



# Global Information Assurance Certification Paper

Copyright SANS Institute  
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permitted without express written permission.

## Interested in learning more?

Check out the list of upcoming events offering  
"Intrusion Detection In-Depth (Security 503)"  
at <http://www.giac.org/registration/gcia>

\*\*\* Northcutt, interesting work, I particularly enjoyed the snmp write, I have always expected to see this, but haven't before: 10 point bonus. Some good detective work, better understanding of history than most student analysts. 86 \*

Tomas Halvarsson  
10 analyzed detects from Tomas Halvarsson, SANS 2000 IDIC track  
Submitted Saturday April 22nd, 2000.

All IP and MAC addresses have been altered to protect the innocent. :)  
The 192.168.x.y networks are "mine", 0.x.x.x networks are hostile.

=====  
Detect #1, from Snort logs:  
-----

```
Apr 18 10:29:53 cplanet snort: SMB Name Wildcard: 0.79.136.154:137 -> 192.168.1.31:137
Apr 18 10:29:53 cplanet snort: SMB Name Wildcard: 0.0.0.100:137 -> 192.168.1.31:137
Apr 18 10:29:53 cplanet snort: SMB Name Wildcard: 0.0.0.62:137 -> 192.168.1.31:137
Apr 18 10:29:55 cplanet snort: SMB Name Wildcard: 0.0.0.62:137 -> 192.168.1.31:137
Apr 18 10:29:55 cplanet snort: SMB Name Wildcard: 0.0.0.100:137 -> 192.168.1.31:137
Apr 18 10:29:55 cplanet snort: SMB Name Wildcard: 0.79.136.154:137 -> 192.168.1.31:137
Apr 18 10:29:56 cplanet snort: SMB Name Wildcard: 0.79.136.154:137 -> 192.168.1.31:137
Apr 18 10:29:56 cplanet snort: SMB Name Wildcard: 0.0.0.100:137 -> 192.168.1.31:137
Apr 18 10:29:56 cplanet snort: SMB Name Wildcard: 0.0.0.62:137 -> 192.168.1.31:137
-----TIME GAP-----
Apr 18 13:59:16 cplanet snort: SMB Name Wildcard: 0.88.216.18:137 -> 192.168.1.80:137
Apr 18 13:59:16 cplanet snort: SMB Name Wildcard: 0.88.216.73:137 -> 192.168.1.80:137
Apr 18 13:59:16 cplanet snort: SMB Name Wildcard: 0.88.50.238:137 -> 192.168.1.80:137
Apr 18 13:59:17 cplanet snort: SMB Name Wildcard: 0.88.50.238:137 -> 192.168.1.80:137
Apr 18 13:59:18 cplanet snort: SMB Name Wildcard: 0.88.216.73:137 -> 192.168.1.80:137
Apr 18 13:59:18 cplanet snort: SMB Name Wildcard: 0.88.216.18:137 -> 192.168.1.80:137
-----TIME GAP-----
Apr 18 15:47:12 cplanet snort: SMB Name Wildcard: 0.99.145.5:137 -> 192.168.1.21:137
Apr 18 15:47:12 cplanet snort: SMB Name Wildcard: 0.217.9.181:1044 -> 192.168.1.21:137
Apr 18 15:47:13 cplanet snort: SMB Name Wildcard: 0.99.145.5:137 -> 192.168.1.21:137
Apr 18 15:47:14 cplanet snort: SMB Name Wildcard: 0.217.9.181:1044 -> 192.168.1.21:137
Apr 18 15:47:14 cplanet snort: SMB Name Wildcard: 0.254.3.166:137 -> 192.168.1.21:137
Apr 18 15:47:15 cplanet snort: SMB Name Wildcard: 0.217.9.181:1044 -> 192.168.1.21:137
Apr 18 15:47:16 cplanet snort: SMB Name Wildcard: 0.254.3.166:137 -> 192.168.1.21:137
Apr 18 15:47:17 cplanet snort: SMB Name Wildcard: 0.254.3.166:137 -> 192.168.1.21:137
-----TIME GAP-----
Apr 19 09:01:53 cplanet snort: SMB Name Wildcard: 0.254.140.186:137 -> 192.168.1.21:137
Apr 19 09:01:54 cplanet snort: SMB Name Wildcard: 0.123.52.213:137 -> 192.168.1.21:137
Apr 19 09:01:54 cplanet snort: SMB Name Wildcard: 0.254.140.186:137 -> 192.168.1.21:137
Apr 19 09:01:56 cplanet snort: SMB Name Wildcard: 0.254.140.186:137 -> 192.168.1.21:137
-----TIME GAP-----
Apr 19 14:39:48 cplanet snort: SMB Name Wildcard: 0.206.143.174:137 -> 192.168.1.103:137
Apr 19 14:39:59 cplanet snort: SMB Name Wildcard: 0.164.36.35:137 -> 192.168.1.103:137
Apr 19 14:40:20 cplanet snort: SMB Name Wildcard: 0.33.219.135:137 -> 192.168.1.103:137
Apr 19 14:40:22 cplanet snort: SMB Name Wildcard: 0.49.166.40:137 -> 192.168.1.103:137
Apr 19 14:40:22 cplanet snort: SMB Name Wildcard: 0.33.219.135:137 -> 192.168.1.103:137
Apr 19 14:40:23 cplanet snort: SMB Name Wildcard: 0.49.166.40:137 -> 192.168.1.103:137
Apr 19 14:40:24 cplanet snort: SMB Name Wildcard: 0.33.219.135:137 -> 192.168.1.103:137
Apr 19 14:40:25 cplanet snort: SMB Name Wildcard: 0.49.166.40:137 -> 192.168.1.103:137
Apr 19 15:02:48 cplanet snort: SMB Name Wildcard: 0.33.219.135:137 -> 192.168.1.21:137
Apr 19 15:03:03 cplanet snort: SMB Name Wildcard: 0.27.193.137:1025 -> 192.168.1.21:137
Apr 19 15:03:06 cplanet snort: SMB Name Wildcard: 0.27.193.137:1025 -> 192.168.1.21:137
Apr 19 15:03:19 cplanet snort: SMB Name Wildcard: 0.248.46.232:137 -> 192.168.1.21:137
Apr 19 15:03:21 cplanet snort: SMB Name Wildcard: 0.248.46.232:137 -> 192.168.1.21:137
Apr 19 15:03:22 cplanet snort: SMB Name Wildcard: 0.27.193.137:1025 -> 192.168.1.21:137
Apr 19 15:03:22 cplanet snort: SMB Name Wildcard: 0.248.46.232:137 -> 192.168.1.21:137
Apr 19 15:03:31 cplanet snort: SMB Name Wildcard: 0.11.116.183:137 -> 192.168.1.21:137
Apr 19 15:03:46 cplanet snort: SMB Name Wildcard: 0.27.193.137:1025 -> 192.168.1.21:137
Apr 19 15:04:21 cplanet snort: SMB Name Wildcard: 0.27.193.137:1025 -> 192.168.1.21:137
```

Analysis:

The technique:

The attacker(s) uses several different source IPs. During the different attacks, at least two source IPs are used in a probe, and in the last attack seven different source IPs are used. While there is time to punch in the requests by hand, I'd guess a script doing a slow probe is being used. It is most often source port 137, but in some instances source port 1025 is being used. Only in the last attack is a source machine attacking more than one target machine, but I don't know if that's significant since the last attack is also the largest. The use of several different source IPs could be an attempt to hide the real source IP.

The intent:

Someone is looking for poorly configured SMB services on our network. Our network is actively targeted, but the hosts on the network are being selected at random; this can be seen from the fact that not all of the targeted

machines exists.

The severity:

Low. The attacker got nothing out of it, except the knowledge that our systems were properly configured. It's disturbing that the attack came from so many source IPs, which indicates either a lot of spoofing to try and cover the tracks, or that the attacker has a lot of resources.

Comment:

This was the first time I've ever seen this sort of attack, so I'll have to look it up further to see exactly what it's about.

=====  
Detect #2, from Snort logs:  
-----

```
Apr 18 16:50:21 cplanet snort: SYN FIN Scan: 0.162.120.239:53 -> 192.168.1.70:53
Apr 18 16:50:24 cplanet snort: SYN FIN Scan: 0.162.120.239:53 -> 192.168.1.251:53
Apr 18 16:50:24 cplanet snort: SYN FIN Scan: 0.162.120.239:53 -> 192.168.1.249:53
Apr 18 16:50:24 cplanet snort: SYN FIN Scan: 0.162.120.239:53 -> 192.168.1.253:53
Apr 18 16:53:59 cplanet snort: SYN FIN Scan: 0.162.120.239:53 -> 192.168.44.1:53
Apr 18 16:53:59 cplanet snort: SYN FIN Scan: 0.162.120.239:53 -> 192.168.44.2:53
Apr 18 16:53:59 cplanet snort: SYN FIN Scan: 0.162.120.239:53 -> 192.168.44.3:53
Apr 18 16:53:59 cplanet snort: SYN FIN Scan: 0.162.120.239:53 -> 192.168.44.4:53
-----SNIP-----
Apr 18 16:54:03 cplanet snort: SYN FIN Scan: 0.162.120.239:53 -> 192.168.44.253:53
Apr 18 16:54:03 cplanet snort: SYN FIN Scan: 0.162.120.239:53 -> 192.168.44.254:53
Apr 18 16:54:03 cplanet snort: SYN FIN Scan: 0.162.120.239:53 -> 192.168.44.255:53
```

Analysis:

The technique:

The attacker is first scanning some known machines on one of our visible networks, (1.251, 1.249, 1.253), and then goes on to scan the the entire 192.168.44/24 network for alive machines. Some automated method (a program or perhaps a Perl script) is being used, since the scan is very fast (255 addresses in four seconds) and the source port is being reused.

The difference in time between the probe of the first four machines and the following 255 could be because the attacker probes the whole 192.168/16 class B network, and it takes time to go from 192.168.1.253 to 192.168.44.1.

The intent:

Someone is trying to find out what machines are alive on our networks, and is doing so by trying to connect to TCP port 53. This is probably a first-stage mapping attempt, for later use in a more determined attack where weaknesses in the alive machines will be tested and if possible exploited. We are being actively targeted, as part of a larger probe.

The severity:

Low, but we should be filtering this.

Comment:

The attacker is not too sophisticated (or is intentionally being clumsy to make us think of this as an amateur and therefore not a serious threat), since after testing TCP port 53 on all hosts, he or she finally tries port 53 on the broadcast address 192.168.44.255.

=====  
Detect #3, from Snort logs:  
-----

```
Apr 17 11:52:39 pplanet snort: WinGate 1080 Attempt: 192.168.1.42:3616 -> 192.168.2.1:1080
Apr 17 11:52:41 pplanet snort: Possible GateCrasher access: 192.168.1.42:4581 -> 192.168.2.1:6969
Apr 17 11:52:43 pplanet snort: Possible SubSeven access: 192.168.1.42:2825 -> 192.168.2.1:6776
Apr 17 11:52:46 pplanet snort: Possible SubSeven access: 192.168.1.42:1445 -> 192.168.2.1:1243
Apr 17 11:52:47 pplanet snort: WinGate 8080 Attempt: 192.168.1.42:2789 -> 192.168.2.1:8080
Apr 17 11:53:07 pplanet snort: Hackers Paradise: 192.168.1.42:38165 -> 192.168.2.1:31
Apr 17 11:53:31 pplanet snort: Silencer, WebEX: 192.168.1.42:38165 -> 192.168.2.1:1001
Apr 17 11:53:32 pplanet snort: Satanz Backdoor: 192.168.1.42:38165 -> 192.168.2.1:666
Apr 17 11:53:39 pplanet snort: Hackers Paradise: 192.168.1.42:38165 -> 192.168.2.1:456
Apr 17 11:54:02 pplanet snort: iNi Killer/Phase Zero/Stealth Spy: 192.168.1.42:38165 -> 192.168.2.1:555
Apr 17 11:54:30 pplanet snort: WinGate 8080 Attempt: 192.168.1.42:1095 -> 192.168.2.1:8080
Apr 17 11:54:31 pplanet snort: NULL Scan: 192.168.1.42:38173 -> 192.168.2.1:21
Apr 17 11:54:31 pplanet snort: Possible NMAP Fingerprint attempt: 192.168.1.42:38174 -> 192.168.2.1:21
Apr 17 11:54:31 pplanet snort: NMAP TCP ping!: 192.168.1.42:38175 -> 192.168.2.1:21
Apr 17 11:54:31 pplanet snort: NMAP TCP ping!: 192.168.1.42:38177 -> 192.168.2.1:5384
Apr 17 11:54:31 pplanet snort: XMAS Scan: 192.168.1.42:38178 -> 192.168.2.1:5384
Apr 17 11:54:37 pplanet snort: Possible SubSeven access: 192.168.1.42:1869 -> 192.168.1.1:6776
Apr 17 11:54:37 pplanet snort: WinGate 8080 Attempt: 192.168.1.42:2060 -> 192.168.2.1:8080
Apr 17 11:54:38 pplanet snort: WinGate 8080 Attempt: 192.168.1.42:2234 -> 192.168.2.1:8080
Apr 17 11:54:40 pplanet snort: Possible SubSeven access: 192.168.1.42:2187 -> 192.168.2.1:6776
Apr 17 11:54:44 pplanet snort: Possible GateCrasher access: 192.168.1.42:3207 -> 192.168.2.1:6969
Apr 17 11:55:12 pplanet snort: WinGate 1080 Attempt: 192.168.1.42:2012 -> 192.168.2.1:1080
Apr 17 11:55:19 pplanet snort: Possible SubSeven access: 192.168.1.42:4510 -> 192.168.2.1:1243
```

```

Apr 17 11:55:28 pplanet snort: WinGate 8080 Attempt: 192.168.1.42:4192 -> 192.168.2.1:8080
Apr 17 11:55:30 pplanet snort: NULL Scan: 192.168.1.42:51737 -> 192.168.2.1:21
Apr 17 11:55:30 pplanet snort: Possible NMAP Fingerprint attempt: 192.168.1.42:51738 -> 192.168.2.1:21
Apr 17 11:55:30 pplanet snort: NMAP TCP ping!: 192.168.1.42:51739 -> 192.168.2.1:21
Apr 17 11:55:30 pplanet snort: NMAP TCP ping!: 192.168.1.42:51741 -> 192.168.2.1:1386
Apr 17 11:55:30 pplanet snort: XMAS Scan: 192.168.1.42:51742 -> 192.168.2.1:1386
Apr 17 11:56:05 pplanet snort: WinGate 8080 Attempt: 192.168.1.42:4586 -> 192.168.1.1:8080
Apr 17 11:56:08 pplanet snort: Possible SubSeven access: 192.168.1.42:3732 -> 192.168.1.1:1243
Apr 17 11:56:11 pplanet snort: WinGate 1080 Attempt: 192.168.1.42:2458 -> 192.168.1.1:1080
Apr 17 11:56:12 pplanet snort: Possible GateCrasher access: 192.168.1.42:4234 -> 192.168.1.1:6969
Apr 17 11:56:22 pplanet snort: NULL Scan: 192.168.1.42:38081 -> 192.168.1.1:21
Apr 17 11:56:22 pplanet snort: Possible NMAP Fingerprint attempt: 192.168.1.42:38082 -> 192.168.1.1:21
Apr 17 11:56:22 pplanet snort: NMAP TCP ping!: 192.168.1.42:38083 -> 192.168.1.1:21
Apr 17 11:56:22 pplanet snort: NMAP TCP ping!: 192.168.1.42:38085 -> 192.168.1.1:9798
Apr 17 11:56:22 pplanet snort: XMAS Scan: 192.168.1.42:38086 -> 192.168.1.1:9798
Apr 17 11:56:37 pplanet snort: IIS NewDSN access attempt: 192.168.1.42:3311 -> 192.168.2.1:80
Apr 17 11:56:58 pplanet snort: Traceroute: 192.168.1.42:53 -> 192.168.2.1:32768
Apr 17 11:56:59 pplanet snort: IIS NewDSN access attempt: 192.168.1.42:3322 -> 192.168.1.1:80
Apr 17 11:57:03 pplanet snort: PCAnywhere: 192.168.1.42:1024 -> 192.168.2.1:22
Apr 17 11:57:03 pplanet snort: PCAnywhere: 192.168.1.42:1024 -> 192.168.2.1:22
Apr 17 11:57:06 pplanet snort: WinGate 8080 Attempt: 192.168.1.42:3343 -> 192.168.2.1:8080
Apr 17 11:57:10 pplanet snort: WinGate 8080 Attempt: 192.168.1.42:3344 -> 192.168.2.1:8080
Apr 17 11:57:12 pplanet snort: SNMP public access: 192.168.1.42:1025 -> 192.168.2.1:161
Apr 17 11:57:17 pplanet snort: NPH-publish CGI access attempt: 192.168.1.42:3350 -> 192.168.2.1:80
Apr 17 11:57:19 pplanet snort: Guestbook CGI access attempt: 192.168.1.42:3354 -> 192.168.2.1:80
Apr 17 11:57:20 pplanet snort: NPH-publish CGI access attempt: 192.168.1.42:3361 -> 192.168.2.1:80
Apr 17 11:57:20 pplanet snort: Traceroute: 192.168.1.42:53 -> 192.168.1.1:32768
Apr 17 11:57:21 pplanet snort: Wrap CGI access attempt: 192.168.1.42:3367 -> 192.168.2.1:80
Apr 17 11:57:22 pplanet snort: IIS NewDSN access attempt: 192.168.1.42:3371 -> 192.168.1.1:80
Apr 17 11:57:23 pplanet snort: Websendmail CGI access attempt: 192.168.1.42:3372 -> 192.168.2.1:80
Apr 17 11:57:23 pplanet snort: Webgais CGI access attempt: 192.168.1.42:3373 -> 192.168.2.1:80
Apr 17 11:57:25 pplanet snort: Upload CGI access attempt: 192.168.1.42:3391 -> 192.168.2.1:80
Apr 17 11:57:25 pplanet snort: WinGate 8080 Attempt: 192.168.1.42:3392 -> 192.168.2.1:8080
Apr 17 11:57:25 pplanet snort: PCAnywhere: 192.168.1.42:1025 -> 192.168.1.1:22
Apr 17 11:57:25 pplanet snort: PCAnywhere: 192.168.1.42:1025 -> 192.168.1.1:22
Apr 17 11:57:27 pplanet snort: IIS NewDSN access attempt: 192.168.1.42:3397 -> 192.168.1.1:80
Apr 17 11:57:28 pplanet snort: SNMP public access: 192.168.1.42:1026 -> 192.168.1.1:161
Apr 17 11:57:29 pplanet snort: Websendmail CGI access attempt: 192.168.1.42:3407 -> 192.168.2.1:80
Apr 17 11:57:29 pplanet snort: TEST-CGI probe!: 192.168.1.42:3408 -> 192.168.2.1:80
Apr 17 11:57:29 pplanet snort: Websendmail CGI access attempt: 192.168.1.42:3412 -> 192.168.2.1:80
Apr 17 11:57:29 pplanet snort: Cgiwrap CGI access attempt: 192.168.1.42:3414 -> 192.168.2.1:80
Apr 17 11:57:29 pplanet snort: NPH-publish CGI access attempt: 192.168.1.42:3415 -> 192.168.2.1:80
Apr 17 11:57:30 pplanet snort: PHP CGI access attempt: 192.168.1.42:3418 -> 192.168.2.1:80
Apr 17 11:57:31 pplanet snort: PHF CGI access attempt: 192.168.1.42:3420 -> 192.168.2.1:80
Apr 17 11:57:32 pplanet snort: Cgichk Pfdispaly (sic) access attempt: 192.168.1.42:3422 -> 192.168.2.1:80
Apr 17 11:57:32 pplanet snort: CGI Perl access attempt: 192.168.1.42:3424 -> 192.168.2.1:80
Apr 17 11:57:32 pplanet snort: NPH CGI access attempt: 192.168.1.42:3425 -> 192.168.2.1:80
Apr 17 11:57:32 pplanet snort: JJ CGI access attempt: 192.168.1.42:3433 -> 192.168.2.1:80
Apr 17 11:57:33 pplanet snort: NPH-publish CGI access attempt: 192.168.1.42:3434 -> 192.168.1.1:80
Apr 17 11:57:33 pplanet snort: Upload CGI access attempt: 192.168.1.42:3435 -> 192.168.1.1:80
Apr 17 11:57:33 pplanet snort: Info2www CGI access attempt: 192.168.1.42:3437 -> 192.168.2.1:80
Apr 17 11:57:35 pplanet snort: Guestbook CGI access attempt: 192.168.1.42:3451 -> 192.168.1.1:80
Apr 17 11:57:36 pplanet snort: Cgiwrap CGI access attempt: 192.168.1.42:3458 -> 192.168.1.1:80
Apr 17 11:57:36 pplanet snort: JJ CGI access attempt: 192.168.1.42:3461 -> 192.168.1.1:80
Apr 17 11:57:37 pplanet snort: Wrap CGI access attempt: 192.168.1.42:3462 -> 192.168.1.1:80
Apr 17 11:57:39 pplanet snort: Websendmail CGI access attempt: 192.168.1.42:3465 -> 192.168.1.1:80
Apr 17 11:57:39 pplanet snort: Webgais CGI access attempt: 192.168.1.42:3466 -> 192.168.1.1:80
Apr 17 11:57:39 pplanet snort: Cgiwrap CGI access attempt: 192.168.1.42:3470 -> 192.168.1.1:80
Apr 17 11:57:41 pplanet snort: Upload CGI access attempt: 192.168.1.42:3476 -> 192.168.1.1:80
Apr 17 11:58:15 pplanet snort: Guestbook CGI access attempt: 192.168.1.42:3482 -> 192.168.2.1:80
Apr 17 11:58:15 pplanet snort: Htmlscript CGI access attempt: 192.168.1.42:3485 -> 192.168.2.1:80
Apr 17 11:58:15 pplanet snort: HANDLER probe!: 192.168.1.42:3486 -> 192.168.2.1:80
Apr 17 11:58:15 pplanet snort: Aglimpse CGI access attempt: 192.168.1.42:3487 -> 192.168.2.1:80
Apr 17 11:58:16 pplanet snort: FrontPage Author PWD Scan: 192.168.1.42:3488 -> 192.168.2.1:80
Apr 17 11:58:19 pplanet snort: HANDLER probe!: 192.168.1.42:3490 -> 192.168.2.1:80
Apr 17 11:58:19 pplanet snort: FAXSURVEY probe!: 192.168.1.42:3491 -> 192.168.2.1:80
Apr 17 11:58:19 pplanet snort: WinGate 8080 Attempt: 192.168.1.42:3493 -> 192.168.2.1:8080
Apr 17 11:58:22 pplanet snort: TEST-CGI probe!: 192.168.1.42:3496 -> 192.168.1.1:80
Apr 17 11:58:22 pplanet snort: HANDLER probe!: 192.168.1.42:3500 -> 192.168.1.1:80
Apr 17 11:58:23 pplanet snort: PHP CGI access attempt: 192.168.1.42:3505 -> 192.168.1.1:80
Apr 17 11:58:24 pplanet snort: PHF CGI access attempt: 192.168.1.42:3506 -> 192.168.1.1:80
Apr 17 11:58:24 pplanet snort: Upload CGI access attempt: 192.168.1.42:3507 -> 192.168.1.1:80
Apr 17 11:58:24 pplanet snort: Cgichk Pfdispaly (sic) access attempt: 192.168.1.42:3508 -> 192.168.1.1:80
Apr 17 11:58:24 pplanet snort: Webgais CGI access attempt: 192.168.1.42:3509 -> 192.168.1.1:80
Apr 17 11:58:24 pplanet snort: CGI Perl access attempt: 192.168.1.42:3510 -> 192.168.1.1:80
Apr 17 11:58:24 pplanet snort: NPH CGI access attempt: 192.168.1.42:3511 -> 192.168.1.1:80
Apr 17 11:58:25 pplanet snort: Webgais CGI access attempt: 192.168.1.42:3516 -> 192.168.1.1:80
Apr 17 11:58:25 pplanet snort: JJ CGI access attempt: 192.168.1.42:3518 -> 192.168.1.1:80
Apr 17 11:58:26 pplanet snort: Info2www CGI access attempt: 192.168.1.42:3519 -> 192.168.1.1:80
Apr 17 11:58:36 pplanet snort: COUNT.cgi probe!: 192.168.1.42:3532 -> 192.168.2.1:80

```

```

Apr 17 11:58:37 pplanet snort: FrontPage Author PWD Scan: 192.168.1.42:3533 -> 192.168.2.1:80
Apr 17 11:58:37 pplanet snort: Campas CGI access attempt: 192.168.1.42:3535 -> 192.168.2.1:80
Apr 17 11:58:41 pplanet snort: NULL Scan: 192.168.1.42:21 -> 192.168.2.1:21
Apr 17 11:58:50 pplanet snort: NULL Scan: 192.168.1.42:21 -> 192.168.2.1:21
Apr 17 11:59:01 pplanet snort: NULL Scan: 192.168.1.42:21 -> 192.168.2.1:21
Apr 17 11:59:09 pplanet snort: NULL Scan: 192.168.1.42:21 -> 192.168.2.1:21
Apr 17 11:59:17 pplanet snort: Upload CGI access attempt: 192.168.1.42:3576 -> 192.168.1.1:80
Apr 17 11:59:17 pplanet snort: Htmlscript CGI access attempt: 192.168.1.42:3577 -> 192.168.1.1:80
Apr 17 11:59:17 pplanet snort: HANDLER probe!: 192.168.1.42:3578 -> 192.168.1.1:80
Apr 17 11:59:17 pplanet snort: Aglimpse CGI access attempt: 192.168.1.42:3579 -> 192.168.1.1:80
Apr 17 11:59:18 pplanet snort: NULL Scan: 192.168.1.42:21 -> 192.168.2.1:21
Apr 17 11:59:18 pplanet snort: FrontPage Author PWD Scan: 192.168.1.42:3580 -> 192.168.1.1:80
Apr 17 11:59:20 pplanet snort: Finger CGI access attempt: 192.168.1.42:3582 -> 192.168.1.1:80
Apr 17 11:59:20 pplanet snort: FAXSURVEY probe!: 192.168.1.42:3583 -> 192.168.1.1:80
Apr 17 11:59:20 pplanet snort: FrontPage Author PWD Scan: 192.168.1.42:3584 -> 192.168.1.1:80
Apr 17 11:59:28 pplanet snort: NULL Scan: 192.168.1.42:21 -> 192.168.2.1:21
Apr 17 11:59:35 pplanet snort: COUNT.cgi probe!: 192.168.1.42:3587 -> 192.168.1.1:80
Apr 17 11:59:36 pplanet snort: COUNT.cgi probe!: 192.168.1.42:3588 -> 192.168.1.1:80
Apr 17 11:59:36 pplanet snort: Campas CGI access attempt: 192.168.1.42:3590 -> 192.168.1.1:80
Apr 17 11:59:37 pplanet snort: NULL Scan: 192.168.1.42:21 -> 192.168.2.1:21
Apr 17 11:59:38 pplanet snort: Finger CGI access attempt: 192.168.1.42:3600 -> 192.168.1.1:80
Apr 17 12:00:04 pplanet snort: Possible Portal of Doom access: 192.168.1.42:1026 -> 192.168.2.1:10167
Apr 17 12:00:15 pplanet snort: NULL Scan: 192.168.1.42:21 -> 192.168.1.1:21
Apr 17 12:00:24 pplanet snort: NULL Scan: 192.168.1.42:21 -> 192.168.1.1:21
Apr 17 12:00:30 pplanet snort: NULL Scan: 192.168.1.42:21 -> 192.168.1.1:21
Apr 17 12:00:33 pplanet snort: SMB Name Wildcard: 192.168.1.42:1026 -> 192.168.2.1:137
Apr 17 12:00:37 pplanet snort: NULL Scan: 192.168.1.42:21 -> 192.168.1.1:21
Apr 17 12:00:40 pplanet snort: WinGate 8080 Attempt: 192.168.1.42:3618 -> 192.168.2.1:8080
Apr 17 12:00:42 pplanet snort: NULL Scan: 192.168.1.42:21 -> 192.168.1.1:21
Apr 17 12:00:42 pplanet snort: NULL Scan: 192.168.1.42:21 -> 192.168.1.1:21
Apr 17 12:00:42 pplanet snort: WinGate 8080 Attempt: 192.168.1.42:3619 -> 192.168.2.1:8080
Apr 17 12:00:48 pplanet snort: Possible GirlFriend access: 192.168.1.42:3623 -> 192.168.2.1:21554
Apr 17 12:00:48 pplanet snort: Possible NetSphere access: 192.168.1.42:3624 -> 192.168.2.1:30100
Apr 17 12:00:48 pplanet snort: Finger CGI access attempt: 192.168.1.42:3625 -> 192.168.2.1:80
Apr 17 12:00:49 pplanet snort: NULL Scan: 192.168.1.42:21 -> 192.168.1.1:21
Apr 17 12:00:55 pplanet snort: NULL Scan: 192.168.1.42:21 -> 192.168.1.1:21
Apr 17 12:01:02 pplanet snort: NULL Scan: 192.168.1.42:21 -> 192.168.1.1:21
Apr 17 12:01:09 pplanet snort: NULL Scan: 192.168.1.42:21 -> 192.168.1.1:21
Apr 17 12:01:15 pplanet snort: Possible Portal of Doom access: 192.168.1.42:1026 -> 192.168.1.1:10167
Apr 17 12:01:21 pplanet snort: SMB Name Wildcard: 192.168.1.42:1026 -> 192.168.1.1:137
Apr 17 12:01:29 pplanet snort: Possible GirlFriend access: 192.168.1.42:3647 -> 192.168.1.1:21554
Apr 17 12:01:29 pplanet snort: Possible NetSphere access: 192.168.1.42:3648 -> 192.168.1.1:30100
Apr 17 12:01:30 pplanet snort: Aglimpse CGI access attempt: 192.168.1.42:3654 -> 192.168.1.1:80

```

Analysis:

The technique:

Someone on my network is using some attack tool to test for a multitude of different weaknesses on several different machines. There is no attempt to try and hide the source.

Comment (could as well spoil this before going on to intent and severity):

This turned out to be a sort of false positive; a colleague tried out the latest version of Nessus on our network.

The intent:

Looking for weaknesses in the different machines on the network, and possibly also map the network. Definitely active targeting.

The severity:

Could have been serious had the attack tool found an exploitable weakness and the attacker been a bad guy.

=====  
Detect #4, dug up and compiled from several Snort output files:  
-----

---First comes probes of three server machines:---

```

[**] HTTP [**]
02/09-04:20:45.537103 0:0:0:55:B6:43 -> 0:0:0:C4:25:8C type:0x800 len:0x3C
0.183.32.145:9721 -> 192.168.2.249:80 TCP TTL:247 TOS:0x0 ID:41058
S***** Seq: 0x1F7000FA Ack: 0x0 Win: 0x1234
00 00 00 00 00 00 .....

```

```

[**] FIN Scan [**]
02/09-04:20:45.542019 0:0:0:55:B6:43 -> 0:0:0:C4:25:8C type:0x800 len:0x3C
0.183.32.145:9723 -> 192.168.2.249:80 TCP TTL:247 TOS:0x0 ID:41060
*F**** Seq: 0x1F7000FA Ack: 0x0 Win: 0x1234
33 56 45 5A 52 60 3VEZR`

```

```

[**] SYN FIN Scan [**]
02/09-04:20:45.543555 0:0:0:55:B6:43 -> 0:0:0:C4:25:8C type:0x800 len:0x3C

```

0.183.32.145:9725 -> 192.168.2.249:80 TCP TTL:247 TOS:0x0 ID:41062  
SF\*\*\*\* Seq: 0x1F7000FA Ack: 0x0 Win: 0x1234  
31 59 40 51 4E 29 1Y@QN)

[\*\*] Possible Queso Fingerprint attempt [\*\*]  
02/09-04:20:45.545131 0:0:0:55:B6:43 -> 0:0:0:C4:25:8C type:0x800 len:0x3C  
0.183.32.145:9727 -> 192.168.2.249:80 TCP TTL:247 TOS:0x0 ID:41064  
S\*\*\*\*\*21 Seq: 0x1F7000FA Ack: 0x0 Win: 0x1234  
74 61 6B 65 74 68 taketh

[\*\*] HTTP [\*\*]  
02/09-04:20:47.378567 0:0:0:55:B6:43 -> 0:0:0:F7:E9:B type:0x800 len:0x3C  
0.183.32.145:18757 -> 192.168.2.251:80 TCP TTL:247 TOS:0x0 ID:50094  
S\*\*\*\*\* Seq: 0x48E23F88 Ack: 0x0 Win: 0x1234  
74 61 6B 65 74 68 taketh

[\*\*] FIN Scan [\*\*]  
02/09-04:20:47.411801 0:0:0:55:B6:43 -> 0:0:0:F7:E9:B type:0x800 len:0x3C  
0.183.32.145:18759 -> 192.168.2.251:80 TCP TTL:247 TOS:0x0 ID:50096  
\*F\*\*\*\* Seq: 0x48E23F88 Ack: 0x0 Win: 0x1234  
0A 3E 73 68 65 65 .>shee

[\*\*] SYN FIN Scan [\*\*]  
02/09-04:20:47.450688 0:0:0:55:B6:43 -> 0:0:0:F7:E9:B type:0x800 len:0x3C  
0.183.32.145:18761 -> 192.168.2.251:80 TCP TTL:247 TOS:0x0 ID:50098  
SF\*\*\*\* Seq: 0x48E23F88 Ack: 0x0 Win: 0x1234  
5A 3B 48 0D 0A 4D Z;H..M

[\*\*] Possible Queso Fingerprint attempt [\*\*]  
02/09-04:20:47.490297 0:0:0:55:B6:43 -> 0:0:0:F7:E9:B type:0x800 len:0x3C  
0.183.32.145:18763 -> 192.168.2.251:80 TCP TTL:247 TOS:0x0 ID:50100  
S\*\*\*\*\*21 Seq: 0x48E23F88 Ack: 0x0 Win: 0x1234  
31 40 35 31 2D 5E 1@51-^

[\*\*] HTTP [\*\*]  
02/09-04:20:49.450407 0:0:0:55:B6:43 -> 0:0:0:DA:79:F9 type:0x800 len:0x3C  
0.183.32.145:18539 -> 192.168.2.253:80 TCP TTL:247 TOS:0x0 ID:49876  
S\*\*\*\*\* Seq: 0x7270D8E8 Ack: 0x0 Win: 0x1234  
53 49 36 56 2C 42 SI6V,B

[\*\*] FIN Scan [\*\*]  
02/09-04:20:49.452133 0:0:0:55:B6:43 -> 0:0:0:DA:79:F9 type:0x800 len:0x3C  
0.183.32.145:18541 -> 192.168.2.253:80 TCP TTL:247 TOS:0x0 ID:49878  
\*F\*\*\*\* Seq: 0x7270D8E8 Ack: 0x0 Win: 0x1234  
48 28 26 0D 0A 4D H(&..M

[\*\*] SYN FIN Scan [\*\*]  
02/09-04:20:49.525257 0:0:0:55:B6:43 -> 0:0:0:DA:79:F9 type:0x800 len:0x3C  
0.183.32.145:18543 -> 192.168.2.253:80 TCP TTL:247 TOS:0x0 ID:49880  
SF\*\*\*\* Seq: 0x7270D8E8 Ack: 0x0 Win: 0x1234  
68 69 76 61 0D 0A hiva..

[\*\*] Possible Queso Fingerprint attempt [\*\*]  
02/09-04:20:49.609067 0:0:0:55:B6:43 -> 0:0:0:DA:79:F9 type:0x800 len:0x3C  
0.183.32.145:18545 -> 192.168.2.253:80 TCP TTL:247 TOS:0x0 ID:49882  
S\*\*\*\*\*21 Seq: 0x7270D8E8 Ack: 0x0 Win: 0x1234  
50 61 74 68 3A 20 Path:

---And almost 12 hours later, every address on another net where we---  
---have client machines is probed by the same attacker:---

[\*\*] HTTP [\*\*]  
02/09-15:13:24.860630 0:0:0:55:B6:43 -> 0:0:0:C4:25:8C type:0x800 len:0x3C  
0.183.32.37:5613 -> 192.168.1.1:80 TCP TTL:247 TOS:0x0 ID:36950  
S\*\*\*\*\* Seq: 0x6286237 Ack: 0x0 Win: 0x1234  
38 40 26 29 55 2D 8@&)U-

[\*\*] FIN Scan [\*\*]  
02/09-15:13:24.912293 0:0:0:55:B6:43 -> 0:0:0:C4:25:8C type:0x800 len:0x3C  
0.183.32.37:5615 -> 192.168.1.1:80 TCP TTL:247 TOS:0x0 ID:36952  
\*F\*\*\*\* Seq: 0x6286237 Ack: 0x0 Win: 0x1234  
95 6B 95 43 D1 FB .k.C..

[\*\*] SYN FIN Scan [\*\*]  
02/09-15:13:25.054456 0:0:0:55:B6:43 -> 0:0:0:C4:25:8C type:0x800 len:0x3C  
0.183.32.37:5617 -> 192.168.1.1:80 TCP TTL:247 TOS:0x0 ID:36954  
SF\*\*\*\* Seq: 0x6286237 Ack: 0x0 Win: 0x1234  
50 61 74 68 3A 20 Path:

[\*\*] Possible Queso Fingerprint attempt [\*\*]

```
02/09-15:13:25.056163 0:0:0:55:B6:43 -> 0:0:0:C4:25:8C type:0x800 len:0x3C
0.183.32.37:5619 -> 192.168.1.1:80 TCP TTL:247 TOS:0x0 ID:36956
S*****21 Seq: 0x6286237 Ack: 0x0 Win: 0x1234
00 00 00 79 E6 FF ...y..
```

```
[**] HTTP [**]
02/09-15:13:28.672197 0:0:0:55:B6:43 -> 0:0:0:C4:25:8C type:0x800 len:0x3C
0.183.32.37:16148 -> 192.168.1.2:80 TCP TTL:247 TOS:0x0 ID:47485
S***** Seq: 0x5954D82A Ack: 0x0 Win: 0x1234
2D 5B 60 5F 5B 57 -[_]W
```

```
[**] FIN Scan [**]
02/09-15:13:28.721536 0:0:0:55:B6:43 -> 0:0:0:C4:25:8C type:0x800 len:0x3C
0.183.32.37:16150 -> 192.168.1.2:80 TCP TTL:247 TOS:0x0 ID:47487
*F**** Seq: 0x5954D82A Ack: 0x0 Win: 0x1234
2D 50 82 77 09 DD -P.w..
```

```
[**] SYN FIN Scan [**]
02/09-15:13:28.722721 0:0:0:55:B6:43 -> 0:0:0:C4:25:8C type:0x800 len:0x3C
0.183.32.37:16152 -> 192.168.1.2:80 TCP TTL:247 TOS:0x0 ID:47489
SF**** Seq: 0x5954D82A Ack: 0x0 Win: 0x1234
3C 0D 0A 4D 49 28 <..MI(
```

```
[**] Possible Queso Fingerprint attempt [**]
02/09-15:13:28.820332 0:0:0:55:B6:43 -> 0:0:0:C4:25:8C type:0x800 len:0x3C
0.183.32.37:16154 -> 192.168.1.2:80 TCP TTL:247 TOS:0x0 ID:47491
S*****21 Seq: 0x5954D82A Ack: 0x0 Win: 0x1234
43 58 5F 43 36 52 CX_C6R
```

-----...all the way up to:-----

```
[**] HTTP [**]
02/09-15:18:43.344942 0:0:0:55:B6:43 -> 0:0:0:C4:25:8C type:0x800 len:0x3C
0.183.32.37:10935 -> 192.168.1.254:80 TCP TTL:247 TOS:0x0 ID:42272
S***** Seq: 0x68BABCED Ack: 0x0 Win: 0x1234
50 61 74 68 3A 20 Path:
```

```
[**] FIN Scan [**]
02/09-15:18:43.345834 0:0:0:55:B6:43 -> 0:0:0:C4:25:8C type:0x800 len:0x3C
0.183.32.37:10937 -> 192.168.1.254:80 TCP TTL:247 TOS:0x0 ID:42274
*F**** Seq: 0x68BABCED Ack: 0x0 Win: 0x1234
00 AE 70 04 7F 54 ..p..T
```

```
[**] SYN FIN Scan [**]
02/09-15:18:43.371860 0:0:0:55:B6:43 -> 0:0:0:C4:25:8C type:0x800 len:0x3C
0.183.32.37:10939 -> 192.168.1.254:80 TCP TTL:247 TOS:0x0 ID:42276
SF**** Seq: 0x68BABCED Ack: 0x0 Win: 0x1234
36 5A 4F 5D 42 5D 6ZO]B]
```

```
[**] Possible Queso Fingerprint attempt [**]
02/09-15:18:43.423031 0:0:0:55:B6:43 -> 0:0:0:C4:25:8C type:0x800 len:0x3C
0.183.32.37:10941 -> 192.168.1.254:80 TCP TTL:247 TOS:0x0 ID:42278
S*****21 Seq: 0x68BABCED Ack: 0x0 Win: 0x1234
74 61 6B 65 74 68 taketh
```

Analysis:

The technique:

Again, the speed is indicating that a script or program is being used, and this is supported by the fact that the source ports changes drastically when changing target machine, but only changes by two between the different probes of the same machine. Some quick calculations based on the timestamps in the first three probes indicates that the entire class B network is being scanned.

The intent:

Someone is trying to map the entire 192.168/16 class B network.

The severity:

Low. We could see this as we're being actively targeted since we're part of the network being targeted, but we're only two of 254 networks. Nevertheless, we should try to filter this kind of traffic.

Comment:

I've never seen this four-step sequence before. It seems a bit amateur-ish, since the same port is being targeted all the time. Any of the probes would be enough to determine if a machine is alive, and the last one would be enough to determine OS.

=====

Detect #5, dug up and compiled from several Snort output files:

-----

```
[**] BackOrificel-scan [**]
02/11-22:10:30.547355 0:0:0:55:B6:43 -> 0:0:0:C4:25:8C type:0x800 len:0x3D
0.159.123.171:2032 -> 192.168.1.120:31337 UDP TTL:112 TOS:0x0 ID:53281
Len: 6912
CE 63 D1 D2 16 E7 13 CF 38 A5 A5 86 B2 75 4B 99 .c.....8....uK.
AA 32 58 .2X
```

```
[**] BackOrificel-scan [**]
02/11-22:10:30.548994 0:0:0:55:B6:43 -> 0:0:0:C4:25:8C type:0x800 len:0x3D
0.159.123.171:2032 -> 192.168.1.225:31337 UDP TTL:112 TOS:0x0 ID:53793
Len: 6912
CE 63 D1 D2 16 E7 13 CF 38 A5 A5 86 B2 75 4B 99 .c.....8....uK.
AA 32 58 .2X
```

```
[**] BackOrificel-scan [**]
02/11-22:10:30.546863 0:0:0:55:B6:43 -> 0:0:0:C4:25:8C type:0x800 len:0x3D
0.159.123.171:2032 -> 192.168.1.69:31337 UDP TTL:112 TOS:0x0 ID:53025
Len: 6912
CE 63 D1 D2 16 E7 13 CF 38 A5 A5 86 B2 75 4B 99 .c.....8....uK.
AA 32 58 .2X
```

```
[**] BackOrificel-scan [**]
02/11-22:10:30.548154 0:0:0:55:B6:43 -> 0:0:0:C4:25:8C type:0x800 len:0x3D
0.159.123.171:2032 -> 192.168.1.172:31337 UDP TTL:112 TOS:0x0 ID:53537
Len: 6912
CE 63 D1 D2 16 E7 13 CF 38 A5 A5 86 B2 75 4B 99 .c.....8....uK.
AA 32 58 .2X
```

Analysis:

The technique:

The selection of target machines seems to be random; first of all, these are the only four probes in the logs; and second, only the .69 machine actually exists. Some sort of program is being used for the probe (perhaps a BO client?); this can for instance be seen by the small timeframe in which the probes were detected, and the reuse of source address also indicates this.

The intent:

Someone is looking for the BackOrifice trojan. The scan looks like it's random, part of a bigger scan, but the fact that the one machine that is alive is a Windows machine could mean that someone is actively targeting the .69 machine and hiding it by making it look like random targeting.

The severity:

Medium. If the .69 machine is infected, this is serious.

Comment:

During a security audit performed a few weeks after this happened, the .69 machine did not answer on port 31337, so I hope that means it's clean.

=====  
Detect #6, from Snort logs:  
-----

```
Apr 19 03:53:26 cplanet snort: Traceroute: 0.67.29.9:2814 -> 192.168.2.253:33434
Apr 19 03:59:39 cplanet snort: Traceroute: 0.67.29.10:53 -> 192.168.2.253:33434
Apr 19 04:01:07 cplanet snort: Traceroute: 0.67.29.10:53 -> 192.168.2.253:33434
Apr 19 04:01:18 cplanet snort: Traceroute: 0.67.29.10:53 -> 192.168.2.253:33434
Apr 19 04:31:18 cplanet snort: Traceroute: 0.67.29.8:2814 -> 192.168.2.253:33434
Apr 19 04:32:26 cplanet snort: Traceroute: 0.67.29.8:2814 -> 192.168.2.253:33434
Apr 19 04:33:34 cplanet snort: Traceroute: 0.67.29.8:2814 -> 192.168.2.253:33434
Apr 19 04:34:42 cplanet snort: Traceroute: 0.67.29.8:2814 -> 192.168.2.253:33434
Apr 19 04:39:31 cplanet snort: Traceroute: 0.67.29.9:2814 -> 192.168.2.253:33434
Apr 19 04:40:38 cplanet snort: Traceroute: 0.67.29.9:2814 -> 192.168.2.253:33434
Apr 19 04:41:43 cplanet snort: Traceroute: 0.67.29.9:2814 -> 192.168.2.253:33434
```

Analysis:

The technique:

This seems to be a semi-slow series of traceroutes to our mail server. There is a weak pattern in the seconds part of the timestamps, but I think it's a manual traceroute performed from a few different hosts. Someone is logging in on different hosts manually to do these traceroutes.

The intent:

Probably just checking if our mail server is alive and reachable. I'd guess someone is having trouble sending mail to us.

The severity:

Low. There can be perfectly legitimate reasons to do a traceroute, especially to a mail server; perhaps someone was trying to send mail and kept getting errors?

=====  
Detect #7, from the /var/messages file on a Linux machine running ipchains:



```

-----
Apr  3 20:19:10 saauthor kernel: Packet log: input DENY eth1 PROTO=17 0.0.0.0:68 255.255.255.255:67 L=328 S=0x00 I=0
F=0x0000 T=128 (#5)
Apr  3 20:19:16 saauthor kernel: Packet log: input DENY eth1 PROTO=17 0.0.0.0:68 255.255.255.255:67 L=328 S=0x00 I=256
F=0x0000 T=128 (#5)
Apr  3 20:19:22 saauthor kernel: Packet log: input DENY eth1 PROTO=17 0.0.0.0:68 255.255.255.255:67 L=328 S=0x00 I=512
F=0x0000 T=128 (#5)
Apr  3 20:19:28 saauthor kernel: Packet log: input DENY eth1 PROTO=17 0.0.0.0:68 255.255.255.255:67 L=328 S=0x00 I=768
F=0x0000 T=128 (#5)
Apr  3 20:21:34 saauthor kernel: Packet log: input DENY eth1 PROTO=17 0.0.0.0:68 255.255.255.255:67 L=328 S=0x00 I=6400
F=0x0000 T=128 (#5)
Apr  3 20:21:40 saauthor kernel: Packet log: input DENY eth1 PROTO=17 0.0.0.0:68 255.255.255.255:67 L=328 S=0x00 I=6656
F=0x0000 T=128 (#5)
Apr  3 20:21:46 saauthor kernel: Packet log: input DENY eth1 PROTO=17 0.0.0.0:68 255.255.255.255:67 L=328 S=0x00 I=6912
F=0x0000 T=128 (#5)
Apr  3 20:21:52 saauthor kernel: Packet log: input DENY eth1 PROTO=17 0.0.0.0:68 255.255.255.255:67 L=328 S=0x00 I=7168
F=0x0000 T=128 (#5)

```

Analysis:

The technique:

This definitely seems to be a machine searching for a bootp server. The time intervals as well as the characteristic addresses makes me suspect a Windows machine using DHCP just got turned on.

The intent:

Not malicious. Someone haven't configured their machine correctly, since this is not taken from a network where bootp/dhcp is used.

The severity:

Low.

Comment:

One alternative explanation could be that someone has forged their return address to be 0.0.0.0, and is trying to connect to UDP port 67 on 192.168.3.255, which is translated to 255.255.255.255 as shown on page 64 in the IDIC-3 Course Book from Vicky Irwin's speech (this log is taken from a machine on a switched network using Cisco equipment). Why someone would try to do that is beyond me, since it's way too slow to be some kind of DoS attack.

```

=====
Detect #8, dug up and compiled from several Snort output files:
-----

```

```

[**] SYN FIN Scan [**]
01/29-13:51:11.046812 0:0:0:55:B6:43 -> 0:0:0:C4:25:8C type:0x800 len:0x3C
0.238.9.1:0 -> 192.168.1.1:109 TCP TTL:224 TOS:0x0 ID:34564
SF**** Seq: 0x4A490000 Ack: 0x0 Win: 0x200
53 48 58 2C 4A 5B SHX,J[

```

```

[**] SYN FIN Scan [**]
01/29-13:51:11.047530 0:0:0:55:B6:43 -> 0:0:0:C4:25:8C type:0x800 len:0x3C
0.238.9.1:0 -> 192.168.1.2:109 TCP TTL:224 TOS:0x0 ID:771
SF**** Seq: 0x4A490000 Ack: 0x0 Win: 0x200
40 28 57 35 29 25 @(W5)%

```

```

[**] SYN FIN Scan [**]
01/29-13:51:11.049021 0:0:0:55:B6:43 -> 0:0:0:C4:25:8C type:0x800 len:0x3C
0.238.9.1:0 -> 192.168.1.3:109 TCP TTL:224 TOS:0x0 ID:25345
SF**** Seq: 0x4A490000 Ack: 0x0 Win: 0x200
74 61 6B 65 74 68 taketh

```

---and so on up to:---

```

[**] SYN FIN Scan [**]
01/29-13:51:15.956137 0:0:0:55:B6:43 -> 0:0:0:C4:25:8C type:0x800 len:0x3C
0.238.9.1:0 -> 192.168.1.254:109 TCP TTL:225 TOS:0x0 ID:61185
SF**** Seq: 0x4A490000 Ack: 0x0 Win: 0x200
90 7A 38 31 F0 C0 .z81..

```

```

[**] SYN FIN Scan [**]
01/29-13:51:15.964528 0:0:0:55:B6:43 -> 0:0:0:C4:25:8C type:0x800 len:0x3C
0.238.9.1:0 -> 192.168.1.255:109 TCP TTL:225 TOS:0x0 ID:1539
SF**** Seq: 0x4A490000 Ack: 0x0 Win: 0x200
74 61 6B 65 74 68 taketh

```

Analysis:

The technique:

Pretty straightforward. This particular SYN FIN scan using source port 0 is well documented, and also mentioned in the course material. A program or script is used, since the attack is very fast and reuses the source port. It

is interesting to note that the TTL is higher in the last packets, though I don't know what it could mean. I guess it could be that the program being used is setting different TTLs, but my guess would be that the packets simply took different paths to reach us.

The intent:

To map our network, finding out what hosts are alive.

The severity:

Medium. A guess is that we're being actively targeted, since our other networks didn't get hit at about the same time. It could be someone selecting class C networks at random, but I don't think so.

Comment:

Notice the last packet: it's addressed to 192.168.1.255. This is stupid for two reasons: first, it's going to a TCP port, and second, machines 1-254 have already been probed. This is someone not really knowing what they're doing, or a clumsy programmer.

=====

Detect #9, dug up and compiled from several Snort output files:

-----

```
[**] SNMP-write-write [**]
02/16-22:45:56.398226 0:0:0:55:B6:43 -> 0:0:0:C4:25:8C type:0x800 len:0x5B
0.17.3.44:54064 -> 192.168.1.1:161 UDP TTL:10 TOS:0x0 ID:26881
Len: 14592
30 2F 02 01 00 04 05 77 72 69 74 65 A3 23 02 04 0/.....write.#..
1D 65 1B 74 02 01 00 02 01 00 30 15 30 13 06 0B .e.t.....0.0...
2B 06 01 04 01 84 11 09 05 03 00 40 04 82 11 0E +.....@....
FE .
```

```
[**] SNMP-write-write [**]
02/16-22:45:56.399686 0:0:0:55:B6:43 -> 0:0:0:C4:25:8C type:0x800 len:0x67
0.17.3.44:54064 -> 192.168.1.1:161 UDP TTL:10 TOS:0x0 ID:26882
Len: 17664
30 3B 02 01 00 04 05 77 72 69 74 65 A3 2F 02 04 0;.....write./..
1D 65 1B 75 02 01 00 02 01 00 30 21 30 1F 06 0B .e.u.....0!0...
2B 06 01 04 01 84 11 09 05 04 00 04 10 31 39 32 +.....192
2E 31 36 38 2E 31 2E 31 2E 63 66 67 .168.1.1.cfg
```

```
[**] SNMP-write-write [**]
02/16-22:45:56.400959 0:0:0:55:B6:43 -> 0:0:0:C4:25:8C type:0x800 len:0x58
0.17.3.44:54064 -> 192.168.1.1:161 UDP TTL:10 TOS:0x0 ID:26883
Len: 13824
30 2C 02 01 00 04 05 77 72 69 74 65 A3 20 02 04 0,.....write. ..
1D 65 1B 76 02 01 00 02 01 00 30 12 30 10 06 0B .e.v.....0.0...
2B 06 01 04 01 84 11 09 05 01 00 02 01 01 +.....
```

```
[**] SNMP-write-write [**]
02/16-22:45:56.402283 0:0:0:55:B6:43 -> 0:0:0:C4:25:8C type:0x800 len:0x5B
0.17.3.44:54064 -> 192.168.1.1:161 UDP TTL:10 TOS:0x0 ID:26884
Len: 14592
30 2F 02 01 00 04 05 77 72 69 74 65 A3 23 02 04 0/.....write.#..
1D 65 1B 77 02 01 00 02 01 00 30 15 30 13 06 0B .e.w.....0.0...
2B 06 01 04 01 84 11 09 05 03 00 40 04 00 00 00 +.....@....
00 .
```

---These four packets, with small variations in the payload---  
---depending on the target machine, are sent to 129 other machines,---  
---several of which does not exist.---

Analysis:

The technique:

The source port is being reused, the packets arrive in a very fast succession, and the IDs are incremented by one for each packet. All of this indicates that an automated method is being used. Also notice the low TTL: I doubt these packets have been traveling that far, so the sender is probably intentionally setting a low TTL when constructing the packets.

The intent:

This is definitely someone hostile trying to mess with our machines, rewriting some snmp info.

The severity:

Medium. Unfortunately, I don't know much about snmp, but I don't see any community string in the packets, so I guess and hope that this attack failed. I will however look into it thoroughly.

=====

Detect #10, dug up and compiled from several Snort output files:

-----

```
[**] RPC-portmap-statd-req [**]
02/03-20:15:44.008602 0:0:0:55:B6:43 -> 0:0:0:DA:79:F9 type:0x800 len:0x62
0.76.137.4:682 -> 192.168.2.253:111 UDP TTL:41 TOS:0x0 ID:6855
Len: 16384
39 94 BC 03 00 00 00 00 00 00 02 00 01 86 A0 9.....
00 00 00 02 00 00 00 03 00 00 00 00 00 00 00 .....
00 00 00 00 00 00 00 00 00 01 86 A5 00 00 00 01 .....
00 00 00 06 00 00 00 00 .....
.....
```

```
[**] RPC-portmap-statd-req [**]
02/03-20:15:49.386610 0:0:0:55:B6:43 -> 0:0:0:DA:79:F9 type:0x800 len:0x62
0.76.137.4:683 -> 192.168.2.253:111 UDP TTL:41 TOS:0x0 ID:7175
Len: 16384
39 98 FA 7E 00 00 00 00 00 00 02 00 01 86 A0 9..~.....
00 00 00 02 00 00 00 03 00 00 00 00 00 00 00 .....
00 00 00 00 00 00 00 00 00 01 86 A5 00 00 00 01 .....
00 00 00 11 00 00 00 00 .....
.....
```

```
[**] RPC-portmap-statd-req [**]
02/03-20:22:39.770238 0:0:0:55:B6:43 -> 0:0:0:DA:79:F9 type:0x800 len:0x62
0.243.86.13:809 -> 192.168.2.253:111 UDP TTL:54 TOS:0x0 ID:39533
Len: 16384
39 90 62 83 00 00 00 00 00 00 02 00 01 86 A0 9.b.....
00 00 00 02 00 00 00 03 00 00 00 00 00 00 00 .....
00 00 00 00 00 00 00 00 00 01 86 A5 00 00 00 01 .....
00 00 00 06 00 00 00 00 .....
.....
```

```
[**] RPC-portmap-statd-req [**]
02/03-20:22:41.432716 0:0:0:55:B6:43 -> 0:0:0:DA:79:F9 type:0x800 len:0x62
0.243.86.13:819 -> 192.168.2.253:111 UDP TTL:54 TOS:0x0 ID:39669
Len: 16384
39 9F FF 31 00 00 00 00 00 00 02 00 01 86 A0 9..1.....
00 00 00 02 00 00 00 03 00 00 00 00 00 00 00 .....
00 00 00 00 00 00 00 00 00 01 86 A5 00 00 00 01 .....
00 00 00 11 00 00 00 00 .....
.....
```

Analysis:

The technique:

This could be done by hand, since the packets are not arriving at breakneck speed. The TTL is kind of low, but some machines does set the TTL to 64, and since the packets doesn't look crafted I'd say they're using the default TTL of the source machine. Someone is using a standard program to do these probes.

The intent:

Probably looking for machines running statd, to find ones that has a weakness that can be exploited. I do not know why only one of our machines was targeted. Probably someone wanting to break into our mail server without first checking what OS it was running.

The severity:

Low. The targeted machine is a Windows machine, and is thus not running statd.

Comment:

I have treated these two separate attacks as one, since they were so close in time, and it is possible that it is the same person, with access to machines on different networks, that is performing them.

© SANS

# Upcoming Training

Click Here to  
**{Get CERTIFIED!}**



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 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
Community SANS Nashville SEC401^	Nashville, TN	Jan 08, 2018 - Jan 13, 2018	Community SANS
SANS Security East 2018	New Orleans, LA	Jan 08, 2018 - Jan 13, 2018	Live Event
Las Vegas 2018 - SEC503: Intrusion Detection In-Depth	Las Vegas, NV	Jan 28, 2018 - Feb 02, 2018	vLive
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	McLean, 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 Security West 2018	San Diego, CA	May 11, 2018 - May 18, 2018	Live Event
Community SANS Columbia SEC503	Columbia, MD	Aug 13, 2018 - Aug 18, 2018	Community SANS
SANS OnDemand	Online	Anytime	Self Paced
SANS SelfStudy	Books & MP3s Only	Anytime	Self Paced