Global Information Assurance Certification Paper

*** Northcutt, Stan covers the bases, fine job! 79 *

GCIA Practical Stan Hargus

Trace 1

History: This detect comes from a Network Associates sniffer located on the exterior side of the checkpoint firewall. These anomalous packets were accidentally detected using an incoming capture filter for ICMP type 8. The tcp source port coincidentally matched the hex filter criteria.

Source Address	Dest. Address	Delta Time	Abs. Time	Summary
[aaa.bbb.48.85]	[aaa.bbb.56.70]	04/11/2000	08:26:32 PM	TCP: D=81 S=2048 SYN SEQ=52903132 LEN=0 WIN=8192
[aaa.bbb.48.85]	[aaa.bbb.56.70]	04/11/2000	08:26:35 PM	TCP: D=81 S=2048 SYN SEQ=52903132 LEN=0 WIN=8192
[aaa.bbb.48.85]	[aaa.bbb.56.70]	04/11/2000	08:26:41 PM	TCP: D=81 S=2048 SYN SEQ=52903132 LEN=0 WIN=8192
[aaa.bbb.48.85]	[aaa.bbb.56.70]	04/11/2000	08:26:54 PM	TCP: D=81 S=2048 SYN SEQ=52903132 LEN=0 WIN=8192

Active Targeting: Yes

Technique: This is anomalous traffic. It looks like a possible SYN host scan to port 81. The sequence numbers are identical. The specific host destination address is the inside interface of our SMTP gateway. The SMTP gateway sits on the DMZ with a back door interface to our internal network. This design is a major vulnerability.

Intent: The intent would be to solicit a response from the host on port 81. The source (sl-tc-ppp84.monmouth.com) is a private home page.

Analysis: This server should not be originating or terminating any traffic other than SMTP. Because of the vulnerability of this machine and the anomalous appearance of the packets captured the following actions are in progress: Run tcpdump on the SMTP gateway filtering for all traffic other than SMTP. Speed up implementation of new firewall infrastructure design.

Criticality:	5	vulnerable design of the SMTP gateway-core access
Lethality	3	An attacker exploiting this back door would have access to our internal network. Likelihood of damage is unclear not knowing specific intent.
Counter Measures		
System	3	Gateway OS is up to date. Tcpdump not running at time of trace.
Network	3	ISS real secure server on outside firewall network. No network ID for partner access

Severity is 2

Trace 2

History: This trace comes from our checkpoint firewall log for April 10th and 21st. Filters were set for aaa.bbb.200.16 (our internal DNS server)

```
"10Apr2000" "9:19:45" "hme0" "igw-uskzo" "log" "drop" "domain-udp" "user-33qt8sr.dialup.mindspring.com" "aaa.bbb.200.16" "udp" "71" "1071" "len 66"
"10Apr2000" "9:19:46" "hme0" "igw-uskzo" "log" "drop" "domain-udp" "user-33qt8sr.dialup.mindspring.com" "aaa.bbb.200.16" "udp" "71" "1074" "len 66"
"10Apr2000" "9:19:52" "hme0" "igw-uskzo" "log" "drop" "domain-udp" "user-33qt8sr.dialup.mindspring.com" "aaa.bbb.200.16" "udp" "71" "1077" "len 63"
"10Apr2000" "9:19:58" "hme0" "igw-uskzo" "log" "drop" "domain-udp" "user-33qt8sr.dialup.mindspring.com" "aaa.bbb.200.16" "udp" "71" "1086" "len 64"
"10Apr2000" "9:20:00" "hme0" "igw-uskzo" "log" "drop" "domain-udp" "user-33qt8sr.dialup.mindspring.com" "aaa.bbb.200.16" "udp" "71" "1095" "len 63"
"10Apr2000" "9:20:01" "hme0" "igw-uskzo" "log" "drop" "domain-udp" "user-33qt8sr.dialup.mindspring.com" "aaa.bbb.200.16" "udp" "71" "1099" "len 62"

"21Apr2000" "11:05:27" "hme0" "igw-uskzo" "log" "drop" "domain-udp" "d107.as7.klmz.mi.voyager.net" "aaa.bbb.200.16" "udp" "71" "1040" "len 70"
"21Apr2000" "11:05:35" "hme0" "igw-uskzo" "log" "drop" "domain-udp" "d107.as7.klmz.mi.voyager.net" "aaa.bbb.200.16" "udp" "71" "1045" "len 67"
"21Apr2000" "11:05:36" "hme0" "igw-uskzo" "log" "drop" "domain-udp" "d107.as7.klmz.mi.voyager.net" "aaa.bbb.200.16" "udp" "71" "1049" "len 69"
"21Apr2000" "11:05:46" "hme0" "igw-uskzo" "log" "drop" "domain-udp" "d107.as7.klmz.mi.voyager.net" "aaa.bbb.200.16" "udp" "71" "1056" "len 68"
"21Apr2000" "11:05:50" "hme0" "igw-uskzo" "log" "drop" "domain-udp" "d107.as7.klmz.mi.voyager.net" "aaa.bbb.200.16" "udp" "71" "1061" "len 80"
```

Active Targeting: yes

Technique: Continuous domain-udp queries from external sites to our internal DNS server. Traces were taken from two separate days. No attack signature here. The ISS real secure detector does not report alarm for this pattern. Anomalous by the fact that no outside source should be addressing our internal DNS. Notice from the April 10th trace that these are dialup access connections.

Intent: The likely intent is to simply request a DNS query. No known hostile source address. No associated hostile activity. The volume of this traffic leads to some concern.

Analysis: It is very likely that this traffic is coming from mis-configured clients. Users may have internal DNS hard coded on their laptops. Next step is to track down the identity of the source and investigate how the client is configured.

Criticality:	5	DNS Server
Lethality	0	No hostile intent
Counter Measures		
System	3	NT with current service pack with hot fixes.
Network	3	ISS real secure server on outside firewall network. No network ID for partner access

Severity = -1

Trace 3

History: This trace was discovered in the checkpoint internet gateway firewall. The firewall dropped these packets on the anti-spoofing rule 0.

```
"21Apr2000" " 3:36:55" "qfe0" "igw-uskzo" "log" "drop" "nbdatagram" "150.10.1.2" "150.12.1.2" "udp" "0" "nbdatagram" len 248"
"21Apr2000" " 3:36:55" "qfe0" "aaa.bbb.44.2" "log" "drop" "nbdatagram" "150.10.1.2" "100.100.100.70" "udp" "0" "nbdatagram" len 248"
"21Apr2000" " 3:36:55" "qfe0" "aaa.bbb.44.2" "log" "drop" "nbdatagram" "150.10.1.2" "150.11.1.2" "udp" "0" "nbdatagram" len 248"
"21Apr2000" " 3:36:55" "qfe0" "aaa.bbb.44.2" "log" "drop" "nbdatagram" "150.10.1.2" "200.168.13.12" "udp" "0" "nbdatagram" len 248"
"21Apr2000" " 3:36:56" "qfe0" "aaa.bbb.44.2" "log" "drop" "nbdatagram" "150.10.1.2" "100.100.100.1" "udp" "0" "nbdatagram" len 248"

From internal routing table
150.10.0.0      255.255.0.0      20   aaa.bbb.47.18   Learned OSPF-TYPE2    --
150.11.0.0      255.255.0.0      20   aaa.bbb.47.18   Learned OSPF-TYPE2    --
 150.12.0.0      255.255.0.0      20  aaa.bbb.47.18   Learned OSPF-TYPE2    --
150.13.0.0      255.255.0.0      20   aaa.bbb.47.18   Learned OSPF-TYPE2    --

Tracing route to PDC [150.10.1.2]
1   <10 ms   <10 ms   <10 ms aaa.bbb.196.1
2   <10 ms   <10 ms   <10 ms  uspowcb01_47.kzo.us.pnu.com [aaa.bbb.47.18 3   <10 ms   <10 ms   <10 ms  infkzofr1.kzo.us.pnu.com [aaa.bbb.48.4]
4   711 ms   721 ms   711 ms  aaa.bbb.150.73
5   721 ms   711 ms   721 ms  davi7.infonet.com [aaa.bbb.45.7] 6   751 ms   771 ms   761 ms  160.1.1.1
7   771 ms   791 ms   771 ms  PDC [aaa.bbb.1.2]
```

Active Targeting: no

Technique: The firewall trace shows an unknown network inside the firewall. Review of internal OSPF routing tables showed a total of 4 consecutive unknown networks. All four 150.x.x.x. network routes are being advertised from our internal corporate site in India. Protocol is netbios nbdatagram. IP host address is low number.

Intent: The intent is unclear. IP addresses are centrally controlled within the company. Heightened caution because of the potential for malicious intent. There is no associated hostile activity.

Analysis: We are waiting for access permissions for the local India routers. Also further explanation of these unauthorized advertised networks is pending. Routing will be blocked from these networks.

Criticality:	5	unauthorized network access—entire network is impacted.
Lethality	3	Sensitive to potential harm tempered with no known hostile activity.
Counter Measures		
System	2	Standard NT client\Server environment current service pack levels. Client virus detection 90%. No host based intrusion detection
Network	1	No internal ID methodology. No planned review of firewall logs or routing tables. No ID for Partner access.

Severity: 5

Trace 4

History: Trace discovered using the Checkpoint FW1 firewall log filters. ISS Real Secure on earlier occasions have detected numerous DNS zone high port traces incoming to our network.

```
"21Apr2000" " 0:12:00" "hme0" "accept" "domain-udp" "ns1.webster.edu" "ns2" "udp" "56" "1743" "ns1.webster.edu" "ns2" "1743" " len 63"
"21Apr2000" " 0:17:21" "hme0" "accept" "domain-udp" "serv2.cl.msu.edu" "ns2" "udp" "56" "1303" "serv2.cl.msu.edu" "ns2" "1303" len 56"
"21Apr2000" " 0:31:15" "hme0" "accept" "domain-udp" "cdl.mrs.umn.edu" "ns2" "udp" "56" "1613" "cdl.mrs.umn.edu" "ns2" "1613" " len 56"
```

Active Targeting: yes

Technique: DNS zone transfer between our DNS server and what appears to be a client process. Source port is non-privileged above 1024. This indicates a client process. Also note that all source addresses are from edu.

Intent: Most likely attempts to discover systems on our network--potential targets.

Analysis: Next steps are to watch for repeated activity from same source addresses. Also consider restricting zone transfers from high ports.

Criticality:	4	DNS server on DMZ
Lethality	3	An attacker could identify systems. If DNS is compromised then trust relationship with other services could be exploited.
Counter Measures		
System	4	Up to date OS.
Network	3	ISS real secure server on outside firewall interface. Checkpoint firewall running with up to date OS and application software. No network ID for partner access.

Severity: 0

Trace 5

History: The next three traces were created within our test environment using NMAP. Plans are to implement internal ID with TCPDUMP and possibly SHADOW . Our focus will be our Partner connections and critical servers. This trace was retrieved from the system log files with no explanation of the attack signature. The attack was targeting a Unix server running SunOS. Since installation of our ISS real secure last fall this signature has not been detected.

10:34:23.294922 attacker.com.36623 > igw-mngr.173: udp 0 (DF)
10:34:23.295500 attacker.com.36623 > igw-mngr.884: udp 0 (DF)
10:34:23.296321 attacker.com.36623 > igw-mngr.938: udp 0 (DF)
10:34:23.297549 attacker.com.36623 > igw-mngr.408: udp 0 (DF)
10:34:23.298435 attacker.com.36623 > igw-mngr.7008: udp 0 (DF)
10:34:23.299281 attacker.com.36623 > igw-mngr.299: udp 0 (DF)

Active Targeting: yes

Technique: Rapid sequence targeting what appears to be random UDP ports. No data is sent. This is a UDP port scan directed at our firewall management server, which resides on the inside network.

Intent: The intent is to find which ports are active on this host. Closed ports will respond with an ICMP port unreachable error message. Active ports will not respond.

Analysis: This attack should be detected by our ISS service. We would be immediately notified and the source would be sent a stern warning. If the attack originated from a connected partner it would most likely go undetected. Allowing an attacker to compromise our firewall management station would result in a dangerous situation. The policy files for all our firewalls our contained in this server. The attacker would have the keys to the kingdom.

Criticality:	5	Firewall Management
Lethality	4	Knowledge of what ports are active could allow the attacker to run an exploit to compromise system.
Counter Measures		
System	4	OS up to date. No host ID system in place.
Network	3	ISS real secure server on outside firewall interface. Checkpoint firewall running with up to date OS and application software. No network ID for partner access.

Severity 2

Trace 6

History: See Trace 5 above. This signature has not been detected by the ISS real secure service since implementation last fall. The attack was targeting the checkpoint firewall manager. Since installation of our ISS real secure last fall this signature has not been detected.

10:53:44.739669 chaoskid.edu.34795 > igw-mngr.162: S 842103828:842103828(0) win 1024 (DF)
10:53:44.739693 igw-mngr.162 > chaoskid.edu .34795: R 0:0(0) ack 842103829 win 0 (DF)
10:53:44.740858 chaoskid.edu.34795 > igw-mngr.390: S 842103828:842103828(0) win 1024 (DF)
10:53:44.740882 igw-mngr.390 > chaoskid.edu.34795: R 0:0(0) ack 842103829 win 0 (DF)
10:53:44.741807 chaoskid.edu.34795 > igw-mngr.1513: S 842103828:842103828(0) win 1024 (DF)
10:53:44.741831 igw-mngr.1513 > chaoskid.edu.34795: R 0:0(0) ack 842103829 win 0 (DF)

Active Targeting: yes

Technique: Very rapid SYN packets directed to the firewall manager using random destination ports. Same source port number used. Every active open request sequence number is identical. This is a custom built SYN port scan. Server is

responding with a reset ack telling the attacker that these ports are closed. This scan is not directed at well-known service ports.

Intent: To identify open ports for the likely purpose of running an attack exploit.

Analysis: This attack should be detected by our ISS service. The checkpoint firewall established rule would also stop this scan. If the attack originated from a connected partner it would most likely go undetected. Allowing an attacker to compromise our firewall management station would result in a dangerous situation. The policy files for all our firewalls our contained in this server. Since this attack is focused on a critical service we should take immediate actions to prevent a successful system compromise. Investigating any associated hostile activity. Implementing system ID on this server and other critical services monitoring traffic to well known service ports. Protecting the Partner connection network with a Network ID system.

Criticality:	5	Firewall Management
Lethality	4	Knowledge of what ports are active could allow the attacker to run an exploit to compromise system.
Counter Measures		
System	4	OS up to date. No server ID system in place.
Network	3	ISS real secure server on outside firewall interface. Checkpoint firewall running with up to da application software. No network ID for partner access.

Severity 2

Trace 7

History: See Trace 5 above. This signature has not been detected by the ISS real secure service since implementation last fall. The attack was targeting the checkpoint firewall manager located inside the firewall. Since installation of our ISS real secure last fall this signature has not been detected.

```
01:55:44.836589 malice.net.44646 > igw-mngr.956: S 4172366005:4172366005(0) win 8760 <mss 1460> (DF)
01:55:44.839133 malice.net.44647 > igw-mngr.387: S 4172491063:4172491063(0) win 8760 <mss 1460> (DF)
01:55:44.842775 malice.net.44648 > igw-mngr.205: S 4172493079:4172493079(0) win 8760 <mss 1460> (DF)
01:55:44.854163 malice.net.44649 > igw-mngr.1418: S 4172503255:4172503255(0) win 8760 <mss 1460> (DF)
01:55:44.856277 malice.net.44650 > igw-mngr.1535: S 4172607723:4172607723(0) win 8760 <mss 1460> (DF)
```

Technique: Frequent SYN packets sent directed at our firewall manager. Unlike trace 6 the source port is incrementing by 1. The sequence number are also incrementing for every active open request. These packets appear to be generated by the connect system call. . Destination ports appear to be random. This is another SYN scan.

Intent: As in trace 6 the attacker is attempting to identify open TCP ports for the likely purpose of running an attack exploit.

Analysis: Again, this attack should be detected by our ISS service. The checkpoint firewall established rule would also stop this scan. If the attack originated from a connected partner it would most likely go undetected. Allowing an attacker to compromise our firewall management station would result in a dangerous situation. The policy files for all our firewalls our contained in this server. Since this attack is focused on a critical service we should take immediate actions to prevent a successful system compromise. Investigating any associated hostile activity. Implementing system ID on this server and other critical services monitoring traffic to well known service ports. Protecting the Partner connection network with a

Network ID system. Because of the changing source port numbers and sequence numbers this scan would be more difficult to detect within the interior network.

Criticality:	5	Firewall Management
Lethality	4	Knowledge of what ports are active could allow the attacker to run an exploit to compromise
Counter Measures		
System	4	OS up to date. No host ID in place.
Network	3	ISS real secure server on outside firewall interface. Checkpoint firewall running with up to date OS and application software. No network ID for partner access.

Severity 2

Trace 8

History: This trace is taken from the checkpoint firewall log.

"23Mar2000" "10:39:40" "hme0" "igw-uskzo" "log" "drop" "chargen" "smtp-gateway" "aaa.bbb.200.16" "udp" "116" "echo-udp"

Technique: Destination port 19 and a source port of udp echo. Port 19 is the diagnostic chargen character generator. If allowed through the firewall this would start an unending series of packets between source and destination machines.

Intent: The intent is a denial of service attack. The source ip address is most likely not the attacker but a victim. Unclear if intent is to clog our services or the source.

Analysis: The ISS real secure ID system will detect this attack. The checkpoint firewall drops this as well. We have no internal network or system ID in place to detect this attack from the inside or originating from partners.

Criticality:	5	SMTP gateway
Lethality	3	Likelihood of harm is moderate. If ID and firewall were not in place result would be poor per or total loss of internet access.
Counter Measures		
System	4	OS up to date. No host ID in place.
Network	3	ISS real secure server on outside firewall interface. Checkpoint firewall running with up to date OS and application software. Well protected for this type of attack from outside. Vulnerable from inside or partner connections.

Severity 1

Trace 9

History: This trace was found in the firewall logs for two on April 2nd , and April 3rd, filtering on destination port 7—tcp-echo. It looked suspicious.

"2Apr2000" "10:14:40" "hme0" "aaa.bbb.44.2" "log" "drop" "1381" "aaa.bbb.1.139" "aaa.bbb.70.43" "tcp" "71" "echo-tcp" " len 40"
"2Apr2000" "10:15:21" "hme0" "aaa.bbb.44.2" "log" "drop" "1236" "aaa.bbb.1.139" "aaa.bbb.102.80" "tcp" "71" "echo-tcp" " len 40"
"2Apr2000" "10:23:10" "hme0" "aaa.bbb.44.2" "log" "drop" "1236" "aaa.bbb.1.139" "aaa.bbb.222.73" "tcp" "71" "echo-tcp" " len 40"
"2Apr2000" "10:31:00" "hme0" "aaa.bbb.44.2" "log" "drop" "1236" "aaa.bbb.1.139" "aaa.bbb.86.67" "tcp" "71" "echo-tcp" " len 40"
"2Apr2000" "10:35:55" "hme0" "aaa.bbb.44.2" "log" "drop" "1236" "aaa.bbb.1.139" "aaa.bbb.65.15" "tcp" "71" "echo-tcp" " len 40"
"2Apr2000" "10:50:36" "hme0" "aaa.bbb.44.2" "log" "drop" "1236" "aaa.bbb.1.139" "aaa.bbb.2.115" "tcp" "71" "echo-tcp" " len 40"
"2Apr2000" "10:52:50" "hme0" "aaa.bbb.44.2" "log" "drop" "1381" "aaa.bbb.1.139" "aaa.bbb.111.123" "tcp" "71" "echo-tcp"" " len 40"
"2Apr2000" "10:57:43" "hme0" "aaa.bbb.44.2" "log" "drop" "1381" "aaa.bbb.1.139" "aaa.bbb.90.71" "tcp" "71" "echo-tcp" " len 40"
"2Apr2000" "11:16:20" "hme0" "aaa.bbb.44.2" "log" "drop" "1381" "aaa.bbb.1.139" "aaa.bbb.215.103" "tcp" "71" "echo-tcp" " len 40"

"2Apr2000" "11:36:52" "hme0" "aaa.bbb.44.2" "log" "drop" "1381" "aaa.bbb.1.139" "aaa.bbb.178.38" "tcp" "71" "echo-tcp" " len 40"
"2Apr2000" "11:40:30" "hme0" "aaa.bbb.44.2" "log" "drop" "1236" "aaa.bbb.1.139" "aaa.bbb.95.121" "tcp" "71" "echo-tcp" " len 40"

"3Apr2000" " 7:23:54" "hme0" "igw-uskzo" "log" "drop" "1236" "expect.a.deathtrap.org.uk" "aaa.bbb.102.80" "tcp" "71" "echo-tcp" " len 40"
"3Apr2000" " 7:24:45" "hme0" "aaa.bbb.44.2" "log" "drop" "1381" "aaa.bbb.101.16" "aaa.bbb.117.58" "tcp" "71" "echo-tcp" "" " len 40"
"3Apr2000" " 7:26:51" "hme0" "aaa.bbb.44.2" "log" "drop" "1236" "aaa.bbb.101.16" "aaa.bbb.149.95" "tcp" "71" "echo-tcp" "" " len 40"
"3Apr2000" " 7:32:50" "hme0" "aaa.bbb.44.2" "log" "drop" "1236" "aaa.bbb.101.16" "aaa.bbb.243.125" "tcp" "71" "echo-tcp" "" " len 40"
"3Apr2000" " 7:35:47" "hme0" "aaa.bbb.44.2" "log" "drop" "1236" "aaa.bbb.101.16" "aaa.bbb.34.13" "tcp" "71" "echo-tcp" " len 40"
"3Apr2000" "13:24:17" "hme0" "aaa.bbb.44.2" "log" "drop" "1381" "aaa.bbb.154.14" "aaa.bbb.121.73" "tcp" "71" "echo-tcp"" " len 40"
"3Apr2000" "14:04:05" "hme0" "aaa.bbb.44.2" "log" "drop" "1381" "aaa.bbb.154.14" "aaa.bbb.79.97" "tcp" "71" "echo-tcp" "" " len 40"
"3Apr2000" "14:18:48" "hme0" "aaa.bbb.44.2" "log" "drop" "1236" "aaa.bbb.154.14" "aaa.bbb.252.51" "tcp" "71" "echo-tcp" "" " len 40"
"3Apr2000" "14:26:49" "hme0" "aaa.bbb.44.2" "log" "drop" "1236" "aaa.bbb.154.14" "aaa.bbb.90.82" "tcp" "71" "echo-tcp" "" " len 40"
"3Apr2000" "14:27:57" "hme0" "aaa.bbb.44.2" "log" "drop" "1381" "aaa.bbb.154.14" "aaa.bbb.105.60" "tcp" "71" "echo-tcp" "" " len 40"
"3Apr2000" "14:31:52" "hme0" "aaa.bbb.44.2" "log" "drop" "1381" "aaa.bbb.154.14" "aaa.bbb.152.75" "tcp" "71" "echo-tcp" "" " len 40"

$ nslookup expect.a.deathtrap.org.uk
Server: pwdns.us.pnu.com
Address: aaa.bbb.54.11

Non-authoritative answer:
Name: expect.a.deathtrap.org.uk
Address: aaa.bbb.101.16

Active Targeting: no

Technique: I see different source ip addresses on different days. TCP-echo is used for the source port. Only two non-privileged destination ports are used—either 1236 or 1381. The name of one of the sources is suspicious--"expect.a.deathtrap.org.uk". Destination ip addresses are random covering a wide range of the internal space. Appears to be crafted with spoofed source addresses.

Intent: Appears to be an attempt at a denial of service attack. Not certain on the significance of these destination ports. Could be a particular OS vulnerability.

Analysis: This is being block by the default rule in the firewall. ISS real secure did not detect this trace. This has been reported to them.

Criticality:	1	No specific target
Lethality	2	No known vulnerability
Counter Measures		
System	2	Standard NT OS
Network	3	ISS real secure server on outside firewall interface. Checkpoint firewall running with up to date OS and application software. Well protected for this type of attack from outside. Vulnerable from inside or partner connections.

Severity -2

Trace 10

History: This detect comes from a Network Associates sniffer located on the exterior side of the partner firewall. This trace was detected by filtering on ICMP echo from the exterior side of the firewall.

	Source Address	Dest. Address	Delta Time	Abs. Time	Summary
223	[aaa.bbb.196.49]	[aaa.bbb.200.214]	92 0:00:02.357	0.001.174	04/11/2000 02:47:14 PM ICMP: Echo
224	[aaa.bbb.196.49]	[aaa.bbb.200.215]	92 0:00:02.358	0.001.274	04/11/2000 02:47:14 PM ICMP: Echo
225	[aaa.bbb.196.49]	[aaa.bbb.200.216]	92 0:00:02.360	0.001.875	04/11/2000 02:47:14 PM ICMP: Echo
226	[aaa.bbb.196.49]	[aaa.bbb.200.217]	92 0:00:02.361	0.000.514	04/11/2000 02:47:14 PM ICMP: Echo
227	[aaa.bbb.196.49]	[aaa.bbb.200.218]	92 0:00:02.362	0.001.497	04/11/2000 02:47:14 PM ICMP: Echo
228	[aaa.bbb.196.49]	[aaa.bbb.200.219]	92 0:00:02.363	0.001.261	04/11/2000 02:47:14 PM ICMP: Echo
229	[aaa.bbb.196.49]	[aaa.bbb.200.220]	92 0:00:02.364	0.000.987	04/11/2000 02:47:14 PM ICMP: Echo
230	[aaa.bbb.196.49]	[aaa.bbb.200.221]	92 0:00:02.367	0.002.494	04/115/2000 02:47:14 PM ICMP: Echo
231	[aaa.bbb.196.49]	[aaa.bbb.200.222]	92 0:00:02.367	0.000.519	04/11/2000 02:47:14 PM ICMP: Echo
232	[aaa.bbb.196.49]	[aaa.bbb.200.223]	92 0:00:02.369	0.001.863	04/11/2000 02:47:14 PM ICMP: Echo
233	[aaa.bbb.196.49]	[aaa.bbb.200.224]	92 0:00:02.370	0.000.509	04/11/2000 02:47:14 PM ICMP: Echo

Active Targeting: no

Technique: Use of ICMP echo to many hosts on the same subnet. Appears to be a network scan. Network subnet scanned contains global services. Source originating from known partner site.

Intent: Purpose is to identify active hosts within specific internal network range. No associated hostile activity. Some knowledge of internal network is likely since the target subnet contains many global servers.

Analysis: ICMP is not blocked incoming from trusted partner connections. No network ID is in service. Firewall logs are not reviewed on a regular basis. Next steps are to notify originating company, block ICMP from external source network and implement network ID for the partner connections.

Criticality:	3	Important server subnet
Lethality	1	Harm not likely. ICMP reconnaissance
Counter Measures		
System	3	Standard up to date OS. No host ID system in place
Network	1	Firewall in place. No network ID system in service

Severity 0

Last Updated: July 21st, 2017

Upcoming Training

SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
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
SANS Seattle 2017	Seattle, WA	Oct 30, 2017 - Nov 04, 2017	Live Event
San Diego Fall 2017 - SEC503: Intrusion Detection In-Depth	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	vLive
SANS San Diego 2017	San Diego, CA	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