host. This type of Trojan allows attackers to connect to the compromised hosts remotely and use the infected host to launch denial of service attacks. A signature of this Trojan is to wait for connections on port 55850 on the infected host. a

www.incidents.org/archives/y2k/082200.htm
http://list.insecure.org/incidents/2000/Oct/0141.html

Sample of Myserver

This portion of the log shows a potential response to a stimulus since the source port is 55850. This would indicate that the internal host is searching MY.NET.229.38 is searching for host infected with the "Myserver" Trojan.

Source	Source Port	Target	Target Port
199.20.66.1	55850	MY.NET.229.38	6346
199.20.66.1	55850	MY.NET.229.38	6346
199.20.66.1	55850	MY.NET.229.38	6346
199.20.66.1	55850	MY.NET.229.38	6346
199.20.66.1	55850	MY.NET.229.38	6346

This is further supported by the following traffic from MY.NET.218.86 to multiple host.

Source	Source Port	Target	Target Port
MY.NET.218.86	2000	213.44.175.50	55850
MY.NET.218.86	2000	213.44.175.50	55850
MY.NET.218.86	2000	172.154.1.109	55850
MY.NET.218.86	2000	172.154.1.109	55850

This alert was triggered 26 times.

Defense Measures

If this traffic is outbound there may be no defense measures needed. The internal security policies may have regulations against this type of behavior.

Tiny Packets

This is a measure used to get attacks past Intrusion Detection Systems and firewalls. Fragmenting a packet makes it difficult for an Intrusion Detection System to identify attacks or scans. This could be harmless and caused by network congestion. There are some attacks that use fragmented packets to crash hosts. This is possible because the receiving host has to reassembles fragmented packets. A large amount of fragmented packets can cause the host to run out of memory to process the packets causing the host to crash.

Sample Tiny Packets Logs

Source	Target	Source Info
202.39.78.124	MY.NET.202.166	Taiwan Network Information Center
202.39.78.124	MY.NET.202.166	Taiwan Network Information Center
202.39.78.124	MY.NET.220.62	Taiwan Network Information Center
202.39.78.124	MY.NET.220.62	Taiwan Network Information Center
202.39.78.125	MY.NET.204.218	Taiwan Network Information Center
202.39.78.125	MY.NET.205.18	Taiwan Network Information Center
202.39.78.125	MY.NET.207.254	Taiwan Network Information Center
202.39.78.125	MY.NET.208.142	Taiwan Network Information Center
202.39.78.125	MY.NET.208.142	Taiwan Network Information Center
202.39.78.125	MY.NET.208.30	Taiwan Network Information Center
202.39.78.125	MY.NET.208.30	Taiwan Network Information Center
202.39.78.125	MY.NET.208.30	Taiwan Network Information Center

The likelihood of this address are being spoofed is very high. If this is a malicious attack the attacker would want to hide their IP address and would not want to see the return packets.

Defensive Measure

Most operating systems have patched or fixed this vulnerability prevent host from crashing from this type of behavior. This is still a tactic to get around Intrusion Detection Systems. Firewall can be set to drop packets that have been fragmented very small. The hosts that were the target of this attack should be checked for any such vulnerability.

OOS (Out of Spec) Log Analysis

Source	Target	Connection Count	Source Info
206.65.191.129	MY.NET.220.6	200	UUNet
131.118.95.84	MY.NET.205.254	162	UUNet
MY.NET.201.146	207.172.3.46	31	UUNet
194.70.235.33	MY.NET.212.70	13	UUNet

206.65.191.129

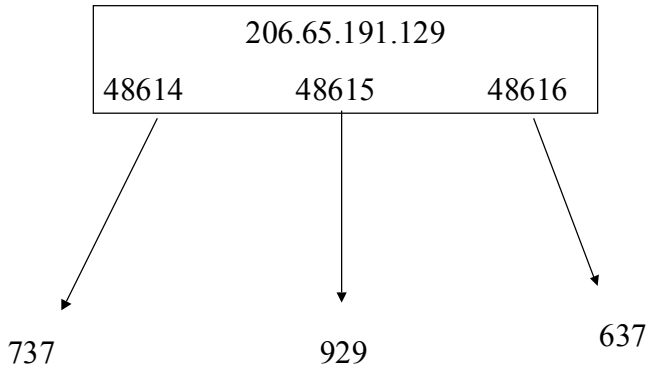
The below example shows reserve bits of the TCP header are set in this SYN packet. In addition the source ports change sequentially. This is evidence of packet crafting.

```
03/15-10:26:46.650177 206.65.191.129:48614 -> MY.NET.220.6:737
TCP TTL:50 TOS:0x0 ID:0  DF
21S***** Seq: 0x92237B70   Ack: 0x0   Win: 0x16D0
TCP Options => MSS: 1460 SackOK TS: 110456399 0 EOL EOL EOL EOL

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
03/15-10:26:46.650255 206.65.191.129:48615 -> MY.NET.220.6:929
TCP TTL:50 TOS:0x0 ID:0  DF
21S***** Seq: 0x928646D6   Ack: 0x0   Win: 0x16D0
TCP Options => MSS: 1460 SackOK TS: 110456399 0 EOL EOL EOL EOL

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
03/15-10:26:46.650349 206.65.191.129:48616 -> MY.NET.220.6:637
TCP TTL:50 TOS:0x0 ID:0  DF
21S***** Seq: 0x91E186BC   Ack: 0x0   Win: 0x16D0
TCP Options => MSS: 1460 SackOK TS: 110456399 0 EOL EOL EOL EOL
```

Link Graph



OOS analysis Summary

- One-way traffic
- All Syn Packets
- Reserved Bits Set

Scan Summary Logs

The table below is a list of all the source of Sans

Source	Host Scanned	TCP	UDP	Source Info
193.251.27.118	20906	21883	1	France Telecom, France
203.128.6.220	16678	16951	4	Singapore ISP
MY.NET.220.42	16094	2	16278	Internal Host
203.149.183.154	12330	12544	7	NO FQDN
MY.NET.218.102	8770	0	8906	Internal Host
MY.NET.217.222	7538	1	7639	Internal Host
212.25.81.239	6855	6920	0	Sibirsky-Aluminium
202.66.162.130	5752	5976	3	NO FQDN
MY.NET.253.24	3785	4095	0	Internal Host
MY.NET.219.86	3710	3940	0	Internal Host
MY.NET.98.168	3501	7	3778	Internal Host

MY.NET.217.230	3322	0	3916	Internal Host
194.224.168.50	3240	3452	1	Spain ISP
MY.NET.98.156	3210	0	3259	Internal Host
MY.NET.98.123	3038	0	3150	Internal Host
144.132.40.90	2979	3173	4	Australia, ISP
210.169.129.35	2817	2989	1	No FQDN
24.180.134.156	2643	2700	0	Baltimore, ISP
MY.NET.97.37	2026	0	2043	Internal Host
MY.NET.100.230	1983	234	1836	Internal Host
211.178.63.4	1865	2175	0	HANKUK-DIGMEDIA Korean, ISP
MY.NET.71.235	1787	0	2166	Internal Host
210.178.81.129	1755	1884	0	Chuam Comprehensive High School, Korea
MY.NET.225.54	1683	2	2006	Internal Host
MY.NET.218.162	1502	0	2697	Internal Host
MY.NET.202.2	1451	1	1863	Internal Host
MY.NET.97.66	1096	0	1112	Internal Host
MY.NET.208.30	1090	0	1201	Internal Host
MY.NET.218.206	1080	0	1304	Internal Host
MY.NET.202.166	1061	0	1350	Internal Host
MY.NET.225.66	1034	51	1762	Internal Host
MY.NET.98.220	1022	0	1029	Internal Host
MY.NET.71.77	976	0	1195	Internal Host
MY.NET.140.21	917	0	929	Internal Host
MY.NET.202.34	917	65	958	Internal Host
MY.NET.160.138	912	0	1003	Internal Host
MY.NET.97.121	878	0	905	Internal Host
65.14.160.211	845	0	879	@Home Network Washington, D.C.
MY.NET.230.42	805	0	883	Internal Host
MY.NET.211.106	804	0	987	Internal Host
MY.NET.71.66	727	2	865	Internal Host
MY.NET.227.110	722	0	756	Internal Host
MY.NET.69.204	712	0	1249	Internal Host
MY.NET.218.86	708	150	867	Internal Host
MY.NET.203.150	692	0	754	Internal Host
164.67.21.41	643	663	0	University of California, Los Angeles
MY.NET.224.110	643	0	726	Internal Host
MY.NET.219.38	636	0	894	Internal Host
MY.NET.97.25	636	0	638	Internal Host
MY.NET.215.18	627	36	751	Internal Host
MY.NET.205.242	604	0	863	Internal Host

MY.NET.217.102	581	0	916	Internal Host
MY.NET.97.28	568	0	935	Internal Host
MY.NET.98.106	500	0	507	Internal Host
MY.NET.207.50	497	0	581	Internal Host
MY.NET.211.78	479	0	554	Internal Host
MY.NET.224.130	465	2	501	Internal Host
MY.NET.98.151	463	0	471	Internal Host
MY.NET.227.206	440	0	463	Internal Host
MY.NET.229.58	438	0	510	Internal Host
MY.NET.213.98	372	0	447	Internal Host
MY.NET.223.34	360	0	389	Internal Host
MY.NET.218.210	355	0	555	Internal Host
MY.NET.98.235	340	0	364	Internal Host
MY.NET.60.43	335	0	335	Internal Host
MY.NET.220.62	324	0	483	Internal Host
MY.NET.220.190	318	0	362	Internal Host
MY.NET.218.190	318	6	348	Internal Host
MY.NET.6.45	316	0	317	Internal Host
MY.NET.221.26	303	328	0	Internal Host
62.31.68.89	280	287	0	UK ISP
MY.NET.210.86	267	0	293	Internal Host
MY.NET.98.141	265	0	273	Internal Host
MY.NET.218.26	261	0	311	Internal Host
24.161.78.5	245	246	0	Road Runner, Va ISP
63.10.224.231	244	0	256	UUNet, Washington
MY.NET.97.226	226	0	288	Internal Host
MY.NET.204.190	223	0	287	Internal Host
MY.NET.212.230	211	0	263	Internal Host
MY.NET.227.194	190	0	247	Internal Host
MY.NET.228.46	189	0	219	Internal Host
217.1.32.130	189	186	0	UUNET Technologies, Inc
MY.NET.98.174	183	0	217	Internal Host
24.132.123.102	181	196	0	Amsterdam, ISP
MY.NET.212.190	178	0	225	Internal Host
MY.NET.217.134	177	0	218	Internal Host
MY.NET.150.41	176	0	221	Internal Host
216.162.44.140	170	173	0	iNET Systems Corp, Atlanta, Georgia
MY.NET.217.86	169	0	186	Internal Host
MY.NET.225.78	168	0	297	Internal Host
MY.NET.221.130	156	0	183	Internal Host
MY.NET.202.6	155	0	166	Internal Host
MY.NET.204.26	142	145	0	Internal Host
MY.NET.97.191	140	0	141	Internal Host

MY.NET.224.34	140	0	183	Internal Host
MY.NET.225.182	135	0	249	Internal Host
MY.NET.217.174	133	0	224	Internal Host
MY.NET.206.182	123	0	149	Internal Host
MY.NET.206.146	119	0	164	Internal Host
MY.NET.206.178	117	0	159	Internal Host
MY.NET.97.13	110	0	120	Internal Host
MY.NET.204.70	110	0	159	Internal Host
MY.NET.228.138	109	0	136	Internal Host
MY.NET.223.134	105	0	130	Internal Host
MY.NET.70.225	104	106	0	Internal Host
MY.NET.221.246	104	0	105	Internal Host
MY.NET.253.53	103	96	0	Internal Host
MY.NET.221.6	102	113	0	Internal Host
MY.NET.209.62	101	0	111	Internal Host
MY.NET.227.130	100	106	4	Internal Host
MY.NET.98.124	98	0	93	Internal Host
MY.NET.224.54	98	0	119	Internal Host
MY.NET.212.238	97	0	141	Internal Host
MY.NET.212.202	86	0	75	Internal Host
MY.NET.98.169	85	0	121	Internal Host
4.3.193.56	83	89	0	BBN Planet, Mass
MY.NET.209.106	81	0	54	Internal Host
209.217.53.190	81	81	0	Ethos Communications, Texas
MY.NET.209.250	77	0	150	Internal Host
MY.NET.208.150	75	0	94	Internal Host
MY.NET.201.86	73	0	88	Internal Host
MY.NET.211.42	68	0	79	Internal Host
MY.NET.212.106	68	0	97	Internal Host
MY.NET.201.198	67	0	74	Internal Host
163.152.45.200	65	65	0	Korea University, Korea
MY.NET.229.38	64	72	16	Internal Host
MY.NET.203.94	63	0	83	Internal Host
MY.NET.98.149	63	0	79	Internal Host
MY.NET.98.186	61	1	60	Internal Host
MY.NET.203.154	61	0	58	Internal Host
MY.NET.219.202	59	6	60	Internal Host
MY.NET.205.162	58	53	0	Internal Host
MY.NET.202.42	58	0	76	Internal Host
MY.NET.6.35	58	65	0	Internal Host
MY.NET.218.42	56	0	62	Internal Host
MY.NET.98.247	56	0	60	Internal Host
MY.NET.206.150	55	0	76	Internal Host
MY.NET.98.132	55	5	97	Internal Host

MY.NET.97.83	52	0	72	Internal Host
MY.NET.71.39	52	68	8	Internal Host
MY.NET.219.114	52	34	32	Internal Host
MY.NET.222.118	51	0	84	Internal Host
MY.NET.98.198	50	1	50	Internal Host
MY.NET.219.226	49	1	53	Internal Host
MY.NET.98.140	46	0	51	Internal Host
MY.NET.17.48	46	54	0	Internal Host
209.189.124.214	45	50	0	No FQDN
MY.NET.208.118	44	0	53	Internal Host
MY.NET.226.114	43	45	0	Internal Host
MY.NET.53.57	43	0	43	Internal Host
MY.NET.97.204	41	0	80	Internal Host
MY.NET.202.58	40	0	54	Internal Host
141.151.22.56	40	42	0	Verio, Inc.
MY.NET.97.53	39	0	36	Internal Host
MY.NET.253.51	39	36	0	Internal Host
MY.NET.153.165	36	0	36	Internal Host
MY.NET.98.127	36	0	40	Internal Host
212.131.172.130	34	34	0	INTERBUSINESS, Italy
MY.NET.98.139	33	0	36	Internal Host
MY.NET.253.52	33	39	0	Internal Host
MY.NET.228.14	32	0	31	Internal Host
MY.NET.97.24	32	0	35	Internal Host
MY.NET.97.50	32	0	28	Internal Host
MY.NET.98.171	32	0	32	Internal Host
MY.NET.98.219	32	0	32	Internal Host
MY.NET.217.70	31	0	37	Internal Host
MY.NET.97.40	30	0	30	Internal Host
MY.NET.214.210	30	32	0	Internal Host
MY.NET.219.142	30	0	40	Internal Host
MY.NET.97.240	30	1	38	Internal Host
63.123.106.6	30	31	0	UUNET Technologies, Inc
MY.NET.98.181	30	14	30	Internal Host
MY.NET.208.102	29	30	0	Internal Host
MY.NET.6.47	28	30	0	Internal Host
MY.NET.209.206	28	0	52	Internal Host
MY.NET.204.130	26	0	27	Internal Host
MY.NET.208.106	26	0	33	Internal Host
209.219.49.10	26	27	0	@Home Network / @Work Division
MY.NET.60.8	25	47	73	Internal Host
MY.NET.219.250	24	22	0	Internal Host
MY.NET.97.57	20	0	20	Internal Host

MY.NET.209.82	20	0	18	Internal Host
MY.NET.208.238	20	0	33	Internal Host
MY.NET.98.192	19	1	26	Internal Host
MY.NET.213.30	19	0	22	Internal Host
MY.NET.212.30	19	0	25	Internal Host
212.125.177.199	18	20	0	UUNET
MY.NET.219.234	18	0	18	Internal Host
MY.NET.219.46	18	0	11	Internal Host
63.109.70.97	16	19	0	UUNET
38.162.57.27	16	17	0	Performance Systems International, Va
MY.NET.211.22	16	0	15	Internal Host
MY.NET.97.242	16	1	40	Internal Host
MY.NET.215.34	16	0	25	Internal Host
MY.NET.105.59	16	8	16	Internal Host
MY.NET.98.134	15	1	16	Internal Host
205.238.235.88	15	16	0	epix Internet Services, PA
MY.NET.97.101	14	0	19	Internal Host
MY.NET.98.226	13	0	13	Internal Host
MY.NET.204.170	13	0	13	Internal Host
MY.NET.98.147	12	0	13	Internal Host
MY.NET.60.11	11	153	130	Internal Host
MY.NET.219.218	11	11	1	Internal Host
MY.NET.6.7	11	0	12	Internal Host
MY.NET.97.100	11	12	0	Internal Host
213.45.5.54	10	12	0	Interbusiness, IT
MY.NET.229.158	10	0	11	Internal Host
MY.NET.203.234	10	13	2	Internal Host
MY.NET.219.174	9	0	12	Internal Host
MY.NET.146.95	9	12	0	Internal Host
MY.NET.98.180	8	5	56	Internal Host
158.75.57.4	8	12	0	Computer Centre, Nicolaus Copernicus University, Poland
144.51.17.1	7	0	85	National Computer Security Center, MD
MY.NET.60.39	6	1040	1	Internal Host
MY.NET.98.164	5	4	34	Internal Host
MY.NET.109.53	5	413	0	Internal Host
MY.NET.178.42	5	49	0	Internal Host
MY.NET.5.54	3	4301	0	Internal Host
MY.NET.60.16	3	0	35	Internal Host
MY.NET.97.230	3	1	24	Internal Host
62.4.71.179	3	0	32	INTEL Hardware, France
212.224.24.70	3	0	32	mbmedia

				computersysteme, Demark
212.224.25.198	3	0	35	mbmedia computersysteme, Demark
62.4.71.173	2	0	18	INTEL Hardware, France
129.133.163.19	2	248	0	Wesleyan University, CT
MY.NET.111.156	2	66	0	Internal Host
151.39.100.34	2	0	16	UUNET, IT
62.4.71.178	2	0	17	INTEL Hardware, France
62.4.71.177	2	0	23	INTEL Hardware, France
62.4.71.175	2	0	17	INTEL Hardware, France
199.0.216.222	2	0	23	
62.4.71.174	2	0	22	INTEL Hardware, France
212.73.235.196	2	0	16	Capital Area Internet Service, Washington DC
212.224.25.202	2	0	20	mbmedia computersysteme, Denmark
62.4.71.171	2	0	22	INTEL Hardware, France
MY.NET.179.78	2	1978	0	Internal Host
212.73.235.195	2	0	16	CREANET, France
211.170.79.123	2	0	21	BORANET, Korea
64.50.140.200	1	787	1	CapuNet, LLC, Maryland
MY.NET.218.46	1	0	12	Internal Host
MY.NET.144.54	1	307	0	Internal Host
62.4.71.172	1	0	12	INTEL Hardware, France
24.6.147.104	1	188	0	@Home Network
206.132.179.136	1	46	0	Global Crossing,CA
MY.NET.221.70	1	18	0	Internal Host
209.163.147.37	1	0	13	Fibrcom, TX
208.191.54.3	1	157	0	Southwestern Bell Internet Services, Tx
24.13.97.72	1	201	0	@Home Network

Scans are common on any network because of the simplicity and available of the tools used to perform these scans. It is also possible to scan multiple networks with from a single host. The most serious types of scans have been identified earlier in this document. The host "102.251.27.118" covered 20906 hosts in one day.

Analysis Summary

The Snort logs show the following types of traffic on this network:

Reconnaissance: This traffic is used to gain information about host or host for future attacks. Even though the reconnaissance traffic is harmless the information they proved to an attacker can lead to multiple attacks. The majority of this traffic can be blocked with the use of a stateful firewall.

Reconnaissance Traffic
Queso Finger Printing
Null Scan
NMAP Ping
Wingate

OS Vulnerability Exploits: This traffic is used to attack a host with known vulnerabilities. The best defense for this traffic is to ensure all the latest software and security patches are applied to the host.

OS Vulnerability Exploits
RPC Connection Attempts
External RPC Call
Connections to Port 515
SMB Wildcard

Trojans and Worms: These are programs installed on the host that can later be accessed remotely. These programs can attack other host or give the attacker control over the machine. Anti-Virus software and security patches are good defenses from Trojans and Worms.

Trojans and Worms
Ramen Server Activity
Back Orifice
MyServer

Miscellaneous: This traffic shows no real threat but should be investigate further. Even though traffic shows no documented threat it still can be malicious. The use of a packet sniffer like TCP dump will give more details on this traffic.

Miscellaneous Traffic
Watchlist
Source and Destination outside network
Tiny Packets

Top 10 Talkers

This is a list compiled of all the Source addresses that triggered alerts. They were then grouped by the amount of time the appeared in alert logs.

Source	Alerts Generated	Source Info
63.121.232.185	11832	UUNET Technologies, Inc.
212.179.4.50	6473	SCP-SYSTEMS-LAN, IT
MY.NET.224.2	3212	Internal Host
212.144.16.169	2208	Mannesmann o.tel.o, Denmark
212.179.72.226	2164	BEZEQ INTERNATIONAL, Israel
212.179.127.41	2160	BEZEQ INTERNATIONAL, Israel
MY.NET.221.198	1669	Internal Host
MY.NET.227.206	1548	Internal Host
10.0.0.1*	1502	Reserved Address

*Maybe network translated by a firewall or router.

Analysis Process

Due to the binary output of Snort log files there are many ways to analyze them. I chose to review the alert logs and then import them into Microsoft Excel. The logs were imported using space and ":" as delimiters. Once the logs were imported I was able to sort log files into many different views depending on information captured in the log. Using this method I was able to extract the different types of alerts into multiple logs and sort them individually.

In some cases the Excel sorted log files were exported to Microsoft Access tables. This allowed me to search on patterns and group data together to analyze by occurrence. Samples of the data sorted and group of by Microsoft Access were inserted into this document in the sample sections.

References and Resources:

Source information was gathered using www.networktool.com. This web page uses multiple methods and databases to find information about a host.

www.incidents.org
www.whitehat.org
www.securityforcus.com
http://lists.insecure.org
www.netice.com/advice/exploits/ports
www.insecure.org
www.ncmage.com
www.cisco.com
www.checkpoint.com
www.wingate.com
www.microsoft.com
www.sans.org/y2k/practical/Lenny_Zeltser.htm
www.sans.org/y2k/practical/Beck_Bogle_GCIA.doc
http://www.tripwire.com/products/servers/platforms.cfml
http://www.networkcomputing.com/1023/1023f1.html
http://enterprisesecurity.symantec.com/products/products.cfm?ProductID=48&PID=7715670
http://www.gocsi.com/roundtable.htm
http://www.linux.ie/articles/portsentryandsnortcompared.php
NMAP Man Pages