*** Northcutt, Good use of an analysis process, there is evidence of research, this student has done a pretty good job at running down the source addresses. This is a standard technique in military CIRTs and can provide useful information. As an analyst you really can't say " There are numerous attacks generate from that country." What you can do is say of 5000 examined attacks, 2168 were apparently from country XYZ. In three, if you take on a challenge, need to actually find out what tiny fragments are! The load balancing work is good, a lot of your peers chalked this pattern up to "high UDP port scans". Per six, port 98 is probably linuxconf. Keep after it, you certainly are on a path to become a solid analyst! 79 ***

GCIA Certification - Practical
10 Detects with Analysis

Wayne Simpson
04/11/2000

Background:
All detects were retrieved from the SANS GIAC web site. The sensitivity of the data on my network is such that it is not allowed to leave the premises. Besides, the network is currently closed and there's nothing really worth analyzing.

Comments:
Out of the 10 detects I looked at, I found it interesting that 2 are traceroute related and both were associated with Speedera.com. I believe Speedera has automated load-balancing product running.

ANAYLSIS #1

DATA PROVIDED

Proxy scanning from Belgium. same again, net, host, broadcast.

```
Mar 24 07:30:59 ardvark kernel: Packet log: input DENY eth0 PROTO=6
194.78.174.5:35525 xxx.xxx.xxx.11:8080 L=44 S=0x00 I=807 F=0x4000 T=238 SYN

[**] WinGate 8080 Attempt [**]
03/24-07:30:59.531919 0:E0:D0:15:11:94 -> FF:FF:FF:FF:FF:FF type:0x800 len:0x3C
194.78.174.5:35522 -> xxx.xxx.xxx.8:8080 TCP TTL:238 TOS:0x0 ID:797 DF
S***** Seq: 0xE40B8062 Ack: 0x0 Win: 0x2238
TCP Options => MSS: 1460
00 00 ..

[**] WinGate 8080 Attempt [**]
03/24-07:30:59.542500 0:E0:D0:15:11:94 -> 0:0:C0:29:8F:D2 type:0x800 len:0x3C
194.78.174.5:35525 -> xxx.xxx.xxx.11:8080 TCP TTL:238 TOS:0x0 ID:807 DF
S***** Seq: 0xE40DC872 Ack: 0x0 Win: 0x2238
TCP Options => MSS: 1460
00 00 ..

[**] WinGate 8080 Attempt [**]
03/24-07:30:59.555164 0:E0:D0:15:11:94 -> FF:FF:FF:FF:FF:FF type:0x800 len:0x3C
194.78.174.5:35529 -> xxx.xxx.xxx.15:8080 TCP TTL:238 TOS:0x0 ID:807 DF
S***** Seq: 0xE411D0F2 Ack: 0x0 Win: 0x2238
TCP Options => MSS: 1460
00 00 ..
```

TARGETING

Yes, there evidence of active targeting. The attacker is looking for machines that will respond to a SYN/ACK packet on TCP port 8080. Port 8080 is used by the Wingate proxy and also commonly used as an alternate port for HTTP servers.

INTENT

I believe the attacker is on a reconnaissance mission trying to locate machines running the wingate server.

If the attacker is successful in finding a vulnerable Wingate application, the mscan or multiscan tool provides information to the user that may be useful in hiding their probe attempts against a subnet by bouncing their scans off the Wingate host. Reference CIAC bulletin I-073 dated July 20, 1998.

The attacker is looking for Wingate servers to attack or to help stealth further attacks against other networks.

TECHNIQUES

The timestamps and sequential nature of the source ports indicates this is a sequential automated scan of the xxx.xxx.xxx.??? network.

By sending an unsolicited SYN/ACK packet the attacker is trying to generate a response indicating the presence of a server/listener.

Because the source IP address 194.73.174.5 is a fairly easy to locate and identify, this could be a spoofed source IP with the attacker monitoring/sniffing the network for any RST responses. If the source IP was not spoofed then I believe this attacker to be an amateur or novice at best.

HISTORY
194.73.174.5 is mail.lknet.com which is locate in Belgium. There are numerous attacks generate from that country.

EXISTENCE
INFO on the source IP 194.78.174.5
194.78.174.5 is mail.lknet.com.

The authoritative DNS for this domain are:
alpha.lnet.com - 194.78.174.7
beta.lknet.com - 194.78.174.8
SOA record shows webmin.lknet.com and abs.lkmarketing.be
There are only 8 A records listed in the lknet.com domain

194.78.174.5 is running Solaris 2.6.

The machine appears to be located in or near Brussels Belgium.

A simple port scan of 194.78.174.5 shows the following ports open:
7, 9, 13, 19, 21, 23, 25, 37, 79, 110, 111,143

The mail server is running Netscape Messaging Server version 3.5

SEVERITY – NONE to LOW
This does bear further watching base on the country it is originating from.

ANALYSIS #2

DATA PROVIDED

```
Mar 27 17:01:03.516 host kernel: 226 IP packet dropped
(www7.clever.net[209.235.11.254]->host1[x.x.x.x1]: Protocol=TCP[SYN] Port
53050->5556): Restricted Port: Protocol=TCP[SYN] Port 53050->5556 (received
on interface x.x.x.x)
Mar 27 17:01:03.516 host kernel: 226 IP packet dropped
(www7.clever.net[209.235.11.254]->host1[x.x.x.x1]: Protocol=TCP[SYN] Port
53051->512): Restricted Port: Protocol=TCP[SYN] Port 53051->512 (received
on interface x.x.x.x)
Mar 27 17:01:03.521 host kernel: 226 IP packet dropped
(www7.clever.net[209.235.11.254]->host2[x.x.x.x2]: Protocol=TCP[SYN] Port
53052->5556): Restricted Port: Protocol=TCP[SYN] Port 53052->5556 (received
on interface x.x.x.x)
Mar 27 17:01:03.522 host kernel: 226 IP packet dropped
(www7.clever.net[209.235.11.254]->host2[x.x.x.x2]: Protocol=TCP[SYN] Port
53053->512): Restricted Port: Protocol=TCP[SYN] Port 53053->512 (received
on interface x.x.x.x)
Mar 27 17:01:03.528 host kernel: 226 IP packet dropped
(www7.clever.net[209.235.11.254]->x.x.x.x3: Protocol=TCP[SYN] Port
53054->5556): Restricted Port: Protocol=TCP[SYN] Port 53054->5556 (received
on interface x.x.x.x)
Mar 27 17:01:03.528 host kernel: 226 IP packet dropped
(www7.clever.net[209.235.11.254]->x.x.x.x3: Protocol=TCP[SYN] Port
53055->512): Restricted Port: Protocol=TCP[SYN] Port 53055->512 (received
on interface x.x.x.x)
```

TARGETING

YES, the x.x.x.x network is being targeted. This is a deliberate probe against the network, specifically to TCP ports 512 and 5556.

INTENT

The attacker is on reconnaissance looking for machines that will respond to a connect on ports 512 and 5556.

Port 512 normally supports the Unix remote execution service (rexec).
Port 5556 is the BO Facil port.

Responses on port 512 would indicate the presence of a Unix OS while responses on port 5556 would indicate the presence of a Microsoft OS infected with Back Orifice.

The only conclusion is, any machine responding to these packets would be further probed or attacked.

TECHNIQUES

The attack is automated as indicated by the timestamps of the packets and the sequential scanning of the IP addresses in the x.x.x network, first for port 512 and then 5556.

There is nothing in the data provided that would indicate crafted packets.
The source ports are sequential indicating the probing software is letting the TCP driver handle the communication. It would be interesting to see if the id numbers or data contained any patterns that would indicate crafted packets.

There appears to be no attempt to hide source IP or the scan itself.

HISTORY
Clever.net is a fairly large ISP that also provide commercial web hosting. There are some privately owned domains within the clever.net domain. I was able to find some history of attacks generating from the clever.net domain dating back to 1996. There are reports of the entire *.clever.net domain being denied access to some sites, but nothing recently.

EXISTENCE
Info on the source IP:
www7.clever.net (209.235.11.254) is reversible in DNS.

The machine appears to be running BSD as reported in the telnet banner.

The source address has the following ports available:
13,21,22,23,25,37,80,110,111,199

It does allow anonymous FTP

Clever.net appears to offer internet services. It was acquired by Interliant, Inc. in 1998.

SEVERITY – LOW to NONE
I believe this to be a "script kiddie" playing with a new tool. The attacker doesn't seem to be trying to hide, evident by the sequential scan of IP addresses and no apparent attempt to spoof the source IP.

ANALYSIS #3

DATA PROVIDED

(Report from a .edu, apparently this is already run to ground. GCIA candidates looking for something to research, this is a good one!)

```
[**] Tiny Fragments - Possible Hostile Activity [**]
03/27-14:21:27.733768 213.224.17.104 -> MY.NET.220.66
```

TARGETING

Yes there is targeting. Tiny fragmented packets to your IP address is targeting.

INTENT

There is not a lot of information to work with.

The minimum length of a TCP packet is 20 bytes with no options. If "tiny fragments" refers to something less than 20 this could be fragment scan.

There are a number of attacks that revolve around fragmented packets.

- Ping O' Death (Although normally larger fragments)
- Teardrop (Missing fragrment)
- Possible denial of service
- Fragmented filtering (used to bypass router filtering)

This is either an attempt to map the network using fragmented packets or and attempted denial of service depending on the number of packets received.

TECHNIQUES

"Tiny" fragments are almost always crafted packets.

From an nslookup, the attack originated in Belgium from a provider that uses DHCP making it hard to trace.

HISTORY

There are numerous incidents originating from the kabel.pandora.be domain. In some cases access from this domain has been blocked or denied.

EXISTENCE

```
nslookup 213.224.17.104
Server:  mtedi01.ops.ew3.att.net
Address:  204.159.38.42

Name:    dhcp-213-224-17-104.kabel.pandora.be
Address:  213.224.17.104
```

SEVERITY - MEDIUM

Because tiny fragmented packets are normally passed by a packet filtering device these packets could very well by-pass the perimeter defense and reach the target.

ANALYSIS #4

DATA SUPPLIED

(Brian Friday from .edu has a close encounter with Brazil, I deleted about 60 f the attempts)

```
Mar 31 05:08:28 myhost portsentry[172]: attackalert:
Connect from host: 150.183.91.134/150.183.91.134
to TCP port: 111
Mar 31 10:36:38 myhost portsentry[173]: attackalert:
Connect from host: dgt048.cpunet.com.br/200.254.53.48
to UDP port: 111
Mar 31 10:38:36 myhost portsentry[173]: attackalert:
Connect from host: dgt048.cpunet.com.br/200.254.53.48
to UDP port: 111

Mar 31 12:34:44 myhost portsentry[173]: attackalert:
Connect from host: user-33qs1hs.dialup.mindspring.com/199.174.6.60
to UDP port: 31337
Mar 31 12:35:10 myhost2 portsentry[8311]: attackalert:
Connect from host: user-33qs1hs.dialup.mindspring.com/199.174.6.60
to UDP port: 31337
```

<<<ANALYSIS>>>

TARGETING

Yes, the destination was targeted on three different times. Three packets are scanning for RPC and the third is looking for Back Orifice. It doesn't appear that all the packets were from Brazil.

INTENT

This data provided actually contains three attempted attacks. The first two are an attempt to locate a machine answering on port 111 (RPC), and the third is someone looking for Back Orifice.

The first three packets are to port 111(RPC). This is someone looking for machines running an RPC service. There are a large number of variations of probes and attacks associated with RPC. It is without doubt, that if a response is found to the probe, further attacks will occur. The first is from an IP address that is not in DNS but appears to have orginated in Korea. The other two orginated from Brazil.

The BO probe is someone looking for machines infected with Back Orifice. If found, further attempts to connect to the Back Orifice program would be expected.

TECHNIQUES

The packets destined tp port 111(RPC) is not a new probe. This appears to be someone on a reconnaissance mission trying to locate vulnerable machines.

The Back Orifice scan; Nothing mystical here, someone coming through Mindspring is scanning IPs in an attempt to locate systems infected with Back Orifice. They actually scanned twice about 25 seconds apart.

HISTORY

I found a little information on the seri.re.kr domain that could be regarded as dubious behavior but not much more that a few questionable newsgroup posting, I found nothing on the IP address 150.183.91.134.

On the BO probe; Mindspring is a large full service ISP. I believe this attack to be a “script kiddie” running some new tool downloaded off the net. Mindspring recently merged with EarthLink Inc.

EXISTENCE
The first RPC scan orginated from 150.183.91.134. This IP in not in DNS but 150.183.91.133 and 150.183.91.135 are. I believe this IP belongs to the domain seri.re.kr in Korea. The DNS server that has this information is serims.seri.re.kr(134.75.96.150). Connecting this this DNS and doing the "ls -d seri.re.kr" command gives you information on the 150.183.91 network. According to IANA 150.183.0.0 is assigned to the Korea Institute of Science and Technology(NET-SERI-B).

The other two packets looking for RPC, orginated from the cpunet.com.br domain. This is an ISP in Brazil. If the RPC scan persist you can try contacting the ISP:

Av. Tancredo Neves, no 1485, Ed. Esplanada Trade Center, sala: 207
CEP. 41.820-021 - Tel.: (071) 341-7711
Salvador - Bahia - BRASIL
Comercial - comercial@cpunet.com.br
Support - suporte@cpunet.com.br
Webmaster - webmaster@cpunet.com.br
Administration - admfin@cpunet.com.br

If the BO probes persists from Mindspring, report it to EarthLink:

EarthLink, Inc.
1430 West Peachtree St. NW, Suite 400,
Atlanta, GA 30309
Office: 404-815-0770 or 800-719-4664
Sales: 404-815-0082 or 888-MSPRING (677-7464)
Customer Service: 404-815-9111 or 800-719-4660
Technical Support: 404-815-9111 or 800-719-4660

SEVERITY –
LOW on the RPC probe from 150.183.91.134 (bears further watching due to the originating country and lack of a DNS record).

LOW on the RPC probes from dgt048.cpunet.com.br.

VERY LOW on the Back Orifice probe.

ANALYSIS #5

DATA SUPPLIED
(Great opportunity for the IDIC students that keep flooding me with "what do I analyze" questions, from Andy at .edu)

Any observations regarding the traffic to MY.NET.70.227 are more than welcome.
Thanks, - andy)

```
04/01-15:59:26.043293 158.94.234.51:1674 -> MY.NET.70.227:6346
TCP TTL:117 TOS:0x0 ID:27853 DF
SFR**U21 Seq: 0x97FCBA Ack: 0x1141D Win: 0x5018
TCP Options => EOL EOL Opt 80 (40): 579C BBE0 E44A 83B0 0EC3
0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
0E C3 ..

04/01-16:00:33.741385 158.94.234.51:230 -> MY.NET.70.227:1674
TCP TTL:117 TOS:0x0 ID:3310 DF
SF**** Seq: 0x18CA0098 Ack: 0x5C0B141D Win: 0x5018
TCP Options => EOL EOL Opt 163 (40): E9E3 DC07 D411 A275 0060
0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000

04/01-16:04:40.716885 158.94.234.51:1674 -> MY.NET.70.227:6346
TCP TTL:117 TOS:0x0 ID:61266 DF
SFRP**1 Seq: 0x996CFA Ack: 0x141D Win: 0x5018
TCP Options => EOL EOL Opt 238 (26): 0AE5 E007 D411 9F79 0010
0000 0000 0000 0000 0000 0000 0000 EOL EOL EOL EOL EOL EOL EOL
EOL EOL EOL EOL EOL

04/01-16:06:18.182252 158.94.234.51:1674 -> MY.NET.70.227:6346
TCP TTL:117 TOS:0x0 ID:46459 DF
SF*P*U1 Seq: 0xC30099 Ack: 0xDBD9141E Win: 0x5018
06 8A 18 CA 00 C3 00 99 DB D9 14 1E 06 AB 50 18 ..............P.
00 00 D3 0A 00 00 A0 15 49 6C C4 07 D4 11 9F 25 ........Il.....%
00 10 ..

04/01-16:07:17.708685 24.201.15.107:0 -> MY.NET.202.6:4623
TCP TTL:112 TOS:0x0 ID:53039 DF
SF**AU2 Seq: 0x4C0A90 Ack: 0x9B8D0564 Win: 0x5010
TCP Options => EOL EOL EOL EOL EOL EOL Opt 98 (39): 1E61 040C 000A
0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
0000 0000 0000

04/01-16:10:45.964767 158.94.234.51:1674 -> MY.NET.70.227:6346
TCP TTL:117 TOS:0x0 ID:5343 DF
SFRPAU21 Seq: 0xDB009A Ack: 0x7786141E Win: 0x5018
39 FF 50 18 00 00 EC A2 00 00 7B 15 49 6C C4 07 9.P.......{.Il..
D4 11 9F 25 00 10 ...%..

04/01-16:15:31.394180 24.201.15.107:4623 -> MY.NET.202.6:76
TCP TTL:112 TOS:0x0 ID:34903 DF
SF*P** Seq: 0xA909B8D Ack: 0x5A063E Win: 0x5010
00 00 00 00 00 00 ......

04/01-16:38:37.904840 129.123.236.50:1116 -> MY.NET.70.227:6346
TCP TTL:110 TOS:0x0 ID:2907 DF
```

```
SFR***1 Seq: 0x47D9DA59 Ack: 0x1C81443 Win: 0x5010
TCP Options => EOL EOL EOL EOL EOL EOL Opt 85 (40): 2054 5950 453D
0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
0000 0000 0000

04/01-17:15:33.055773 24.112.44.237:6688 -> MY.NET.205.106:4042
TCP TTL:115 TOS:0x0 ID:27570 DF
SF*P*U21 Seq: 0x405819 Ack: 0xF01F38 Win: 0xA010
22 38 BD CB 00 00 01 01 05 12 1F 38 64 37 1F 38 "8.........8d7.8
69 EB i.

04/01-17:49:35.202459 24.68.74.248:6699 -> MY.NET.206.202:2019
TCP TTL:114 TOS:0x0 ID:24611 DF
SF*P*U21 Seq: 0x12F710 Ack: 0x485 Win: 0x8010
TCP Options => EOL EOL NOP NOP Sack: 1157@54251 EOL EOL EOL EOL
EOL EOL EOL EOL EOL EOL EOL EOL EOL EOL
```

TARGETING
Yes, this is a definite attack on the the MY.NET network. Assuming all the data is present, this seems to be a focused attack on MY.NET.70.227, MY.NET.202.6, MY.NET.205.106, MY.NET.206.202.

INTENT
This attack is either an attempt at fingerprint the destination OS or a an attempt at a denial of service attempt against MY.NET using bogus TCP flag settings.

TECHNIQUES
This is a rather slow attack, 10 packets over 2 hours.

The packets are crafted as the TCP flags are all bogus.

Source ports of 0 and 223 are anomalous as they are not normally chosen by the TCP driver.

The use of 5 different IP addresses could be the result of running the attack tool several times, reconfiguring in between runs.

It is feasible that the attacker has control of the 5 machines used in this attack.

The TTL values appear reasonable based on the location of the source IPs.

The mixture of TCP flag settings covers a variety of attack signatures and probes.

There doesn't seem to be any significance to the selection of destination ports. I'm not aware of any known vulnerabilities or Trojans using ports 6346, 1674, 4623, 4042, or 2019.

HISTORY
Canada is known to be the source of more and more attacks/probes.

EXISTENCE
I am unable to identify any individuals or groups.

The source IPs are interesting, primarily Canada:
158.94.234.51 - ~KALOO~ - Middlesex England

24.201.15.107 - modemcable107.15-201-24.timi.mc.videotron.net, Montreal Canada

129.123.236.50 - std6.dorms.usu.edu - Utah State Univ.

24.112.44.237 - cr460744-a.nmkt1.on.wave.home.com, Rogers WAVE (NETBLK-ON-ROG-NMKT-1)
Ontario

24.68.74.248 - 24.68.74.248.on.wave.home.com, Canada

SEVERITY - LOW to MEDIUM
This attacker appears to know more than the average "script kiddie". He knows how to manipulate TCP packets and could very well be in control of 5 different machines. If attacks persist, if possible, I would try and contact the owner of the machines.

ANALYSIS #6

DATA SUPPLIED

```
Mar 31 19:09:35 hosth snort[75541]:
spp_portscan: PORTSCAN DETECTED from 203.85.30.129
Mar 31 19:09:41 hosth snort[75541]: spp_portscan:
portscan status from 203.85.30.129: 14 connections
across 14 hosts: TCP(14), UDP(0)
Mar 31 19:09:47 hosth snort[75541]: spp_portscan:
End of portscan from 203.85.30.129
--------
Mar 31 19:09:34 203.85.30.129:1542 -> A.B.C.30:98 SYN **S*****
Mar 31 19:09:34 203.85.30.129:1545 -> A.B.C.33:98 SYN **S*****
Mar 31 19:09:38 203.85.30.129:1710 -> A.B.C.197:98 SYN **S*****
Mar 31 19:09:38 203.85.30.129:1714 -> A.B.C.201:98 SYN **S*****
Mar 31 19:09:38 203.85.30.129:1717 -> A.B.C.204:98 SYN **S*****
Mar 31 19:09:38 203.85.30.129:1720 -> A.B.C.207:98 SYN **S*****
Mar 31 19:09:38 203.85.30.129:1727 -> A.B.C.214:98 SYN **S*****
Mar 31 19:09:38 203.85.30.129:1728 -> A.B.C.215:98 SYN **S*****
Mar 31 19:09:38 203.85.30.129:1731 -> A.B.C.218:98 SYN **S*****
Mar 31 19:09:36 203.85.30.129:1748 -> A.B.C.235:98 SYN **S*****
Mar 31 19:09:36 203.85.30.129:2021 -> A.B.D.252:98 SYN **S*****
Mar 31 19:09:37 203.85.30.129:1531 -> A.B.C.19:98 SYN **S*****
Mar 31 19:09:39 203.85.30.129:2006 -> A.B.D.237:98 SYN **S*****
Mar 31 19:09:39 203.85.30.129:2073 -> A.B.E.48:98 SYN **S*****
```

TARGETING
Yes, the A.B.C, A.B.D, and A.B.E networks are being probed.

INTENT
The attack is attempting to map the A.B.C, A.B.D, and A.B.E networks by sending SYN packets to port 98. Because port 98 is not a normal port that is probed, the attacker could also be looking for trojans.

TECHNIQUES
The attack is choosing random hosts from A.B.C, A.B.D and A.B.E networks, with all packets destined to TCP port 98. Port 98 is normally TAC news which I don't believe has any known exploits.

The attack is delayed somewhat as the timestamps are little spread out, this is most likely due to the attacker may be scanning other networks at the same time.

The attacker doesn't appear to be hiding their source IP.

HISTORY
No known history of attacks from this particular network.

EXISTENCE
203.85.30.129 is pc129.epublisher.com.hk which is OLS Co Ltd; Hong Kong (OLS-HK).

SEVERITY - LOW to NONE

ANALYSIS #7

DATA SUPPLIED

```
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
```

TARGETING
Yes, definite signs of targeting the host a.b.c.34.

INTENT
This looks like a traceroute.

If this same pattern shows up from other sources, the final attack may come in the form of a DOS of your gateway routers, coordinated traceroutes. It could be someone scanning the host for open UDP ports.

TECHNIQUES
The attacker is using an automated tool based on the timestamps and is scanning host a.b.c.34 for open UDP ports. This is standard sequential UDP host scan. Packets are probably from a *nix machine doing traceroutes.

If the packets carried a large amount of data it could be an attempt at a denial of service.

HISTORY
No history on 208.185.54.22 or Speedera.com

EXISTENCE
208.185.54.22 is 208.185.54.22.speedera.com according to DNS. Speedera.com offers content distribution network. I believe the traceroutes are an attempt to provide load balancing.
The machine is listening on ports 22 (SSH) and 53 (DNS). The DNS port denies all queries sent to it.

SEVERITY – LOW to NONE

ANALYSIS #8

DATA PROVIDED

(More and more evidence is surfacing of way out of spec packets and these aren't coming from demon internet! If anyone has thoughts on this, we would love to hear them)

```
04/06-00:42:49.191152 MY.NET.202.150:1152 -> 207.87.10.150:44668
TCP TTL:126 TOS:0x0 ID:16025 DF
SFR*** Seq: 0xC91 Ack: 0x3FBED1BA Win: 0x5010
3E 07 50 10 22 38 57 B5 20 20 20 20 20 00 >.P."8W. .

04/06-00:58:18.260191 130.166.82.163:166 -> MY.NET.207.254:6699
TCP TTL:109 TOS:0x0 ID:15785 DF
SFRPA*2 Seq: 0xE790043 Ack: 0x9FD70D8D Win: 0x5010
TCP Options => EOL EOL Opt 255 (40): 707C FC80 02F0 56DF 69E3
0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000

04/06-00:58:29.765586 130.166.82.163:6699 -> MY.NET.207.254:3705
TCP TTL:109 TOS:0x0 ID:13226 DF
SF****21 Seq: 0x4747D7 Ack: 0xD8DDB5F Win: 0x5010
1A 2B 0E 79 00 47 47 D7 0D 8D DB 5F 00 C3 50 10 .+.y.GG...._..P.
21 EC A4 04 00 00 DC B0 E9 4D 9C C6 49 B2 EA FE !........M..I...
85 32 .2

04/06-00:58:35.387856 130.166.82.163:6699 -> MY.NET.207.254:3705
TCP TTL:109 TOS:0x0 ID:63660 DF
SF*P*U Seq: 0x4900F3 Ack: 0xD8DDB5F Win: 0x5010
1A 2B 0E 79 00 49 00 F3 0D 8D DB 5F 00 2B 50 10 .+.y.I....._.+P.
21 EC 53 7E 00 00 00 00 00 00 !.S~......
```

TARGETING

Maybe. There are some screwy packets being sent to MYNET.207.254 machine.

INTENT

Possibly. These packets are totally hosed. Based on the comment that the packets didn't come from the demon Internet, this could be the result of a failing piece of hardware. If these were all the packets that were captured then I would tend to lean toward a bad piece of hardware. Otherwise, this is a denial service attach or OS fingerprinting using bogus TCP flags.

TECHNIQUES

If this is an attack, then the packets were crafted as the TCP flag setting don't occur in nature. The possible attack is slow with no apparent direction.

HISTORY

None.

EXISTENCE

130.166.82.163 is s082n163.csun.edu

SEVERITY – LOW to NONE

ANALYSIS #9

DATA PROVIDED

```
Apr 6 13:07:18 dns1 snort[164344]: spp_portscan:
PORTSCAN DETECTED from 209.24.35.17
Apr 6 13:07:24 dns1 snort[164344]: spp_portscan:
portscan status from 209.24.35.17: 4 connections across 1 hosts:
TCP(0), UDP(4)
Apr 6 13:07:30 dns1 snort[164344]: spp_portscan:
End of portscan from 209.24.35.17
--------
Apr 6 13:07:18 209.24.35.17:47282 -> a.b.c.34:33709 UDP
Apr 6 13:07:18 209.24.35.17:47282 -> a.b.c.34:33710 UDP
Apr 6 13:07:18 209.24.35.17:47282 -> a.b.c.34:33711 UDP
Apr 6 13:07:18 209.24.35.17:47282 -> a.b.c.34:33712 UDP
```

TARGETING

Yes, the machine a.b.c.34 is the target.

INTENT

This is the result of a traceroute. Network reconnaissance, or possibly load balancing.

TECHNIQUES

Packets are probably from an *nix machine doing traceroutes.

HISTORY

See also analysis #7. I believe this to be a traceroute for load balancing.

EXISTENCE

209.24.25.17 has no DNS record. IANA shows the IP address assigned to Best Internet communications, INC, CA. (NETBLK-BEST6). A traceroute shows this machine to be associated with Speedera. See analyses #7, another traceroute type detect.

SEVERITY – LOW to NONE

ANALYSIS #10

DATA PROVIDED

```
Apr 7 02:38:58 dns2 in.ftpd[828]: refused connect from 212.3.23.144
```

TARGETING

Yes, the machine dns2 is the target.

INTENT

Because the destination appears to be a DNS machine, this is an attempt to connect using FTP. The intent would be to try and obtain a copy of the DNS files to save time in mapping the network.

TECHNIQUES

One packet is not a lot of data to be able to determine technique. This most likely is this is the result of someone pointing their FTP client at your DNS2 machine to see what they would get.

HISTORY

None.

EXISTENCE

No DNS entry for 212.3.23.144. A traceroute shows the machine name as KRAMIZ. The IP range belongs to SE-LEISSNER-980312, Sweden.

A port scan of 212.3.23.144 shows it to be running Microsoft Windows as port 135 and 139 are open. The machine is also running a telnet server called RemotelyAnywere.

I found a few entries on the Internet referencing KRAMIZ but nothing that lead anywhere.

SEVERITY – LOW to NONE