Global Information Assurance Certification Paper

*** Northcutt, fine work. Analyst has clearly learned a lot in her journey to acquire detects. Good use of an analysis process. Love the correlation work. Write ups are a shade terse, but chalking that to English as a second language and so no deduction for this. 85 *

SANS GIAC Intrusion Analyst Certification
Practical Exam – 10 Detects with Analysis

Ingeborg Østrem Hellemo
April 17, 2000
Attended SANS 2000 in Orlando, Florida, March 21-28, 2000

First, about the difficulty of finding detects when you need them: Working in an open educational environment means no firewall to collect detects from. Having a switched network infrastructure also makes it hard to collect interesting data. I ended up with a couple of detects from our border router and some from a shadow sensor I was able to put in front of two of our subnets. Nobody scans you when you want them to so I also had to ask a former colleague of mine (hei til deg, forresten :-) if I could have a look at a log from his border router (part of their firewall setup), and luckily (!) they are getting scanned… At last I had to get one trace from the GIAC web site.

Then, the detects: For all detects, unless otherwise stated, X.Y.Z is the offending host, while a.b.c is our host.

Detect 1

udp: X.Y.Z.186 (5) (17)/161 23

```
Apr 10 09:47:46 gw.My.Net 60416: Apr 10 09:47:45.504: %SEC-6-IPACCESSLOGP: list 111 denied udp X.Y.Z.186(4563) (ATM0/1/0.1 VC 26) -> a.b.e.158(161), 1 packet
Apr 10 09:47:47 gw.My.Net 60417: Apr 10 09:47:46.984: %SEC-6-IPACCESSLOGP: list 111 denied udp X.Y.Z.186(4563) (ATM0/1/0.1 VC 26) -> a.b.c.188(161), 1 packet
Apr 10 09:47:48 gw.My.Net 60418: Apr 10 09:47:47.984: %SEC-6-IPACCESSLOGP: list 111 denied udp X.Y.Z.186(4563) (ATM0/1/0.1 VC 26) -> a.b.h.71(161), 1 packet
Apr 10 09:47:49 gw.My.Net 60419: Apr 10 09:47:48.984: %SEC-6-IPACCESSLOGP: list 111 denied udp X.Y.Z.186(4563) (ATM0/1/0.1 VC 26) -> a.b.g.59(161), 1 packet
Apr 10 09:47:53 gw.My.Net 60422: Apr 10 09:47:52.484: %SEC-6-IPACCESSLOGP: list 111 denied udp X.Y.Z.186(4563) (ATM0/1/0.1 VC 26) -> a.b.c.236(161), 1 packet
Apr 10 09:47:54 gw.My.Net 60423: Apr 10 09:47:53.496: %SEC-6-IPACCESSLOGP: list 111 denied udp X.Y.Z.186(4563) (ATM0/1/0.1 VC 26) -> a.b.g.80(161), 1 packet
Apr 10 09:47:56 gw.My.Net 60425: Apr 10 09:47:55.616: %SEC-6-IPACCESSLOGP: list 111 denied udp X.Y.Z.186(4567) (ATM0/1/0.1 VC 26) -> a.b.c.246(161), 1 packet
Apr 10 09:47:57 gw.My.Net 60426: Apr 10 09:47:56.632: %SEC-6-IPACCESSLOGP: list 111 denied udp X.Y.Z.186(4564) (ATM0/1/0.1 VC 26) -> a.b.c.236(161), 1 packet
Apr 10 09:47:59 gw.My.Net 60427: Apr 10 09:47:58.632: %SEC-6-IPACCESSLOGP: list 111 denied udp X.Y.Z.186(4563) (ATM0/1/0.1 VC 26) -> a.b.d.119(161), 1 packet
Apr 10 09:48:01 gw.My.Net 60428: Apr 10 09:48:00.180: %SEC-6-IPACCESSLOGP: list 111 denied udp X.Y.Z.186(4563) (ATM0/1/0.1 VC 26) -> a.b.d.101(161), 1 packet
Apr 10 09:48:03 gw.My.Net 60430: Apr 10 09:48:02.632: %SEC-6-IPACCESSLOGP: list 111 denied udp X.Y.Z.186(4567) (ATM0/1/0.1 VC 26) -> a.b.h.71(161), 1 packet
Apr 10 09:48:05 gw.My.Net 60431: Apr 10 09:48:04.616: %SEC-6-IPACCESSLOGP: list 111 denied udp X.Y.Z.186(4564) (ATM0/1/0.1 VC 26) -> a.b.g.80(161), 1 packet
Apr 10 09:48:27 gw.My.Net 60432: Apr 10 09:48:26.640: %SEC-6-IPACCESSLOGP: list 111 denied udp X.Y.Z.186(4563) (ATM0/1/0.1 VC 26) -> a.b.j.254(161), 1 packet
Apr 10 09:48:42 gw.My.Net 60433: Apr 10 09:48:41.452: %SEC-6-IPACCESSLOGP: list 111 denied udp X.Y.Z.186(4563) (ATM0/1/0.1 VC 26) -> a.b.i.34(161), 1 packet
Apr 10 09:49:27 gw.My.Net 60434: Apr 10 09:49:26.108: %SEC-6-IPACCESSLOGP: list 111 denied udp X.Y.Z.186(4566) (ATM0/1/0.1 VC 26) -> a.b.g.59(161), 1 packet
Apr 10 09:49:42 gw.My.Net 60435: Apr 10 09:49:41.364: %SEC-6-IPACCESSLOGP: list 111 denied udp X.Y.Z.186(4565) (ATM0/1/0.1 VC 26) -> a.b.g.53(161), 1 packet
Apr 10 09:49:58 gw.My.Net 60436: Apr 10 09:49:57.200: %SEC-6-IPACCESSLOGP: list 111 denied udp X.Y.Z.186(4567) (ATM0/1/0.1 VC 26) -> a.b.g.50(161), 1 packet
Apr 10 09:51:24 gw.My.Net 60437: Apr 10 09:51:23.673: %SEC-6-IPACCESSLOGP: list 111 denied udp X.Y.Z.186(4564) (ATM0/1/0.1 VC 26) -> a.b.f.115(161), 1 packet
Apr 10 09:52:54 gw.My.Net 60438: Apr 10 09:52:53.669: %SEC-6-IPACCESSLOGP: list 111 denied udp X.Y.Z.186(4566) (ATM0/1/0.1 VC 26) -> a.b.f.60(161), 1 packet
Apr 10 09:53:02 gw.My.Net 60439: Apr 10 09:53:01.501: %SEC-6-IPACCESSLOGP: list 111 denied udp X.Y.Z.186(4565) (ATM0/1/0.1 VC 26) -> a.b.d.124(161), 1 packet
Apr 10 09:53:12 gw.My.Net 60440: Apr 10 09:53:11.345: %SEC-6-IPACCESSLOGP: list 111 denied udp X.Y.Z.186(4567) (ATM0/1/0.1 VC 26) -> a.b.d.119(161), 1 packet
Apr 10 09:53:40 gw.My.Net 60441: Apr 10 09:53:39.301: %SEC-6-IPACCESSLOGP: list 111 denied udp X.Y.Z.186(4566) (ATM0/1/0.1 VC 26) -> a.b.d.101(161), 1 packet
```

Trace Information: This trace is from the log from our border Cisco router. First part of the trace is output from a script that searches for denied packets in the log. (Interpretation: 23 udp packets from 5 source ports on source address X.Y.Z.186 to port 161 on 17 different addresses) The second part is the relevant parts of the Cisco log itself. The border router denies incoming SNMP packets. Source address is .hscis.net. Target hosts are PCs and department servers.
Active Targeting: Yes. They try more than once, even though we do not allow inbound SNMP traffic.
History: None
Technique: Automated scan from 5 different source ports on remote host to selected hosts on 9 different subnets. Time span is 6 minutes, that is not very quick. The router does only deny packets to some ports, so other ports on the targets are possibly scanned at the same time. (I have not access to syslogs on these hosts to verify this.) The fact that mostly servers are scanned indicate that the attacker has collected information about our network earlier.
Intent: This is probably information gathering via SNMP, possibly for later use.
Severity: Low (0).

Criticality: 4 (servers and PCs)
Lethality: 2 (depends a bit on what they intend to use the information for)
System Countermeasures: 3 (unknown)
Net Countermeasures: 3 (router denies inbound SNMP)

Detect 2

tcp:	X.Y.Z.47/1407	a.b.c.177/12346	1
tcp:	X.Y.Z.47/1419	a.b.c.177/12346	1
tcp:	X.Y.Z.47/4480	a.b.e.27/12346	1
tcp:	X.Y.Z.47/1415	a.b.c.177/12346	1
tcp:	X.Y.Z.47/4635	a.b.c.172/12346	4
tcp:	X.Y.Z.47/1411	a.b.c.177/12346	1
tcp:	X.Y.Z.47/1029	a.b.f.47/12346	4
tcp:	X.Y.Z.47/2867	a.b.d.123/12346	3
tcp:	X.Y.Z.47/1412	a.b.c.177/20034	3
tcp:	X.Y.Z.47/2868	a.b.d.123/20034	1

Apr 10 10:08:42 gw.My.Net 60463: Apr 10 10:08:41.746: %SEC-6-IPACCESSLOGP: list 111 denied tcp X.Y.Z.47(1411) (ATM0/1/0.1 VC 26) -> a.b.c.177(12346), 1 packet
Apr 10 10:08:44 gw.My.Net 60464: Apr 10 10:08:43.342: %SEC-6-IPACCESSLOGP: list 111 denied tcp X.Y.Z.47(1407) (ATM0/1/0.1 VC 26) -> a.b.c.177(12346), 1 packet
Apr 10 10:09:33 gw.My.Net 60465: Apr 10 10:09:32.838: %SEC-6-IPACCESSLOGP: list 111 denied tcp X.Y.Z.47(1415) (ATM0/1/0.1 VC 26) -> a.b.c.177(12346), 1 packet
Apr 10 10:09:35 gw.My.Net 60466: Apr 10 10:09:34.234: %SEC-6-IPACCESSLOGP: list 111 denied tcp X.Y.Z.47(1419) (ATM0/1/0.1 VC 26) -> a.b.c.177(12346), 1 packet
Apr 10 10:14:40 gw.My.Net 60472: Apr 10 10:14:39.639: %SEC-6-IPACCESSLOGP: list 111 denied tcp X.Y.Z.47(1412) (ATM0/1/0.1 VC 26) -> a.b.c.177(20034), 3 packets
Apr 10 11:54:01 gw.My.Net 60610: Apr 10 11:54:00.532: %SEC-6-IPACCESSLOGP: list 111 denied tcp X.Y.Z.47(2868) (ATM0/1/0.1 VC 26) -> a.b.d.123(20034), 1 packet
Apr 10 11:54:04 gw.My.Net 60611: Apr 10 11:54:03.572: %SEC-6-IPACCESSLOGP: list 111 denied tcp X.Y.Z.47(2867) (ATM0/1/0.1 VC 26) -> a.b.d.123(12346), 1 packet
Apr 10 11:59:42 gw.My.Net 60615: Apr 10 11:59:41.329: %SEC-6-IPACCESSLOGP: list 111 denied tcp X.Y.Z.47(2867) (ATM0/1/0.1 VC 26) -> a.b.d.123(12346), 2 packets
Apr 10 12:39:31 gw.My.Net 60678: Apr 10 12:39:30.632: %SEC-6-IPACCESSLOGP: list 111 denied tcp X.Y.Z.47(4480) (ATM0/1/0.1 VC 26) -> a.b.e.27(12346), 1 packet
Apr 10 12:42:02 gw.My.Net 60682: Apr 10 12:42:01.588: %SEC-6-IPACCESSLOGP: list 111 denied tcp X.Y.Z.47(4635) (ATM0/1/0.1 VC 26) -> a.b.c.172(12346), 1 packet
Apr 10 12:45:45 gw.My.Net 60689: Apr 10 12:45:44.841: %SEC-6-IPACCESSLOGP: list 111 denied tcp X.Y.Z.47(1029) (ATM0/1/0.1 VC 26) -> a.b.f.47(12346), 1 packet
Apr 10 12:47:43 gw.My.Net 60691: Apr 10 12:47:42.101: %SEC-6-IPACCESSLOGP: list 111 denied tcp X.Y.Z.47(4635) (ATM0/1/0.1 VC 26) -> a.b.c.172(12346), 3 packets
Apr 10 12:51:43 gw.My.Net 60698: Apr 10 12:51:42.166: %SEC-6-IPACCESSLOGP: list 111 denied tcp X.Y.Z.47(1029) (ATM0/1/0.1 VC 26) -> a.b.f.47(12346), 3 packets

Trace Information: Same as in detect #1. Source address is .ideal.net.au, targets are student machines
Active Targeting: Yes. It can't be an accident when one source tries to connect to well known trojan ports an several machines.
History: None
Technique: This trace have three phases: First 4 attempts against tcp port 12346 on one host, but from different source port, that is they are not merely retransmits. After a 5 minutes break port 20034 is tried. Note that the router is only denying a couple of trojan ports.

Other ports can be scanned in the meantime. Two hours later next host is scanned on both ports, and then after 40 minutes 3 other hosts are scanned on port 12346.
Intent: Ports 12346 and 20034 are well known ports for the trojan NetBus. Since the targets are just a few student PCs on different subnets I don't think it is a part of a large-scale trojan scan, but more likely somebody scanning his "friends".
Severity: Medium (2), but the size of the attack is very small.

Criticality: 1 (student PCs)
Lethality: 5
System Countermeasures: 1 (PC in this case implies Microsoft and speaking from experience I doubt that the antivirus software is updated)
Net Countermeasures: 3 (router denies this kind of traffic)

Detect 3

udp:	X.Y.Z.22/40424	a.b.c.140/161	2
udp:	X.Y.Z.22/40780	a.b.d.243/161	1
udp:	X.Y.Z.22/40814	a.b.e.50/161	2
udp:	X.Y.Z.22/40210	a.b.c.170/161	2
udp:	X.Y.Z.22/44339	a.b.f.201/161	1
udp:	X.Y.Z.22/40212	a.b.g.16/161	1
udp:	X.Y.Z.22/39983	a.b.g.42/161	1
udp:	X.Y.Z.22/40589	a.b.c.100/161	1
udp:	X.Y.Z.22/43674	a.b.h.30/161	1

Apr 11 02:22:44 gw.Uit.No 61698: Apr 11 02:22:43.532: %SEC-6-IPACCESSLOGP: list 111 denied udp X.Y.Z.22(39983) (ATM0/1/0.1 VC 26) -> a.b.g.42(161), 1 packet
Apr 11 02:23:32 gw.Uit.No 61700: Apr 11 02:23:31.276: %SEC-6-IPACCESSLOGP: list 111 denied udp X.Y.Z.22(40210) (ATM0/1/0.1 VC 26) -> a.b.c.170(161), 1 packet
Apr 11 02:23:33 gw.Uit.No 61701: Apr 11 02:23:32.660: %SEC-6-IPACCESSLOGP: list 111 denied udp X.Y.Z.22(40212) (ATM0/1/0.1 VC 26) -> a.b.g.16(161), 1 packet
Apr 11 02:24:05 gw.Uit.No 61703: Apr 11 02:24:04.396: %SEC-6-IPACCESSLOGP: list 111 denied udp X.Y.Z.22(40424) (ATM0/1/0.1 VC 26) -> a.b.c.140(161), 1 packet
Apr 11 02:24:31 gw.Uit.No 61704: Apr 11 02:24:30.264: %SEC-6-IPACCESSLOGP: list 111 denied udp X.Y.Z.22(40589) (ATM0/1/0.1 VC 26) -> a.b.c.100(161), 1 packet
Apr 11 02:25:07 gw.Uit.No 61706: Apr 11 02:25:06.024: %SEC-6-IPACCESSLOGP: list 111 denied udp X.Y.Z.22(40780) (ATM0/1/0.1 VC 26) -> a.b.d.243(161), 1 packet
Apr 11 02:25:14 gw.Uit.No 61707: Apr 11 02:25:13.472: %SEC-6-IPACCESSLOGP: list 111 denied udp X.Y.Z.22(40814) (ATM0/1/0.1 VC 26) -> a.b.e.50(161), 1 packet
Apr 11 02:28:56 gw.Uit.No 61710: Apr 11 02:28:55.396: %SEC-6-IPACCESSLOGP: list 111 denied udp X.Y.Z.22(40210) (ATM0/1/0.1 VC 26) -> a.b.c.170(161), 1 packet
Apr 11 02:29:56 gw.Uit.No 61711: Apr 11 02:29:55.412: %SEC-6-IPACCESSLOGP: list 111 denied udp X.Y.Z.22(40424) (ATM0/1/0.1 VC 26) -> a.b.c.140(161), 1 packet
Apr 11 02:30:01 gw.Uit.No 61712: Apr 11 02:30:00.760: %SEC-6-IPACCESSLOGP: list 111 denied udp X.Y.Z.22(43674) (ATM0/1/0.1 VC 26) -> a.b.h.30(161), 1 packet
Apr 11 02:30:56 gw.Uit.No 61713: Apr 11 02:30:55.428: %SEC-6-IPACCESSLOGP: list 111 denied udp X.Y.Z.22(40814) (ATM0/1/0.1 VC 26) -> a.b.e.50(161), 1 packet
Apr 11 02:31:58 gw.Uit.No 61714: Apr 11 02:31:57.268: %SEC-6-IPACCESSLOGP: list 111 denied udp X.Y.Z.22(44339) (ATM0/1/0.1 VC 26) -> a.b.f.201(161), 1 packet

Trace Information: Same as in detect #1. Source host at CS-department at a University in Germany. Destination hosts are all printers.
Active Targeting: Yes.
History: The exact same hosts are scanned each night for at least a week – except in the weekend.
Technique: One host tries to connect to 9 different hosts on udp port 161 (SNMP). The source ports are all different. In the log trace we se three cases of retransmit. Time span is 8 minutes.
Intent: This looks a lot like the information gathering in detect #1, but in this case the targets are all printers and the scans repeats every night, except in the weekend when most machines are turned off. In this detect we also have unique source ports. This is probably a case of over-zealous printer administration software trying to administrate the whole world.
Severity: Very low (-4)

Criticality: 1 (printers)
Lethality: 1 (not really an attack)
System Countermeasures: 1
Net Countermeasures: 5

Detect 4

```
17:35:20.247606 a.b.4.254.59771 > X.Y.Z.2.53: 56886+ (41)
17:35:20.247699 a.b.4.254.59771 > X.Y.Z.2.53: 60383+ (41)
17:35:20.466287 X.Y.Z.2.53 > a.b.4.254.59771: 56886* 1/4/4 (212)
17:35:20.490939 X.Y.Z.2.53 > a.b.4.254.59771: 60383* 1/4/4 (212)
17:35:27.935933 X.Y.Z.2.16402 > a.b.4.200.109: S 212705028:212705028(0) win 512 <mss 1460>
17:35:27.936346 a.b.4.200.109 > X.Y.Z.2.16402: R 0:0(0) ack 212705029 win 0
17:35:27.973223 X.Y.Z.2.16404 > a.b.4.201.109: S 2763612818:2763612818(0) win 512 <mss 1460>
17:35:27.973579 a.b.4.201.109 > X.Y.Z.2.16404: R 0:0(0) ack 2763612819 win 0
17:35:28.042087 X.Y.Z.2.16406 > a.b.4.202.109: S 4132139931:4132139931(0) win 512 <mss 1460>
17:35:33.116143 X.Y.Z.2.16410 > a.b.4.204.109: S 3681613774:3681613774(0) win 512 <mss 1460>
17:35:33.153817 X.Y.Z.2.16411 > a.b.4.205.109: S 1558007659:1558007659(0) win 512 <mss 1460>
17:35:33.214733 X.Y.Z.2.16412 > a.b.4.206.109: S 2423556583:2423556583(0) win 512 <mss 1460>
17:35:33.251486 X.Y.Z.2.16413 > a.b.4.207.109: S 2082977510:2082977510(0) win 512 <mss 1460>
17:35:33.315403 X.Y.Z.2.16414 > a.b.4.246.109: S 3846620956:3846620956(0) win 512 <mss 1460>
17:35:33.419308 X.Y.Z.2.16416 > a.b.4.34.109: S 4108381592:4108381592(0) win 512 <mss 1460>
17:35:44.067062 X.Y.Z.2.16443 > a.b.6.106.109: S 2897104215:2897104215(0) win 512 <mss 1460>
17:35:44.113615 X.Y.Z.2.16444 > a.b.6.107.109: S 234548107:234548107(0) win 512 <mss 1460>
17:35:44.168085 X.Y.Z.2.16446 > a.b.6.108.109: S 2260514480:2260514480(0) win 512 <mss 1460>
17:35:44.212131 X.Y.Z.2.16448 > a.b.6.11.109: S 631659256:631659256(0) win 512 <mss 1460>
17:35:44.276274 X.Y.Z.2.16449 > a.b.6.180.109: S 4266065275:4266065275(0) win 512 <mss 1460>
```

17:35:44.311066 X.Y.Z.2.16450 > a.b.6.181.109: S 1978510815:1978510815(0) win 512 <mss 1460>
17:35:44.476255 X.Y.Z.2.16453 > a.b.6.184.109: S 1597833310:1597833310(0) win 512 <mss 1460>
17:35:47.369619 X.Y.Z.2.16451 > a.b.6.182.109: S 3736318037:3736318037(0) win 32120 <mss 1460>
17:35:47.406575 X.Y.Z.2.16452 > a.b.6.183.109: S 2844418124:2844418124(0) win 32120 <mss 1460>
17:35:49.546272 X.Y.Z.2.16454 > a.b.6.242.109: S 1473280594:1473280594(0) win 512 <mss 1460>
17:35:49.632588 X.Y.Z.2.16457 > a.b.6.41.109: S 4221468830:4221468830(0) win 512 <mss 1460>
17:35:49.733503 X.Y.Z.2.16459 > a.b.6.46.109: S 117960218:117960218(0) win 512 <mss 1460>
17:35:49.781014 X.Y.Z.2.16460 > a.b.6.47.109: S 115695983:115695983(0) win 512 <mss 1460>
17:35:49.834296 X.Y.Z.2.16461 > a.b.6.52.109: S 829382969:829382969(0) win 512 <mss 1460>
17:35:49.880550 X.Y.Z.2.16463 > a.b.6.67.109: S 919805333:919805333(0) win 512 <mss 1460>
17:35:49.933525 X.Y.Z.2.16465 > a.b.6.68.109: S 208549420:208549420(0) win 512 <mss 1460>
17:35:52.877650 X.Y.Z.2.16463 > a.b.6.67.109: S 919805333:919805333(0) win 32120 <mss 1460>
17:35:55.003497 X.Y.Z.2.16467 > a.b.6.83.109: S 1123616004:1123616004(0) win 512 <mss 1460>
17:35:55.059322 X.Y.Z.2.16468 > a.b.6.84.109: S 1117970316:1117970316(0) win 512 <mss 1460>
17:35:55.104767 X.Y.Z.2.16470 > a.b.6.85.109: S 250961568:250961568(0) win 512 <mss 1460>
17:35:55.152756 X.Y.Z.2.16474 > a.b.6.87.109: S 3184324384:3184324384(0) win 512 <mss 1460>
17:35:55.202917 X.Y.Z.2.16475 > a.b.6.91.109: S 2916822828:2916822828(0) win 512 <mss 1460>
17:35:55.255703 X.Y.Z.2.16476 > a.b.6.92.109: S 3574405000:3574405000(0) win 512 <mss 1460>
17:35:55.303643 X.Y.Z.2.16477 > a.b.6.93.109: S 2679365907:2679365907(0) win 512 <mss 1460>
17:35:55.357240 X.Y.Z.2.16478 > a.b.6.94.109: S 1552978835:1552978835(0) win 512 <mss 1460>
17:35:55.405581 X.Y.Z.2.16479 > a.b.6.99.109: S 2111790860:2111790860(0) win 512 <mss 1460>

Trace Information: This trace is from tcpdump after Shadow warned us of a possible host scan. Only traffic to two of our subnets is collected. Reset packets are removed from listing for brevity. Source address is .netinternet.net
Active Targeting: Yes
History: None
Technique: First we observe that our name server, a.b.4.254, is doing a lookup of some sort on port 53 at the remote host and gets an answer. Then suddenly, 7 seconds later the remote host begins to scan all hosts on our two subnets on tcp port 109 (POP2). Notice the 11 seconds break between the scan of a.b.4 and a.b.6 accompanied by a similar break in source port numbering. The attacker is probably busy scanning a.b.5 (which is not behind our sniffer). It is not clear if the name server lookup from our site initiated this scan or the lookup was a result of some host with tcpwrapper in front of POP2 being scanned earlier on. If the attacker started with a.b.1/24 the latter was not the case.
Intent: This is first of all a scan after POP2-servers, but can also be used as a host scan (two for the price of one…)
Severity: For these two subnets, low (1), but the completeness of the scan indicates that also other subnets at our site are scanned, possibly containing hosts that are not as secure. We should notify the administrators on the other subnets and ask them to check their hosts.

Criticality: 3 (Unix desktops and servers)
Lethality: 4 (Known security holes)
System Countermeasures: 5 (Patched systems and not running POP2)
Net Countermeasures: 1 (No firewall or other blocking)

Detect 5

Apr 14 03:17:56 ns inetd[12741]: ftp/tcp: Connection from cm-X-Y-Z-33.nycap.rr.com (X.Y.Z.33) at Fri Apr 14 03:17:56 2000
Apr 14 03:17:57 ns inetd[12748]: telnet/tcp: Connection from cm-X-Y-Z-33.nycap.rr.com (24.25.137.33) at Fri Apr 14 03:17:57 2000
Apr 14 03:21:12 ns ftpd[12741]: refused connect from cm-X-Y-Z-33.nycap.rr.com
Apr 14 03:21:13 ns telnetd[12748]: refused connect from cm-X-Y-Z-33.nycap.rr.com

03:18:34.714233 X.Y.X.33 > a.b.c.254: icmp: echo request
03:18:34.716503 a.b.c.254 > X.Y.X.33: icmp: echo reply
03:18:36.009291 X.Y.X.33 > a.b.c.254: icmp: echo request
03:18:36.009591 a.b.c.254 > X.Y.X.33: icmp: echo reply
03:18:37.346190 X.Y.X.33 > a.b.c.254: icmp: echo request
03:18:37.346470 a.b.c.254 > X.Y.X.33: icmp: echo reply
03:19:32.105480 X.Y.X.33.1066 > a.b.c.254.5: S 578307:578307(0) win 8192 <mss 1456,nop,nop,sackOK> (DF)
03:19:32.105715 a.b.c.254.5 > X.Y.X.33.1066: R 0:11(11) ack 578308 win 0 (DF)
03:19:32.114892 X.Y.X.33.1067 > a.b.c.254.101: S 578307:578307(0) win 8192 <mss 1456,nop,nop,sackOK> (DF)
03:19:32.114897 a.b.c.254.101 > X.Y.X.33.1067: R 0:11(11) ack 578308 win 0 (DF)
03:19:32.121218 X.Y.X.33.1068 > a.b.c.254.37: S 578308:578308(0) win 8192 <mss 1456,nop,nop,sackOK> (DF)
03:19:32.121441 a.b.c.254.37 > X.Y.X.33.1068: R 0:11(11) ack 578309 win 0 (DF)
03:19:32.130899 X.Y.X.33.1069 > a.b.c.254.107: S 578309:578309(0) win 8192 <mss 1456,nop,nop,sackOK> (DF)
03:19:32.130905 a.b.c.254.107 > X.Y.X.33.1069: R 0:11(11) ack 578310 win 0 (DF)
03:19:32.138888 X.Y.X.33.1070 > a.b.c.254.18: S 578309:578309(0) win 8192 <mss 1456,nop,nop,sackOK> (DF)
03:19:32.144687 X.Y.X.33.1071 > a.b.c.254.109: S 578314:578314(0) win 8192 <mss 1456,nop,nop,sackOK> (DF)
03:19:32.153854 X.Y.X.33.1072 > a.b.c.254.42: S 578315:578315(0) win 8192 <mss 1456,nop,nop,sackOK> (DF)
03:19:32.162896 X.Y.X.33.1073 > a.b.c.254.110: S 578316:578316(0) win 8192 <mss 1456,nop,nop,sackOK> (DF)
03:19:32.269090 X.Y.X.33.1076 > a.b.c.254.43: S 578318:578318(0) win 8192 <mss 1456,nop,nop,sackOK> (DF)
03:19:32.274870 X.Y.X.33.1077 > a.b.c.254.113: S 578319:578319(0) win 8192 <mss 1456,nop,nop,sackOK> (DF)
03:19:32.307012 X.Y.X.33.1079 > a.b.c.254.115: S 578321:578321(0) win 8192 <mss 1456,nop,nop,sackOK> (DF)
03:19:32.316828 X.Y.X.33.1080 > a.b.c.254.49: S 578323:578323(0) win 8192 <mss 1456,nop,nop,sackOK> (DF)
03:19:32.325494 X.Y.X.33.1081 > a.b.c.254.9: S 578323:578323(0) win 8192 <mss 1456,nop,nop,sackOK> (DF)
03:19:32.332624 X.Y.X.33.1082 > a.b.c.254.53: S 578324:578324(0) win 8192 <mss 1456,nop,nop,sackOK> (DF)
03:19:32.332875 a.b.c.254.53 > X.Y.X.33.1082: S 1604920152:1604920152(0) ack 578325 win 32768 <mss 1456>
03:19:32.340835 X.Y.X.33.1083 > a.b.c.254.20: S 578325:578325(0) win 8192 <mss 1456,nop,nop,sackOK> (DF)

03:19:32.349345 X.Y.X.33.1084 > a.b.c.254.70: S 578326:578326(0) win 8192 <mss 1456,nop,nop,sackOK> (DF)
03:19:32.355733 X.Y.X.33.1085 > a.b.c.254.11: S 578327:578327(0) win 8192 <mss 1456,nop,nop,sackOK> (DF)
03:19:32.365540 X.Y.X.33.1086 > a.b.c.254.79: S 578328:578328(0) win 8192 <mss 1456,nop,nop,sackOK> (DF)
03:19:32.373218 X.Y.X.33.1087 > a.b.c.254.21: S 578329:578329(0) win 8192 <mss 1456,nop,nop,sackOK> (DF)
03:19:32.373437 a.b.c.254.21 > X.Y.X.33.1087: S 1604987228:1604987228(0) ack 578330 win 32768 <mss 1456>
03:19:32.380158 X.Y.X.33.1088 > a.b.c.254.80: S 578330:578330(0) win 8192 <mss 1456,nop,nop,sackOK> (DF)
03:19:32.389402 X.Y.X.33.1089 > a.b.c.254.13: S 578331:578331(0) win 8192 <mss 1456,nop,nop,sackOK> (DF)
03:19:32.399282 X.Y.X.33.1090 > a.b.c.254.84: S 578332:578332(0) win 8192 <mss 1456,nop,nop,sackOK> (DF)
03:19:32.405406 X.Y.X.33.1091 > a.b.c.254.23: S 578333:578333(0) win 8192 <mss 1456,nop,nop,sackOK> (DF)
03:19:32.405621 a.b.c.254.23 > X.Y.X.33.1091: S 1605054303:1605054303(0) ack 578334 win 32768 <mss 1456>
03:19:32.413750 X.Y.X.33.1092 > a.b.c.254.88: S 578334:578334(0) win 8192 <mss 1456,nop,nop,sackOK> (DF)
03:19:32.422763 X.Y.X.33.1093 > a.b.c.254.17: S 578334:578334(0) win 8192 <mss 1456,nop,nop,sackOK> (DF)
03:19:32.428144 X.Y.X.33.1094 > a.b.c.254.92: S 578336:578336(0) win 8192 <mss 1456,nop,nop,sackOK> (DF)
03:19:32.438527 X.Y.X.33.1095 > a.b.c.254.25: S 578336:578336(0) win 8192 <mss 1456,nop,nop,sackOK> (DF)
03:19:32.438740 a.b.c.254.25 > X.Y.X.33.1095: S 1605129570:1605129570(0) ack 578337 win 32768 <mss 1456>
03:19:32.447037 X.Y.X.33.1096 > a.b.c.254.93: S 578337:578337(0) win 8192 <mss 1456,nop,nop,sackOK> (DF)
03:19:32.453308 X.Y.X.33.1097 > a.b.c.254.119: S 578339:578339(0) win 8192 <mss 1456,nop,nop,sackOK> (DF)
03:19:32.462733 X.Y.X.33.1098 > a.b.c.254.123: S 578339:578339(0) win 8192 <mss 1456,nop,nop,sackOK> (DF)
03:19:32.476359 X.Y.X.33.1099 > a.b.c.254.129: S 578340:578340(0) win 8192 <mss 1456,nop,nop,sackOK> (DF)
03:19:32.492854 X.Y.X.33.1101 > a.b.c.254.169: S 578342:578342(0) win 8192 <mss 1456,nop,nop,sackOK> (DF)
03:19:32.503698 X.Y.X.33.1102 > a.b.c.254.194: S 578343:578343(0) win 8192 <mss 1456,nop,nop,sackOK> (DF)
03:19:32.508119 X.Y.X.33.1103 > a.b.c.254.512: S 578344:578344(0) win 8192 <mss 1456,nop,nop,sackOK> (DF)
03:19:32.518050 X.Y.X.33.1104 > a.b.c.254.513: S 578345:578345(0) win 8192 <mss 1456,nop,nop,sackOK> (DF)
03:19:32.525998 X.Y.X.33.1105 > a.b.c.254.514: S 578346:578346(0) win 8192 <mss 1456,nop,nop,sackOK> (DF)
03:19:32.533238 X.Y.X.33.1106 > a.b.c.254.515: S 578347:578347(0) win 8192 <mss 1456,nop,nop,sackOK> (DF)
03:19:32.543008 X.Y.X.33.1107 > a.b.c.254.517: S 578348:578348(0) win 8192 <mss 1456,nop,nop,sackOK> (DF)
03:19:32.551402 X.Y.X.33.1108 > a.b.c.254.519: S 578349:578349(0) win 8192 <mss 1456,nop,nop,sackOK> (DF)
03:19:32.558945 X.Y.X.33.1109 > a.b.c.254.540: S 578350:578350(0) win 8192 <mss 1456,nop,nop,sackOK> (DF)
03:19:32.568569 X.Y.X.33.1110 > a.b.c.254.543: S 578351:578351(0) win 8192 <mss 1456,nop,nop,sackOK> (DF)
03:19:32.576648 X.Y.X.33.1111 > a.b.c.254.544: S 578352:578352(0) win 8192 <mss 1456,nop,nop,sackOK> (DF)
03:19:32.583199 X.Y.X.33.1112 > a.b.c.254.550: S 578353:578353(0) win 8192 <mss 1456,nop,nop,sackOK> (DF)
03:19:32.594828 X.Y.X.33.1113 > a.b.c.254.555: S 578354:578354(0) win 8192 <mss 1456,nop,nop,sackOK> (DF)
03:19:32.601297 X.Y.X.33.1114 > a.b.c.254.556: S 578355:578355(0) win 8192 <mss 1456,nop,nop,sackOK> (DF)
03:19:32.607771 X.Y.X.33.1115 > a.b.c.254.560: S 578356:578356(0) win 8192 <mss 1456,nop,nop,sackOK> (DF)
03:19:32.617685 X.Y.X.33.1116 > a.b.c.254.561: S 578357:578357(0) win 8192 <mss 1456,nop,nop,sackOK> (DF)
03:19:32.670464 X.Y.X.33.1118 > a.b.c.254.565: S 578359:578359(0) win 8192 <mss 1456,nop,nop,sackOK> (DF)
03:19:32.676158 X.Y.X.33.1119 > a.b.c.254.754: S 578360:578360(0) win 8192 <mss 1456,nop,nop,sackOK> (DF)
03:19:32.685745 X.Y.X.33.1120 > a.b.c.254.758: S 578361:578361(0) win 8192 <mss 1456,nop,nop,sackOK> (DF)
03:19:32.694024 X.Y.X.33.1121 > a.b.c.254.774: S 578381:578381(0) win 8192 <mss 1456,nop,nop,sackOK> (DF)
03:19:32.703129 X.Y.X.33.1122 > a.b.c.254.8080: S 578381:578381(0) win 8192 <mss 1456,nop,nop,sackOK> (DF)

```
03:19:32.711912 X.Y.X.33.1082 > a.b.c.254.53: . ack 1 win 8736 (DF)
03:19:32.720049 X.Y.X.33.1087 > a.b.c.254.21: . ack 1 win 8736 (DF)
03:19:32.727720 X.Y.X.33.1095 > a.b.c.254.25: . ack 1 win 8736 (DF)
03:19:33.474667 a.b.c.254.52746 > X.Y.X.33.113: S 1605532106:1605532106(0) win 0 <mss 1460,wscale 0,nop>
03:19:33.744178 X.Y.X.33.113 > a.b.c.254.52746: R 0:0(0) ack 1605532107 win 0
03:19:34.452258 a.b.c.254.23 > X.Y.X.33.1091: S 1605054303:1605054303(0) ack 578334 win 32768 <mss 1456>
03:19:34.711385 X.Y.X.33.1091 > a.b.c.254.23: . ack 1 win 8736 (DF)
03:19:34.752321 a.b.c.254.52747 > X.Y.X.33.113: S 1605863497:1605863497(0) win 0 <mss 1460,wscale 0,nop>
03:19:35.004281 X.Y.X.33.113 > a.b.c.254.52747: R 0:0(0) ack 1605863498 win 0
03:19:36.247456 a.b.c.254.52748 > X.Y.X.33.113: S 1606264031:1606264031(0) win 0 <mss 1460,wscale 0,nop>
03:19:36.509711 X.Y.X.33.113 > a.b.c.254.52748: R 0:0(0) ack 1606264032 win 0
03:19:37.206724 a.b.c.254.25 > X.Y.X.33.1095: P 1:89(88) ack 1 win 32768
03:19:37.478592 X.Y.X.33.1095 > a.b.c.254.25: F 1:1(0) ack 89 win 8648 (DF)
03:19:37.478814 a.b.c.254.25 > X.Y.X.33.1095: . ack 2 win 32768
03:19:37.479327 a.b.c.254.25 > X.Y.X.33.1095: F 89:89(0) ack 2 win 0
03:19:37.722919 X.Y.X.33.1095 > a.b.c.254.25: . ack 90 win 8648 (DF)

03:20:51.060370 a.b.c.254.52753 > X.Y.X.33.79: S 1616930635:1616930635(0) win 32768 <mss 1460,wscale 0,nop>
03:20:52.210497 a.b.c.254.52754 > X.Y.X.33.79: S 1617122750:1617122750(0) win 32768 <mss 1460,wscale 0,nop>
03:20:55.141019 a.b.c.254.52753 > X.Y.X.33.79: S 1616930635:1616930635(0) win 32768 <mss 1460,wscale 0,nop>

Traffic from remote site to our web server removed

03:22:54.145171 a.b.c.254.21 > X.Y.X.33.1087: F 1:1(0) ack 1 win 32768
03:22:54.399241 X.Y.X.33.1087 > a.b.c.254.21: . ack 2 win 8736 (DF)
03:22:54.406682 X.Y.X.33.1087 > a.b.c.254.21: F 1:1(0) ack 2 win 8736 (DF)
03:22:54.406913 a.b.c.254.21 > X.Y.X.33.1087: . ack 2 win 32768
03:22:55.485469 a.b.c.254.23 > X.Y.X.33.1091: F 1:1(0) ack 1 win 32768
03:22:55.743563 X.Y.X.33.1091 > a.b.c.254.23: . ack 2 win 8736 (DF)
03:22:55.750968 X.Y.X.33.1091 > a.b.c.254.23: F 1:1(0) ack 2 win 8736 (DF)
03:22:55.751172 a.b.c.254.23 > X.Y.X.33.1091: . ack 2 win 32768
03:23:00.016119 X.Y.X.33.1082 > a.b.c.254.53: R 578325:578325(0) win 0 (DF)
```

Trace Information: This is a very long trace, but the original was approximately 600 lines. First four lines are from the syslog at our name server. Our name server is also behind a Shadow sniffer and the rest of the trace is tcpdump output from the sniffer. This kind of portscan is not detected by Shadow, but the syslog output made me look closer on the tcpdump. In the complete trace we see 60 connection from remote host per second. Reset packets are removed from listing for brevity. After the initial scan of ports the ports

which have not returned a Syn-Ack is scanned 3 or 4 more times with the same source port - destination port pair. This is also removed from the trace and is what happens between 03:19 and 03:22
Active Targeting: Yes
History: None
Technique: First out name server is pinged three times by the remote host. Then some, but not all of the low tcp ports plus 8080 are scanned in rapid succession. In the trace we see the complete three-way-handshake on the ports the server listens on (21 - ftp, 23 - telnet, 25 - smtp and of course 53 - dns) . Port 21 and 23 are behind tcpwrapper and is why this scan ended up in the syslog. Near the end of the trace we see the result of tcpwrapper trying to find out who this is with connections to port 113 (ident) and 79 (finger). None of these succeed. While all this automated stuff is going on, somebody on the remote machine is surfing our web! The last lines are the remote host politely closing down the established connections.
Not all the low ports are scanned., i.e. is port 22 (ssh) and 111 (sunrpc with lots of security "features") left out. Different OS have different ports listed in /etc/services. It might be possible to look at the ports scanned and deduce which OS this attack is crafted for.
Intent: Tcp port scan to find out which services the server runs. The attacker did not find the ones he was looking for or will come back later.
Severity: Low (1)

Criticality: 5 (primary DNS server)
Lethality: 2 (we do not know what the attacker is planning to do)
System Countermeasures: 5 (recently patched, tcpwrapper and no unnecessary services)
Net Countermeasures: 1 (no firewall)

Detect 6

```
206.99.115.90 > a.b.c.186
12:56:20.503174 proxy.monitor.dal.net.43910 > isdn-56.Modem.My.Net.1080: S 818551286:818551286(0) win 8760  (DF)
12:56:23.997789 proxy.monitor.dal.net.43910 > isdn-56.Modem.My.Net.1080: S 818551286:818551286(0) win 8760  (DF)
12:56:24.250696 proxy.monitor.dal.net.44000 > isdn-56.Modem.My.Net.23: S 3900820643:3900820643(0) win 8760  (DF)
```

Trace Information: Collected from shadow with sniffer connected in front of our dial-in network. We do not have the complete tcpdump
Active Targeting: Yes, we see inbound connections to a home machine not supposed to run any services.
History: None
Technique: The remote host connects to port 1080 (SOCKS) and 23 (telnet) on the home machine. Different source port to different destination port.

Intent: As we see from the name of the remote machine, this is an IRC server. The connections are then merely self-defense to check if the host trying to connect to their IRC services is running an insecure Wingate or Socks server. This is harmless traffic and almost all well-maintained IRC servers do this. (We have an IRC server inside our net and every once in a while we get complaints from people being "scanned")
Severity: Low.

Detect 7

tcp: 208.218.89.7/65000 (37) (37) 37

Apr 13 16:50:38 gw.My.Net 352567: 44w2d: %SEC-6-IPACCESSLOGP: list gw.nospoof-2 denied tcp 208.218.89.7(65000) (Ethernet1/1) -> a.b.77.63(54613), 1 packet
Apr 13 16:51:22 gw.My.Net 352570: 44w2d: %SEC-6-IPACCESSLOGP: list gw.nospoof-2 denied tcp 208.218.89.7(65000) (Ethernet1/1) -> a.b.88.109(857), 1 packet
Apr 13 16:52:34 gw.My.Net 352572: 44w2d: %SEC-6-IPACCESSLOGP: list gw.nospoof-2 denied tcp 208.218.89.7(65000) (Ethernet1/1) -> a.b.84.62(16028), 1 packet
Apr 13 16:53:44 gw.My.Net 352577: 44w2d: %SEC-6-IPACCESSLOGP: list gw.nospoof-2 denied tcp 208.218.89.7(65000) (Ethernet1/1) -> a.b.69.95(28321), 1 packet
Apr 13 16:54:46 gw.My.Net 352579: 44w2d: %SEC-6-IPACCESSLOGP: list gw.nospoof-2 denied tcp 208.218.89.7(65000) (Ethernet1/1) -> a.b.70.53(35028), 1 packet
Apr 13 16:55:26 gw.My.Net 352580: 44w2d: %SEC-6-IPACCESSLOGP: list gw.nospoof-2 denied tcp 208.218.89.7(65000) (Ethernet1/1) -> a.b.73.26(29386), 1 packet
Apr 13 16:55:40 gw.My.Net 352583: 44w2d: %SEC-6-IPACCESSLOGP: list gw.nospoof-2 denied tcp 208.218.89.7(65000) (Ethernet1/1) -> a.b.94.65(57324), 1 packet
Apr 13 16:55:46 gw.My.Net 352584: 44w2d: %SEC-6-IPACCESSLOGP: list gw.nospoof-2 denied tcp 208.218.89.7(65000) (Ethernet1/1) -> a.b.92.81(54231), 1 packet
Apr 13 16:55:59 gw.My.Net 352585: 44w2d: %SEC-6-IPACCESSLOGP: list gw.nospoof-2 denied tcp 208.218.89.7(65000) (Ethernet1/1) -> a.b.90.66(12872), 1 packet
Apr 13 16:59:54 gw.My.Net 352588: 44w2d: %SEC-6-IPACCESSLOGP: list gw.nospoof-2 denied tcp 208.218.89.7(65000) (Ethernet1/1) -> a.b.94.127(63569), 1 packet
Apr 13 17:03:46 gw.My.Net 352604: 44w2d: %SEC-6-IPACCESSLOGP: list gw.nospoof-2 denied tcp 208.218.89.7(65000) (Ethernet1/1) -> a.b.91.23(42089), 1 packet
Apr 13 17:04:53 gw.My.Net 352606: 44w2d: %SEC-6-IPACCESSLOGP: list gw.nospoof-2 denied tcp 208.218.89.7(65000) (Ethernet1/1) -> a.b.85.70(33848), 1 packet
Apr 13 17:07:07 gw.My.Net 352609: 44w2d: %SEC-6-IPACCESSLOGP: list gw.nospoof-2 denied tcp 208.218.89.7(65000) (Ethernet1/1) -> a.b.73.8(34867), 1 packet
Apr 13 17:07:36 gw.My.Net 352611: 44w2d: %SEC-6-IPACCESSLOGP: list gw.nospoof-2 denied tcp 208.218.89.7(65000) (Ethernet1/1) -> a.b.92.32(5363), 1 packet
Apr 13 17:07:42 gw.My.Net 352612: 44w2d: %SEC-6-IPACCESSLOGP: list gw.nospoof-2 denied tcp 208.218.89.7(65000) (Ethernet1/1) -> a.b.78.108(35562), 1 packet
Apr 13 17:08:37 gw.My.Net 352614: 44w2d: %SEC-6-IPACCESSLOGP: list gw.nospoof-2 denied tcp 208.218.89.7(65000) (Ethernet1/1) -> a.b.72.49(14051), 1 packet
Apr 13 17:09:23 gw.My.Net 352617: 44w2d: %SEC-6-IPACCESSLOGP: list gw.nospoof-2 denied tcp 208.218.89.7(65000) (Ethernet1/1) -> a.b.89.85(1822), 1 packet
Apr 13 17:09:59 gw.My.Net 352619: 44w2d: %SEC-6-IPACCESSLOGP: list gw.nospoof-2 denied tcp 208.218.89.7(65000) (Ethernet1/1) -> a.b.65.13(54666), 1 packet
Apr 13 17:12:45 gw.My.Net 352623: 44w2d: %SEC-6-IPACCESSLOGP: list gw.nospoof-2 denied tcp 208.218.89.7(65000) (Ethernet1/1) -> a.b.65.94(64843), 1 packet
Apr 13 17:12:51 gw.My.Net 352624: 44w2d: %SEC-6-IPACCESSLOGP: list gw.nospoof-2 denied tcp 208.218.89.7(65000) (Ethernet1/1) -> a.b.76.57(24653), 1 packet
Apr 13 17:14:20 gw.My.Net 352627: 44w2d: %SEC-6-IPACCESSLOGP: list gw.nospoof-2 denied tcp 208.218.89.7(65000) (Ethernet1/1) -> a.b.65.123(34151), 1 packet
Apr 13 17:14:48 gw.My.Net 352628: 44w2d: %SEC-6-IPACCESSLOGP: list gw.nospoof-2 denied tcp 208.218.89.7(65000) (Ethernet1/1) -> a.b.71.79(41431), 1 packet
Apr 13 17:16:10 gw.My.Net 352631: 44w2d: %SEC-6-IPACCESSLOGP: list gw.nospoof-2 denied tcp 208.218.89.7(65000) (Ethernet1/1) -> a.b.68.10(29585), 1 packet
Apr 13 17:16:49 gw.My.Net 352632: 44w2d: %SEC-6-IPACCESSLOGP: list gw.nospoof-2 denied tcp 208.218.89.7(65000) (Ethernet1/1) -> a.b.94.56(7591), 1 packet
Apr 13 17:21:19 gw.My.Net 352639: 44w2d: %SEC-6-IPACCESSLOGP: list gw.nospoof-2 denied tcp 208.218.89.7(65000) (Ethernet1/1) -> a.b.70.102(16123), 1 packet
Apr 13 17:21:44 gw.My.Net 352640: 44w2d: %SEC-6-IPACCESSLOGP: list gw.nospoof-2 denied tcp 208.218.89.7(65000) (Ethernet1/1) -> a.b.89.80(28914), 1 packet
Apr 13 17:21:56 gw.My.Net 352641: 44w2d: %SEC-6-IPACCESSLOGP: list gw.nospoof-2 denied tcp 208.218.89.7(65000) (Ethernet1/1) -> a.b.71.106(3453), 1 packet
Apr 13 17:22:15 gw.My.Net 352643: 44w2d: %SEC-6-IPACCESSLOGP: list gw.nospoof-2 denied tcp 208.218.89.7(65000) (Ethernet1/1) -> a.b.70.87(54092), 1 packet
Apr 13 17:25:02 gw.My.Net 352647: 44w2d: %SEC-6-IPACCESSLOGP: list gw.Any2DMZ-3 denied tcp 208.218.89.7(65000) (Ethernet1/1) -> a.b.64.91(39720), 1 packet
Apr 13 17:26:41 gw.My.Net 352651: 44w2d: %SEC-6-IPACCESSLOGP: list gw.nospoof-2 denied tcp 208.218.89.7(65000) (Ethernet1/1) -> a.b.83.120(43363), 1 packet
Apr 13 17:28:12 gw.My.Net 352653: 44w2d: %SEC-6-IPACCESSLOGP: list gw.nospoof-2 denied tcp 208.218.89.7(65000) (Ethernet1/1) -> a.b.69.107(64381), 1 packet

```
Apr 13 17:29:53 gw.My.Net 352661: 44w2d: %SEC-6-IPACCESSLOGP: list gw.nospoof-2 denied tcp 208.218.89.7(65000) (Ethernet1/1) -> a.b.71.85(43586), 1 packet
Apr 13 17:31:13 gw.My.Net 352669: 44w2d: %SEC-6-IPACCESSLOGP: list gw.nospoof-2 denied tcp 208.218.89.7(65000) (Ethernet1/1) -> a.b.74.34(39834), 1 packet
Apr 13 17:31:28 gw.My.Net 352670: 44w2d: %SEC-6-IPACCESSLOGP: list gw.nospoof-2 denied tcp 208.218.89.7(65000) (Ethernet1/1) -> a.b.76.95(52435), 1 packet
Apr 13 17:32:36 gw.My.Net 352673: 44w2d: %SEC-6-IPACCESSLOGP: list gw.Any2DMZ-3 denied tcp 208.218.89.7(65000) (Ethernet1/ ) -> a.b.64.46(37806), 1 packet
Apr 13 17:33:37 gw.My.Net 352674: 44w2d: %SEC-6-IPACCESSLOGP: list gw.nospoof-2 denied tcp 208.218.89.7(65000) (Ethernet1/1) -> a.b.80.121(64414), 1 packet
```

Trace Information: This trace is from a site with stronger security policy than we have. The log is from their border router, which is part of their firewall setup. 208.218.89.7 is dalnet.webbernet.net and the local ip addresses are not in use. The Cisco logs does not tell us where in the tcp connection we are (Syn vs. Syn-Ack)
Active Targeting: At first glance, yes. We see incoming packets to ip addresses not supposed to get any traffic.
History: Not directly related to these hosts, but one day earlier an IRC server on our net suffered under a DoS attack aimed at port 65000 so heavy that our ISP had to stop incoming traffic to our host at the border router to our country.
Technique: Lot of incoming tcp packets from same host/port pair to 37 local addresses on different subnets with different destination ports. This happens over a period of 30 minutes, that is not very fast. There is no pattern in the destination ports used. 65000 is the port number of a trojan called Devil.
Intent: This is not a host scan even though we see a lot of packets from one source to a lot of different local destinations. This is probably a case of a company's address space being misused as forged source addresses in a DoS attack against an IRC server. This company's ip range is perfect for such use. They have a lot of class C subnets assigned to the company, but after they put up their firewall they are using private addresses behind the firewall and only a dozen of the real ip addresses are in use.
Severity: Low. It is difficult to put together any arithmetic on this case since this site is not the one under attack. Their only risk is being accused of an attack against the IRC server.

Detect 8

tcp: 63.26.93.42 (58) (58)/53 58

```
Apr 13 02:15:33 gw.My.Net 351383: 44w1d: %SEC-6-IPACCESSLOGP: list gw.Any2DMZ-3 denied tcp X.Y.Z.42(5239) (Ethernet1/1) -> a.b.64.6(53), 1 packet
Apr 13 02:17:43 gw.My.Net 351386: 44w1d: %SEC-6-IPACCESSLOGP: list gw.nospoof-2 denied tcp X.Y.Z.42(16444) (Ethernet1/1) -> a.b.65.6(53), 1 packet
Apr 13 02:22:03 gw.My.Net 351387: 44w1d: %SEC-6-IPACCESSLOGP: list gw.nospoof-2 denied tcp X.Y.Z.42(4702) (Ethernet1/1) -> a.b.67.6(53), 1 packet
Apr 13 02:24:13 gw.My.Net 351388: 44w1d: %SEC-6-IPACCESSLOGP: list gw.nospoof-2 denied tcp X.Y.Z.42(15967) (Ethernet1/1) -> a.b.68.6(53), 1 packet
Apr 13 02:26:23 gw.My.Net 351389: 44w1d: %SEC-6-IPACCESSLOGP: list gw.nospoof-2 denied tcp X.Y.Z.42(27472) (Ethernet1/1) -> a.b.69.6(53), 1 packet
Apr 13 02:28:33 gw.My.Net 351390: 44w1d: %SEC-6-IPACCESSLOGP: list gw.nospoof-2 denied tcp X.Y.Z.42(5425) (Ethernet1/1) -> a.b.70.6(53), 1 packet
Apr 13 02:30:43 gw.My.Net 351391: 44w1d: %SEC-6-IPACCESSLOGP: list gw.nospoof-2 denied tcp X.Y.Z.42(16968) (Ethernet1/1) -> a.b.71.6(53), 1 packet

[snip]

Apr 13 11:28:11 gw.My.Net 351704: 44w2d: %SEC-6-IPACCESSLOGP: list gw.Any2DMZ-3 denied tcp X.Y.Z.42(20851) (Ethernet1/1) -> a.b.64.7(53), 1 packet
Apr 13 11:30:22 gw.My.Net 351705: 44w2d: %SEC-6-IPACCESSLOGP: list gw.nospoof-2 denied tcp X.Y.Z.42(31038) (Ethernet1/1) -> a.b.65.7(53), 1 packet
Apr 13 11:34:42 gw.My.Net 351710: 44w2d: %SEC-6-IPACCESSLOGP: list gw.nospoof-2 denied tcp X.Y.Z.42(21229) (Ethernet1/1) -> a.b.67.7(53), 1 packet
Apr 13 11:36:52 gw.My.Net 351715: 44w2d: %SEC-6-IPACCESSLOGP: list gw.nospoof-2 denied tcp X.Y.Z.42(31075) (Ethernet1/1) -> a.b.68.7(53), 1 packet
Apr 13 11:39:02 gw.My.Net 351720: 44w2d: %SEC-6-IPACCESSLOGP: list gw.nospoof-2 denied tcp X.Y.Z.42(11910) (Ethernet1/1) -> a.b.69.7(53), 1 packet
Apr 13 11:41:12 gw.My.Net 351726: 44w2d: %SEC-6-IPACCESSLOGP: list gw.nospoof-2 denied tcp X.Y.Z.42(20840) (Ethernet1/1) -> a.b.70.7(53), 1 packet
Apr 13 11:43:22 gw.My.Net 351728: 44w2d: %SEC-6-IPACCESSLOGP: list gw.nospoof-2 denied tcp X.Y.Z.42(31501) (Ethernet1/1) -> a.b.71.7(53), 1 packet
```

Trace Information: Same source as in detect #7. Source address is .da.uu.net. All of their class C nets are scanned with at total of 58 packets logged.
Active Targeting: Yes, this traffic violates the security policy.
History: None
Technique: Automated scan of port 53 on a lot of hosts. One packet is sent every other minute. Part one of the scan is in the middle of the night against all a.b.c.6 addresses. Part two is in the middle of the day against all a.b.c.7 addresses. (It would have been nice to have a look at the logs for the days before and after to see if we find scans against a.b.c.5 or a.b.c.8.) The spacing between the packets indicates that other nets are scanned at the same time, or they are trying not to get caught in any intrusion detection filters. There is no pattern in the source port numbers, which indicates that this is a busy host.
Intent: Large scale scan for DNS servers. It is at the same time a host scan.
Severity: Medium (2). I would keep an eye on that DNS server, just in case.

Criticality: 5 (DNS servers)
Lethality: 4 (Depends on what they are planning to do)
System Countermeasures: 4 (The DNS server that is running at this site (if the scan finally finds it) is properly patched.)
Net Countermeasures: 3 (Restrictive firewall, but traffic to port 53 at the real DNS server will not have any protection)

Detect 9

tcp:	X.Y.Z.15 (6)	(8)/1345	38
tcp:	X.Y.Z.15 (7)	(7)/1490	32

```
Apr 13 16:04:21 gw.My.Net 352512: 44w2d: %SEC-6-IPACCESSLOGP: list gw.nospoof-2 denied tcp X.Y.Z.15(79) (Ethernet1/1) -> a.b.c.115(1345), 1 packet
Apr 13 16:04:24 gw.My.Net 352513: 44w2d: %SEC-6-IPACCESSLOGP: list gw.nospoof-2 denied tcp X.Y.Z.15(9) (Ethernet1/1) -> a.b.c.115(1345), 1 packet
Apr 13 16:04:26 gw.My.Net 352515: 44w2d: %SEC-6-IPACCESSLOGP: list gw.nospoof-2 denied tcp X.Y.Z.15(23) (Ethernet1/1) -> a.b.c.115(1345), 1 packet
Apr 13 16:06:07 gw.My.Net 352519: 44w2d: %SEC-6-IPACCESSLOGP: list gw.nospoof-2 denied tcp X.Y.Z.15(79) (Ethernet1/1) -> a.b.d.93(1490), 1 packet
Apr 13 16:06:12 gw.My.Net 352520: 44w2d: %SEC-6-IPACCESSLOGP: list gw.nospoof-2 denied tcp X.Y.Z.15(23) (Ethernet1/1) -> a.b.d.93(1490), 1 packet
Apr 13 16:06:13 gw.My.Net 352521: 44w2d: %SEC-6-IPACCESSLOGP: list gw.nospoof-2 denied tcp X.Y.Z.15(110) (Ethernet1/1) -> a.b.d.93(1490), 1 packet
Apr 13 16:06:14 gw.My.Net 352522: 44w2d: %SEC-6-IPACCESSLOGP: list gw.nospoof-2 denied tcp X.Y.Z.15(143) (Ethernet1/1) -> a.b.d.93(1490), 1 packet
Apr 13 16:06:16 gw.My.Net 352523: 44w2d: %SEC-6-IPACCESSLOGP: list gw.nospoof-2 denied tcp X.Y.Z.15(7) (Ethernet1/1) -> a.b.d.93(1490), 1 packet
Apr 13 18:53:24 gw.My.Net 352755: 44w2d: %SEC-6-IPACCESSLOGP: list gw.nospoof-2 denied tcp X.Y.Z.15(9) (Ethernet1/1) -> a.b.d.104(1345), 1 packet
Apr 13 18:53:41 gw.My.Net 352756: 44w2d: %SEC-6-IPACCESSLOGP: list gw.nospoof-2 denied tcp X.Y.Z.15(79) (Ethernet1/1) -> a.b.d.104(1345), 1 packet
Apr 13 18:54:14 gw.My.Net 352757: 44w2d: %SEC-6-IPACCESSLOGP: list gw.nospoof-2 denied tcp X.Y.Z.15(23) (Ethernet1/1) -> a.b.d.104(1345), 1 packet
Apr 13 18:54:18 gw.My.Net 352758: 44w2d: %SEC-6-IPACCESSLOGP: list gw.nospoof-2 denied tcp X.Y.Z.15(53) (Ethernet1/1) -> a.b.d.104(1345), 1 packet
Apr 13 18:54:45 gw.My.Net 352759: 44w2d: %SEC-6-IPACCESSLOGP: list gw.nospoof-2 denied tcp X.Y.Z.15(143) (Ethernet1/1) -> a.b.d.104(1345), 1 packet
Apr 13 18:56:07 gw.My.Net 352761: 44w2d: %SEC-6-IPACCESSLOGP: list gw.nospoof-2 denied tcp X.Y.Z.15(7) (Ethernet1/1) -> a.b.d.104(1345), 1 packet
```

Trace Information: Same source as in detect #7. The total trace consists of 70 lines, but I have only included enough to state my point. First log line is from 16:01, the last from 20:15. Source address is disasta.XXX.de. None of the local addresser are in use.
Active Targeting: At first glance, Yes.
History: None
Technique: We see from the first two lines that 15 different hosts at this site with destination ports 1345 and 1490 are receiving packets from 7 different ports at the remote site. The source ports are low tcp ports as 7 (echo), 9 (discard), 23 (telnet), 53 (dns), 79 (finger), 110 (POP3) and 143(IMAP). All of these have either known security holes or can be used in connection with DoS attacks (echo). Discard is mostly being used for host mapping since connections are rarely logged.
Intent: What we see here is the result of this site's address space being used as a smoke screen to hide the real port scanning of X.Y.Z.15. That is X.Y.Z 15 is a target, not an attacker. (As stated in detect #7 this company's address space is perfect for this kind of (mis)use.) This theory is supported by the fact that only two different port numbers are used as destination ports.
Severity: Low (as in detect #7)

Detect 10

```
Apr 3 08:49:22 dns1 snort[4415]: spp_portscan:
PORTSCAN DETECTED from 208.185.54.22
Apr 3 08:49:28 dns1 snort[4415]: spp_portscan: portscan status
from 208.185.54.22: 14 connections across 1 hosts: TCP(0), UDP(14)
Apr 3 08:49:34 dns1 snort[4415]: spp_portscan: End of portscan
from 208.185.54.22
Apr 3 08:49:22 208.185.54.22:33161 -> a.b.c.34:33512 UDP
Apr 3 08:49:22 208.185.54.22:33161 -> a.b.c.34:33513 UDP
Apr 3 08:49:22 208.185.54.22:33161 -> a.b.c.34:33514 UDP
Apr 3 08:49:22 208.185.54.22:33161 -> a.b.c.34:33515 UDP
Apr 3 08:49:22 208.185.54.22:33161 -> a.b.c.34:33516 UDP
Apr 3 08:49:22 208.185.54.22:33161 -> a.b.c.34:33517 UDP
Apr 3 08:49:22 208.185.54.22:33161 -> a.b.c.34:33518 UDP
Apr 3 08:49:22 208.185.54.22:33161 -> a.b.c.34:33519 UDP
Apr 3 08:49:22 208.185.54.22:33161 -> a.b.c.34:33520 UDP
Apr 3 08:49:22 208.185.54.22:33161 -> a.b.c.34:33521 UDP
Apr 3 08:49:22 208.185.54.22:33161 -> a.b.c.34:33522 UDP
Apr 3 08:49:22 208.185.54.22:33161 -> a.b.c.34:33523 UDP
Apr 3 08:49:22 208.185.54.22:33161 -> a.b.c.34:33524 UDP
Apr 3 08:49:22 208.185.54.22:33161 -> a.b.c.34:33525 UDP
```

Trace Information: This trace is from http://www.sans.org/y2k/041200.htm and is output from snort. We know nothing about the destination host. The source address is .speedera.com.
Active Targeting: Yes
History: None
Technique: Remote address/source port scans 14 udp ports on local host in rapid succession (within one second). Snort claims this to be a port scan, but both source and destination ports are within the 33000 range, which are ports used by traceroute.
Intent: This is probably not malicious traffic, but some kind of load balancing. It is hard to tell more without the TTLs.
Severity: Low. (It is difficult to put together any arithmetic on this case since we know nothing of the target system)

Last Updated: July 22nd, 2017

Upcoming Training

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