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
"Network Monitoring and Threat Detection In-Depth (Security 503)"
at http://www.giac.org/registration/gcia

*** Northcutt, good use of an analysis process, good research. A bit more care in the write ups would enhance clarity. Detect 7 raises an interesting issue, I always try to tell my students that if you lie it will cost you, your mama taught you the same thing! If the src address is spoofed it is really hard to get the data back. There are ways, but the analyst would have to make a case for this. 81 ***

# 10 Detects with Analysis for

# IDIC Track Practical Test

Lee R Brandt

Monday, April 10, 2000

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

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

The traces were acquired from Incidents@SecurityFocus.com.

## Detect 1:

Mar 28 12:04:44 7of9 in.ftpd[15115]: refused connect from 212.177.241.127
Mar 28 12:04:44 7of9 in.telnetd[15117]: refused connect from 212.177.241.127
Mar 28 12:04:44 7of9 in.fingerd[15119]: refused connect from 212.177.241.127
Mar 28 12.04:45 7of9 sshd[15116]: refused connect from 212.177.241.127
Mar 28 12:06:06 7of9 in.telnetd[15125]: refused connect from 212.177.241.127
Mar 28 12:06:38 7of9 in.telnetd[15128]: connect from 212.177.241.127

Mar 28 12:06:54 7of9 login: LOGIN ON 2 BY r0x FROM 212.177.241.127
Mar 28 12:06:54 7of9 PAM_pwdb[15129]: (login) session opened for user r0x by (uid=0)
Mar 28 12:09:08 7of9 sshd[15158]: Did not receive ident string from 212.177.241.127
Mar 28 12:12:43 7of9 in.telnetd[15173]: connect from 212.177.241.127
Mar 28 12:12:59 7of9 login: LOGIN ON 3 BY r0x FROM 212.177.241.127
Mar 28 12:12:59 7of9 PAM_pwdb[15174]: (login) session opened by user r0x by (uid=0)
Mar 28 12:14:31 7of9 in.telnetd[15192]: connect from 212.177.241.127
Mar 28 12:14:43 7of9 login: LOGIN ON 2 BY r0x FROM 212.177.241.127
Mar 28 12:14:43 7of9 PAM_pwdb[15193]: (login) session opened for user r0x by (uid=0)

**Source of Trace:** Dschauer@VCSD.COM sent this trace to Incidents@SecurityFocus.com

**Active Targeting:** Yes

**History:** The machine had just had RedHat 6.1 installed and not all the updates were installed. He found the following directory in his bind default directory:

Drwxr-xr-x 2root root 1024 Mar 28 12:05 ADMROCKS

This directory was not installed by the administrator. The version of bind running on the machine was bind-8..2.1-7 (it had bind-8.2.2_P3-1 before 6.1 was reinstalled on it, that was somehow overlooked)

**Technique:** Single IP address: Source IP address is assigned to UUNET International - UK.UU.NET, the source IP address is probably spoof . (Use WWW.geektools.com whois to find the name of the source IP address)
Hit four services with known vulnerabilities.
Automated, several connections in one second.
Not a sudtle attack.

**Intent:** The source is looking for a vulnerable service with the intent to break into the system for future activities.

**Analysis:** The source is scanning services with known vulnerabilities with the intent of breaking into the network. The attacker used an automated scan to scan several connections in one second. Once the source was able to get into the through the telnet service they created the ADMROCKS directory in /var/named. Then they used "ADM named 8.2/8.2.1 NXT remote overflow" exploit to get into the network. Once the source is has planted their backdoor, they can come in anytime and take control of your server. This machine has been compromise.

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

**Severity of Attack:** High

| Component | Score | Comments |
|---|---|---|
| Criticality | 5 | The server is being directly targeted. |
| Lethality | 5 | The server was compromised and the attack could be very lethal. |
| System Countermeasures | 4 | Modern operating system, not all the patches were installed. |
| Network Countermeasures | 1 | The firewall was permissive. |
| Severity Score | 5 | Severity = (Criticality + Lethality) – (system countermeasures + net countermeasures) |

## Detect 2:

xxx.xxx.xxx.xxx is the same IP throughout.

```
Mar 17 19:56:39 xxx.xxx.xxx.xxx:1025 -> 216.35.27.7:6112 SYN **S*****
Mar 17 19:56:39 xxx.xxx.xxx.xxx:1026 -> 209.67.136.174:6112 SYN **S*****
Mar 17 19:56:39 xxx.xxx.xxx.xxx:1028 -> 216.148.246.9:6112 SYN **S*****
Mar 17 19:56:39 xxx.xxx.xxx.xxx:1029 -> 209.67.136.172:6112 SYN **S*****
Mar 17 19:56:39 xxx.xxx.xxx.xxx:1030 -> 206.79.254.192:6112 SYN **S*****
Mar 17 19:56:39 xxx.xxx.xxx.xxx:1031 -> 209.67.136.170:6112 SYN **S*****
Mar 17 19:56:39 xxx.xxx.xxx.xxx:1032 -> 64.14.113.138:6112 SYN **S*****
Mar 17 19:56:39 xxx.xxx.xxx.xxx:1033 -> 216.148.246.7:6112 SYN **S*****
Mar 17 19:56:39 xxx.xxx.xxx.xxx:1034 -> 203.248.250.72:6112 SYN **S*****
Mar 17 19:56:40 xxx.xxx.xxx.xxx:6112 -> 216.148.246.8:6112 UDP
Mar 17 19:56:41 xxx.xxx.xxx.xxx:1036 -> 216.148.246.8:6112 SYN **S*****
Mar 17 19:57:48 xxx.xxx.xxx.xxx:6112 -> 210.91.217.81:6112 UDP
Mar 17 19:57:48 xxx.xxx.xxx.xxx:6112 -> 209.254.234.129:6112 UDP
Mar 17 19:57:48 xxx.xxx.xxx.xxx:6112 -> 24.66.226.176:6112 UDP
Mar 17 19:57:48 xxx.xxx.xxx.xxx:6112 -> 207.172.143.149:6112 UDP
Mar 17 19:57:48 xxx.xxx.xxx.xxx:6112 -> 152.166.167.141:6112 UDP
Mar 17 19:57:48 xxx.xxx.xxx.xxx:6112 -> 152.166.6.27:6112 UDP
Mar 17 19:57:48 xxx.xxx.xxx.xxx:6112 -> 63.23.28.242:6112 UDP
Mar 17 19:57:48 xxx.xxx.xxx.xxx:6112 -> 209.63.112.237:6112 UDP
Mar 17 19:57:48 xxx.xxx.xxx.xxx:6112 -> 147.26.248.229:6112 UDP
Mar 17 19:57:48 xxx.xxx.xxx.xxx:6112 -> 206.81.198.173:6112 UDP
Mar 17 19:57:48 xxx.xxx.xxx.xxx:6112 -> 63.30.190.15:6112 UDP
Mar 17 19:57:48 xxx.xxx.xxx.xxx:6112 -> 152.174.245.84:6112 UDP
Mar 17 19:57:48 xxx.xxx.xxx.xxx:6112 -> 162.33.132.175:6112 UDP
Mar 17 19:57:48 xxx.xxx.xxx.xxx:6112 -> 63.29.216.91:6112 UDP
Mar 17 19:57:48 xxx.xxx.xxx.xxx:6112 -> 152.172.136.102:6112 UDP
Mar 17 19:57:48 xxx.xxx.xxx.xxx:6112 -> 152.166.114.240:6112 UDP
Mar 17 19:57:48 xxx.xxx.xxx.xxx:6112 -> 24.13.85.150:6112 UDP
Mar 17 19:57:48 xxx.xxx.xxx.xxx:6112 -> 216.215.33.8:6112 UDP
Mar 17 19:57:48 xxx.xxx.xxx.xxx:6112 -> 166.62.140.19:6112 UDP
Mar 17 19:57:48 xxx.xxx.xxx.xxx:6112 -> 63.28.190.5:6112 UDP
Mar 17 19:58:46 xxx.xxx.xxx.xxx:1037 -> 216.148.246.8:6112 SYN **S*****
Mar 17 19:58:47 xxx.xxx.xxx.xxx:6112 -> 209.254.234.129:6112 UDP
Mar 17 19:58:47 xxx.xxx.xxx.xxx:6112 -> 4.4.176.126:6112 UDP
Mar 17 19:58:47 xxx.xxx.xxx.xxx:6112 -> 24.48.139.29:6112 UDP
Mar 17 19:58:47 xxx.xxx.xxx.xxx:6112 -> 152.166.167.141:6112 UDP
Mar 17 19:58:47 xxx.xxx.xxx.xxx:6112 -> 207.30.21.65:6112 UDP
Mar 17 19:58:47 xxx.xxx.xxx.xxx:6112 -> 24.66.150.3:6112 UDP
Mar 17 19:58:47 xxx.xxx.xxx.xxx:6112 -> 63.24.200.1:6112 UDP
```

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

Mar 17 19:58:47 xxx.xxx.xxx.xxx:6112 -> 207.144.97.163:6112 UDP
Mar 17 19:58:47 xxx.xxx.xxx.xxx:6112 -> 24.68.38.20:6112 UDP
Mar 17 19:58:47 xxx.xxx.xxx.xxx:6112 -> 204.244.206.15:6112 UDP
Mar 17 19:58:47 xxx.xxx.xxx.xxx:6112 -> 63.28.138.45:6112 UDP
Mar 17 19:58:47 xxx.xxx.xxx.xxx:6112 -> 216.100.155.178:6112 UDP
Mar 17 19:58:47 xxx.xxx.xxx.xxx:6112 -> 209.180.136.227:6112 UDP
Mar 17 19:58:47 xxx.xxx.xxx.xxx:6112 -> 216.190.205.32:6112 UDP
Mar 17 19:58:47 xxx.xxx.xxx.xxx:6112 -> 156.56.120.210:6112 UDP
Mar 17 19:58:47 xxx.xxx.xxx.xxx:6112 -> 63.23.230.23:6112 UDP
Mar 17 19:58:47 xxx.xxx.xxx.xxx:6112 -> 207.172.126.129:6112 UDP
Mar 17 19:58:47 xxx.xxx.xxx.xxx:6112 -> 199.174.210.189:6112 UDP
Mar 17 19:58:47 xxx.xxx.xxx.xxx:6112 -> 24.1.208.102:6112 UDP
Mar 17 19:58:47 xxx.xxx.xxx.xxx:6112 -> 171.209.98.248:6112 UDP

**Source of Trace:** Stuart@SILICONDEFENSE.COM sent this trace to Incidents@SecurityFocus.com

**Active Targeting:** Yes, active scanning of port 6112

**History:** Unknown – access to previous logs was not available.

**Technique:** Automated, several connections in one second.
The packets are directed towards port 6112.
TCP and UDP scan.

**Intent:** Port 6112 is commonly used to run the game Diablo. The source could also be trying to find that service for a way to find a exploit.

**Analysis:** After looking at this trace several times, I came up with two alternatives. The first alternative focus around the fact that when you dialup to the internet you are constantly scanned. The server that running Diablo is noted for being a ver aggressive server that is constantly trying to reestablish the pervious connection. Since these scan concentrating on the game port that Diablo runs on, the scan may be not be of a malicious nature but the product of the server trying to reestablishing the connection. The second alternative is that someone is spoofing the Diablo web server to find an open port in the network or map the network. I think the this is the scan is just normal activity cause by someone on the network playing Diablo. I would recommend that the network administrator to contact some of these users to find out if they are playing Diablo , if they denied playing this game, then, I would close this port on the firewall in both directions. This will prevent the network from being scan on this port in the future and close up this vulnerability. Overall, this was a hard trace to analyzed with analyzing additional logs to see if there was an sudden increase in active scanning of this port or we been experiencing this scan since the users were allow to access the internet from their workstation.

**Severity of Attack:** Low

| Component | Score | Comments |
|---|---|---|
| Criticality | 3 | No specific machines are being targeted. |
| Lethality | 2 | It is unknown how the visitor would use any information gathered from this scan. |
| System Countermeasures | 4 | Modern operating system, but can not determine if all the patches were installed. |
| Network Countermeasures | 2 | The firewall was permissive. |
| Severity Score | -1 | Severity = (Criticality + Lethality) – (system countermeasures + net countermeasures) |

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

## Detect 3:

Wed 03/22 14:06:00 tcp x.x.x.x.2140 > host.whoi.edu.80
Wed 03/22 14:06:46 tcp x.x.x.x.2196 > host.whoi.edu.8080
Wed 03/22 14:07:32 tcp x.x.x.x.2238 > host.whoi.edu.3128

**Source of Trace:** Scott@WHOI.EDU sent this trace into Incidents@SecurityFocus.Com

**Active Targeting:** Yes

**History:** For the past few months Scott have been seen some web-related probes using the above pattern. It's always the same three ports, and they typically represent, however, the destinations are often nodes within our network address space that don't exist and/or have never existed. The scr address makes no other connection attempts to the box on the network, and there are no other attempts to cantact that destination box, just this cluster of three pokes.

**Technique:** Single host, Single source, multiple src ports.
Src ports for each given service remain the same 80, 8080, 3128
TCP scan
Scan in a pattern of three ports.
Source is sending only one packet at a time.

**Intent:** The source is looking for a host that will respond on port 3128. Looking for trojan horse.

**Analysis:** This scan is the result of the host infected with the RingZero Trojan. The target port is port 3128, the squid proxy service, and report back to a central location.

**Severity of Attack:** Medium

| Component | Score | Comments |
|---|---|---|
| Criticality | 5 | Host.WHOI.Edu is the target of this scan. |
| Lethality | 3 | It is unknown how the visitor would use any information gathered from this scan. |
| System Countermeasures | 4 | Modern operating system, can not determine if all the patches were installed. |
| Network Countermeasures | 2 | The firewall was permissive. |
| Severity Score | 2 | Severity = (Criticality + Lethality) – (system countermeasures + net countermeasures) |

## Detect 4:

Mar 27 22:00:25 input PROTO=17 204.210.104.156:137 *.16:137 L=78 S=0x00 I=63748 F=0x0000 T=112
Mar 27 22:00:27 input PROTO=17 204.210.104.156:137 *.16:137 L=78 S=0x00 I=5381 F=0x0000 T=112
Mar 27 22:00:28 input PROTO=17 204.210.104.156:137 *.16:137 L=78 S=0x00 I=5637 F=0x0000 T=112
Mar 27 22:00:36 input PROTO=17 204.210.104.156:137 *.16:137 L=78 S=0x00 I=58373 F=0x0000 T=112
Mar 27 22:00:37 input PROTO=17 204.210.104.156:137 *.16:137 L=78 S=0x00 I=58629 F=0x0000 T=112
Mar 27 22:00:39 input PROTO=17 204.210.104.156:137 *.16:137 L=78 S=0x00 I=59141 F=0x0000 T=112
Mar 27 22:00:57 input PROTO=17 204.210.104.156:137 *.16:137 L=78 S=0x00 I=4360 F=0x0000 T=112

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

Mar 27 22:00:58 input PROTO=17 204.210.104.156:137 *.16:137 L=78 S=0x00 I=4616 F=0x0000 T=112
Mar 27 22:01:00 input PROTO=17 204.210.104.156:137 *.16:137 L=78 S=0x00 I=4872 F=0x0000 T=112

**Source of Trace:** Bryan@visi.com sent this trace into Incidents@SecurityFocus.com

**Active Targeting:** Yes

**History:** Unknown – access to previous logs was not available.

**Technique:** UDP Port 137 scanning
Automated, single scan, single port
Internal Scan (Blocked the port on the Firewall and activity is still being logged)

**Intent:** Scanning for Netbios-NS vulnerabilities. The intent here is malicious in nature.

**Analysis:** At first, I thought this was an external scan looking to take advantage of Microsoft vulnerabilities in Port 137. After investigating the background in this trace, I found that they blocked this port on their firewall and the activities dramatically increased for port 137 scans that hit every IP# in the network. This is a good indication that this is an internal scan cause by malicious coding , such as a virus or worm. Search the virus alert from the different anti-virus vendors I discover there is a worm that work on the Network.VBS file that resides in the root dir, and in the startup folder. This worm propogates onto a machine, and then sits and tries to infect random workstations on the network by looking for shared C drives with no passwords. This worm can be cleaned from the infected machine.

**Severity of Attack:** Low

| Component | Score | Comments |
|---|---|---|
| Criticality | 2 | Desktop computer 204.210.104.156 is targeted. |
| Lethality | 2 | The attack is caused by a worm that designed to be malicious in nature, but not lethal. |
| System Countermeasures | 4 | Modern operating system, can not tell if all the patches were installed. |
| Network Countermeasures | 3 | The firewall restricted the scan from coming in. |
| Severity Score | -3 | Severity = (Criticality + Lethality) – (system countermeasures + net countermeasures) |

## Detect 5:

> Connection attempt to TCP xxx.xxx.xxx.xxx:1243 from 209.94.212.136:3575
> Connection attempt to TCP xxx.xxx.xxx.xxx:1243 from 209.94.212.136:3576
> Connection attempt to TCP xxx.xxx.xxx.xxx:1243 from 209.94.212.136:3577
> Connection attempt to TCP xxx.xxx.xxx.xxx:1243 from 209.94.212.136:3578
> Connection attempt to TCP xxx.xxx.xxx.xxx:1243 from 209.94.212.136:3579
> Connection attempt to TCP xxx.xxx.xxx.xxx:1243 from 209.94.212.136:3616
> Connection attempt to TCP xxx.xxx.xxx.xxx:1243 from 209.94.212.136:3617
> Connection attempt to TCP xxx.xxx.xxx.xxx:1243 from 209.94.212.136:3620
> Connection attempt to TCP xxx.xxx.xxx.xxx:1243 from 209.94.212.136:3619
> Connection attempt to TCP xxx.xxx.xxx.xxx:1243 from 209.94.212.136:3687
> Connection attempt to TCP xxx.xxx.xxx.xxx:1243 from 209.94.212.136:3688
> Connection attempt to TCP xxx.xxx.xxx.xxx:1243 from 209.94.212.136:3689
> Connection attempt to TCP xxx.xxx.xxx.xxx:1243 from 209.94.212.136:3690
> Connection attempt to TCP xxx.xxx.xxx.xxx:1243 from 209.94.212.136:3691

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

> Connection attempt to TCP xxx.xxx.xxx.xxx:1243 from 209.94.212.136:3692
> Connection attempt to TCP xxx.xxx.xxx.xxx:1243 from 209.94.212.136:3693
> Connection attempt to TCP xxx.xxx.xxx.xxx:1243 from 209.94.212.136:3695
> Connection attempt to TCP xxx.xxx.xxx.xxx:1243 from 209.94.212.136:3694
> Connection attempt to TCP xxx.xxx.xxx.xxx:1243 from 209.94.212.136:3696
> Connection attempt to TCP xxx.xxx.xxx.xxx:1243 from 209.94.212.136:3697
> Connection attempt to TCP xxx.xxx.xxx.xxx:1243 from 209.94.212.136:3698
> Connection attempt to TCP xxx.xxx.xxx.xxx:1243 from 209.94.212.136:3699
> Connection attempt to TCP xxx.xxx.xxx.xxx:1243 from 209.94.212.136:3700
> Connection attempt to TCP xxx.xxx.xxx.xxx:1243 from 209.94.212.136:3701
> Connection attempt to TCP xxx.xxx.xxx.xxx:1243 from 209.94.212.136:3702
> Connection attempt to TCP xxx.xxx.xxx.xxx:1243 from 209.94.212.136:3703
> Connection attempt to TCP xxx.xxx.xxx.xxx:1243 from 209.94.212.136:3704

**Source of Trace:** Omachonu Ogali of Intranova.net sent this trace to Security Focus Incidents Reporting

**Active Targeting:** Yes

**History:** Unknown – access to previous logs was not available.

**Technique:** The source port is constant (1243).
TCP scan
Single Service Port Scanned
Source port increases by one – slowed scan

**Intent:** Malicious in nature. This appears to be a Trojan scan.

**Analysis:** This appears to be a SubSeven version 2.1 scan which uses port 1234 and 27374 by default. There has been a noticable increase in SubSeven scans.

**Severity of Attack:** Medium

| Component | Score | Comments |
|---|---|---|
| Criticality | 5 | Attack is focus on a single server. |
| Lethality | 5 | The attacker could gain access to the root and this could be lethal. |
| System Countermeasures | 4 | Modern operating system, can not tell if all the patches were installed. |
| Network Countermeasures | 3 | The network has been preventing connection. This could be because SubSeven has not been installed in the network. |
| Severity Score | 3 | Severity = (Criticality + Lethality) – (system countermeasures + net countermeasures) |

## Detect 6:

Mar 16 21:23:13 gate iplog[10085]: UDP: dgram to port 2140 from host 213.1.128.105.btinternet.com:60000 (2data bytes)
Mar 16 22:34:38 gate iplog[10085]: UDP: dgram to port 2140 from host 5.99.47.84.btinternet.com:60000 (2data bytes)
Mar 16 23:18:14 gate iplog[10085]: UDP: dgram to port 2140 from host 62.6.69.21.btinternet.com:60000 (2data bytes)

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

**Source of Trace:** Fernando Cardoso from National Library of Portugal sent the trace into Security Focus Incident Reporting.

**Active Targeting:** Yes

**History:** Unknown – access to previous logs was not available.

**Technique:** The source port is constant (2140).
The host scan is constant (60000)
The host are dynamically assigned IP address.
UDP scan
Single Service Port Scanned
Slowed scan

**Intent:** Malicious in nature. This appears to be a Trojan scan.

**Analysis:** This appears to be a Deep Throat Trojan scan which uses port 2140 and 60000 by default. The BTInternet.com is a free internet service that is experiencing security problems with their dialup service, which make it a primary target to launch attackes from

**Severity of Attack:** Medium

| Component | Score | Comments |
|---|---|---|
| Criticality | 5 | Attack is focus on a single server. |
| Lethality | 5 | The attacker could gain access to the root and this could be lethal. |
| System Countermeasures | 4 | Modern operating system, can not tell if all the patches were installed. |
| Network Countermeasures | 3 | The network has been preventing connection. This could be because Deep Throat Trojan has not been installed in the network. |
| Severity Score | 3 | Severity = (Criticality + Lethality) – (system countermeasures + net countermeasures) |

## Detect 7:

| -source- | -dest- | -sport- | -dport- | -protocol- |
|---|---|---|---|---|
| 212.187.65.86 | 203.5.67.63 | 7744 | 7 | 17 |
| 212.187.65.86 | 205.5.66.128 | 6537 | 7 | 17 |
| 212.187.65.86 | 205.5.66.63 | 29432 | 7 | 17 |
| 212.187.65.86 | 205.5.66.128 | 15793 | 7 | 17 |
| 212.187.65.86 | 205.5.66.191 | 17367 | 7 | 17 |
| 212.187.65.86 | 205.5.67.63 | 29210 | 7 | 17 |
| 212.187.65.86 | 205.5.67.127 | 351 | 7 | 17 |
| 212.187.65.86 | 205.5.66.127 | 17330 | 7 | 17 |

**Source of Trace:** Joe@ITS.UNIMELB.EDU.AU sent this trace to the Security Focus Incident Reporting System.

**Active Targeting:** Yes

**History:** Unknown – access to previous logs was not available.

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

**Technique:** The Destination port is constant (7 - echo).
The source address appears to be spoofed
The destination address are broadcast addresses.
UDP scan
Single Service Port Scanned

**Intent:** Malicious in nature. Looking for a vulnerable host to launch a DOS Attack.

**Analysis:** This appears to be fraggle attack. The attacker is looking for a victims to launch a larger Denial of Service (DdoS) against someone. Again, this could be the a recon for a possible DoS against this network.

**Severity of Attack:** Medium

| Component | Score | Comments |
|---|---|---|
| Criticality | 4 | Attack is not focusing on a single host. |
| Lethality | 4 | The network could subject to a DoS attack |
| System Countermeasures | 4 | Modern operating system, can not tell if all the patches were installed. |
| Network Countermeasures | 2 | The network firewall has been permissive |
| Severity Score | 2 | Severity = (Criticality + Lethality) – (system countermeasures + net countermeasures) |

## Detect 8:

Mar 13 18:50:33 xxx.xxx.xxx.xxx:1510 -> 208.25.112.20:53 UDP
Mar 13 18:50:33 xxx.xxx.xxx.xxx:27960 -> 192.246.40.56:27950 UDP
Mar 13 18:50:34 xxx.xxx.xxx.xxx:27960 -> 24.28.21.205:27960 UDP
Mar 13 18:50:34 xxx.xxx.xxx.xxx:27960 -> 206.191.192.47:27960 UDP
Mar 13 18:50:34 xxx.xxx.xxx.xxx:27960 -> 207.127.210.34:27960 UDP
Mar 13 18:50:34 xxx.xxx.xxx.xxx:27960 -> 212.140.216.69:37963 UDP
Mar 13 18:50:34 xxx.xxx.xxx.xxx:27960 -> 212.140.216.69:37961 UDP
Mar 13 18:50:34 xxx.xxx.xxx.xxx:27960 -> 206.136.149.10:27960 UDP
Mar 13 18:50:34 xxx.xxx.xxx.xxx:27960 -> 207.238.206.13:27965 UDP
Mar 13 18:50:34 xxx.xxx.xxx.xxx:27960 -> 207.105.234.8:27960 UDP
Mar 13 18:50:34 xxx.xxx.xxx.xxx:27960 -> 210.97.228.42:27961 UDP
Mar 13 18:50:34 xxx.xxx.xxx.xxx:27960 -> 216.202.141.69:27960 UDP
Mar 13 18:50:34 xxx.xxx.xxx.xxx:27960 -> 195.250.175.164:27960 UDP
Mar 13 18:50:34 xxx.xxx.xxx.xxx:27960 -> 209.30.137.20:27960 UDP
Mar 13 18:50:34 xxx.xxx.xxx.xxx:27960 -> 200.27.132.9:26000 UDP
Mar 13 18:50:34 xxx.xxx.xxx.xxx:27960 -> 212.93.4.18:27962 UDP
Mar 13 18:50:34 xxx.xxx.xxx.xxx:27960 -> 216.46.240.6:27962 UDP
Mar 13 18:50:35 xxx.xxx.xxx.xxx:27960 -> 210.97.228.42:27963 UDP
Mar 13 18:50:35 xxx.xxx.xxx.xxx:27960 -> 216.202.141.69:27963 UDP

**Source of Trace:** Stuart@SILICONDEFENSE.COM sent this trace to Incidents@SecurityFocus.com

**Active Targeting:** Yes, active scanning of port 27960

**History:** Unknown – access to previous logs was not available.

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

**Technique:** Automated, several connections in one second.
UDP scan.
This is a Fast scan
Src port is static
Not a subtle scan

**Intent:** Port 27960 is commonly used to run the Quake3 arena's server. The source could also be trying to find that service for a way to find a exploit.

**Analysis:** After looking at this trace several times, I came up with two alternatives. The first alternative focus around the fact that when you dialup to the internet you are constantly scanned. The server that running Quake III is noted for being a ver aggressive server that is constantly trying to reestablish the pervious connection. Since these scan concentrating on the game port that Quake III runs on, the scan may be not be of a malicious nature but the product of the server trying to reestablishing the connection. The second alternative is that someone is spoofing the Quake III server to find an open port in the network or map the network. I think the this is the scan is just normal activity cause by someone on the network playing Quake III. I would recommend that the network administrator to contact some of these users to find out if they are playing Diablo , if they denied playing this game, then, I would close this port on the firewall in both directions. This will prevent the network from being scan on this port in the future and close up this vulnerability. Overall, this was a hard trace to analyzed with analyzing additional logs to see if there was an sudden increase in active scanning of this port or we been experiencing this scan since the users were allow to access the internet from their workstation.

**Severity of Attack:** Low

| Component | Score | Comments |
|---|---|---|
| Criticality | 3 | No specific machines are being targeted. |
| Lethality | 2 | It is unknown how the visitor would use any information gathered from this scan. |
| System Countermeasures | 4 | Modern operating system, but can not determine if all the patches were installed. |
| Network Countermeasures | 2 | The firewall was permissive. |
| Severity Score | -1 | Severity = (Criticality + Lethality) – (system countermeasures + net countermeasures) |

## Detect 9:

Webcache.tue.nl - - [19/mar/2000:00:49:12-0500] "POST /cgi-bin/perl HTTP/1.0" 404 206
Webcache.tue.nl - - [20/mar/2000:21:44:53-0500] "POST /cgi-bin/phf?Qname=x%0a/bin/sh+-s%0a HTTP/1.0" 404 205

Mar 19 04:23:04 server kernel: TCP connection rejected from 131.155.69.100, port 5556
Mar 19 05:48:22 server kernel: TCP connection rejected from 131.155.69.100, port 512
Mar 19 08:28:46 server kernel: TCP connection rejected from 131.155.69.100, port 512

Mar 18 23:51:35 4C: workstation rexecd[14591]: refused connect from svstud.win.tue.nl
Mar 19 01:03:14 4C: workstation rexecd[14635]: refused connect from svstud.win.tue.nl
Mar 19 01:49:15 4C: workstation rexecd[14655]: refused connect from svstud.win.tue.nl
Mar 19 04:28:21 4C: workstation rexecd[14731]: refused connect from svstud.win.tue.nl
Mar 19 05:36:30 4C: workstation rexecd[14774]: refused connect from svstud.win.tue.nl
Mar 19 05:39:34 4C: workstation rexecd[14775]: refused connect from svstud.win.tue.nl
Mar 19 08:20:00 4C: workstation rexecd[14857]: refused connect from svstud.win.tue.nl
Mar 19 09:23:25 4C: workstation rexecd[14897]: refused connect from svstud.win.tue.nl

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

**Source of Trace:** Jose@BIOCSERVER.BIOC.CWRU.EDU sent this trace into the Security Focus Incident Reporting System

**Active Targeting:** Yes

**History:** Unknown – access to previous logs was not available.

**Technique:** Fairly slow scan.
TCP scan.
Cgi/bin scan
Rexec vulnerability scan
Phf style attack

**Intent:** This attack is malicious in nature. The intent is exploit the vulnerabilities in the cgi/bin and rexec.

**Analysis:** The attacker is trying to take control of the web server by trying to use the vulnerabilities in the cgi/bin and rexec directories. Also, the atttacker may be trying to access a Trojan horse.

**Severity of Attack:** Low

| Component | Score | Comments |
|---|---|---|
| Criticality | 5 | The attack was focused on the web server. |
| Lethality | 2 | It is unknown how the visitor would use any information gathered from this scan. |
| System Countermeasures | 4 | Modern operating system, can not verify that all the patches were installed. |
| Network Countermeasures | 2 | The firewall was permissive. |
| Severity Score | 1 | Severity = (Criticality + Lethality) – (system countermeasures + net countermeasures) |

## Detect 10:

```
Mar 20 18:17:24 X:1669 -> Y:80 FIN ***F****
Mar 20 18:17:24 X:1669 -> Y:80 SYN **S*****
[**] IDS027 – SCAN-FIN [**}
03/20-18:17:24.259062 X:1669 -> Y:80
TCP TTL:116 TOS:0x0 ID:44867 DF
***F**** Seq: 0xB3FA71 Ack: 0x0 Win: 0x0

Mar 20 18:19:55 X:1684 -> Y:80 SYN **S*****
Mar 20 18:19:55 X:1684 -> Y:80 FIN ***F****
[**] IDS027 – SCAN-FIN [**}
03/20-18:19:55.288742 X:1684 -> Y:80
TCP TTL:116 TOS:0x0 ID:44942 DF
***F**** Seq: 0xB64866 Ack: 0x0 Win: 0x0

Mar 20 19:02:37 X:1985 -> Y:80 SYN **S*****
Mar 20 19:02:37 X:1985 -> Y:80 FIN ***F****
[**] IDS027 – SCAN-FIN [**}
03/20-19:02:37.563409 X:1985 -> Y:80
```

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

TCP TTL:116 TOS:0x0 ID:46049 DF
***F**** Seq: 0xDD5FE6 Ack: 0x0 Win: 0x0

(X and Y are fixed IP addresses)

**Source of Trace:** Stuart@SILICONDEFENSE.COM sent this trace to Incidents@SecurityFocus.com

**Active Targeting:** Yes

**History:** Unknown – access to previous logs was not available.

**Technique:** Fairly slow scan.
TCP scan.
Syn/Fin packets
Focus on the same IP address and port
Packets sent in pattern (3 packets at time arriving almost at the same time)
Automated scan

**Intent:** This attack is malicious in nature. Possible host scan for open port 80.

**Analysis:** I feel that may be NMAP FIN scan looking for an open port 80 host. The attacker would like to find the servers on the network that will repond to a connection on HTTP. This port is noted for vulnerabilities. Could also be used to launch a DoS attack on the network.

**Severity of Attack:** Low

| Component | Score | Comments |
|---|---|---|
| Criticality | 3 | No specific machines are being targeted. |
| Lethality | 4 | The port have known vulnerabilities that could prove lethal. |
| System Countermeasures | 3 | Modern Operating System, can not verify if all patches were installed |
| Network Countermeasures | 3 | Running Snort and some packet filtering |
| Severity Score | 1 | Severity = (Criticality + Lethality) – (system countermeasures + net countermeasures) |

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