Global Information Assurance Certification Paper

*** Northcutt, there are some really nice reads in this practical don't miss detect 2! I hadn't seen that before so the bonus gets added. The research is good on attacks and source addresses. Good use of an analysis process. Bravo! 95 *

Note: Detects are from either systems outside our corporate firewall or from systems connected to a cable modem (cable modem land is kinda scary!!!). In all cases a host-based firewall was used. Most addresses have been changed to protect the guilty/innocent. Packet dumps were read via Ethereal (http://ethereal.zing.org), an open source network protocol analyzer. I think our next step will be to implement a SHADOW system at work!

Detect #1

Time	Source	Destination	Protocol	Info		
11:16:43.6230	219.80.x.x	cablemodem.net	TCP 3516 > 21	[SYN] Seq=14937903	Ack=0 Win=8192	Len=0
11:16:59.8209	219.80.x.x	cablemodem.net	TCP 3517 > 21	[SYN] Seq=14937916	Ack=0 Win=8192	Len=0
11:16:59.8209	219.80.x.x	cablemodem.net	TCP 3518 > 21	[SYN] Seq=14937928	Ack=0 Win=8192	Len=0
11:16:59.8240	219.80.x.x	cablemodem.net	TCP 3519 > 21	[SYN] Seq=14937939	Ack=0 Win=8192	Len=0
11:16:59.8240	219.80.x.x	cablemodem.net	TCP 3516 > 21	[SYN] Seq=14937903	Ack=0 Win=8192	Len=0
11:16:59.8240	219.80.x.x	cablemodem.net	TCP 3520 > 21	[SYN] Seq=14937949	Ack=0 Win=8192	Len=0
11:16:59.8240	219.80.x.x	cablemodem.net	TCP 3517 > 21	[SYN] Seq=14937916	Ack=0 Win=8192	Len=0
11:16:59.8300	219.80.x.x	cablemodem.net	TCP 3521 > 21	[SYN] Seq=14937958	Ack=0 Win=8192	Len=0
11:16:59.8300	219.80.x.x	cablemodem.net	TCP 3518 > 21	[SYN] Seq=14937928	Ack=0 Win=8192	Len=0
11:16:59.8300	219.80.x.x	cablemodem.net	TCP 3522 > 21	[SYN] Seq=14937966	Ack=0 Win=8192	Len=0
11:16:59.8300	219.80.x.x	cablemodem.net	TCP 3519 > 21	[SYN] Seq=14937939	Ack=0 Win=8192	Len=0
11:16:59.8339	219.80.x.x	cablemodem.net	TCP 3523 > 21	[SYN] Seq=14937973	Ack=0 Win=8192	Len=0
11:16:59.8339	219.80.x.x	cablemodem.net	TCP 3520 > 21	[SYN] Seq=14937949	Ack=0 Win=8192	Len=0
11:16:59.8339	219.80.x.x	cablemodem.net	TCP 3524 > 21	[SYN] Seq=14937980	Ack=0 Win=8192	Len=0
11:16:59.8339	219.80.x.x	cablemodem.net	TCP 3521 > 21	[SYN] Seq=14937958	Ack=0 Win=8192	Len=0
11:16:59.8389	219.80.x.x	cablemodem.net	TCP 3525 > 21	[SYN] Seq=14937986	Ack=0 Win=8192	Len=0
11:16:59.8389	219.80.x.x	cablemodem.net	TCP 3522 > 21	[SYN] Seq=14937966	Ack=0 Win=8192	Len=0
11:16:59.8389	219.80.x.x	cablemodem.net	TCP 3526 > 21	[SYN] Seq=14937991	Ack=0 Win=8192	Len=0
11:16:59.8389	219.80.x.x	cablemodem.net	TCP 3523 > 21	[SYN] Seq=14937973	Ack=0 Win=8192	Len=0
11:16:59.8439	219.80.x.x	cablemodem.net	TCP 3527 > 21	[SYN] Seq=14937995	Ack=0 Win=8192	Len=0
11:16:59.8439	219.80.x.x	cablemodem.net	TCP 3516 > 21	[SYN] Seq=14937903	Ack=0 Win=8192	Len=0
11:16:59.8439	219.80.x.x	cablemodem.net	TCP 3524 > 21	[SYN] Seq=14937980	Ack=0 Win=8192	Len=0
11:16:59.8439	219.80.x.x	cablemodem.net	TCP 3528 > 21	[SYN] Seq=14937998	Ack=0 Win=8192	Len=0
11:16:59.8489	219.80.x.x	cablemodem.net	TCP 3517 > 21	[SYN] Seq=14937916	Ack=0 Win=8192	Len=0
11:16:59.8489	219.80.x.x	cablemodem.net	TCP 3525 > 21	[SYN] Seq=14937986	Ack=0 Win=8192	Len=0

History	Taken from a computer attached to a cable modem. I had not seen any previous activity from the source address. The attack lasted for several minutes.
Active Targeting?	Yes.

Criticality	2	Home computer without any critical data.
Lethality	4	DoS attack.
System Countermeasures	4	OS is up to date.
Network Countermeasures	4	Host-based firewall is installed.
Severity	-2	*Severity = (Criticality + Lethality) – (System Countermeasures + Network Countermeasures)*
Notes	Appears to be a DoS attack against port 21 (FTP) based upon the intervals and duration. The above attack lasted for several minutes. Source address belongs to an ISP.	

Detect #2

Time	Source	Destination	Protocol	Info
23:03:19.9379	206.251.4.210	cablemodem.net	UDP	Source port: 1070 Destination port: 371
09:53:45.7975	206.251.4.210	cablemodem.net	UDP	Source port: 1045 Destination port: 371
09:53:51.5325	206.251.4.210	cablemodem.net	UDP	Source port: 1031 Destination port: 371
09:54:01.8435	206.251.4.210	cablemodem.net	UDP	Source port: 1077 Destination port: 371
09:54:14.5085	206.251.4.210	cablemodem.net	UDP	Source port: 1075 Destination port: 371
09:54:23.7125	206.251.4.210	cablemodem.net	UDP	Source port: 1072 Destination port: 371
01:26:09.8009	206.251.4.210	cablemodem.net	UDP	Source port: 1055 Destination port: 371
01:26:13.1410	206.251.4.210	cablemodem.net	UDP	Source port: 1050 Destination port: 371
01:26:19.0080	206.251.4.210	cablemodem.net	UDP	Source port: 1033 Destination port: 371
01:26:29.6579	206.251.4.210	cablemodem.net	UDP	Source port: 1074 Destination port: 371
01:26:39.9379	206.251.4.210	cablemodem.net	UDP	Source port: 1031 Destination port: 371
01:26:51.1130	206.251.4.210	cablemodem.net	UDP	Source port: 1053 Destination port: 371
03:52:48.6009	206.251.4.210	cablemodem.net	UDP	Source port: 1071 Destination port: 371
03:52:51.4320	206.251.4.210	cablemodem.net	UDP	Source port: 1067 Destination port: 371
03:52:57.4079	206.251.4.210	cablemodem.net	UDP	Source port: 1067 Destination port: 371
03:53:07.0520	206.251.4.210	cablemodem.net	UDP	Source port: 1075 Destination port: 371
03:53:18.1679	206.251.4.210	cablemodem.net	UDP	Source port: 1069 Destination port: 371
03:53:29.7580	206.251.4.210	cablemodem.net	UDP	Source port: 1077 Destination port: 371
06:18:04.8079	206.251.4.210	cablemodem.net	UDP	Source port: 1060 Destination port: 371
06:18:08.1380	206.251.4.210	cablemodem.net	UDP	Source port: 1059 Destination port: 371
06:18:12.2910	206.251.4.210	cablemodem.net	UDP	Source port: 1078 Destination port: 371
06:18:22.4620	206.251.4.210	cablemodem.net	UDP	Source port: 1031 Destination port: 371
06:18:37.6380	206.251.4.210	cablemodem.net	UDP	Source port: 1060 Destination port: 371
06:18:48.6879	206.251.4.210	cablemodem.net	UDP	Source port: 1067 Destination port: 371

History	Taken from a friend's Compaq Presario attached to a cable modem. The above scans were very common and typically followed the above time and frequency pattern.
Active Targeting?	Yes.

Criticality	5	Home computer with personal/financial data on it.
Lethality	3	Not sure how to rate this one, but since system updated may be installed by this, I gave it a 3.
System Countermeasures	4	OS is up to date.
Network Countermeasures	4	Host-based firewall installed.
Severity	0	Severity = (Criticality + Lethality) – (System Countermeasures + Network Countermeasures)
Notes	After seeing the above activity I did an nslookup on 206.251.4.210, which returned Compaq as the owner. Being curious why Compaq would scan their customer's computers, I did a little research. UPD 371 is associated with either Clearcase, which is source control product from Rational Software (http://www.rational.com/products/clearcase/index.jtmpl) or Backweb (http://www.backweb.com/), which is a push based software distribution solution. A quick search of Backweb's site verified the Compaq relationship (http://www.backweb.com/html/compaq.html). On the client computer an application named *Compaq Service Connection* is automatically started upon boot up. The software allows Compaq to deliver software updates and patches automatically. I'm not sure I like that idea! In any case we configured the firewall to trust this address so the updates could be delivered.	

Detect #3

```
Time          Source       Destination       Protocol          Info
20:05:29.0659   208.x.x.x   cablemodem.net    TCP       23 > 23  [ACK] Seq=475530002 Ack=2045767734 Win=1028 Len=0
20:10:04.6150   208.x.x.x   cablemodem.net    TCP       4 > 23   [FIN, SYN] Seq=777055218 Ack=596894454 Win=1028 Len=0
20:10:04.6150   208.x.x.x   cablemodem.net    TCP       5 > 23   [PSH] Seq=777055218 Ack=596894454 Win=1028 Len=0
20:20:36.5310   00:50:80:35:f6:08     ff:ff:ff:ff:ff:ff     ARP      Who has 208.223.13.42?  Tell 208.223.13.1
```

History	Taken from a friend's computer attached to a cable modem. I was not able to dig through the logs and look for previous activity.	
Active Targeting?	Yes.	
Criticality	5	Home computer with personal/financial data on it.
Lethality	5	Probably an *sscan* probe.
System Countermeasures	4	OS is up to date.
Network Countermeasures	4	Host-based firewall installed.
Severity	2	*Severity = (Criticality + Lethality) – (System Countermeasures + Network Countermeasures)*

Notes	The first thing I noticed about the above activity was the single ACK being sent to port 23 (telnet). Several minutes later port 23 was probed again with the FIN SIN flags set from source port 4. At the same time port 23 was probed from source port 5 with the PSH flag set. This pattern is *similar* to that of an sscan probe (http://www.cert.org/incident_notes/IN-99-01.html), but the above traffic doesn't completely match the CERT Incident Note. Typically an sscan script will not continue if the first probe to port 23 fails, and several other source ports are typically used along with ports 4 & 5 in the probe. Additionally other behavior associated with sscan was not detected. With this in mind I can't be certain that this is an sscan probe. The combination of flags set may be an attempt to identify the OS running. Good thing the firewall was installed! I traced this back to a shipping company in California. Their technical contact did not respond to my emails and voicemails concerning this activity.

Detect #4

Time	Source	Destination	Protocol	Info
02:32:14.3108	my.lan.com	4.2.74.139	ICMP	Destination unreachable
02:32:14.3108	my.lan.com	4.2.74.139	ICMP	Destination unreachable
02:32:14.3108	my.lan.com	4.2.74.139	ICMP	Destination unreachable
02:32:14.3108	my.lan.com	4.2.74.139	ICMP	Destination unreachable
02:32:14.3208	my.lan.com	4.2.74.139	ICMP	Destination unreachable
02:32:14.3309	my.lan.com	4.2.74.139	ICMP	Destination unreachable
02:32:14.4610	my.lan.com	4.2.74.139	ICMP	Destination unreachable
02:32:14.4610	my.lan.com	4.2.74.139	ICMP	Destination unreachable
02:32:14.4610	my.lan.com	4.2.74.139	ICMP	Destination unreachable
02:32:14.4711	my.lan.com	4.2.74.139	ICMP	Destination unreachable
02:32:14.4811	my.lan.com	4.2.74.139	ICMP	Destination unreachable
02:32:14.6213	my.lan.com	4.2.74.139	ICMP	Destination unreachable
02:32:14.6213	my.lan.com	4.2.74.139	ICMP	Destination unreachable
02:32:14.6213	my.lan.com	4.2.74.139	ICMP	Destination unreachable
02:32:14.6613	my.lan.com	4.2.74.139	ICMP	Destination unreachable
02:32:14.6613	my.lan.com	4.2.74.139	ICMP	Destination unreachable
02:32:14.6613	my.lan.com	4.2.74.139	ICMP	Destination unreachable
02:32:14.7615	my.lan.com	4.2.74.139	ICMP	Destination unreachable
02:32:14.7615	my.lan.com	4.2.74.139	ICMP	Destination unreachable
02:32:14.8917	my.lan.com	4.2.74.139	ICMP	Destination unreachable

History	None.	
Active Targeting?	Unknown.	
Criticality	3	My workstation.
Lethality	2	Low.

System Countermeasures	4	OS is up to date.
Network Countermeasures	4	Host-based firewall.
Severity	-3	*Severity = (Criticality + Lethality) – (System Countermeasures + Network Countermeasures)*
Notes	I was using trying out a web based telephony service called Dialpad (http://www.dialpad.com/) when the above activity was logged. Moments after this activity came in, the audio portion of Dialpad quit working. At first I thought someone was using spoofed addresses for a DoS attack. Upon further investigation the destination address was valid (fa0.ewaldc-egw46.bbnplanet.net). I did a whois and got the contact information for the destination address and called. After getting transferred to several different people, the individual I finally spoke with indicated that they have been getting similar reports from other sites. She also suggested I turn off my firewall in order to use the Dialpad service!	

Detect #5

```
Time            Source          Destination          Protocol Info
16:11:07.4370   cablemodem.net   my.cablemodem.net    TCP      1313 > 1 [SYN] Seq=8345199 Ack=0 Win=8192 Len=0
16:11:07.4400   cablemodem.net   my.cablemodem.net    TCP      1314 > 2 [SYN] Seq=8345207 Ack=0 Win=8192 Len=0
16:11:07.4400   cablemodem.net   my.cablemodem.net    TCP      1315 > 3 [SYN] Seq=8345221 Ack=0 Win=8192 Len=0
16:11:07.4400   cablemodem.net   my.cablemodem.net    TCP      1316 > 4 [SYN] Seq=8345225 Ack=0 Win=8192 Len=0
16:11:07.4400   cablemodem.net   my.cablemodem.net    TCP      1317 > 5 [SYN] Seq=8345235 Ack=0 Win=8192 Len=0
16:11:07.4400   cablemodem.net   my.cablemodem.net    TCP      1318 > 6 [SYN] Seq=8345236 Ack=0 Win=8192 Len=0
16:11:07.4400   cablemodem.net   my.cablemodem.net    TCP      1319 > 7 [SYN] Seq=8345243 Ack=0 Win=8192 Len=0
16:11:07.4400   cablemodem.net   my.cablemodem.net    TCP      1320 > 8 [SYN] Seq=8345256 Ack=0 Win=8192 Len=0
16:11:07.4400   cablemodem.net   my.cablemodem.net    TCP      1321 > 9 [SYN] Seq=8345259 Ack=0 Win=8192 Len=0
16:11:07.4400   cablemodem.net   my.cablemodem.net    TCP      1322 > 10 [SYN] Seq=8345268 Ack=0 Win=8192 Len=0
16:11:07.4400   cablemodem.net   my.cablemodem.net    TCP      1323 > 11 [SYN] Seq=8473268 Ack=0 Win=8192 Len=0
16:11:07.4400   cablemodem.net   my.cablemodem.net    TCP      1324 > 12 [SYN] Seq=8473274 Ack=0 Win=8192 Len=0
16:11:07.4400   cablemodem.net   my.cablemodem.net    TCP      1325 > 13 [SYN] Seq=8473286 Ack=0 Win=8192 Len=0
16:11:07.4400   cablemodem.net   my.cablemodem.net    TCP      1326 > 14 [SYN] Seq=8473288 Ack=0 Win=8192 Len=0
16:11:07.4400   cablemodem.net   my.cablemodem.net    TCP      1327 > 15 [SYN] Seq=8473296 Ack=0 Win=8192 Len=0
16:11:07.4400   cablemodem.net   my.cablemodem.net    TCP      1328 > 16 [SYN] Seq=8473311 Ack=0 Win=8192 Len=0
16:11:07.4400   cablemodem.net   my.cablemodem.net    TCP      1329 > 17 [SYN] Seq=8473316 Ack=0 Win=8192 Len=0
16:11:07.4400   cablemodem.net   my.cablemodem.net    TCP      1330 > 18 [SYN] Seq=8473327 Ack=0 Win=8192 Len=0
16:11:07.4400   cablemodem.net   my.cablemodem.net    TCP      1331 > 19 [SYN] Seq=8473328 Ack=0 Win=8192 Len=0
16:11:07.4400   cablemodem.net   my.cablemodem.net    TCP      1332 > 20 [SYN] Seq=8473336 Ack=0 Win=8192 Len=0
```

History	No previous history from this particular source address.	
Active Targeting?	Yes.	
Criticality	2	My home computer without any critical data.

Lethality	5	Very deliberate port scan.
System Countermeasures	4	Os is up to date.
Network Countermeasures	4	Host-based firewall.
Severity	-1	*Severity = (Criticality + Lethality) – (System Countermeasures + Network Countermeasures)*
Notes	This type of port mapping is pretty common on the cable modem network I subscribe to. Due to the fact that the source address is from the same cable modem network I'm on along with the speed of the scan and the time of day, I suspect this is a local kid running a script to map neighboring computers. They certainly are not worried about setting off an IDS (note the speed and consecutive nature of the scan)! I usually see this type of activity after 3PM and on weekends, hence my suspicion that kids are playing around.	

Detect #6

```
Time            Source          Destination     Protocol Info
18:09:51.1369   dialup.net      my.lan.com      TCP      4250 > 53 [SYN] Seq=1682342 Ack=0 Win=8192 Len=0
18:09:51.1419   dialup.net      my.lan.com      TCP      4250 > 53 [SYN] Seq=1682342 Ack=0 Win=8192 Len=0
18:09:51.1419   dialup.net      my.lan.com      TCP      4250 > 53 [SYN] Seq=1682342 Ack=0 Win=8192 Len=0
18:09:51.1449   dialup.net      my.lan.com      TCP      4250 > 53 [SYN] Seq=1682342 Ack=0 Win=8192 Len=0
```

History	From a workstation in our DMZ. Several times a month we see this activity. The source is an IP block assigned to an ISP.	
Active Targeting?	Not Sure.	
Criticality	3	Workstations.
Lethality	2	These computers are not running DNS.
System Countermeasures	4	All computers are up to date with patches.
Network Countermeasures	4	Host-based firewalls are installed.
Severity	-3	*Severity = (Criticality + Lethality) – (System Countermeasures + Network Countermeasures)*
Notes	DNS probe. The source addresses are from a local dialup ISP. Due to the source and the randomness of the probe, I suspect this is a misconfigured computer. Unfortunately I can't rule out Back Orifice since some hackers will search for it on TCP 53. Fortunately our anti-virus software detects Back Orifice and would neutralize the problem.	

Detect #7

```
Time            Source          Destination     Protocol Info
07:12:15.2369   dialup.ISP.net  my.lan.com      TCP      4370 > 37 [SYN] Seq=1682682 Ack=0 Win=8192 Len=0
07:12:15.2400   dialup.ISP.net  my.lan.com      TCP      4371 > 13 [SYN] Seq=1682694 Ack=0 Win=8192 Len=0
07:12:15.2400   dialup.ISP.net  my.lan.com      TCP      4371 > 13 [SYN] Seq=1682694 Ack=0 Win=8192 Len=0
07:13:27.1469   dialup.ISP.net  my.lan.com      NTP      NTP
07:13:27.1469   dialup.ISP.net  my.lan.com      TCP      4371 > 13 [SYN] Seq=1682694 Ack=0 Win=8192 Len=0
07:13:27.1499   dialup.ISP.net  my.lan.com      TCP      4371 > 13 [SYN] Seq=1682694 Ack=0 Win=8192 Len=0
07:13:27.1499   dialup.ISP.net  my.lan.com      TCP      4373 > 37 [SYN] Seq=1682713 Ack=0 Win=8192 Len=0
07:13:27.1499   dialup.ISP.net  my.lan.com      TCP      4373 > 37 [SYN] Seq=1682713 Ack=0 Win=8192 Len=0
07:13:27.1549   dialup.ISP.net  my.lan.com      TCP      4373 > 37 [SYN] Seq=1682713 Ack=0 Win=8192 Len=0
07:13:27.1549   dialup.ISP.net  my.lan.com      TCP      4373 > 37 [SYN] Seq=1682713 Ack=0 Win=8192 Len=0
07:13:39.6119   dialup.ISP.net  my.lan.com      NTP      NTP
```

History	Taken from a computer in the DMZ. We see this type of activity 2-3 times a month but from different source addresses.	
Active Targeting?	Yes.	
Criticality	5	Web server.
Lethality	3	Recon.
System Countermeasures	4	OS is up to date with patches.
Network Countermeasures	4	Host-based firewall.
Severity	0	*Severity = (Criticality + Lethality) – (System Countermeasures + Network Countermeasures)*
Notes	This may be either network mapping or OS fingerprinting. Source IP address comes from an IP block belonging to a dialup ISP. TCP 13 is the *daytime* protocol (http://www.cis.ohio-state.edu/htbin/rfc/rfc867.html) and TCP 37 is the *time* protocol (http://www.cis.ohio-state.edu/htbin/rfc/rfc738.html). My suspicion is OS fingerprinting.	

Detect #8

Time	Source	Destination	Protocol	Info
00:49:31.6608	hacker.com	my.lan.com	ICMP	Echo (ping) request
00:49:31.6608	my.lan.com	hacker.com	ICMP	Echo (ping) reply
00:49:31.6608	hacker.com	my.lan.com	TCP	256 > 257 [ACK] Seq=286331153 Ack=572662306 Win=4096 Len=12
00:49:31.6608	hacker.com	my.lan.com	IP	Fragmented IP protocol (proto=TCP 0x06, off=4)
00:49:31.6608	my.lan.com	hacker.com	TCP	257 > 256 [RST] Seq=572662306 Ack=572662306 Win=0 Len=0
00:49:31.6608	hacker.com	my.lan.com	IP	Fragmented IP protocol (proto=TCP 0x06, off=32)
00:49:31.6608	hacker.com	my.lan.com	IP	Fragmented IP protocol (proto=TCP 0x06, off=64)
00:49:31.6608	hacker.com	my.lan.com	TCP	256 > 257 [ACK] Seq=286331153 Ack=572662306 Win=4096 Len=12
00:49:31.6608	hacker.com	my.lan.com	IP	Fragmented IP protocol (proto=TCP 0x06, off=4)
00:49:31.6608	my.lan.com	hacker.com	TCP	257 > 256 [RST] Seq=572662306 Ack=572662306 Win=0 Len=0
00:49:31.6608	hacker.com	my.lan.com	IP	Fragmented IP protocol (proto=TCP 0x06, off=32)
00:49:31.6608	hacker.com	my.lan.com	IP	Fragmented IP protocol (proto=TCP 0x06, off=64)
00:49:31.6709	hacker.com	my.lan.com	TCP	256 > 257 [ACK] Seq=286331153 Ack=572662306 Win=4096 Len=12
00:49:31.6709	hacker.com	my.lan.com	IP	Fragmented IP protocol (proto=TCP 0x06, off=4)
00:49:31.6709	my.lan.com	hacker.com	TCP	257 > 256 [RST] Seq=572662306 Ack=572662306 Win=0 Len=0
00:49:31.6709	hacker.com	my.lan.com	IP	Fragmented IP protocol (proto=TCP 0x06, off=32)
00:49:31.6709	hacker.com	my.lan.com	IP	Fragmented IP protocol (proto=TCP 0x06, off=64)
00:49:31.6709	hacker.com	my.lan.com	TCP	256 > 257 [ACK] Seq=286331153 Ack=572662306 Win=4096 Len=12
00:49:31.6709	hacker.com	my.lan.com	IP	Fragmented IP protocol (proto=TCP 0x06, off=4)
00:49:31.6709	my.lan.com	hacker.com	TCP	257 > 256 [RST] Seq=572662306 Ack=572662306 Win=0 Len=0

History	None recalled with the source address. Taken from a workstation in our DMZ but running a host-based firewall.	
Active Targeting?	Yes.	
Criticality	0	Just an NT box used as a test bed. We re-Ghost the disk image on a regular basis.
Lethality	3	DoS attack.
System Countermeasures	4	OS has latest service pack (6a) installed.
Network Countermeasures	4	Host-based firewall.
Severity	-5	*Severity = (Criticality + Lethality) – (System Countermeasures + Network Countermeasures)*
Notes	This is a DoS attack using fragmented packets. The hacker *may* have fingerprinted the workstation earlier and discovered it is an NT box. Older versions of NT did not handle fragmented packets well, but this has been fixed several service packs ago.	

Detect #9

```
Time            Source           Destination        Protocol Info
14:34:08.4679   hacker.com       my.computer.com    TCP  1044 > 20034 [SYN] Seq=1127040 Ack=0 Win=8192 Len=0
14:34:08.4679   my.computer.com  hacker.com         TCP  20034 > 1044 [RST, ACK] Seq=0 Ack=1127041 Win=0 Len=0
14:34:08.4980   ****************************** Non-relevant traffic deleted ******************************
14:34:08.4980   ****************************** Non-relevant traffic deleted ******************************
14:34:08.6081   ****************************** Non-relevant traffic deleted ******************************
14:34:08.6782   ****************************** Non-relevant traffic deleted ******************************
14:34:08.8284   ****************************** Non-relevant traffic deleted ******************************
14:34:08.8985   hacker.com       my.computer.com    TCP  1044 > 20034 [SYN] Seq=1127040 Ack=0 Win=8192 Len=0
14:34:08.8985   my.computer.com  hacker.com         TCP  20034 > 1044 [RST, ACK] Seq=0 Ack=1127041 Win=0 Len=0
14:34:09.1589   ****************************** Non-relevant traffic deleted ******************************
14:34:09.1889   ****************************** Non-relevant traffic deleted ******************************
14:34:09.3892   ****************************** Non-relevant traffic deleted ******************************
14:34:09.3992   hacker.com       my.computer.com    TCP  1044 > 20034 [SYN] Seq=1127040 Ack=0 Win=8192 Len=0
14:34:09.3992   my.computer.com  hacker.com         TCP  20034 > 1044 [RST, ACK] Seq=0 Ack=1127041 Win=0 Len=0
14:34:09.9000   hacker.com       my.computer.com    TCP  1044 > 20034 [SYN] Seq=1127040 Ack=0 Win=8192 Len=0
14:34:09.9000   my.computer.com  hacker.com         TCP  20034 > 1044 [RST, ACK] Seq=0 Ack=1127041 Win=0 Len=0
```

History	None recorded from this source address.	
Active Targeting?	Yes!	
Criticality	3	Workstation.
Lethality	5	Remote control Trojan.
System Countermeasures	3	Patches are up to date, but our antivirus software doesn't catch Net Bus.
Network Countermeasures	4	Host-based firewall.
Severity	1	*Severity = (Criticality + Lethality) – (System Countermeasures + Network Countermeasures)*
Notes	This came from a computer in our DMZ. Looks like a Net Bus 2 Pro scan (http://netbus.org/) based upon the TCP port 20034 probe (http://www.simovits.com/nyheter9902.html). Fortunately the firewall rejected the attempt. This is the only Net Bus scan I've detected (so far!).	

Detect #10

Time	Source	Destination	Protocol	Info
23:40:06.4716	cablemodem.net	my.cablemodem.net	UDP	Source port: 1417 Destination port: **31337**
23:40:11.4788	cablemodem.net	my.cablemodem.net	UDP	Source port: 1417 Destination port: **31337**
23:40:16.4860	cablemodem.net	my.cablemodem.net	UDP	Source port: 1417 Destination port: **31337**
23:40:21.4932	cablemodem.net	my.cablemodem.net	UDP	Source port: 1417 Destination port: **31337**
23:40:26.5004	cablemodem.net	my.cablemodem.net	UDP	Source port: 1417 Destination port: **31337**

History	Taken from a computer attached to a cable modem. I don't know if this source address has probed this system before. I don't really keep track of BO Pings on this system because it happens so often.	
Active Targeting?	Yes.	
Criticality	2	Just a home computer without any critical data on it.
Lethality	4	Trojan that gives the hacker remote control of the system.
System Countermeasures	5	Antivirus software was installed and up to date, which would catch if BO were running (http://vil.nai.com/villib/dispVirus.asp?virus_k=10002). OS is running latest patches.
Network Countermeasures	4	Firewall.
Severity	-3	*Severity = (Criticality + Lethality) – (System Countermeasures + Network Countermeasures)*
Notes	This is a probe to see if the Back Orifice Trojan (http://www.cultdeadcow.com/tools/) is running on my computer. Given that Back Orifice is configurable, more sophisticated hackers will modify the destination port from the default of 31337. Since this scan is on the default UDP port of 31337 (http://www.simovits.com/nyheter9902.html), I suspect a "script kiddie" at play. This particular scan came from the same cable modem system that I'm on.	

Last Updated: July 25th, 2017

Upcoming Training

SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
SANS vLive - SEC503: Intrusion Detection In-Depth	SEC503 - 201709,	Sep 11, 2017 - Oct 18, 2017	vLive
Baltimore Fall 2017 - SEC503: Intrusion Detection In-Depth	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Scottsdale SEC503	Scottsdale, AZ	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS October Singapore 2017	Singapore, Singapore	Oct 09, 2017 - Oct 28, 2017	Live Event
Community SANS Ottawa SEC503	Ottawa, ON	Oct 16, 2017 - Oct 21, 2017	Community SANS
SANS Berlin 2017	Berlin, Germany	Oct 23, 2017 - Oct 28, 2017	Live Event
San Diego Fall 2017 - SEC503: Intrusion Detection In-Depth	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	vLive
SANS San Diego 2017	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS Seattle 2017	Seattle, WA	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS Paris November 2017	Paris, France	Nov 13, 2017 - Nov 18, 2017	Live Event
Community SANS Pensacola SEC503	Pensacola, FL	Nov 27, 2017 - Dec 02, 2017	Community SANS
SIEM & Tactical Analytics Summit & Training	Scottsdale, AZ	Nov 28, 2017 - Dec 05, 2017	Live Event
SANS Cyber Defense Initiative 2017	Washington, DC	Dec 12, 2017 - Dec 19, 2017	Live Event
SANS Security East 2018	New Orleans, LA	Jan 08, 2018 - Jan 13, 2018	Live Event
SANS Las Vegas 2018	Las Vegas, NV	Jan 28, 2018 - Feb 02, 2018	Live Event
SANS Dallas 2018	Dallas, TX	Feb 19, 2018 - Feb 24, 2018	Live Event
SANS OnDemand	Online	Anytime	Self Paced
SANS SelfStudy	Books & MP3s Only	Anytime	Self Paced