Global Information Assurance Certification Paper

*** Northcutt, Competent analysis, clearly knows what he is doing. A hex dump of 4,5,6 might have been fun reading. Detect 8 was done well and pulled the score up. I started to get excited when I saw detect 10, but no additional research or analysis was submitted. 74 *

Sans SNAP Level One Certification Practical

10 Detects with Analyses

Submitted by Darrell M. Pettyjohn

exam written March 25, 1999 at the SANS 2000 conference in Orlando FL USA.

Trojan port information from http://www.sans.org/y2k/ports.htm

---

Detect 1, NNTP scan

```
16:33:47.502554 24.0.94.130.37673 > 9.9.9.1.119: S 460772377:460772377(0) win 8760 <mss 1460>
16:33:47.552977 9.9.9.1.119 > 24.0.94.130.37673: R 0:0(0) ack 460772378 win 0
16:34:06.140102 24.0.94.130.47551 > 9.9.9.1.119: S 1107870780:1107870780(0) win 8760 <mss 1460>
16:34:06.140239 9.9.9.1.119 > 24.0.94.130.47551: R 0:0(0) ack 1107870781 win 0


21:15:44.282356 24.0.94.130.65372 > 9.9.9.1.119: S 1870216779:1870216779(0) win 8760 <mss 1460>
21:15:44.330920 9.9.9.1.119 > 24.0.94.130.65372: R 0:0(0) ack 1870216780 win 0
21:16:09.766746 24.0.94.130.46484 > 9.9.9.1.119: S 2780805719:2780805719(0) win 8760 <mss 1460>
21:16:09.766888 9.9.9.1.119 > 24.0.94.130.46484: R 0:0(0) ack 2780805720 win 0


01:47:33.276456 24.0.94.130.46368 > 9.9.9.1.119: S 2865858790:2865858790(0) win 8760 <mss 1460>
01:47:33.342407 9.9.9.1.119 > 24.0.94.130.46368: R 0:0(0) ack 2865858791 win 0

01:47:52.551724 24.0.94.130.57997 > 9.9.9.2.119: S 3628759848:3628759848(0) win 8760 <mss 1460>
01:47:53.265351 24.0.94.130.57997 > 9.9.9.2.119: R 3628759849:3628759849(0) win 8760
01:47:53.268882 24.0.94.130.58368 > 9.9.9.2.119: S 3652371679:3652371679(0) win 8760 <mss 1460>
01:47:53.816020 24.0.94.130.58368 > 9.9.9.2.119: R 3652371680:3652371680(0) win 8760

01:48:10.435743 24.0.94.130.35905 > 9.9.9.1.119: S 32431883:32431883(0) win 8760 <mss 1460>
01:48:10.435893 9.9.9.1.119 > 24.0.94.130.35905: R 0:0(0) ack 32431884 win 0


06:16:47.434401 24.0.94.130.51529 > 9.9.9.1.119: S 2068151737:2068151737(0) win 8760 <mss 1460>
06:16:47.478711 9.9.9.1.119 > 24.0.94.130.51529: R 0:0(0) ack 2068151738 win 0

06:16:57.673870 24.0.94.130.57973 > 9.9.9.2.119: S 2493130384:2493130384(0) win 8760 <mss 1460>
06:16:58.702608 24.0.94.130.57973 > 9.9.9.2.119: R 2493130385:2493130385(0) win 8760
06:16:58.719963 24.0.94.130.58687 > 9.9.9.2.119: S 2539622940:2539622940(0) win 8760 <mss 1460>
06:17:00.389735 24.0.94.130.58687 > 9.9.9.2.119: R 2539622941:2539622941(0) win 8760

06:17:16.019928 24.0.94.130.36476 > 9.9.9.1.119: S 3235682137:3235682137(0) win 8760 <mss 1460>
06:17:16.020075 9.9.9.1.119 > 24.0.94.130.36476: R 0:0(0) ack 3235682138 win 0
```

Description:

This detect appeared in a tcpdump log of traffic on my residence cable modem connection on March 31 and April 1 2000. This traffic indicates a scan for NNTP, TCP port 119, servers. The source ephemeral port indicates a fairly busy host.

History/Background/Methods:

I did a reverse DNS lookup on the scanning hosts IP address and was rewarded with the name AUTHORIZED-SCAN.SECURITY.HOME.NET. I then sent an e-mail to my ISP requesting confirmation that this scanning activity is indeed authorized and being done by the ISP. In the same e-mail I also reported a number of Trojan scans. The response was interesting (-:.

My ISP informed me via e-mail that yes, the NNTP scans were being conducted by them. I was also told that appropriate action would be taken against the people running the Trojan scans and, in the case where the people doing the scans were not with the same ISP, the appropriate ISP would be informed of the activity. I was then informed that packet sniffing was against the usage policy and if I continued that my service could be cut off. (-:.

Threat: Low Severity: Low
Subsequent Action: None

==========

Detect 2: SubSeven Trojan scan

TCP 27374, SubSeven 2.1 Trojan

```
19:28:48.131958 24.67.209.214.2232 > 9.9.9.1.27374: S 217492950:217492950(0) win 8192 <mss
1460,nop,nop,sackOK> (DF)
19:28:48.176707 9.9.9.1.27374 > 24.67.209.214.2232: R 0:0(0) ack 217492951 win 0

19:28:48.760974 24.67.209.214.2232 > 9.9.9.1.27374: S 217492950:217492950(0) win 8192 <mss
1460,nop,nop,sackOK> (DF)
19:28:48.761117 9.9.9.1.27374 > 24.67.209.214.2232: R 0:0(0) ack 1 win 0

19:28:49.398730 24.67.209.214.2232 > 9.9.9.1.27374: S 217492950:217492950(0) win 8192 <mss
1460,nop,nop,sackOK> (DF)
19:28:49.398868 9.9.9.1.27374 > 24.67.209.214.2232: R 0:0(0) ack 1 win 0

19:28:49.989459 24.67.209.214.2232 > 9.9.9.1.27374: S 217492950:217492950(0) win 8192 <mss
1460,nop,nop,sackOK> (DF)
19:28:49.989572 9.9.9.1.27374 > 24.67.209.214.2232: R 0:0(0) ack 1 win 0
```

Description:

This detect appeared in a tcpdump log of traffic on my residence cable modem connection on March 31 and April 1 2000.

History/Background/Methods:

Persistent SYN packets with the same source port to a known Trojan port. As the source port does not increment after a number of RESET packets have been sent to the scanning host I would say that the packets have been crafted.

Reverse DNS lookup on source host gives 24.67.209.214.bc.wave.home.com.

Threat: Medium Severity: Low

Subsequent Action: The target host was scanned for known Trojans and viruses. The ISP of the scanning host was notified of the activity.

==========

Detect 3: Netbus Trojan scan

TCP 12345, netbus remote control trojan

20:21:11.808385 24.67.212.143.1827 > 9.9.9.2.12345: S 1787948169:1787948169(0) win 8192 <mss 1460,nop,nop,sackOK> (DF)
20:21:14.760270 24.67.212.143.1827 > 9.9.9.2.12345: S 1787948169:1787948169(0) win 8192 <mss 1460,nop,nop,sackOK> (DF)

Description:
These detects appeared in tcpdump logs of traffic on my residence cable modem connection from March 31 to April 4/2000.

History/Background/Methods:
Persistent SYN packets with the same source port to a known Trojan port.

Reverse DNS lookup on source host gives 24.67.212.143.bc.wave.home.com.

Threat: Medium Severity: Low

Subsequent Action: The target host was scanned for known Trojans and viruses. The ISP of the scanning host was notified of the activity.

==========

Detect 4, 5 and 6: Hack 'a' Tack Trojan scan

udp 31789 and 31790, Hack 'a' Tack Trojan

Detect 4

16:57:40.049014 24.42.67.46.31790 > 9.9.9.1.31789: udp 1
16:57:40.095837 9.9.9.1 > 24.42.67.46: icmp: 9.9.9.1 udp port 31789 unreachable

17:55:58.909015 24.42.67.46.31790 > 9.9.9.1.31789: udp 1
17:55:58.955642 9.9.9.1 > 24.42.67.46: icmp: 9.9.9.1 udp port 31789 unreachable

---

Detect 5

13:12:54.395448 24.19.135.26.31790 > 9.9.9.1.31789: udp 1
13:12:55.427671 24.19.135.26.31790 > 9.9.9.2.31789: udp 1

Detect 6

22:15:39.045661 24.65.242.208.31790 > 9.9.9.2.31789: udp 1
22:15:39.046013 9.9.9.2 > 24.65.242.208: icmp: 9.9.9.2 udp port 31789 unreachable
22:15:39.234710 24.65.242.208.31790 > 9.9.9.1.31789: udp 1
22:15:39.252156 9.9.9.1 > 24.65.242.208: icmp: 9.9.9.1 udp port 31789 unreachable

Description:
These detects appeared in tcpdump logs of traffic on my residence cable modem connection from March 31 to April 4/2000.

History/Background/Methods:
Persistent SYN packets with the same source port to a known Trojan port. As the source port does not change, I would say that the packets have been crafted. The same source/destination port pair used by three different attackers on attempted connections to two different hosts leads me to believe a canned script/program is being used. Script Kiddies at work.

Threat: Medium Severity: Low

Subsequent Action: The target host was scanned for known Trojans and viruses. The ISP of the scanning host was notified of the activity.

==========

Detect 7: Deep Throat Trojan scan

Udp 2140 Deep Throat, The Invasor

15:23:43.013362 216.68.39.36.60000 > 9.9.9.1.2140: udp 2
15:23:45.025711 216.68.39.36.60000 > 9.9.9.2.2140: udp 2
16:11:27.857786 216.68.39.36.60000 > 9.9.9.1.2140: udp 2
16:11:29.272555 216.68.39.36.60000 > 9.9.9.2.2140: udp 2

Description:
These detects appeared in tcpdump logs of traffic on my residence cable modem connection from March 31 to April 4/2000.

History/Background/Methods:

Persistent SYN packets with the same source port to a known Trojan port. As the source port does not increment, I would say that the packets have been crafted.

Reverse DNS lookup on source host gives as1-216-68-39-36.fuse.net.

Threat: Medium Severity: Low

Subsequent Action: The target host was scanned for known Trojans and viruses. The ISP of the scanning host was notified of the activity.

==========

Detect 8: DNS Load Balancing scan using the 3dns package

num	date	time	orig	type	action	alert	i/f_name	i/f_dir	proto	src	dst	service
2081	8-Apr-00	11:50:13	uriel.adomain.trg	alert	drop	![alert]	E100B1	inbound	udp	167.8.29.92	Uriel	
2082	8-Apr-00	11:50:14	uriel.adomain.trg	alert	drop	![alert]	E100B1	inbound	udp	167.8.29.92	Uriel	
2083	8-Apr-00	11:50:15	uriel.adomain.trg	alert	drop	![alert]	E100B1	inbound	udp	167.8.29.92	Uriel	
2084	8-Apr-00	11:50:16	uriel.adomain.trg	alert	drop	![alert]	E100B1	inbound	udp	167.8.29.92	Uriel	
2248	8-Apr-00	12:09:47	uriel.adomain.trg	alert	drop	![alert]	E100B1	inbound	udp	167.8.29.92	Uriel	
2249	8-Apr-00	12:09:47	uriel.adomain.trg	alert	drop	![alert]	E100B1	inbound	udp	167.8.29.92	Uriel	
2250	8-Apr-00	12:09:47	uriel.adomain.trg	alert	drop	![alert]	E100B1	inbound	udp	167.8.29.92	Uriel	
2253	8-Apr-00	12:10:07	uriel.adomain.trg	Log	reject		daemon	inbound	tcp	167.8.29.92	Uriel	nameser
2254	8-Apr-00	12:10:07	uriel.adomain.trg	Log	reject		daemon	inbound	tcp	167.8.29.92	Uriel	nameser
2255	8-Apr-00	12:10:07	uriel.adomain.trg	Log	reject		daemon	inbound	tcp	167.8.29.92	Uriel	nameser
7989	9-Apr-00	0:40:32	uriel.adomain.trg	Log	drop		E100B1	inbound	udp	167.8.29.92	Pinky	
7990	9-Apr-00	0:40:33	uriel.adomain.trg	Log	drop		E100B1	inbound	udp	167.8.29.92	Pinky	
7991	9-Apr-00	0:40:35	uriel.adomain.trg	Log	drop		E100B1	inbound	udp	167.8.29.92	Pinky	
7992	9-Apr-00	0:40:36	uriel.adomain.trg	Log	drop		E100B1	inbound	udp	167.8.29.92	Pinky	
8300	9-Apr-00	1:32:59	uriel.adomain.trg	Alert	drop	![alert]	E100B1	inbound	udp	167.8.29.92	Uriel	
8301	9-Apr-00	1:33:00	uriel.adomain.trg	Alert	drop	![alert]	E100B1	inbound	udp	167.8.29.92	Uriel	
8302	9-Apr-00	1:33:02	uriel.adomain.trg	Alert	drop	![alert]	E100B1	inbound	udp	167.8.29.92	Uriel	
8303	9-Apr-00	1:33:03	uriel.adomain.trg	Alert	drop	![alert]	E100B1	inbound	udp	167.8.29.92	Uriel	
8313	9-Apr-00	1:34:19	uriel.adomain.trg	Alert	drop	![alert]	E100B1	inbound	udp	167.8.29.92	Uriel	
8314	9-Apr-00	1:34:20	uriel.adomain.trg	Alert	drop	![alert]	E100B1	inbound	udp	167.8.29.92	Uriel	
8315	9-Apr-00	1:34:21	uriel.adomain.trg	Alert	drop	![alert]	E100B1	inbound	udp	167.8.29.92	Uriel	
8316	9-Apr-00	1:34:22	uriel.adomain.trg	Alert	drop	![alert]	E100B1	inbound	udp	167.8.29.92	Uriel	
8850	9-Apr-00	4:15:27	uriel.adomain.trg	Log	drop		E100B1	inbound	udp	167.8.29.92	Pinky	
8851	9-Apr-00	4:15:28	uriel.adomain.trg	Log	drop		E100B1	inbound	udp	167.8.29.92	Pinky	
8852	9-Apr-00	4:15:29	uriel.adomain.trg	Log	drop		E100B1	inbound	udp	167.8.29.92	Pinky	
8853	9-Apr-00	4:15:30	uriel.adomain.trg	Log	drop		E100B1	inbound	udp	167.8.29.92	Pinky	
8770	9-Apr-00	3:51:59	uriel.adomain.trg	Log	reject		daemon	inbound	tcp	167.8.29.92	Pinky	nameser
8771	9-Apr-00	3:51:59	uriel.adomain.trg	Log	reject		daemon	inbound	tcp	167.8.29.92	Pinky	nameser
8772	9-Apr-00	3:51:59	uriel.adomain.trg	Log	reject		daemon	inbound	tcp	167.8.29.92	Pinky	nameser
6933	8-Apr-00	21:00:10	uriel.adomain.trg	log	reject		daemon	inbound	tcp	200.211.187.195	Uriel	nameser
7004	8-Apr-00	21:11:52	uriel.adomain.trg	log	reject		daemon	inbound	tcp	200.211.187.195	Uriel	nameser
7005	8-Apr-00	21:11:52	uriel.adomain.trg	log	reject		daemon	inbound	tcp	200.211.187.195	Uriel	nameser
8555	9-Apr-00	2:36:02	uriel.adomain.trg	log	reject		daemon	inbound	tcp	200.211.187.195	Pinky	nameser
8556	9-Apr-00	2:36:02	uriel.adomain.trg	log	reject		daemon	inbound	tcp	200.211.187.195	Pinky	nameser

8557	9-Apr-00	2:36:02	uriel.adomain.trg	log	reject		daemon	inbound	tcp	200.211.187.195	Pinky	nameser
8919	9-Apr-00	4:37:10	uriel.adomain.trg	log	reject		daemon	inbound	tcp	200.211.187.195	www	nameser
8920	9-Apr-00	4:37:10	uriel.adomain.trg	log	reject		daemon	inbound	tcp	200.211.187.195	www	nameser
8921	9-Apr-00	4:37:10	uriel.adomain.trg	log	reject		daemon	inbound	tcp	200.211.187.195	www	nameser
2202	8-Apr-00	12:04:25	uriel.adomain.trg	alert	drop	![alert]	E100B1	inbound	udp	206.251.19.89	Uriel	
2203	8-Apr-00	12:04:25	uriel.adomain.trg	alert	drop	![alert]	E100B1	inbound	udp	206.251.19.89	Uriel	
2204	8-Apr-00	12:04:25	uriel.adomain.trg	alert	drop	![alert]	E100B1	inbound	udp	206.251.19.89	Uriel	
5071	8-Apr-00	14:50:33	uriel.adomain.trg	log	drop		E100B1	inbound	udp	206.251.19.89	Pinky	
5072	8-Apr-00	14:50:35	uriel.adomain.trg	log	drop		E100B1	inbound	udp	206.251.19.89	Pinky	
5073	8-Apr-00	14:50:36	uriel.adomain.trg	log	drop		E100B1	inbound	udp	206.251.19.89	Pinky	
5074	8-Apr-00	14:50:37	uriel.adomain.trg	log	drop		E100B1	inbound	udp	206.251.19.89	Pinky	
5085	8-Apr-00	14:51:27	uriel.adomain.trg	log	drop		E100B1	inbound	udp	206.251.19.89	Pinky	
7464	8-Apr-00	22:58:36	uriel.adomain.trg	log	drop		E100B1	inbound	udp	206.251.19.89	www	
7465	8-Apr-00	22:58:36	uriel.adomain.trg	log	drop		E100B1	inbound	udp	206.251.19.89	www	
7466	8-Apr-00	22:58:36	uriel.adomain.trg	log	drop		E100B1	inbound	udp	206.251.19.89	www	
2132	8-Apr-00	11:54:38	uriel.adomain.trg	log	reject		daemon	inbound	tcp	206.251.19.89	Uriel	nameser
2133	8-Apr-00	11:54:38	uriel.adomain.trg	log	reject		daemon	inbound	tcp	206.251.19.89	Uriel	nameser
2134	8-Apr-00	11:54:38	uriel.adomain.trg	log	reject		daemon	inbound	tcp	206.251.19.89	Uriel	nameser
2205	8-Apr-00	12:04:45	uriel.adomain.trg	log	reject		daemon	inbound	tcp	206.251.19.89	Uriel	nameser
2206	8-Apr-00	12:04:45	uriel.adomain.trg	log	reject		daemon	inbound	tcp	206.251.19.89	Uriel	nameser
2207	8-Apr-00	12:04:45	uriel.adomain.trg	log	reject		daemon	inbound	tcp	206.251.19.89	Uriel	nameser
4901	8-Apr-00	14:27:27	uriel.adomain.trg	log	reject		daemon	inbound	tcp	206.251.19.89	Pinky	nameser
4902	8-Apr-00	14:27:27	uriel.adomain.trg	log	reject		daemon	inbound	tcp	206.251.19.89	Pinky	nameser
4903	8-Apr-00	14:27:27	uriel.adomain.trg	log	reject		daemon	inbound	tcp	206.251.19.89	Pinky	nameser
5283	8-Apr-00	15:34:40	uriel.adomain.trg	log	reject		daemon	inbound	tcp	206.251.19.89	Pinky	nameser
5284	8-Apr-00	15:34:40	uriel.adomain.trg	log	reject		daemon	inbound	tcp	206.251.19.89	Pinky	nameser
5285	8-Apr-00	15:34:40	uriel.adomain.trg	log	reject		daemon	inbound	tcp	206.251.19.89	Pinky	nameser
7469	8-Apr-00	22:59:36	uriel.adomain.trg	log	reject		daemon	inbound	tcp	206.251.19.89	www	nameser
7470	8-Apr-00	22:59:36	uriel.adomain.trg	log	reject		daemon	inbound	tcp	206.251.19.89	www	nameser
7471	8-Apr-00	22:59:36	uriel.adomain.trg	log	reject		daemon	inbound	tcp	206.251.19.89	www	nameser
7641	8-Apr-00	23:30:54	uriel.adomain.trg	log	reject		daemon	inbound	tcp	206.251.19.89	www	nameser
7642	8-Apr-00	23:30:54	uriel.adomain.trg	log	reject		daemon	inbound	tcp	206.251.19.89	www	nameser
7643	8-Apr-00	23:30:54	uriel.adomain.trg	log	reject		daemon	inbound	tcp	206.251.19.89	www	nameser

Description:

Wow, there was a lot of this traffic, my apologies for including so much. This seems to perfectly match the traffic described at **http://www.sans.org/y2k/DNS.htm** .

History/Background/Methods:

Some whois lookups and a few reverse DNSs later, I discovered that the bulk of these scans came from Microsoft's Domain. Others using the same technique were from places like Japan and Brazil. Here is a reply to an e-mail I sent about this traffic to one of the scanning domains:

The traffic that you are seeing is actually an automatic feature of the new load balancing dns that we are using (the product is 3dns, www.3dns.com). Basically, as your users hit our sites that use this system, the 3dns system needs to find out which data center that they are closest to, to try and improve performance. The system does this by sending a packet to port 53 at your domain. The system times the round trip, and uses that metric to

calculate the closest servers. It looks like an aborted zone transfer normally, or a dns look-up that went wrong. The system apparently caches the information, and will periodically check (every couple of weeks) to make sure that it is still accurate.

Decent idea in theory but there are some glitches in the implementation. The teams using the software here are working with the vender to get the problems ironed out. Meanwhile, they've implemented an exclusion list for places where these runaway connections occur. If you can send us the IP address range you are seeing this on in CIDR format, the team will add you to the exclusion list.

Threat: Low Severity: Low

Subsequent Action: A request was submitted to have the target site added to the exclusion list for this scanning activity.

Detect 9: Smurf Attack

num	date	time	orig	type	action	alert	i/f_name	i/f_dir	proto	Src	dst	
2924	8-Apr-00	13:29:42	uriel.adomain.trg	log	drop		E100B1	inbound	udp	viktor.ld.ttu.ee	8.8.8.255	echo
2925	8-Apr-00	13:29:42	uriel.adomain.trg	log	drop		E100B1	inbound	udp	viktor.ld.ttu.ee	8.8.8.255	echo
2926	8-Apr-00	13:29:43	uriel.adomain.trg	log	drop		E100B1	inbound	udp	viktor.ld.ttu.ee	8.8.8.255	echo
.												
.												
.												
4550	8-Apr-00	13:36:10	uriel.adomain.trg	log	drop		E100B1	inbound	udp	viktor.ld.ttu.ee	8.8.8.255	echo
4551	8-Apr-00	13:36:10	uriel.adomain.trg	log	drop		E100B1	inbound	udp	viktor.ld.ttu.ee	8.8.8.255	echo
4552	8-Apr-00	13:36:10	uriel.adomain.trg	log	drop		E100B1	inbound	udp	viktor.ld.ttu.ee	8.8.8.255	echo

6355	7-Apr-00	16:06:39	uriel.adomain.trg	log	drop		E100B1	inbound	udp	in.addr-arpa.com	8.8.8.255
6356	7-Apr-00	16:06:40	uriel.adomain.trg	log	drop		E100B1	inbound	udp	in.addr-arpa.com	8.8.8.255
6357	7-Apr-00	16:06:42	uriel.adomain.trg	log	drop		E100B1	inbound	udp	in.addr-arpa.com	8.8.8.255
11079	7-Apr-00	16:34:20	uriel.adomain.trg	log	drop		E100B1	inbound	udp	in.addr-arpa.com	8.8.8.255
11080	7-Apr-00	16:34:20	uriel.adomain.trg	log	drop		E100B1	inbound	udp	in.addr-arpa.com	8.8.8.255
11081	7-Apr-00	16:34:20	uriel.adomain.trg	log	drop		E100B1	inbound	udp	in.addr-arpa.com	8.8.8.255

Description:

These detects appeared in the Internet firewall logs from April 7 and 8/2000. The first attack lasted seven minutes. The second attack lasted twenty minutes.

History/Background/Methods:

A classic Smurf attack. This is an obvious attempt to use the 8.8.8.0 class C ip subnet to attack the hosts viktor.ld.ttu.ee and in.addr-arpa.com with the intention of causing a denial of service

by icmp echo-reply flooding. The 8.8.8.0 subnet is being utilized as a SMURF amplifier in both instances. All packets were dropped at the firewall.

Threat: High Severity: Low

Subsequent Action: None. Due to previous Smurf activity at this site, all ICMP traffic is being dropped at the Internet firewall.

Detect 10: Host scan using UDP port 9200

```
  4054 7-Apr-00 11:28:57uriel.adomain.trg log  drop  E100B1 inbound udp 139.142.87.16 8.8.10.2
  4055 7-Apr-00 11:28:57uriel.adomain.trg log  drop  E100B1 inbound udp 139.142.87.16 8.8.10.3
  4056 7-Apr-00 11:28:57uriel.adomain.trg log  drop  E100B1 inbound udp 139.142.87.16 8.8.10.4
.
.
.
  4249 7-Apr-00 11:29:03uriel.adomain.trg log  drop  E100B1 inbound udp 139.142.87.16 8.8.10.195
  4250 7-Apr-00 11:29:03uriel.adomain.trg log  drop  E100B1 inbound udp 139.142.87.16 8.8.10.197
  4251 7-Apr-00 11:29:03uriel.adomain.trg log  drop  E100B1 inbound udp 139.142.87.16 8.8.10.198
```

Description:

This detect appeared in the Internet firewall logs from April 7/2000.

History/Background/Methods:

Host scanning. The scan was repeated twice and each IP in three class C IP subnets was hit during each scan.

Threat: Medium Severity: Low

Subsequent Action: ISP informed of the scanning activity.

Last Updated: September 21st, 2017

Upcoming Training

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
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 San Diego 2017	San Diego, CA	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 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 Munich December 2017	Munich, Germany	Dec 04, 2017 - Dec 09, 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 London February 2018	London, United Kingdom	Feb 05, 2018 - Feb 10, 2018	Live Event
SANS Dallas 2018	Dallas, TX	Feb 19, 2018 - Feb 24, 2018	Live Event
SANS Northern VA Spring - Tysons 2018	Tysons, VA	Mar 17, 2018 - Mar 24, 2018	Live Event
SANS Secure Canberra 2018	Canberra, Australia	Mar 19, 2018 - Mar 24, 2018	Live Event
SANS 2018	Orlando, FL	Apr 03, 2018 - Apr 10, 2018	Live Event
SANS Baltimore Spring 2018	Baltimore, MD	Apr 21, 2018 - Apr 28, 2018	Live Event
SANS OnDemand	Online	Anytime	Self Paced
SANS SelfStudy	Books & MP3s Only	Anytime	Self Paced