Global Information Assurance Certification Paper

*** Northcutt, now this is what I am talking about, got some of his own detects, solid analysis process, did some research, attributed resources, hoo hah! Helpful hint though, when you download someone else's file, edit properties :) 94 ***

GCIA Certification Practical

10 Detects with Analyses

David K. Leaphart

April 5, 2000

Detects are derived as stated.

I&W Methodology used.

Submitted as practical for SANS 2000 written exam (3/25/2000).

Detect 1 http://www.sans.org/y2k/032800-2000.htm

I noticed this in my logs from yesterday...
-Kathleen
Hello,
I am writing because I noticed that your www7.clever.net server scanned a few of my servers yesterday for exec (TCP port 512) and BO Facil (TCP port 5556). Your host may have been compromised or originated from one of your customers, etc. I would appreciate it if you could investigate that matter and let me know the outcome.
I have sanitized the information below. Please let me know if you need more information to investigate.
Thank you,
Kathleen

```
Mar 27 17:01:03.516 host kernel: 226 IP packet dropped (www7.clever.net[209.235.11.254]->host1[x.x.x.x1]: Protocol=TCP[SYN] Port 53050->5556):
Restricted Port: Protocol=TCP[SYN] Port 53050->5556 (received on interface x.x.x.x)

Mar 27 17:01:03.516 host kernel: 226 IP packet dropped (www7.clever.net[209.235.11.254]->host1[x.x.x.x1]: Protocol=TCP[SYN] Port 53051->512):
Restricted Port: Protocol=TCP[SYN] Port 53051->512 (received on interface x.x.x.x)

Mar 27 17:01:03.521 host kernel: 226 IP packet dropped (www7.clever.net[209.235.11.254]->host2[x.x.x.x2]: Protocol=TCP[SYN] Port 53052->5556):
Restricted Port: Protocol=TCP[SYN] Port 53052->5556 (received on interface x.x.x.x)

Mar 27 17:01:03.522 host kernel: 226 IP packet dropped (www7.clever.net[209.235.11.254]->host2[x.x.x.x2]: Protocol=TCP[SYN] Port 53053->512):
Restricted Port: Protocol=TCP[SYN] Port 53053->512 (received on interface x.x.x.x)

Mar 27 17:01:03.528 host kernel: 226 IP packet dropped (www7.clever.net[209.235.11.254]->x.x.x.x3: Protocol=TCP[SYN] Port 53054->5556):
Restricted Port: Protocol=TCP[SYN] Port 53054->5556 (received on interface x.x.x.x)

Mar 27 17:01:03.528 host kernel: 226 IP packet dropped (www7.clever.net[209.235.11.254]->x.x.x.x3: Protocol=TCP[SYN] Port 53055->512):
Restricted Port: Protocol=TCP[SYN] Port 53055->512 (received on interface x.x.x.x)
```

ANALYSIS:

Evidence of Active Targeting?

Yes. The traffic from the source is detected at the firewall's interface.

Identify the History?

No previous history was noted in the detect report.

Identify the Technique?

TCP SYN packets were directed at the subnet. The SYN packets were directed at two specific ports (5556/TCP and 512/TCP). If the ports were open, they would return a SYN-ACK to the source. As it is, a Raptor firewall returns RES packets for closed ports. The packets arrived at predictable uniform times and occurred over a short duration. These hosts appear to be located in a service network behind the firewall; not on the DMZ. There does not appear to be any previous knowledge of the hosts on their subnet since multiple destinations were probed. The source address is active on the internet and does not appear to have been spoofed.

Evidence of Intent?

This detect is a **host scan** of either the subnet or a larger subnet that includes this network's Class assignments. HP uses the port 5556/TCP for their Remote Watch product. The person could be scanning for this service or the existence of HP-UX for possible exploitation. The following was found on this: *Two vulnerabilities in HP Remote Watch exists allowing users to gain root access. The first was via a socket connection on port 5556. The second was as a result of using the showdisk utility, which is part of the*

Remote Watch product. However, the Back Orifice system also uses this port for its front-end facility. I believe this to be the more likely scenario for this port.

The 512/TCP port is used by rexecd. I found the following on this: *Rexecd allows redirection of stderr stream to an arbitrary port on the client machine. This stream is opened by rexecd before authentication of the user. Spoofing techniques could allow the client to direct the stderr stream towards an arbitrary host as well as an arbitrary port, possibly exploiting a given trust model.*

The targeted scanning of these two ports is indicative of a pursuit for an exploit. The owner should indeed be notified for further investigation (which is what the analyst did per the detect report.)

Identify Hostile Individuals and Groups?

Based on Whois, this is a web server belonging to Clever.net, an ISP based in Atlanta. This would not seem to be likely source for this type of scan. However, it does not preclude some mischief by one trusted with access to these servers. I accessed the source (www7.clever.net) with a browser. The home page is simply three hyperlinks to other clever.net servers. From a web server standpoint, this server does not appear to be "heavily loaded". Maybe this makes it a good candidate for someone to "borrow" for other uses! A point of concern in this case would be that the person, working for an ISP on their servers, would be very knowledgeable.

The time of the detect was right at 5:00pm. If this is also the time in Atlanta at the time of the detect, this may have been a good time to initiate the probe since most employees might be distracted getting ready to leave for the day or change shifts. If true, it might strengthen the argument that an employee at the ISP was responsible.

Severity: -2

Criticality: I note this to be a 5 since all of the "internet" servers as well as the firewall were targeted.
Lethality: This is a 2 since the firewall seems to be protecting its hosts from traffic on these ports and no specific target was seen.
Countermeasures: This is a 5 presuming that all of the "internet" servers are fully patched and hardened and reside in a service network behind the firewall. I presume that none are in the DMZ.
Net Countermeasures: Presuming that some modem and ISDN accesses exist, this is rated at a 4.

Detect 2 http://www.sans.org/y2k/032800.htm

```
Mar 27 12:33:28 myhost portsentry[178]: attackalert: Connect from host: na-165-5.na.avantel.net.mx/148.245.165.5 to UDP port: 111
Mar 27 12:33:28 myhost portsentry[178]: attackalert: Connect from host: na-165-5.na.avantel.net.mx/148.245.165.5 to UDP port: 111
Mar 27 12:33:33 myhost portsentry[178]: attackalert: Connect from host: na-165-5.na.avantel.net.mx/148.245.165.5 to UDP port: 111
Mar 27 12:33:38 myhost portsentry[178]: attackalert: Connect from host: na-165-5.na.avantel.net.mx/148.245.165.5 to UDP port: 111
Mar 27 12:33:43 myhost portsentry[178]: attackalert: Connect from host: na-165-5.na.avantel.net.mx/148.245.165.5 to UDP port: 111
Mar 27 12:33:48 myhost portsentry[178]: attackalert: Connect from host: na-165-5.na.avantel.net.mx/148.245.165.5 to UDP port: 111
Mar 27 12:33:53 myhost portsentry[178]: attackalert: Connect from host: na-165-5.na.avantel.net.mx/148.245.165.5 to UDP port: 111
Mar 27 12:33:58 myhost portsentry[178]: attackalert: Connect from host: na-165-5.na.avantel.net.mx/148.245.165.5 to UDP port: 111
Mar 27 12:34:03 myhost portsentry[178]: attackalert: Connect from host: na-165-5.na.avantel.net.mx/148.245.165.5 to UDP port: 111
Mar 27 12:34:08 myhost portsentry[178]: attackalert: Connect from host: na-165-5.na.avantel.net.mx/148.245.165.5 to UDP port: 111
Mar 27 12:34:13 myhost portsentry[178]: attackalert: Connect from host: na-165-5.na.avantel.net.mx/148.245.165.5 to UDP port: 111
Mar 27 12:34:18 myhost portsentry[178]: attackalert: Connect from host: na-165-5.na.avantel.net.mx/148.245.165.5 to UDP port: 111
Mar 27 12:34:23 myhost portsentry[178]: attackalert: Connect from host: na-165-5.na.avantel.net.mx/148.245.165.5 to UDP port: 111
Mar 27 12:34:28 myhost portsentry[178]: attackalert: Connect from host: na-165-5.na.avantel.net.mx/148.245.165.5 to UDP port: 111
```

```
Mar 27 12:34:33 myhost portsentry[178]: attackalert: Connect from host: na-165-5.na.avantel.net.mx/148.245.165.5 to UDP port: 111
Mar 27 12:34:38 myhost portsentry[178]: attackalert: Connect from host: na-165-5.na.avantel.net.mx/148.245.165.5 to UDP port: 111
Mar 27 12:34:43 myhost portsentry[178]: attackalert: Connect from host: na-165-5.na.avantel.net.mx/148.245.165.5 to UDP port: 111
Mar 27 12:34:48 myhost portsentry[178]: attackalert: Connect from host: na-165-5.na.avantel.net.mx/148.245.165.5 to UDP port: 111
Mar 27 12:34:53 myhost portsentry[178]: attackalert: Connect from host: na-165-5.na.avantel.net.mx/148.245.165.5 to UDP port: 111
Mar 27 12:34:58 myhost portsentry[178]: attackalert: Connect from host: na-165-5.na.avantel.net.mx/148.245.165.5 to UDP port: 111
Mar 27 12:35:03 myhost portsentry[178]: attackalert: Connect from host: na-165-5.na.avantel.net.mx/148.245.165.5 to UDP port: 111
Mar 27 12:35:08 myhost portsentry[178]: attackalert: Connect from host: na-165-5.na.avantel.net.mx/148.245.165.5 to UDP port: 111
Mar 27 12:35:13 myhost portsentry[178]: attackalert: Connect from host: na-165-5.na.avantel.net.mx/148.245.165.5 to UDP port: 111
Mar 27 12:35:18 myhost portsentry[178]: attackalert: Connect from host: na-165-5.na.avantel.net.mx/148.245.165.5 to UDP port: 111
```

ANALYSIS:

Evidence of Active Targeting?

Yes. The traffic from the source is detected at the destination's interface.

Identify the History?

No previous history was noted in the detect report.

Identify the Technique?

UDP packets were directed at a particular host on the subnet. The packets were probing for an active port 111/UDP. The packets arrived every 5 seconds and occurred over a short duration. The detect report indicates that "myhost" is not behind a firewall. (Unless "myhost" is a firewall!) Without further information, I presume this was a targeted probe. It is not clear from the detect report as to whether other hosts were targeted and if "myhost" responded with an ICMP port unreachable message. If no ICMP message was returned, the source would consider 111/UDP to be active on "myhost". This could lead to further problems. The source address is active on the internet and does not appear to have been spoofed.

Evidence of Intent?

This detect is an **attempt to connect to a dangerous port**, port 111 sunrpc. There are numerous serious Unix exploits using this port. The person can access a lot of information as to what services are running on a system and what ports are assigned. The big concern here would also be if NFS is active and accessible on "myhost" since NFS is a well known RPC service. As noted in the previous paragraph, it is not clear from the detect report as to whether other hosts were targeted. If this is a single target detect, it might indicate that the source has knowledge of the network. The victim needs to ensure that this is not a valid vulnerability for "myhost".

Identify Hostile Individuals and Groups?

Based on Whois, this is a host in Mexico. It is or is using the services of ienlaces.net.mx ISP in Ciudad de Mexico. Based on some situations in Mexico, this is probably not a friendly detect.

This ISP needs to be notified of this activity.

Severity: 5

Criticality: I note this to be a 4 assuming that "myhost" is a relatively important internet host.
Lethality: Presuming that "myhost" is a Unix machine, this is a 4 if the port is accessible.
Countermeasures: This is a 3 presuming that "myhost" is running with some patches missing.

Net Countermeasures: Presuming that "myhost" is not behind a firewall (or the firewall itself), this is rated at a 0.

Detect 3 Liberty's firewall logs 3/28/2000 First three octets of our host addresses changed to x.x.x

```
Mar 28 00:09:38.691 226 IP  packet dropped (24.3.17.194->x.x.x.35: Protocol=TCP[SYN] Port 2666->53): Restricted Port: Protocol=TCP[SYN] Port 2666->53
(received on interface x.x.x.38)
Mar 28 00:09:38.693 226 IP  packet dropped (24.3.17.194->x.x.x.36: Protocol=TCP[SYN] Port 2666->53): Restricted Port: Protocol=TCP[SYN] Port 2666->53
(received on interface x.x.x.38)
Mar 28 00:09:38.700 226 IP  packet dropped (24.3.17.194->x.x.x.39: Protocol=TCP[SYN] Port 2666->53): Restricted Port: Protocol=TCP[SYN] Port 2666->53
(received on interface x.x.x.38)
Mar 28 00:09:38.741 226 IP  packet dropped (24.3.17.194->x.x.x.54: Protocol=TCP[SYN] Port 2666->53): Restricted Port: Protocol=TCP[SYN] Port 2666->53
(received on interface x.x.x.38)
```

ANALYSIS:

Evidence of Active Targeting?

Yes. The traffic from the source is detected at the firewall's interface.

Identify the History?

No previous traffic from the source address could be found in the archives.

Identify the Technique?

TCP SYN packets were directed at our subnet from a single host. The SYN packets were directed at port 53/TCP on our hosts and hoping for a SYN-ACK return. The packets arrived at predictable uniform times and occurred over a short duration. Also, the source port is a constant: 2666. These hosts are not on the DMZ subnet but are located in a service network behind our firewall. There does not appear to be any previous knowledge of our hosts. Only the firewall has port 53 active. It is a DNS server for the protected network. The source address is active on the internet and does not appear to have been spoofed.

Evidence of Intent?

This is a **host scan** of either our subnet or a larger subnet that includes our Class assignments. More specifically, it is a **scan for a DNS zone transfer**. This is more than a simple DNS name lookup (i.e., NSLOOKUP) since that uses UDP. Also, the use of a hardwired source port lends itself to a script looking to make an exploitation. The person is hoping to find a DNS server in order to download a host table for further study. The source seems to be a valid address and is reliably ping'd. A double check of the DNS service on the firewall was completed.

Identify Hostile Individuals and Groups?

Based on Whois, this is a home user on the @Home domain in California! This strengthens the idea of mischief behind this detect. Further detects from this source would warrant a stronger investigation.

Severity: 1

Criticality: I note this to be a 5 since all of our "internet" servers as well as our firewall were scanned and the firewall is a DNS server.

Lethality: This is a 5. DNS exploits can be very lethal. The DNS service on the firewall is specifically configured to provide limited information; however, is does contain the service network configuration.

Countermeasures: This is a 5 for us since all of "internet" servers are fully patched and hardened and reside in a service network behind our firewall. None are in the DMZ. The firewall software is fully patched with a limited DNS implemented.
Net Countermeasures: Since we do have some modem and ISDN accesses, this is rated at a 4.

Detect 4 Liberty's firewall logs 3/28/2000 First three octets of our host addresses changed to x.x.x

This is a partial listing of the detect. The whole detect was over 1500 frames! The essence of the detect is represented.

```
Mar 28 17:32:17.176  347 Possible Port Scan detected on Interface  x.x.x.38 (207.94.123.83-> x.x.x.35: Protocol=UDP Port 137->137)
Mar 28 17:32:17.664  347 Possible Port Scan detected on Interface  x.x.x.38 (192.168.2.28-> x.x.x.35: Protocol=UDP Port 137->137)
Mar 28 17:32:17.668  347 Possible Port Scan detected on Interface  x.x.x.38 (207.94.123.83-> x.x.x.35: Protocol=UDP Port 137->137)
Mar 28 17:32:18.131  347 Possible Port Scan detected on Interface  x.x.x.38 (207.94.123.83-> x.x.x.35: Protocol=UDP Port 137->137)
Mar 28 17:32:18.618  347 Possible Port Scan detected on Interface  x.x.x.38 (192.168.2.28-> x.x.x.35: Protocol=UDP Port 137->137)
Mar 28 17:32:18.634  347 Possible Port Scan detected on Interface  x.x.x.38 (207.94.123.83-> x.x.x.35: Protocol=UDP Port 137->137)
Mar 28 17:32:19.156  347 Possible Port Scan detected on Interface  x.x.x.38 (207.94.123.83-> x.x.x.35: Protocol=UDP Port 137->137)
Mar 28 17:32:19.420  347 Possible Port Scan detected on Interface  x.x.x.38 (207.94.123.83-> x.x.x.35: Protocol=UDP Port 137->137)
Mar 28 17:32:19.431  347 Possible Port Scan detected on Interface  x.x.x.38 (192.168.2.28-> x.x.x.35: Protocol=UDP Port 137->137)
Mar 28 17:32:20.300  347 Possible Port Scan detected on Interface  x.x.x.38 (192.168.2.28-> x.x.x.35: Protocol=UDP Port 137->137)
Mar 28 17:32:20.566  347 Possible Port Scan detected on Interface  x.x.x.38 (192.168.2.28-> x.x.x.35: Protocol=UDP Port 137->137)
Mar 28 17:32:20.572  347 Possible Port Scan detected on Interface  x.x.x.38 (207.94.123.83-> x.x.x.35: Protocol=UDP Port 137->137)
Mar 28 17:32:21.147  347 Possible Port Scan detected on Interface  x.x.x.38 (207.94.123.83-> x.x.x.35: Protocol=UDP Port 137->137)
Mar 28 17:32:21.152  347 Possible Port Scan detected on Interface  x.x.x.38 (192.168.2.28-> x.x.x.35: Protocol=UDP Port 137->137)
Mar 28 17:32:21.442  347 Possible Port Scan detected on Interface  x.x.x.38 (192.168.2.28-> x.x.x.35: Protocol=UDP Port 137->137)
Mar 28 17:32:21.452  347 Possible Port Scan detected on Interface  x.x.x.38 (207.94.123.83-> x.x.x.35: Protocol=UDP Port 137->137)
Mar 28 17:32:21.890  347 Possible Port Scan detected on Interface  x.x.x.38 (207.94.123.83-> x.x.x.35: Protocol=UDP Port 137->137)
Mar 28 17:32:22.008  347 Possible Port Scan detected on Interface  x.x.x.38 (207.94.123.83-> x.x.x.35: Protocol=UDP Port 137->137)
Mar 28 17:32:22.010  347 Possible Port Scan detected on Interface  x.x.x.38 (192.168.2.28-> x.x.x.35: Protocol=UDP Port 137->137)
Mar 28 17:32:22.333  347 Possible Port Scan detected on Interface  x.x.x.38 (192.168.2.28-> x.x.x.35: Protocol=UDP Port 137->137)
Mar 28 17:32:22.342  347 Possible Port Scan detected on Interface  x.x.x.38 (207.94.123.83-> x.x.x.35: Protocol=UDP Port 137->137)
Mar 28 17:32:22.734  347 Possible Port Scan detected on Interface  x.x.x.38 (207.94.123.83-> x.x.x.35: Protocol=UDP Port 137->137)
Mar 28 17:32:22.847  347 Possible Port Scan detected on Interface  x.x.x.38 (207.94.123.83-> x.x.x.35: Protocol=UDP Port 137->137)
Mar 28 17:32:22.851  347 Possible Port Scan detected on Interface  x.x.x.38 (192.168.2.28-> x.x.x.35: Protocol=UDP Port 137->137)
Mar 28 17:32:23.142  347 Possible Port Scan detected on Interface  x.x.x.38 (192.168.2.28-> x.x.x.35: Protocol=UDP Port 137->137)
Mar 28 17:32:23.143  347 Possible Port Scan detected on Interface  x.x.x.38 (207.94.123.83-> x.x.x.35: Protocol=UDP Port 137->137)
Mar 28 17:32:23.518  347 Possible Port Scan detected on Interface  x.x.x.38 (207.94.123.83-> x.x.x.35: Protocol=UDP Port 137->137)
Mar 28 17:32:23.628  347 Possible Port Scan detected on Interface  x.x.x.38 (207.94.123.83-> x.x.x.35: Protocol=UDP Port 137->137)
Mar 28 17:32:23.632  347 Possible Port Scan detected on Interface  x.x.x.38 (192.168.2.28-> x.x.x.35: Protocol=UDP Port 137->137)
Mar 28 17:32:23.996  347 Possible Port Scan detected on Interface  x.x.x.38 (192.168.2.28-> x.x.x.35: Protocol=UDP Port 137->137)
Mar 28 17:32:24.004  347 Possible Port Scan detected on Interface  x.x.x.38 (207.94.123.83-> x.x.x.35: Protocol=UDP Port 137->137)
Mar 28 17:32:24.416  347 Possible Port Scan detected on Interface  x.x.x.38 (207.94.123.83-> x.x.x.35: Protocol=UDP Port 137->137)
Mar 28 17:32:24.536  347 Possible Port Scan detected on Interface  x.x.x.38 (207.94.123.83-> x.x.x.35: Protocol=UDP Port 137->137)
Mar 28 17:32:24.540  347 Possible Port Scan detected on Interface  x.x.x.38 (192.168.2.28-> x.x.x.35: Protocol=UDP Port 137->137)
Mar 28 17:32:24.835  347 Possible Port Scan detected on Interface  x.x.x.38 (192.168.2.28-> x.x.x.35: Protocol=UDP Port 137->137)
Mar 28 17:32:24.841  347 Possible Port Scan detected on Interface  x.x.x.38 (207.94.123.83-> x.x.x.35: Protocol=UDP Port 137->137)
Mar 28 17:32:25.288  347 Possible Port Scan detected on Interface  x.x.x.38 (207.94.123.83-> x.x.x.35: Protocol=UDP Port 137->137)
Mar 28 17:32:25.397  347 Possible Port Scan detected on Interface  x.x.x.38 (207.94.123.83-> x.x.x.35: Protocol=UDP Port 137->137)
Mar 28 17:32:25.399  347 Possible Port Scan detected on Interface  x.x.x.38 (192.168.2.28-> x.x.x.35: Protocol=UDP Port 137->137)
Mar 28 17:32:25.722  347 Possible Port Scan detected on Interface  x.x.x.38 (192.168.2.28-> x.x.x.35: Protocol=UDP Port 137->137)
Mar 28 17:32:25.731  347 Possible Port Scan detected on Interface  x.x.x.38 (207.94.123.83-> x.x.x.35: Protocol=UDP Port 137->137)
Mar 28 17:32:26.135  347 Possible Port Scan detected on Interface  x.x.x.38 (207.94.123.83-> x.x.x.35: Protocol=UDP Port 137->137)
Mar 28 17:32:26.242  347 Possible Port Scan detected on Interface  x.x.x.38 (207.94.123.83-> x.x.x.35: Protocol=UDP Port 137->137)
Mar 28 17:32:26.247  347 Possible Port Scan detected on Interface  x.x.x.38 (192.168.2.28-> x.x.x.35: Protocol=UDP Port 137->137)
Mar 28 17:32:26.559  347 Possible Port Scan detected on Interface  x.x.x.38 (192.168.2.28-> x.x.x.35: Protocol=UDP Port 137->137)
Mar 28 17:32:26.567  347 Possible Port Scan detected on Interface  x.x.x.38 (207.94.123.83-> x.x.x.35: Protocol=UDP Port 137->137)
Mar 28 17:32:26.997  347 Possible Port Scan detected on Interface  x.x.x.38 (207.94.123.83-> x.x.x.35: Protocol=UDP Port 137->137)
```

```
Mar 28 17:32:27.106  347 Possible Port Scan detected on Interface  x.x.x.38 (207.94.123.83-> x.x.x.35: Protocol=UDP Port 137->137)
Mar 28 17:32:27.109  347 Possible Port Scan detected on Interface  x.x.x.38 (192.168.2.28-> x.x.x.35: Protocol=UDP Port 137->137)
Mar 28 17:32:27.396  347 Possible Port Scan detected on Interface  x.x.x.38 (192.168.2.28-> x.x.x.35: Protocol=UDP Port 137->137)
Mar 28 17:32:27.402  347 Possible Port Scan detected on Interface  x.x.x.38 (207.94.123.83-> x.x.x.35: Protocol=UDP Port 137->137)
Mar 28 17:32:28.072  347 Possible Port Scan detected on Interface  x.x.x.38 (207.94.123.83-> x.x.x.35: Protocol=UDP Port 137->137)
Mar 28 17:32:28.837  347 Possible Port Scan detected on Interface  x.x.x.38 (192.168.2.28-> x.x.x.35: Protocol=UDP Port 137->137)
Mar 28 17:32:29.193  347 Possible Port Scan detected on Interface  x.x.x.38 (207.94.123.83-> x.x.x.35: Protocol=UDP Port 137->137)
Mar 28 17:32:29.212  347 Possible Port Scan detected on Interface  x.x.x.38 (192.168.2.28-> x.x.x.35: Protocol=UDP Port 137->137)
Mar 28 17:32:30.235  347 Possible Port Scan detected on Interface  x.x.x.38 (192.168.2.28-> x.x.x.35: Protocol=UDP Port 137->137)
Mar 28 17:32:30.245  347 Possible Port Scan detected on Interface  x.x.x.38 (207.94.123.83-> x.x.x.35: Protocol=UDP Port 137->137)
Mar 28 17:32:30.608  347 Possible Port Scan detected on Interface  x.x.x.38 (207.94.123.83-> x.x.x.35: Protocol=UDP Port 137->137)
Mar 28 17:32:30.613  347 Possible Port Scan detected on Interface  x.x.x.38 (207.94.123.83-> x.x.x.36: Protocol=UDP Port 137->137)
Mar 28 17:32:30.714  347 Possible Port Scan detected on Interface  x.x.x.38 (207.94.123.83-> x.x.x.35: Protocol=UDP Port 137->137)
Mar 28 17:32:30.718  347 Possible Port Scan detected on Interface  x.x.x.38 (192.168.2.28-> x.x.x.35: Protocol=UDP Port 137->137)
Mar 28 17:32:31.011  347 Possible Port Scan detected on Interface  x.x.x.38 (192.168.2.28-> x.x.x.35: Protocol=UDP Port 137->137)
```

same pattern repeated for all hosts in this subnet. The messages below marked the end of this detect.

```
Mar 28 17:37:05.197  347 Possible Port Scan detected on Interface  x.x.x.38 (207.94.123.83-> x.x.x.54: Protocol=UDP Port 137->137)
Mar 28 17:37:05.692  347 Possible Port Scan detected on Interface  x.x.x.38 (192.168.2.28-> x.x.x.54: Protocol=UDP Port 137->137)
Mar 28 17:37:06.512  347 Possible Port Scan detected on Interface  x.x.x.38 (192.168.2.28-> x.x.x.54: Protocol=UDP Port 137->137)
Mar 28 17:37:07.207  347 Possible Port Scan detected on Interface  x.x.x.38 (192.168.2.28-> x.x.x.54: Protocol=UDP Port 137->137)
Mar 28 17:37:07.339  347 Possible Port Scan detected on Interface  x.x.x.38 (207.94.123.83-> x.x.x.54: Protocol=UDP Port 137->137)
```

ANALYSIS:

Evidence of Active Targeting?

Yes. The traffic from the source is detected at the firewall's interface.

Identify the History?

No previous traffic from the source address could be found in the archives. Other detects with a similar pattern (i.e., UDP 137->137) were noted in the firewall logs. However, the other detects were from one source address and were of short duration.

Identify the Technique?

Repeated Windows "Nbtstat" commands directed at our subnet would cause this detect. The firewall logs note any hits on addresses for which it protects. The detect traffic had both source and destination ports of 137/UDP. In "similar" scans I found on our firewall, one source sent three frames to each host, then the traffic ended from that source. (This is probably a single nbtstat directed at our subnet.) This detect not only sent many frames to our subnet, but also used decoy scanning with a spoofed source address (192.168.2.28). Note that packets with both the valid address and spoofed address were sent together within the same second. The correlation in times points to a single host sending multiple packets. There are some occurrences of a packet with one of the addresses being sent alone. The detect consisted of 1726 frames being sent in 290 seconds. That is about 6 frames/second being directed at the firewall for almost 5 minutes.

Evidence of Intent?

This detect has the look of a host scan. The use of decoy scanning may have been an attempt to fool an IDS or the analyst! However, the use of a reserved address (i.e. 192.168.x.x) makes the real address pretty obvious and it would have been more effective if they included additional decoys. It is tempting to interpret this detect as a type of WINS denial of service. The rate and length of time the frames were sent seems to makes

the denial observation valid. However, the use of a true IP address, the use of a decoy address, and random host targeting makes me lean more to a scan.

I would have to say, then, that this is a **host scan** looking for netbios information for possible use in an exploit. I do believe the person was probably experimenting with a Nbtstat scan script of some sort due to the presence of the decoy address and the duration of the scan. They may even have had a denial of service in mind! (One note, though, is the bandwidth on our subnet was indeed impacted for these five minutes!) Any further detects from this source would greatly enhance the interpretation that this detect and any other detects from this source might be attempts at some sort of denial attack.

Identify Hostile Individuals and Groups?

Research into the source shows a system using Netcom as its ISP. The valid address resolves to "dal-tx8-19.ix.netcom.com". This machine responds reliably to a ping. This makes me believe this a "constant connect" type of workstation as opposed to a modem. This detect appears to be the work of a single machine rather than a group. No more traffic has been observed from this workstation; therefore, I take that this detect was a single incident and not part of an organized scheme towards our subnet. In making this observation, though, I have no way to know if our subnet was singly targeted or the detect was a subset of a footprint against a larger class subnet than the one assigned to our company.

Severity: -2

Criticality: I note this to be a 5 since all of our "internet" servers as well as our firewall was targeted and these are Windows NT systems.
Lethality: This is a 2 since we have hardened against 137/UDP and the no specific target was seen.
Countermeasures: This is a 5 for us since all of "internet" servers are fully patched and hardened and reside in a service network behind our firewall. None are in the DMZ.
Net Countermeasures: Since we do have some modem and ISDN accesses, this is rated at a 4.

Detect 5 Liberty's firewall logs 3/24/2000 First three octets of our host addresses changed to x.x.x

```
Mar 24 20:34:27.684  226 IP  packet dropped (213.176.0.133->x.x.x.35: Protocol=TCP[SYN] Port 109->109): Restricted Port: Protocol=TCP[SYN] Port 109->109 (received on interface x.x.x.38)
Mar 24 20:34:27.704  226 IP  packet dropped (213.176.0.133->x.x.x.35: Protocol=TCP[SYN] Port 110->110): Restricted Port: Protocol=TCP[SYN] Port 110->110 (received on interface x.x.x.38)
Mar 24 20:34:27.726  226 IP  packet dropped (213.176.0.133->x.x.x.36: Protocol=TCP[SYN] Port 109->109): Restricted Port: Protocol=TCP[SYN] Port 109->109 (received on interface x.x.x.38)
Mar 24 20:34:27.743  226 IP  packet dropped (213.176.0.133->x.x.x.36: Protocol=TCP[SYN] Port 110->110): Restricted Port: Protocol=TCP[SYN] Port 110->110 (received on interface x.x.x.38)
Mar 24 20:34:27.804  226 IP  packet dropped (213.176.0.133->x.x.x.38: Protocol=TCP[SYN] Port 109->109): Restricted Port: Protocol=TCP[SYN] Port 109->109 (received on interface x.x.x.38)
Mar 24 20:34:27.824  226 IP  packet dropped (213.176.0.133->x.x.x.38: Protocol=TCP[SYN] Port 110->110): Restricted Port: Protocol=TCP[SYN] Port 110->110 (received on interface x.x.x.38)
Mar 24 20:34:27.846  226 IP  packet dropped (213.176.0.133->x.x.x.39: Protocol=TCP[SYN] Port 109->109): Restricted Port: Protocol=TCP[SYN] Port 109->109 (received on interface x.x.x.38)
Mar 24 20:34:27.864  226 IP  packet dropped (213.176.0.133->x.x.x.39: Protocol=TCP[SYN] Port 110->110): Restricted Port: Protocol=TCP[SYN] Port 110->110 (received on interface x.x.x.38)
Mar 24 20:34:28.445  226 IP  packet dropped (213.176.0.133->x.x.x.54: Protocol=TCP[SYN] Port 109->109): Restricted Port: Protocol=TCP[SYN] Port 109->109 (received on interface x.x.x.38)
Mar 24 20:34:28.463  226 IP  packet dropped (213.176.0.133->x.x.x.54: Protocol=TCP[SYN] Port 110->110): Restricted Port: Protocol=TCP[SYN] Port 110->110 (received on interface x.x.x.38)
```

ANALYSIS:

Evidence of Active Targeting?

Yes. The traffic from the source is detected at the firewall's interface.

Identify the History?

No previous traffic from the source address could be found in the archives.

Identify the Technique?

TCP SYN packets were directed at our subnet. The SYN packets were directed at POP-2 and POP-3 ports on our hosts and hoping for a SYN-ACK return. The packets arrived at predictable uniform times and occurred over a short duration. These hosts are not on the DMZ but are located in a service network behind our firewall. There does not appear to be any previous knowledge of our active hosts. None of our hosts have ports 109 or 110 active and neither does the firewall pass traffic on these ports. The source address is active on the internet and does not appear to have been spoofed.

Evidence of Intent?

This detect is a **host scan** of either our subnet or a larger subnet that includes our Class assignments. It is probably looking to exploit POP vulnerabilities; however, the Promail trojan resides on 110/TCP. So trojan scanning could also be behind this scan as well.

Identify Hostile Individuals and Groups?

The disturbing aspect of this detect is the source address. Through Whois, I found the address belonging to irost.com. I tried to access www.irost.com and was successful. This domain, according to their website, is *affiliated with the Ministry of Culture and Higher Education of Iran, and has become one of the most important governmental research center in Iran.*

There is an active workstation at the source address that can be reliably ping'd. Since we do not use POP ports and the scan found no vulnerabilities, this detect can be de-emphasized. However, detects from this domain (and/or this source) will definitely be logged and studied!

Severity: -2

Criticality: I note this to be a 5 since all of our "internet" servers as well as our firewall was targeted.
Lethality: This is a 2 since we have hardened against 109/TCP and 110/TCP and the no specific target was seen.
Countermeasures: This is a 5 for us since all of "internet" servers are fully patched and hardened and reside in a service network behind our firewall. None are in the DMZ.
Net Countermeasures: Since we do have some modem and ISDN accesses, this is rated at a 4.

Detect 6 http://www.sans.org/y2k/032700.htm

```
Mar 28 00:16:09.225 firewall kernel: 226 IP packet dropped (24.66.81.36->firewall.mydomain.edu[10.0.0.1]: Protocol=TCP[SYN] Port 2357->27374):
Restricted Port: Protocol=TCP[SYN] Port 2357->27374 (received on interface 10.0.0.1)
Mar 28 00:16:09.226 firewall kernel: 226 IP packet dropped (24.66.81.36->firewall.mydomain.edu[10.0.0.1]: Protocol=TCP[SYN] Port 2357->27374):
Restricted Port: Protocol=TCP[SYN] Port 2357->27374 (received on interface 10.0.0.1) [1 duplicates suppressed]
```

ANALYSIS:

Evidence of Active Targeting?

Yes. The traffic from the source is detected at the firewall's interface.

Identify the History?

No previous history was noted in the detect report.

Identify the Technique?

TCP SYN packets were directed at a single host, the firewall. The SYN packets were directed at a particular port (27374/TCP) on the firewall and hoping for a SYN-ACK return. The packets arrived at predictable uniform times and occurred over a short duration. Note that the source port (2357/TCP) is the same in both packets. I presume other hosts were not targeted since the same "packet dropped" messages would appear for them in the log. (I also presume that the analyst did not delete other messages related to this incident). Presuming that other hosts were not traced, there does appear to be some previous knowledge of the network, namely the detect was targeted at the firewall. The source address is active on the internet and does not appear to have been spoofed.

Evidence of Intent?

This detect is an **attempt to connect to a dangerous port**, port 27374. The Sub-7 trojan listens on this port; however, it is usually on UDP port 27374. This is not to say that this trojan has mutated and also listens on TCP 27374. Conversely, this person may not know the difference and is simply running a canned script looking for this port. The hardwired source port further supports the use of a canned script. In any matter, this should not be considered a friendly detect.

Identify Hostile Individuals and Groups?

Based on Whois, this is an @home user in Calgary, Canada. This strengthens the idea that mischief is behind this detect. The time of midnight should be compared to Calgary. If it translates to late night, this would raise further suspicions for a home hacker. Further detects from this source would warrant a stronger investigation.

Severity: -3

Criticality: I note this to be a 5 since the firewall was targeted.
Lethality: This is a 1 since the firewall appears to be hardened for this and the attempt will likely fail.
Countermeasures: This is a 5 assuming that the firewall is fully patched.
Net Countermeasures: Presuming there are some modem and ISDN accesses, this is rated at a 4.

Detect 7 http://www.sans.org/y2k/032600-2000.htm

```
A friend of mine sent me this. SN suggested I pass it to GIAC. (I've sanitized it, obviously.) Any ideas?
- A.
-----------------------------------------------------
Do you know of any good exploitz that people are probing nntp for?

Mar 22 13:23:36 box.at.victim.com /ipmon[4872]: 13:23:36.638478 le0 @0:19 b 24.0.94.130,38945 -> IP.OF.VICTIM.COM,119 PR tcp len 20 44 -S
Mar 22 13:23:37 box.at.victim.com /ipmon[4872]: 13:23:37.315117 le0 @0:19 b 24.0.94.130,38945 -> IP.OF.VICTIM.COM,119 PR tcp len 20 40 -R
```

```
Mar 22 13:23:37 box.at.victim.com /ipmon[4872]: 13:23:37.326922 le0 @0:19 b 24.0.94.130,39317 -> IP.OF.VICTIM.COM,119 PR tcp len 20 44 -S
Mar 22 13:23:38 box.at.victim.com /ipmon[4872]: 13:23:38.312697 le0 @0:19 b 24.0.94.130,39317 -> IP.OF.VICTIM.COM,119 PR tcp len 20 40 -R
Mar 22 18:04:02 box.at.victim.com /ipmon[4872]: 18:04:01.661131 le0 @0:19 b 24.0.94.130,59273 -> IP.OF.VICTIM.COM,119 PR tcp len 20 44 -S
Mar 22 18:04:03 box.at.victim.com /ipmon[4872]: 18:04:03.188819 le0 @0:19 b 24.0.94.130,59273 -> IP.OF.VICTIM.COM,119 PR tcp len 20 40 -R
Mar 22 18:04:03 box.at.victim.com /ipmon[4872]: 18:04:03.210320 le0 @0:19 b 24.0.94.130,60187 -> IP.OF.VICTIM.COM,119 PR tcp len 20 44 -S
Mar 22 18:04:04 box.at.victim.com /ipmon[4872]: 18:04:03.811455 le0 @0:19 b 24.0.94.130,60187 -> IP.OF.VICTIM.COM,119 PR tcp len 20 40 -R
Mar 22 22:48:17 box.at.victim.com /ipmon[4872]: 22:48:16.835881 le0 @0:19 b 24.0.94.130,50230 -> IP.OF.VICTIM.COM,119 PR tcp len 20 44 -S
Mar 22 22:48:18 box.at.victim.com /ipmon[4872]: 22:48:18.161571 le0 @0:19 b 24.0.94.130,50230 -> IP.OF.VICTIM.COM,119 PR tcp len 20 40 -R
Mar 22 22:48:18 box.at.victim.com /ipmon[4872]: 22:48:18.173064 le0 @0:19 b 24.0.94.130,50678 -> IP.OF.VICTIM.COM,119 PR tcp len 20 44 -S
Mar 22 22:48:19 box.at.victim.com /ipmon[4872]: 22:48:18.986828 le0 @0:19 b 24.0.94.130,50678 -> IP.OF.VICTIM.COM,119 PR tcp len 20 40 -R
Mar 23 03:20:08 box.at.victim.com /ipmon[4872]: 03:20:07.585219 le0 @0:19 b 24.0.94.130,62610 -> IP.OF.VICTIM.COM,119 PR tcp len 20 44 -S
Mar 23 03:20:08 box.at.victim.com /ipmon[4872]: 03:20:08.045238 le0 @0:19 b 24.0.94.130,62610 -> IP.OF.VICTIM.COM,119 PR tcp len 20 40 -R
Mar 23 03:20:08 box.at.victim.com /ipmon[4872]: 03:20:08.056194 le0 @0:19 b 24.0.94.130,62931 -> IP.OF.VICTIM.COM,119 PR tcp len 20 44 -S
Mar 23 03:20:09 box.at.victim.com /ipmon[4872]: 03:20:08.858156 le0 @0:19 b 24.0.94.130,62931 -> IP.OF.VICTIM.COM,119 PR tcp len 20 40 -R
Mar 23 07:46:43 box.at.victim.com /ipmon[4872]: 07:46:42.379020 le0 @0:19 b 24.0.94.130,61302 -> IP.OF.VICTIM.COM,119 PR tcp len 20 44 -S
Mar 23 07:46:44 box.at.victim.com /ipmon[4872]: 07:46:43.418154 le0 @0:19 b 24.0.94.130,61302 -> IP.OF.VICTIM.COM,119 PR tcp len 20 40 -R
Mar 23 07:46:44 box.at.victim.com /ipmon[4872]: 07:46:43.442809 le0 @0:19 b 24.0.94.130,62218 -> IP.OF.VICTIM.COM,119 PR tcp len 20 44 -S
Mar 23 07:46:44 box.at.victim.com /ipmon[4872]: 07:46:44.091157 le0 @0:19 b 24.0.94.130,62218 -> IP.OF.VICTIM.COM,119 PR tcp len 20 40 -R
```

ANALYSIS:

Evidence of Active Targeting?

Yes. The traffic from the source is detected at the host's interface.

Identify the History?

No previous traffic from the source address was noted in the detect report.

Identify the Technique?

TCP SYN packets were directed at a specific host. The SYN packets were directed at TCP port 119. If the port were open, a SYN-ACK would be returned. If the port is closed, a RES is returned. (I'm presuming that the trace is logging incoming traffic only and believe the time difference between SYN and RES supports this.) It is presumed that the victim is returning a SYN-ACK with the scanner host immediately tearing down the connection with a RES packet. This detect, then, has strong characteristics of a port scan using an incomplete three way handshake. The port scan is conducted in short bursts over a number of hours. This is probably an attempt to not trigger an IDS filter. The source address is active on the internet and does not appear to have been spoofed.

.

Evidence of Intent?

This detect is an **attempt to connect to a dangerous port**, port 119. Although this port is associated with NNTP (which is not exactly dangerous), this port is also used by a the Happy99 trojan. I found the following on this: *This trojan does not do actual harm, but when installed, it replaces the winsock DLL (used for TCP/IP communication). Each time the user sends e-mail or posts a newsgroup article (or does any other activity on port 25 or **119**), the trojan sends copies of itself by e-mail and to newsgroups*. A scan to this port could be an indication of trouble. The analyst needs to check the victim for evidence of this trojan.

Identify Hostile Individuals and Groups?

Based on Whois, this is an @home user in California. This might strengthen the idea that mischief is behind this detect; however, the host resolves to: authorized-scan.security.home.net! This appears to be a scan host on this domain that may be looking for vulnerabilities on hosts connected to its network. Before taking

that as fact, the analyst should contact the @home domain responsible in Redwood City, CA. Presuming this is legitimate, this detect looks like **friendly fire**!

Severity: -6
Criticality: I note this to be a 3 presuming this is not a critical server.
Lethality: This is a 0 since this looks like friendly fire.
Countermeasures: This is a 5 assuming that the OS is fully patched.
Net Countermeasures: Presuming there are some modem and ISDN accesses, this is rated at a 4.

Detect 8 http://www.sans.org/y2k/032500.htm

Again, from an @home user…

```
Mar 24 01:54:58 cc1014244-a kernel: securityalert: tcp if=ef0 from 24.3.57.38:11111 to 24.3.21.199 on unserved port 12345
Mar 24 03:14:13 cc1014244-a kernel: securityalert: tcp if=ef0 from 171.214.113.228:2766 to 24.3.21.199 on unserved port 1243
Mar 24 04:45:01 cc1014244-a kernel: securityalert: tcp if=ef0 from 208.61.109.243:3578 to 24.3.21.199 on unserved port 1243
Mar 24 04:45:06 cc1014244-a kernel: securityalert: tcp if=ef0 from 208.61.109.243:3832 to 24.3.21.199 on unserved port 27347
Mar 24 05:40:42 cc1014244-a kernel: securityalert: udp if=ef0 from 24.24.100.172:2147 to 24.3.21.199 on unserved port 137
Mar 24 14:56:08 cc1014244-a kernel: securityalert: udp if=ef0 from 63.17.79.40:4294 to 24.3.21.199 on unserved port 137
Mar 24 17:20:44 cc1014244-a kernel: securityalert: tcp if=ef0 from 62.6.100.45:1828 to 24.3.21.199 on unserved port 27374
Mar 24 20:50:47 cc1014244-a kernel: securityalert: tcp if=ef0 from 194.27.62.179:4857 to 24.3.21.199 on unserved port 27374
```

ANALYSIS:

Evidence of Active Targeting?
Yes. The traffic from the source is detected at the host's interface.

Identify the History?
No previous traffic from the source address was noted in the detect report.

Identify the Technique?
TCP and UDP packets were directed at a specific host. The SYN packets were directed at TCP ports 12345, 1243, 27347, and 27374. The UDP traffic was directed at UDP port 137. The sources are hoping for a SYN-ACK or nor response in the case of UDP. The port scan is coming from different sources over a number of hours. All of the source address are active on the internet and do not appear to have been spoofed.

Evidence of Intent?
This detect is a port scan of the victim looking for various vulnerabilities. These can be summarized as:

Port 12345	Netbus and Ultor's trojan
Port 1243	Subseven and Backdoor-G trojans
Port 27374	Subseven 2.0 (albeit 27374/UDP?)
Port 27347	(Probably typing error for port 27347)
Port 137	Netbios

The analyst needs to check the victim for evidence of trojans and ensure that netbios is not a problem.

Identify Hostile Individuals and Groups?

Based on Whois, these source addresses came from various locales. They appear to be unrelated both in geography and time. However, the last address is of a little more concern as it originates in Turkey. These scans appear to be hostile but the victim seems to be rebuffing the scans.

Severity: 1

Criticality: I note this to be a 2 presuming this is not a critical server.
Lethality: This is a 4 since these exploits can be damaging.
Countermeasures: This is a 5 assuming that the OS is fully patched.
Net Countermeasures: There doesn't seem to be a firewall so this is a 0.

Detect 9 Liberty's firewall logs 3/28/2000 First three octets of our host addresses changed to x.x.x

Note: Host x.x.x.37 was on-line as a standalone Windows NT test machine.

```
Mar 28 11:41:13.898 226 IP  packet dropped (208.5.163.131->x.x.x.36: Protocol=TCP[SYN] Port 4551->98): Restricted Port: Protocol=TCP[SYN] Port 4551-
>98 (received on interface x.x.x.38)
Mar 28 11:41:13.923 226 IP  packet dropped (208.5.163.131->x.x.x.38: Protocol=TCP[SYN] Port 4553->98): Restricted Port: Protocol=TCP[SYN] Port 4553-
>98 (received on interface x.x.x.38)
Mar 28 11:41:13.949 226 IP  packet dropped (208.5.163.131->x.x.x.39: Protocol=TCP[SYN] Port 4554->98): Restricted Port: Protocol=TCP[SYN] Port 4554-
>98 (received on interface x.x.x.38)
```

ANALYSIS:

Evidence of Active Targeting?

Yes. The traffic from the source is detected at the firewall's interface and to specific hosts in our subnet.

Identify the History?

No previous traffic from the source address could be found in the archives.

Identify the Technique?

TCP SYN packets were directed at specific hosts on our subnet. The SYN packets were directed atTCP port 98 on our hosts and hoping for a SYN-ACK return. The packets arrived at predictable uniform times and occurred over a short duration.

All but one these hosts are located in a service network behind our firewall. The host at x.x.x.37 seemed to be scanned as well. This would be the scan packet with source port 4552. This is not in the log above because the firewall did not know about that host. It was located on the DMZ and was online at the time as a test standalone Windows NT machine. It had web services running some demo html for a third party. (The x.x.x.38 address is our firewall.)

None of our hosts have port 98 active and neither does the firewall pass traffic on these ports. The source address is active on the internet and does not appear to have been spoofed.

Evidence of Intent?

This is a targeted **host scan** of some of our hosts for port 98. TCP port 98 is noted to be for the TAC News service. This is an "old" DARPA service for TACACS. This was not the likely service being searched. TCP port 98 is the current target for the Linuxconf exploit to gain root access.

I had the question as to why some of my hosts were not targeted. My theory is they wanted to access Linux. The x.x.x.35 and x.x.x.54 hosts were not hit. These are NT web server/FTP server machines. With a simple browser hit or attempted FTP login, that would be obvious. The other hosts in our domain are not as obvious as to their operating systems. All of this would preclude prior knowledge by either browser/FTP or some type of scan. I did not find any evidence in my archives. That does not mean they did it before my last archive purge! This targeting is little puzzling and I do not have enough information to make a confident observation.

Identify Hostile Individuals and Groups?

The source is identifiable and is reliably ping'd. The workstation seems to be part of a travel agency's network in Vermont. More than likely, the perpetrator is either an employee of the travel agency or someone using their network for mischief. Based on these findings, I would not think of this person as extremely hostile or participating in a group scan of our hosts. This has been an isolated detect at this point.

Severity: -4

Criticality: I note this to be a 4 since some of our "internet" servers as well as our firewall was targeted.
Lethality: This is a 1 since we do not use Linux and so this exploit could never work.
Countermeasures: This is a 5 for us since all of "internet" servers are fully patched and hardened and reside in a service network behind our firewall. The test machine that was in the DMZ was irrelevant.
Net Countermeasures: Since we do have some modem and ISDN accesses, this is rated at a 4.

Detect 10 Liberty's firewall logs 3/29/2000 First three octets of our host addresses changed to x.x.x

```
Mar 29 12:13:51.510 226 IP  packet dropped (210.92.35.5->x.x.x.35: Protocol=TCP[SYN] Port 1337->635): Restricted Port: Protocol=TCP[SYN] Port 1337->635 (received on interface x.x.x.38)
```

ANALYSIS:

Evidence of Active Targeting?

Yes. The traffic from the source is detected at the firewall's interface.

Identify the History?

No previous traffic from the source address could be found in the archives.

Identify the Technique?

A TCP SYN packet was directed at a single host, one of our web servers. The SYN packet was directed at particular open port (635/TCP) on the server and hoping for a SYN-ACK return. The packets arrived during the lunch hour here. The source address is active on the internet and does not appear to have been spoofed.

Evidence of Intent?

This detect is an **attempt to connect to a dangerous port**, port 635. This port can expose a system to mountd and NFS exploits. Linux is apparently having some exploit issues at this time. I think this person was testing to see if our web server was running Linux and if so, see if the mountd was accessible.

Identify Hostile Individuals and Groups?

Based on Whois, this is a host in Korea. This strengthens the idea that mischief is behind this detect. The time of noon here will translate to late night in Korea. Further detects from this source would warrant a stronger investigation. It is also worth noting that only the web server was targeted. I have no evidence that any of our other hosts were targeted. They either knew our network architecture or knew of our web server. I have no other evidence of a scan by them. This should be considered a hostile scan.

Severity: -4

Criticality: I note this to be a 4 since one "internet" server was targeted and it is not a business critical system.
Lethality: This is a 1 since we have hardened against 635/TCP and we do not run Linux.
Countermeasures: This is a 5 for us since all of "internet" servers are fully patched and hardened and reside in a service network behind our firewall. None are in the DMZ.
Net Countermeasures: Since we do have some modem and ISDN accesses, this is rated at a 4.