Global Information Assurance Certification Paper

*** Northcutt, solid piece of work! I enjoyed trace 10, I went to is.secksi.net and there was an apache server installed with no index page, I figured I'd send them a note, then I tried one more, etranz1.flyingcroc.net same thing, but a mis-configured version. Now I hate to leap to conclusions, but this could have something to do with webservers. 88 ***

Jim Edwards
Texas Secretary of State

This is my practical analysis for the GCIA certification. I have changed all my network addresses to my-net. Attacker address have NOT been obscured. All of these traces come from my firewall logs (most were captured in the week I was at the SANS conference).

A few notes about our network. We own 4 class C networks my-net.104 – my-net.107. Our firewall sits between our internal network and the Internet so all these addresses are behind the firewall. We load our firewall logs into an Oracle database every night for easier sorting and analysis.

1.

LOG_DATE	LOG_TIME	ACTION	PROTO	SRC	DST	SERVICE	S_PORT	LEN
21-MAR-2000	09:06:44	drop	udp	rad004070248.radius.teleline.es	my-net.104.255	echo	12549	51
21-MAR-2000	09:06:44	drop	udp	rad004070248.radius.teleline.es	my-net.104.0	echo	60830	51
21-MAR-2000	09:06:44	drop	udp	rad004070248.radius.teleline.es	my-net.105.255	echo	60559	51
21-MAR-2000	09:06:44	drop	udp	rad004070248.radius.teleline.es	my-net.106.0	echo	52288	51
21-MAR-2000	09:06:44	drop	udp	rad004070248.radius.teleline.es	my-net.106.255	echo	49707	51
21-MAR-2000	09:06:44	drop	udp	rad004070248.radius.teleline.es	my-net.105.0	echo	65414	51
21-MAR-2000	10:04:34	drop	udp	rad004070248.radius.teleline.es	my-net.104.255	echo	12549	51
21-MAR-2000	10:04:34	drop	udp	rad004070248.radius.teleline.es	my-net.104.0	echo	60830	51
21-MAR-2000	10:04:34	drop	udp	rad004070248.radius.teleline.es	my-net.105.255	echo	60559	51
21-MAR-2000	10:04:34	drop	udp	rad004070248.radius.teleline.es	my-net.105.0	echo	65414	51
21-MAR-2000	10:04:34	drop	udp	rad004070248.radius.teleline.es	my-net.106.255	echo	49707	51
21-MAR-2000	10:04:34	drop	udp	rad004070248.radius.teleline.es	my-net.106.0	echo	52288	51

Active targeting: All broadcast addresses on 3 of our class C networks

History: None

Technique: The packets definitely look crafted for two reasons. First, they jump all over the place, going up and down in value, in the first block although all 6 packets arrived in the same second, even the ones that come to different broadcast ports on the same network. Second, they repeat in exactly the same order in the second attempt. Non-crafted packets all sent in the same second would have fairly sequential sequence numbers and having that same exact block repeat in the same order an hour later is impossible.

Intent: This is either an attempt to map my network or a denial of service using a spoofed source address. All the traffic goes to the echo port on both the old and new broadcast addresses. In order to try to figure out which it was, I finally tracked down the IP address to an ISP in Madrid, Spain. I tend to think

this is a network mapping attempt since it only happened twice and the resolved name contains a portion of the IP address (213.4.70.248 = 00**4**0**70248**), which seems to be a common practice for dynamic IP assignment. If this were a server that was being attacked, the server would not be using dynamic IP allocation (nearly impossible to reach a server whose address changes). The other clue that this is a network mapping attempt is the they are trying both the 255 and 0 broadcast addresses which suggests they don't know anything about my network and are trying to get more info.

Impact: The overall impact of this attempt was negligible since the packets were dropped by the firewall.

2.

```
LOG_DATE LOG_TIME ACTION PROTO SRC DST LEN ICMP_TYPE ICMP_CODE
26-MAR-2000 04:30:24 drop icmp host213-1-159-176.btinternet.com my-net.104.0   (null) 8 0
26-MAR-2000 04:30:24 drop icmp host213-1-159-176.btinternet.com my-net.104.255 (null) 8 0
26-MAR-2000 04:30:24 drop icmp host213-1-159-176.btinternet.com my-net.105.0   (null) 8 0
26-MAR-2000 04:30:24 drop icmp host213-1-159-176.btinternet.com my-net.105.255 (null) 8 0
26-MAR-2000 04:30:24 drop icmp host213-1-159-176.btinternet.com my-net.106.0   (null) 8 0
26-MAR-2000 04:30:24 drop icmp host213-1-159-176.btinternet.com my-net.106.255 (null) 8 0
```

Active Targeting: Yes

History: None

Technique: This is very similar to #1, it could be either a network mapping attempt or a denial of service attack. These packets are probably not crafted since they contain no. It does look to be scripted since they all arrived in the same second. It also is not a trojan since the packets contain no data, another reason to believe they are not crafted packets.

Intent: Once again, the IP address is included in the resolved name, something common to dynamic IP allocation used by ISP's and this one traced back to an ISP in England. A server would need a dedicated IP address. This is most likely just a network mapping attempt using ping.

Impact: The impact was negligible since the firewall dropped the packets.

3.

```
LOG_DATE LOG_TIME ACTION PROTO SRC DST SERVICE S_PORT LEN
22-MAR-2000 04:19:43 drop tcp bbs.tntnet.co.kr my-net.105.29 domain 2666 40
22-MAR-2000 04:19:43 drop tcp bbs.tntnet.co.kr my-net.105.30 domain 2666 40
22-MAR-2000 04:19:43 drop tcp bbs.tntnet.co.kr my-net.105.31 domain 2666 40
22-MAR-2000 04:19:43 drop tcp bbs.tntnet.co.kr my-net.105.32 domain 2666 40
22-MAR-2000 04:19:43 drop tcp bbs.tntnet.co.kr my-net.105.33 domain 2666 40
22-MAR-2000 04:19:43 drop tcp bbs.tntnet.co.kr my-net.105.34 domain 2666 40
```

```
22-MAR-2000 04:19:43 drop tcp bbs.tntnet.co.kr my-net.105.35 domain 2666 40
22-MAR-2000 04:19:43 drop tcp bbs.tntnet.co.kr my-net.105.36 domain 2666 40
22-MAR-2000 04:19:43 drop tcp bbs.tntnet.co.kr my-net.105.37 domain 2666 40
22-MAR-2000 04:19:43 drop tcp bbs.tntnet.co.kr my-net.105.38 domain 2666 40
22-MAR-2000 04:19:43 drop tcp bbs.tntnet.co.kr my-net.105.39 domain 2666 40
22-MAR-2000 04:19:43 drop tcp bbs.tntnet.co.kr my-net.105.40 domain 2666 40
22-MAR-2000 04:19:43 drop tcp bbs.tntnet.co.kr my-net.105.41 domain 2666 40
22-MAR-2000 04:19:43 drop tcp bbs.tntnet.co.kr my-net.105.42 domain 2666 40
22-MAR-2000 04:19:43 drop tcp bbs.tntnet.co.kr my-net.105.43 domain 2666 40
22-MAR-2000 04:19:43 drop tcp bbs.tntnet.co.kr my-net.105.44 domain 2666 40
22-MAR-2000 04:19:43 drop tcp bbs.tntnet.co.kr my-net.105.45 domain 2666 40
22-MAR-2000 04:19:43 drop tcp bbs.tntnet.co.kr my-net.105.46 domain 2666 40
22-MAR-2000 04:19:43 drop tcp bbs.tntnet.co.kr my-net.105.50 domain 2666 40
22-MAR-2000 04:19:43 drop tcp bbs.tntnet.co.kr my-net.105.54 domain 2666 40
22-MAR-2000 04:19:43 drop tcp bbs.tntnet.co.kr my-net.105.59 domain 2666 40
22-MAR-2000 04:19:43 drop tcp bbs.tntnet.co.kr my-net.105.63 domain 2666 40
22-MAR-2000 04:19:43 drop tcp bbs.tntnet.co.kr my-net.105.68 domain 2666 40
22-MAR-2000 04:19:43 drop tcp bbs.tntnet.co.kr my-net.105.72 domain 2666 40
22-MAR-2000 04:19:43 drop tcp bbs.tntnet.co.kr my-net.105.76 domain 2666 40
22-MAR-2000 04:19:43 drop tcp bbs.tntnet.co.kr my-net.105.80 domain 2666 40
22-MAR-2000 04:19:43 drop tcp bbs.tntnet.co.kr my-net.105.83 domain 2666 40
22-MAR-2000 04:19:43 drop tcp bbs.tntnet.co.kr my-net.105.84 domain 2666 40
22-MAR-2000 04:19:43 drop tcp bbs.tntnet.co.kr my-net.105.86 domain 2666 40
22-MAR-2000 04:19:43 drop tcp bbs.tntnet.co.kr my-net.105.91 domain 2666 40
22-MAR-2000 04:19:43 drop tcp bbs.tntnet.co.kr my-net.105.96 domain 2666 40

<snip>

22-MAR-2000 04:19:43 drop tcp bbs.tntnet.co.kr my-net.105.156 domain 2666 40
22-MAR-2000 04:19:43 drop tcp bbs.tntnet.co.kr my-net.105.183 domain 2666 40
22-MAR-2000 04:19:43 drop tcp bbs.tntnet.co.kr my-net.105.185 domain 2666 40
22-MAR-2000 04:19:43 drop tcp bbs.tntnet.co.kr my-net.105.214 domain 2666 40
22-MAR-2000 04:19:43 drop tcp bbs.tntnet.co.kr my-net.105.218 domain 2666 40
22-MAR-2000 04:19:43 drop tcp bbs.tntnet.co.kr my-net.105.226 domain 2666 40
22-MAR-2000 04:19:43 drop tcp bbs.tntnet.co.kr my-net.105.229 domain 2666 40
22-MAR-2000 04:19:43 drop tcp bbs.tntnet.co.kr my-net.105.244 domain 2666 40
```

Active targeting: Although packets to only 60 addresses in one of our class C networks were actualyy received, I believe this whole network was targeted

History: None

Technique: This is part of a total of 60 packets we got during this attempt. 203.251.180.252 is the IP address this came from and it belongs to something called Sechang in Seoul Korea. The packets appear crafted and scripted since the source port repeats itself and we got over 60 packets in the same second.

It also seems to be coming from either a slow machine or one with a rather slow internet connection. This assumption is based on the fact that the destination addresses start out in sequence and then begin to skip over whole blocks of addresses, as if the sending machine or network got bogged down by the traffic it was trying to send. This get more and more pronounced as they get to the higher numbers.

Intent: This appears to be an attempt to do a DNS zone transfer.

Impact: The impact is negligible since all of the packets got dropped by the firewall.

4.

```
LOG_DATE LOG_TIME ACTION PROTO SRC DST SERVICE S_PORT LEN
24-MAR-2000 06:26:28 drop tcp g08.cna.ne.jp my-net.104.1 domain domain 40
24-MAR-2000 06:26:28 drop tcp g08.cna.ne.jp my-net.104.2 domain domain 40
24-MAR-2000 06:26:28 drop tcp g08.cna.ne.jp my-net.104.3 domain domain 40
24-MAR-2000 06:26:28 drop tcp g08.cna.ne.jp my-net.104.4 domain domain 40
24-MAR-2000 06:26:28 drop tcp g08.cna.ne.jp my-net.104.5 domain domain 40
24-MAR-2000 06:26:28 drop tcp g08.cna.ne.jp my-net.104.6 domain domain 40
24-MAR-2000 06:26:28 drop tcp g08.cna.ne.jp my-net.104.7 domain domain 40
24-MAR-2000 06:26:28 drop tcp g08.cna.ne.jp my-net.104.8 domain domain 40
24-MAR-2000 06:26:28 drop tcp g08.cna.ne.jp my-net.104.9 domain domain 40
24-MAR-2000 06:26:28 drop tcp g08.cna.ne.jp my-net.104.10 domain domain 40
24-MAR-2000 06:26:28 drop tcp g08.cna.ne.jp my-net.104.11 domain domain 40
24-MAR-2000 06:26:28 drop tcp g08.cna.ne.jp my-net.104.12 domain domain 40
24-MAR-2000 06:26:28 drop tcp g08.cna.ne.jp my-net.104.13 domain domain 40
24-MAR-2000 06:26:28 drop tcp g08.cna.ne.jp my-net.104.14 domain domain 40
24-MAR-2000 06:26:28 accept tcp g08.cna.ne.jp my-net.104.15 domain domain 40
24-MAR-2000 06:26:28 drop tcp g08.cna.ne.jp my-net.104.16 domain domain 40
24-MAR-2000 06:26:28 drop tcp g08.cna.ne.jp my-net.104.17 domain domain 40
24-MAR-2000 06:26:28 drop tcp g08.cna.ne.jp my-net.104.18 domain domain 40
24-MAR-2000 06:26:28 drop tcp g08.cna.ne.jp my-net.104.19 domain domain 40
24-MAR-2000 06:26:28 drop tcp g08.cna.ne.jp my-net.104.20 domain domain 40
24-MAR-2000 06:26:28 drop tcp g08.cna.ne.jp my-net.104.21 domain domain 40
24-MAR-2000 06:26:28 drop tcp g08.cna.ne.jp my-net.104.22 domain domain 40
24-MAR-2000 06:26:28 drop tcp g08.cna.ne.jp my-net.104.23 domain domain 40
24-MAR-2000 06:26:28 drop tcp g08.cna.ne.jp my-net.104.24 domain domain 40
24-MAR-2000 06:26:28 drop tcp g08.cna.ne.jp my-net.104.25 domain domain 40
24-MAR-2000 06:26:28 drop tcp g08.cna.ne.jp my-net.104.26 domain domain 40
24-MAR-2000 06:26:28 drop tcp g08.cna.ne.jp my-net.104.27 domain domain 40
24-MAR-2000 06:26:28 drop tcp g08.cna.ne.jp my-net.104.28 domain domain 40
24-MAR-2000 06:26:28 drop tcp g08.cna.ne.jp my-net.104.29 domain domain 40
24-MAR-2000 06:26:28 drop tcp g08.cna.ne.jp my-net.104.30 domain domain 40
24-MAR-2000 06:26:28 drop tcp g08.cna.ne.jp my-net.104.31 domain domain 40
24-MAR-2000 06:26:28 drop tcp g08.cna.ne.jp my-net.104.32 domain domain 40
24-MAR-2000 06:26:28 drop tcp g08.cna.ne.jp my-net.104.33 domain domain 40
```

```
24-MAR-2000 06:26:28 drop tcp g08.cna.ne.jp my-net.104.34 domain domain 40
24-MAR-2000 06:26:28 drop tcp g08.cna.ne.jp my-net.104.35 domain domain 40
24-MAR-2000 06:26:28 drop tcp g08.cna.ne.jp my-net.104.36 domain domain 40
24-MAR-2000 06:26:29 drop tcp g08.cna.ne.jp my-net.104.37 domain domain 40
24-MAR-2000 06:26:29 drop tcp g08.cna.ne.jp my-net.104.38 domain domain 40
24-MAR-2000 06:26:29 accept tcp g08.cna.ne.jp my-net.104.15 domain 20605 44
24-MAR-2000 06:26:29 drop tcp g08.cna.ne.jp my-net.104.39 domain domain 40
24-MAR-2000 06:26:29 drop tcp g08.cna.ne.jp my-net.104.40 domain domain 40
24-MAR-2000 06:26:29 drop tcp g08.cna.ne.jp my-net.104.41 domain domain 40
24-MAR-2000 06:26:29 drop tcp g08.cna.ne.jp my-net.104.42 domain domain 40
24-MAR-2000 06:26:29 drop tcp g08.cna.ne.jp my-net.104.43 domain domain 40
24-MAR-2000 06:26:29 drop tcp g08.cna.ne.jp my-net.104.44 domain domain 40
24-MAR-2000 06:26:29 drop tcp g08.cna.ne.jp my-net.104.45 domain domain 40
24-MAR-2000 06:26:29 drop tcp g08.cna.ne.jp my-net.104.46 domain domain 40
24-MAR-2000 06:26:29 drop tcp g08.cna.ne.jp my-net.104.47 domain domain 40
24-MAR-2000 06:26:29 drop tcp g08.cna.ne.jp my-net.104.48 domain domain 40
24-MAR-2000 06:26:29 drop tcp g08.cna.ne.jp my-net.104.49 domain domain 40
24-MAR-2000 06:26:29 drop tcp g08.cna.ne.jp my-net.104.50 domain domain 40
24-MAR-2000 06:26:29 accept udp g08.cna.ne.jp my-net.104.15 domain-udp 1126 55
24-MAR-2000 06:26:29 drop tcp g08.cna.ne.jp my-net.104.51 domain domain 40
 <snip>
```

Active targeting: Every address in three of our class C networks was targeted

History: None

Technique: The attacker scanned every single address in three of our class c address spaces trying to do a zone transfer. When he hit our DNS server, the zone transfer succeeded. The packets look to be crafted since every single one has the same source port but the interesting thing about this scan is the behavior after a transfer is successful. This seems to be generated by a pretty sophisticated program that can detect a success since it then reconnects and does another zone transfer (TCP) and a regular inquiry (UDP) from different source ports with different payloads. These secondary targeted scans may not be crafted since the source port is different thant the original scan and is varied.

Intent: This is a DNS zone transfer scan.

Impact: The impact of this was moderate since the attacker downloaded our entire DNS data. We have now blocked zone transfers.

5.

```
NUM LOG_DATE LOG_TIME ACTION PROTO SRC DST SERVICE S_PORT LEN
119344 27-MAR-2000 17:38:14 drop tcp 210.92.35.5 my-net.106.220 635 1563 60
119342 27-MAR-2000 17:38:14 drop tcp 210.92.35.5 my-net.106.221 635 1564 60
119343 27-MAR-2000 17:38:14 drop tcp 210.92.35.5 my-net.106.222 635 1565 60
119345 27-MAR-2000 17:38:14 drop tcp 210.92.35.5 my-net.106.223 635 1566 60
```

```
119346 27-MAR-2000 17:38:14 drop tcp 210.92.35.5 my-net.106.224 635 1567 60
119348 27-MAR-2000 17:38:14 drop tcp 210.92.35.5 my-net.106.225 635 1568 60
119347 27-MAR-2000 17:38:14 drop tcp 210.92.35.5 my-net.106.226 635 1569 60
119349 27-MAR-2000 17:38:14 drop tcp 210.92.35.5 my-net.106.227 635 1570 60
119374 27-MAR-2000 17:38:17 drop tcp 210.92.35.5 my-net.106.228 635 1571 60
119350 27-MAR-2000 17:38:14 drop tcp 210.92.35.5 my-net.106.229 635 1572 60
119373 27-MAR-2000 17:38:17 drop tcp 210.92.35.5 my-net.106.230 635 1573 60
119375 27-MAR-2000 17:38:17 drop tcp 210.92.35.5 my-net.106.231 635 1574 60
119376 27-MAR-2000 17:38:17 drop tcp 210.92.35.5 my-net.106.232 635 1575 60
119351 27-MAR-2000 17:38:14 drop tcp 210.92.35.5 my-net.106.233 635 1576 60
119377 27-MAR-2000 17:38:17 drop tcp 210.92.35.5 my-net.106.234 635 1577 60
119378 27-MAR-2000 17:38:17 drop tcp 210.92.35.5 my-net.106.235 635 1578 60
119381 27-MAR-2000 17:38:17 drop tcp 210.92.35.5 my-net.106.236 635 1579 60
119352 27-MAR-2000 17:38:14 drop tcp 210.92.35.5 my-net.106.237 635 1580 60
119379 27-MAR-2000 17:38:17 drop tcp 210.92.35.5 my-net.106.239 635 1582 60
119354 27-MAR-2000 17:38:14 drop tcp 210.92.35.5 my-net.106.240 635 1583 60
119380 27-MAR-2000 17:38:17 drop tcp 210.92.35.5 my-net.106.242 635 1585 60
119353 27-MAR-2000 17:38:14 drop tcp 210.92.35.5 my-net.106.244 635 1587 60
119382 27-MAR-2000 17:38:17 drop tcp 210.92.35.5 my-net.106.245 635 1588 60
119355 27-MAR-2000 17:38:14 drop tcp 210.92.35.5 my-net.106.247 635 1590 60
119383 27-MAR-2000 17:38:17 drop tcp 210.92.35.5 my-net.106.249 635 1592 60
119356 27-MAR-2000 17:38:14 drop tcp 210.92.35.5 my-net.106.251 635 1594 60
<snip>
```

Active targeting: One class C network

History: None

Technique: These packets are probably not crafted since the source ports are all in order and even when they skip numbers, the same amount is skipped on the destination address, suggesting a slow network or originating computer. There is also a high number of missing packets, based on the source port numbers, also suggesting a slow computer or slow network. Another interesting thing about this scan is the order the packets came in. Looking at the log numbers and the arrival times, they arrived seriously out of order suggesting a lot of hops and reroutes. This IP address belongs to the Korea NIC so based on that previous statement, they are probably not spoofed.

Intent: This is a scan of TCP port 635, NFS.

Impact: The impact was negligible since the firewall dropped all the packets.

6.

```
NUM LOG_DATE LOG_TIME ACTION PROTO SRC DST SERVICE S_PORT LEN
<snip>
25744 22-MAR-2000 09:04:59 drop tcp olkck006228.netvigator.com my-net.104.41 1243 1086 48
25751 22-MAR-2000 09:05:01 drop tcp olkck006228.netvigator.com my-net.104.61 1243 1106 48
```

```
25753 22-MAR-2000 09:05:01 drop tcp olkck006228.netvigator.com my-net.104.63 1243 1108 48
25754 22-MAR-2000 09:05:01 drop tcp olkck006228.netvigator.com my-net.104.62 1243 1107 48
25755 22-MAR-2000 09:05:01 drop tcp olkck006228.netvigator.com my-net.104.64 1243 1109 48
25756 22-MAR-2000 09:05:01 drop tcp olkck006228.netvigator.com my-net.104.65 1243 1110 48
25757 22-MAR-2000 09:05:01 drop tcp olkck006228.netvigator.com my-net.104.66 1243 1111 48
25758 22-MAR-2000 09:05:01 drop tcp olkck006228.netvigator.com my-net.104.68 1243 1113 48
25759 22-MAR-2000 09:05:01 drop tcp olkck006228.netvigator.com my-net.104.67 1243 1112 48
25760 22-MAR-2000 09:05:01 drop tcp olkck006228.netvigator.com my-net.104.69 1243 1114 48
25761 22-MAR-2000 09:05:01 drop tcp olkck006228.netvigator.com my-net.104.71 1243 1116 48
25762 22-MAR-2000 09:05:01 drop tcp olkck006228.netvigator.com my-net.104.72 1243 1117 48
25763 22-MAR-2000 09:05:01 drop tcp olkck006228.netvigator.com my-net.104.70 1243 1115 48
25764 22-MAR-2000 09:05:01 drop tcp olkck006228.netvigator.com my-net.104.73 1243 1118 48
25765 22-MAR-2000 09:05:01 drop tcp olkck006228.netvigator.com my-net.104.75 1243 1120 48
25766 22-MAR-2000 09:05:01 drop tcp olkck006228.netvigator.com my-net.104.77 1243 1122 48
25767 22-MAR-2000 09:05:01 drop tcp olkck006228.netvigator.com my-net.104.74 1243 1119 48
25768 22-MAR-2000 09:05:01 drop tcp olkck006228.netvigator.com my-net.104.76 1243 1121 48
25769 22-MAR-2000 09:05:01 drop tcp olkck006228.netvigator.com my-net.104.80 1243 1125 48
25770 22-MAR-2000 09:05:01 drop tcp olkck006228.netvigator.com my-net.104.79 1243 1124 48
25771 22-MAR-2000 09:05:01 drop tcp olkck006228.netvigator.com my-net.104.78 1243 1123 48
25772 22-MAR-2000 09:05:01 drop tcp olkck006228.netvigator.com my-net.104.82 1243 1127 48
25773 22-MAR-2000 09:05:01 drop tcp olkck006228.netvigator.com my-net.104.81 1243 1126 48
25774 22-MAR-2000 09:05:01 drop tcp olkck006228.netvigator.com my-net.104.83 1243 1128 48
25775 22-MAR-2000 09:05:01 drop tcp olkck006228.netvigator.com my-net.104.84 1243 1129 48
25776 22-MAR-2000 09:05:01 drop tcp olkck006228.netvigator.com my-net.104.85 1243 1130 48
25777 22-MAR-2000 09:05:01 drop tcp olkck006228.netvigator.com my-net.104.87 1243 1132 48
25778 22-MAR-2000 09:05:01 drop tcp olkck006228.netvigator.com my-net.104.86 1243 1131 48
25779 22-MAR-2000 09:05:01 drop tcp olkck006228.netvigator.com my-net.104.88 1243 1133 48
25780 22-MAR-2000 09:05:01 drop tcp olkck006228.netvigator.com my-net.104.89 1243 1134 48
25781 22-MAR-2000 09:05:01 drop tcp olkck006228.netvigator.com my-net.104.90 1243 1135 48
25782 22-MAR-2000 09:05:01 drop tcp olkck006228.netvigator.com my-net.104.91 1243 1136 48
<snip>
```

Active Targeting: This attacker scanned almost every address in 3 of my class C networks.

Technique: This attacker scanned almost every address in 3 of my class networks in less than 2 minutes suggesting that this is a scripted scan. The source ports are correctly sequenced and those that are not are matched exactly with the same order of the destination address so these are probably not crafted packets. This address is owned by Hong Kong Telecom and is part of the block 208.167.224.0 - 208.167.255.255. This seems to be a dynamically assigned address since part of the address is reversed and included in the name (006228 = 208.167.**228.6**). A dynamically assigned address would not normally be a server. Also, the packets sometimes came in a different order than they were apparently sent, also suggesting a long time in transit with a lot of hops and reroutes. This is consistent with the Hong Kong location and suggests the address is not spoofed.

Impact: The impact of this was negligible since the firewall dropped all the packets.

Intent: This is a scan for the Sun 7.2 trojan.

7.

NUM	LOG_DATE	LOG_TIME	ACTION	PROTO	SRC	DST	SERVICE	LEN	ICMP_TYPE	ICMP_CODE
127223	30-MAR-2000	20:01:32	drop	icmp	spoof.100	my-net.104.0	(null)	8	0	
127224	30-MAR-2000	20:01:32	drop	icmp	spoof.100	my-net.104.8	(null)	8	0	
127225	30-MAR-2000	20:01:32	drop	icmp	spoof.100	my-net.104.63	(null)	8	0	
127226	30-MAR-2000	20:01:32	drop	icmp	spoof.100	my-net.104.64	(null)	8	0	
127227	30-MAR-2000	20:01:32	drop	icmp	spoof.100	my-net.104.127	(null)	8	0	
127228	30-MAR-2000	20:01:32	drop	icmp	spoof.100	my-net.104.128	(null)	8	0	
127229	30-MAR-2000	20:01:32	drop	icmp	spoof.100	my-net.104.191	(null)	8	0	
127230	30-MAR-2000	20:01:32	drop	icmp	spoof.100	my-net.104.192	(null)	8	0	
127231	30-MAR-2000	20:01:32	drop	icmp	spoof.100	my-net.104.254	(null)	8	0	
127232	30-MAR-2000	20:01:32	drop	icmp	spoof.100	my-net.104.255	(null)	8	0	
127233	30-MAR-2000	20:01:32	drop	icmp	spoof.100	my-net.105.0	(null)	8	0	
127234	30-MAR-2000	20:01:32	drop	icmp	spoof.100	my-net.105.8	(null)	8	0	
127235	30-MAR-2000	20:01:32	drop	icmp	spoof.100	my-net.105.63	(null)	8	0	
127236	30-MAR-2000	20:01:32	drop	icmp	spoof.100	my-net.105.64	(null)	8	0	
127237	30-MAR-2000	20:01:32	drop	icmp	spoof.100	my-net.105.127	(null)	8	0	
127238	30-MAR-2000	20:01:32	drop	icmp	spoof.100	my-net.105.128	(null)	8	0	
127239	30-MAR-2000	20:01:32	drop	icmp	spoof.100	my-net.105.191	(null)	8	0	
127240	30-MAR-2000	20:01:32	drop	icmp	spoof.100	my-net.105.192	(null)	8	0	
127241	30-MAR-2000	20:01:32	drop	icmp	spoof.100	my-net.105.254	(null)	8	0	
127242	30-MAR-2000	20:01:32	drop	icmp	spoof.100	my-net.105.255	(null)	8	0	
127243	30-MAR-2000	20:01:32	drop	icmp	spoof.100	my-net.106.0	(null)	8	0	
127244	30-MAR-2000	20:01:32	drop	icmp	spoof.100	my-net.106.8	(null)	8	0	
127245	30-MAR-2000	20:01:32	drop	icmp	spoof.100	my-net.106.63	(null)	8	0	
127246	30-MAR-2000	20:01:32	drop	icmp	spoof.100	my-net.106.64	(null)	8	0	
127247	30-MAR-2000	20:01:32	drop	icmp	spoof.100	my-net.106.127	(null)	8	0	
127248	30-MAR-2000	20:01:32	drop	icmp	spoof.100	my-net.106.128	(null)	8	0	
127249	30-MAR-2000	20:01:32	drop	icmp	spoof.100	my-net.106.191	(null)	8	0	
127250	30-MAR-2000	20:01:32	drop	icmp	spoof.100	my-net.106.192	(null)	8	0	
127251	30-MAR-2000	20:01:32	drop	icmp	spoof.100	my-net.106.254	(null)	8	0	
127252	30-MAR-2000	20:01:32	drop	icmp	spoof.100	my-net.106.255	(null)	8	0	
127253	30-MAR-2000	20:01:32	drop	icmp	spoof.100	my-net.107.0	(null)	8	0	
127254	30-MAR-2000	20:01:32	drop	icmp	spoof.100	my-net.107.8	(null)	8	0	
127255	30-MAR-2000	20:01:32	drop	icmp	spoof.100	my-net.107.63	(null)	8	0	
127256	30-MAR-2000	20:01:32	drop	icmp	spoof.100	my-net.107.64	(null)	8	0	
127257	30-MAR-2000	20:01:32	drop	icmp	spoof.100	my-net.107.127	(null)	8	0	
127258	30-MAR-2000	20:01:32	drop	icmp	spoof.100	my-net.107.128	(null)	8	0	
127259	30-MAR-2000	20:01:32	drop	icmp	spoof.100	my-net.107.191	(null)	8	0	
127260	30-MAR-2000	20:01:32	drop	icmp	spoof.100	my-net.107.192	(null)	8	0	
127261	30-MAR-2000	20:01:32	drop	icmp	spoof.100	my-net.107.254	(null)	8	0	
127262	30-MAR-2000	20:01:32	drop	icmp	spoof.100	my-net.107.255	(null)	8	0	

NOTE: I obscured the source address of this one since he seems to be a victim as well.

Active Targeting: All common subnet broadcast addresses in all four of my class C networks.

History: We have not seen traffic from this address before but quite regularly get traffic from Korean networks.

Technique: The attacker made sure to hit the more common subnet broadcast addresses on both the old BSD low broadcast address and the newer high broadcast address. This is most likely a scripted attack since they came very fast, all 40 packets arriving in the same second and seemingly in the same order they were sent (based on the numerical sequence of the destination addresses). I am at a loss to explain the purpose of the packets to the .8 addresses.

Intent: This could either be a network mapping attempt or a Smurf attack on spoof.100. The tight time frame and correct order that these packets arrived is somewhat strange since the source address is in Korea and other scans from Korea have arrived in somewhat of a jumbled fashion. This makes me think that the source address is spoofed and that this is a Smurf attack. I tried connecting with a web browser and got the default Apache index.html page where it claims it is a Red Hat Linux box running Apache. I also tried telneting to it and it quite pleasantly identified itself as part of a network belonging to "Boramae Cache Framework" and once again identified itself as a Red Hat box. The Korea NIC identifies this address block as belonging to Yangpyong Middle School. I tried contacting the person listed as the point of contact but have not gotten a response. The bottom line is that the evidence points to a Smurf attack on spoof.100 but there is not enough data to say conclusively.

Impact: The impact is negligible since the firewall blocked all the packets.

8.

```
LOG_DATE LOG_TIME ACTION PROTO SRC DST SERVICE S_PORT LEN
<snip>
03-APR-2000 20:27:09 drop tcp 194.78.174.5 my-net.106.0 3128 36055 44
03-APR-2000 20:27:09 drop tcp 194.78.174.5 my-net.106.1 3128 36056 44
03-APR-2000 20:27:09 drop tcp 194.78.174.5 my-net.106.2 3128 36057 44
03-APR-2000 20:27:09 drop tcp 194.78.174.5 my-net.106.3 3128 36058 44
03-APR-2000 20:27:09 drop tcp 194.78.174.5 my-net.106.4 3128 36059 44
03-APR-2000 20:27:12 drop tcp 194.78.174.5 my-net.106.5 3128 36089 40
03-APR-2000 20:27:10 drop tcp 194.78.174.5 my-net.106.6 3128 36090 44
03-APR-2000 20:27:12 drop tcp 194.78.174.5 my-net.106.7 3128 36091 40
03-APR-2000 20:27:12 drop tcp 194.78.174.5 my-net.106.8 3128 36092 40
03-APR-2000 20:27:10 drop tcp 194.78.174.5 my-net.106.9 3128 36093 44
03-APR-2000 20:27:12 drop tcp 194.78.174.5 my-net.106.10 3128 36094 40
<snip>
```

Active Targeting: Yes

History: None.

Technique: Just a straight-forward scripted scan of all machines in our 4 class C networks (this is a small segment of the entire scan). The sequence numbers are in numerical order even though there are some blocks of skipped numbers, suggesting that the attacking machine was either sending or receiving other traffic at the same time the scan was running. This IP address belongs to a small network in Belgium and this corresponds to the fact that the packets arrived somewhat out of order so the address is probably not spoofed.

Intent: Scanning for a Squid server

Impact: The impact is negligible since the firewall blocked all the packets.

9.

```
NUM LOG_DATE LOG_TIME ACTION PROTO SRC DST SERVICE S_PORT LEN
<snip>
39567 03-MAR-2000 10:27:26 drop tcp pulsar.sao.arizona.edu my-net.106.146 pop-2 65535 40
39568 03-MAR-2000 10:27:26 drop tcp pulsar.sao.arizona.edu my-net.106.143 pop-2 65535 40
39569 03-MAR-2000 10:27:26 drop tcp pulsar.sao.arizona.edu my-net.106.151 pop-2 65535 40
39570 03-MAR-2000 10:27:26 drop tcp pulsar.sao.arizona.edu my-net.106.32 pop-2 65535 40
39571 03-MAR-2000 10:27:26 drop tcp pulsar.sao.arizona.edu my-net.106.35 pop-2 65535 40
39572 03-MAR-2000 10:27:26 drop tcp pulsar.sao.arizona.edu my-net.105.67 pop-2 65535 40
39573 03-MAR-2000 10:27:26 drop tcp pulsar.sao.arizona.edu my-net.106.154 pop-2 65535 40
39574 03-MAR-2000 10:27:26 drop tcp pulsar.sao.arizona.edu my-net.106.156 pop-2 65535 40
39575 03-MAR-2000 10:27:26 drop tcp pulsar.sao.arizona.edu my-net.105.69 pop-2 65535 40
39576 03-MAR-2000 10:27:26 drop tcp pulsar.sao.arizona.edu my-net.105.72 pop-2 65535 40
39577 03-MAR-2000 10:27:26 drop tcp pulsar.sao.arizona.edu my-net.105.79 pop-2 65535 40
```

<snip>

Active Targeting: Yes

History: None.

Technique: This looks like a scripted attack since we received over 400 packets in 2 seconds. The packets are also crafted since all of the source ports are set to 65535.

Intent: Scanning for a pop-2 server

Impact: The impact is negligible since the firewall blocked all the packets

10.

(sort 1)

LOG_DATE	LOG_TIME	ACTION	PROTO	SRC	DST	SERVICE	S_PORT	LEN
04-APR-2000	00:54:58	drop	tcp	etranz1.flyingcroc.net	my-net.107.84		9853	10943 40
31-MAR-2000	02:43:42	drop	tcp	209.247.108.212	my-net.107.9		4312	11230 40
04-APR-2000	19:33:31	drop	tcp	210.92.121.162	my-net.107.1		55775	11949 40
04-APR-2000	21:23:40	drop	tcp	210.92.121.162	my-net.107.1		55775	11949 40
02-APR-2000	03:25:08	drop	tcp	208.51.159.10	my-net.107.14		18538	12033 40
31-MAR-2000	01:50:16	drop	tcp	netcom5.netcom.com	my-net.107.53		61549	12084 40
04-APR-2000	09:28:28	drop	tcp	dialup-unix.rapidenet.net	my-net.107.149		8137	12545 40
03-APR-2000	20:43:41	drop	tcp	200.192.57.42	my-net.107.124		41207	133 40
04-APR-2000	18:12:12	drop	tcp	monet.telebyte.nl	my-net.107.192		58757	13543 40
30-MAR-2000	19:47:10	drop	tcp	216.181.39.5	my-net.107.89		63414	**13678** 40
03-APR-2000	22:32:26	drop	tcp	ahhhh.uhhhhhh.uhhhhh.ahhhhhh.com	my-net.107.89		63411	**13678** 40
02-APR-2000	03:31:41	drop	tcp	216.33.187.17	my-net.107.245		3811	**16163** 40
31-MAR-2000	16:45:40	drop	tcp	209.163.42.235	my-net.107.245		6371	**16163** 40
02-APR-2000	00:23:33	drop	tcp	elite.cyberphreak.net	my-net.107.21		8724	16344 40
30-MAR-2000	15:49:42	drop	tcp	atlanta.ga.us.undernet.org	my-net.107.246		19021	16994 40
30-MAR-2000	18:55:49	drop	tcp	211.40.177.75	my-net.107.246		53581	16995 40
31-MAR-2000	11:08:27	drop	tcp	w1.yahoo.com	my-net.107.65		55226	17478 40
01-APR-2000	17:16:35	drop	tcp	sexhead.org	my-net.107.38		43369	19289 40
02-APR-2000	12:59:05	drop	tcp	is.secksi.net	my-net.107.73		62811	20025 40
02-APR-2000	16:16:37	drop	tcp	webqual.com	my-net.107.83		57356	20911 40

(sort 2)

LOG_DATE	LOG_TIME	ACTION	PROTO	SRC	DST	SERVICE	S_PORT	LEN
01-APR-2000	17:11:01	drop	tcp	sexhead.org	my-net.106.29		41132	6134 40
01-APR-2000	17:13:10	drop	tcp	sexhead.org	my-net.104.29		27757	60852 40
01-APR-2000	17:15:37	drop	tcp	sexhead.org	my-net.106.51		63093	62818 40
01-APR-2000	17:16:35	drop	tcp	sexhead.org	my-net.107.38		43369	19289 40
01-APR-2000	17:24:06	drop	tcp	sexhead.org	my-net.106.11		6213	44373 40
01-APR-2000	17:24:15	drop	tcp	sexhead.org	my-net.105.119		18516	28134 40
01-APR-2000	17:27:28	drop	tcp	sexhead.org	my-net.104.85		22673	20375 40
02-APR-2000	18:01:32	drop	tcp	sexhead.org	my-net.104.111		32550	30767 40
02-APR-2000	18:01:44	drop	tcp	sexhead.org	my-net.107.70		26914	31510 40
02-APR-2000	18:07:35	drop	tcp	sexhead.org	my-net.104.20		64422	62339 40
02-APR-2000	18:28:50	drop	tcp	sexhead.org	my-net.107.37		9302	42953 40
02-APR-2000	18:30:54	drop	tcp	sexhead.org	my-net.107.94		19619	24584 40
02-APR-2000	18:32:11	drop	tcp	sexhead.org	my-net.107.29		48771	39404 40
02-APR-2000	18:34:20	drop	tcp	sexhead.org	my-net.107.7		59582	30449 40

Active Targeting: Yes

History: This started on 31 Mar 2000 and has been going on for several days so far.

Technique: The actual attackers address seem to be hidden within a large amount of spoofed addresses. They are using a low and slow scripted scan to try to probe our network. See comments below for more info on how I came to this conclusion and why I believe this is a directed scan and not just spurious traffic. The traffic I included is general traffic to all my network and specific traffic coming from one of the spoofed addresses.

Intent: This seems to be a scan of some kind although I have not been able to find any commonly scanned ports or trojans.

Impact: The impact is negligible since the firewall blocked all the packets.

Comments: This one is kind of iffy and took me several hours to work out. I had started seeing a lot of spurious traffic to an inactive network. We have one Class C (ny-net.107) that we use for small subnets and special networks, almost all of which are totally in-house and do not connect to the Internet. No PC has ever been assigned these IP addresses. When traffic started showing up, it raised a red flag and then I saw traffic from sexhead.org. Being in an agency that is sensitive to such activity, I immediately checked to see if any outgoing traffic to this site was present and it was not. I even checked all outgoing traffic to the network it belongs to and none showed up. Since we put all our firewall logs in an Oracle database every night, sorting and searching is very easy so I pulled all the traffic from sexhead and found exactly seven packets on two different days, all with non-existent ports, all exactly 40 bytes in length (see sort 2). There was also the fact that the .29 address to 3 different networks showed up which made me think more that this was not just spurious traffic. My first conclusion was that this machine was scanning us for existing networks. While I was working this, however, I noticed several other bits of similar traffic, once again to this non-existent network as well as my active networks. The more I looked the more I found, all seemingly starting on Mar 31st, there was very little of this kind of traffic before then. I eventually was able to sort out some of the activity to the 107 network and sorted it by source port and found something very interesting. There was some traffic to the same IP address, using the same source port but from completely different source addresses on different days. The chances of this happening randomly to a non-existent network is nearly impossible (see sort 1). There were also a few records that matched exactly except for the time. It is very difficult to separate the wheat from the chaff in this case so some of this traffic may not be a part of this scan but what little evidence I have leads me to believe that this is a direct attempt at network mapping or searching for some trojan. I have, unfortunately, not been able to determine exactly which since neither the destination or source ports match to anything known.