GIAC
CERTIFICATIONS

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 permited 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

*** Pretty good job! Last trace was heavily edited to remove redundancy by Northcutt. Evidence
of a search for port 8803 wouldn't hurt a bit. Severity, history and an explanation of some of the less familiar terms such as gabanbus would all be nice. Accuracy is good, keep it up! 81 S. ***

L. Christopher Paul
30 March, 2000

GIAC Certified Intrustion Analyst -- Practical Exam

***** Detect #1 *****

Background:
The following trace was detected by 'Snort' running on the firewall connected to a cable modem. The network contains only a single Internet IP address and the hosts behind the firewall are using a private address space that is not Internet routeable.

Severity: Low (1)

Summary: Scan for for sub-seven trojan.

Trace:
[**] Possible SubSeven access [**]
03/14-13:24:56.900924 212.83.147.46:3294 -> my.firewall.com:1243
TCP TTL:114 TOS:0x0 ID:32524 DF
S***** Seq: 0xCF6BD   Ack: 0x0   Win: 0x2000
TCP Options => MSS: 536 NOP NOP SackOK

Analysis: This is a single connection attempt from a host in France (via ISP worldonline.fr) to a port commonly used for one of the latest Windows Remote Control trojans; SubSeven.

The (packet filtering) firewall itself is running on a non-windows platform and the computers behind it are NAT'ed and therefore can not be routed to.

This appears to simply be someone either scanning randomly or sweeping in order to find previously compromised systems and not an penetration attempt against an individual host or organization.

The security measures in place are sufficent to handle this incident and no further action is recommended.

***** Detect #2 *****

Background:
Trace retrieved from GIAC Web Page dated 3/26/2000. No additional information known.

Severity: Unknown. Without knowlege of the underlying architecture a precise evaluation is not possible. If reviewing additional logs or putting hightened logging in place showed no additional information, I would consider this a low severity. If additional traffic is shown, it could be an indication of direct targeting.

Summary: Potentially compromised system conducting a port scan to ports not previously associated with registered services or trojans.

Trace:
Message: Deny inbound tcp src outside:200.249.238.9/8803
dst DMZ:my.net.60.98/5317 13:26
Message: Deny inbound tcp src outside:200.249.238.9/8803
dst DMZ:my.net.60.98/7877 13:31
Message: Deny inbound tcp src outside:200.249.238.9/8803
dst DMZ:my.net.60.98/18117 13:39

© SANS Institute 2000 - 2005, Author retains full rights.

Message: Deny inbound tcp src outside:200.249.238.9/8803
dst DMZ:my.net.60.98/15557 13:53
Message: Deny inbound tcp src outside:200.249.238.9/8803
dst DMZ:my.net.60.98/20677 13:56
Message: Deny inbound tcp src outside:200.249.238.9/8803
dst DMZ:my.net.60.98/25797 14:07
Message: Deny inbound tcp src outside:200.249.238.9/8803
dst DMZ:my.net.60.98/23237 14:19
Message: Deny inbound tcp src outside:200.249.238.9/8803
dst DMZ:my.net.60.98/25797 14:29
Message: Deny inbound tcp src outside:200.249.238.9/8803
dst DMZ:my.net.60.98/28357 14:39
Message: Deny inbound tcp src outside:200.249.238.9/8803
dst DMZ:my.net.60.98/28357 14:39

Analysis: The consistent source port indicates that these are crafted packets performing some kind of port scan. The timing between scans would seem to indicate that in the the attacker is scanning a range of hosts on one port before moving on and checking another.

I can find no references to the destination port numbers in quesiton, but considering that the source IP is registered to the Brazilian Research Network, I am willing to venture that they have been compromised and that one of their computers is being used in a scan.

My recommendation would be to review any existing logs for all traffic coming in from that network for a and see if there have been any substantive connections. If historical logs do not exist, it is recommended that additional logging be implemented for a time to see if any future connections are attempted.

***** Detect 3 *****

Background:
The following trace was detected by 'Snort' running on the firewall connected to a cable modem. The network contains only a single Internet IP address and utilizes DNS servers outside of the internal network.

Severity: None

Summary: False positive

Trace:
[**] TeleCommando [**]
03/27-12:45:27.485002 8:0:3E:7:DB:F7 -> xx:xx:xx:xx:xx:xx type:0x800 len:0x55
dns.outside.com:53 -> my.firewall.com:61446 UDP TTL:254 TOS:0x0 ID:27303
DF Len: 51

Analysis:
False Positive. The source IP is an DNS server outside of the firewall. The UDP:53 request coming from the inside just happened to be on a potential trojan port (TeleCommando).

Would recommend an additional Snort rule to pass incoming udp port 53 from both the primary and secondary dns servers.

***** Detect 4 *****

Background:
Snort traces retrieved from GIAC Web Page dated 3/24/2000. No additional information known.

Severity: (1) Low

Summary:
This is a series of packets, sent over time from various hosts. They are anomalous in that they have a varying series of flag bits set in anomolous combinations. These could be attempts at a network mapping, but the majority are probably the result of a faulty piece of hardware.

© SANS Institute 2000 - 2005, Author retains full rights.

```
Trace:
Version 1.5
By Martin Roesch (roesch@clark.net, www.clark.net/~roesch)
snaplen = 68
Entering readback mode....
03/24-02:22:23.657053 128.59.122.70:3830 -> MY.NET.10.119:6699
TCP TTL:116 TOS:0x0 ID:2765 DF
SF****2 Seq: 0xA87 Ack: 0x80970072 Win: 0x5010
TCP Options => EOL EOL EOL EOL EOL EOL Opt 140 (9): C484 82CD
0014 0000 EOL EOL EOL EOL EOL EOL EOL EOL EOL EOL EOL EOL

03/24-02:45:57.071197 134.121.137.229:1143 -> MY.NET.201.186:6688
TCP TTL:114 TOS:0x0 ID:27714 DF
SFRP**1 Seq: 0x82F410 Ack: 0xCA0338 Win: 0x5010
TCP Options => EOL EOL EOL EOL EOL EOL Opt 18 (19):
1415 1617 1819 0000 0000 0000 0000 0000 0000

03/24-02:46:15.432213 194.217.242.34:769 -> MY.NET.253.24:14253
TCP TTL:240 TOS:0x0 ID:8575 DF
SFRP*U1 Seq: 0x0 Ack: 0x4500003B Win: 0x4000
03 01 37 AD 00 00 00 00 45 00 00 3B 08 AF 40 00 ..7.....E..;..@.
EC 11 9B 35 82 B8 07 6A C2 9F 9E 0B B9 1E 00 35 ...5...j.......5
00 27 .'

03/24-08:39:56.486535 194.217.242.92:27055 -> MY.NET.1.2:27005
TCP TTL:48 TOS:0x0 ID:16304 DF
SFR**U Seq: 0x6694F8 Ack: 0x38270000 Win: 0x80
38 27 00 80 07 BF 8A 11 44 0F E1 03 11 00 0F 0F 8'......D.......
00 00 02 A0 8F 00 ......

03/24-10:10:36.216826 194.217.16.194:769 -> MY.NET.75.51:43622
TCP TTL:239 TOS:0x0 ID:33723
SF*P**21 Seq: 0x0 Ack: 0x4500003C Win: 0x4000
03 01 AA 66 00 00 00 00 45 00 00 3C 0B CB 40 00 ...f....E..<..@.
EC 11 98 1B 82 B8 07 6A C2 9F 9E 08 B9 1E 00 35 .......j.......5
00 28 .(

03/24-13:53:23.862425 24.3.38.233:1043 -> MY.NET.253.114:80
TCP TTL:116 TOS:0x0 ID:33536 DF
SFRPAU2 Seq: 0x130001 Ack: 0x38497E4D Win: 0x5010
38 49 7E 4D 2C 7F 50 10 22 38 E7 6E 00 00 00 00 8I~M,.P."8.n....
00 00 ..

03/24-16:05:57.153891 195.173.149.205:7788 -> MY.NET.141.166:4618
TCP TTL:239 TOS:0x0 ID:40020
SF**AU Seq: 0x76D196 Ack: 0x5BC6A727 Win: 0xEA29
TCP Options => EOL Opt 61 (40): 2612 5D1A 4A2C 8DD3 B730 C400
0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000

03/24-20:03:35.378643 212.238.69.205:31514 -> MY.NET.253.114:31501
TCP TTL:112 TOS:0x0 ID:3615 DF
SF**AU2 Seq: 0x848986 Ack: 0x982D0000 Win: 0x80
98 2D 00 00 2D 73 00 80 16 3C 0F 00 00 00 00 00 .-..-s...<......
00 00 ..

03/24-22:18:10.568868 194.217.188.38:9999 -> MY.NET.97.57:1028
TCP TTL:48 TOS:0x0 ID:15702 DF
SF****1 Seq: 0x55E831 Ack: 0x2A56B341 Win: 0xA286
TCP Options => Opt 152 (16): 0802 0850 00E0 F3FF F74F 885F 0000
08 50 00 E0 F3 FF F7 4F 88 5F .P.....O._

Analysis:
At first it might seem that these are a series of related or coordinated
scans, the more likely explanation for the majority of these traces is a
known problem with a faulty router owned by 'Demon Internet' (DI). Traces
3,4,5,7,8 and 9 all have source IP addresses within the DI domains.

While I am loath to dismiss these traces because of a known problem, it
does seem the most likely probability; yet it should be mentioned that
this type of 'known' problem would be an excellent way for attackers to
cover their actions while performing some sort of recon scan.
```

© SANS Institute 2000 - 2005, Author retains full rights.

Traces 1 and 2 bear striking similarities to one another in that their destination ports are similar (6699 & 6688), TCP options set, the EOLs in the options fields, TTLs only 2 hops apart, and the same window size. Also, both came from .edu domains. These two appear to be some form of scan, possibly with the same tool or by the same individual.

Trace number 6 also appears to be a recon scan (Xmas Tree) from an @home address (cable modem). Possibly from nmap or a similar program.

***** Detect 5 *****

Background:
Trace retrieved from GIAC Web Page dated 3/25/2000. The host in question was an @home (cable modem) user. No additional information known.

Severity: Low

Summary: Port scanning for trojans.

Trace:
Mar 24 01:54:58 cc1014244-a kernel:
securityalert: tcp if=ef0 from
24.3.57.38:11111 to 24.3.21.199 on unserved port 12345
Mar 24 03:14:13 cc1014244-a kernel:
securityalert: tcp if=ef0 from
171.214.113.228:2766 to 24.3.21.199 on unserved port 1243
Mar 24 04:45:01 cc1014244-a kernel:
securityalert: tcp if=ef0 from
208.61.109.243:3578 to 24.3.21.199 on unserved port 1243
Mar 24 04:45:06 cc1014244-a kernel:
securityalert: tcp if=ef0 from
208.61.109.243:3832 to 24.3.21.199 on unserved port 27347
Mar 24 05:40:42 cc1014244-a kernel:
securityalert: udp if=ef0 from
24.24.100.172:2147 to 24.3.21.199 on unserved port 137

Mar 24 14:56:08 cc1014244-a kernel:
securityalert: udp if=ef0 from
63.17.79.40:4294 to 24.3.21.199 on unserved port 137
Mar 24 17:20:44 cc1014244-a kernel:
securityalert: tcp if=ef0 from
62.6.100.45:1828 to 24.3.21.199 on unserved port 27374
Mar 24 20:50:47 cc1014244-a kernel:
securityalert: tcp if=ef0 from
194.27.62.179:4857 to 24.3.21.199 on unserved port 27374

Analysis:
Several attempts to find various trojans and access the WINS service on port 137/udp.

The trojans being scanned for are:

SubSeven(1243), and NetBus/GabanBus(12345, 27374). I am unclear as to the scan on port 27347 unless it was simply a typo of port 27374 or possibly a scan for one of the many trojans whose listening port can be changed. Another option would be a here-to-fore unknown trojan.

Other than verifying that the virus-scanning software is up-to-date on this computer, and that netbios traffic is not accessable from the internet, there is no further action indicated.

***** Detect 6 *****

Background:
The following trace was detected by 'Snort' running on the firewall connected to a cable modem. The network contains only a single Internet IP address and the hosts behind the firewall are using a private address space that is not Internet routable.

© SANS Institute 2000 - 2005, Author retains full rights.

Severity: Medium

Summary:
Portmapper Scan. Contrary to policy, portmap was running on this machine -- it had apparently been missed when the machine was built. This service has since been disabled.

Trace:
```
03/27-20:25:19.492568 8:0:3E:7:DB:F7 -> xx:xx:xx:xx:xx:xx type:0x800 len:0x4A
210.218.62.14:1490 -> my.firewall.com:111 TCP TTL:44 TOS:0x0 ID:9494  DF
S***** Seq: 0x27FB821E   Ack: 0x0   Win: 0x7D78
TCP Options => MSS: 1460 SackOK TS: 33651367 0 NOP WS: 0

03/27-20:25:20.471905 8:0:3E:7:DB:F7 -> xx:xx:xx:xx:xx:xx type:0x800 len:0x4A
210.218.62.14:1528 -> my.filewall.com:111 TCP TTL:44 TOS:0x0 ID:9594  DF
S***** Seq: 0x28C4BC6E   Ack: 0x0   Win: 0x7D78
TCP Options => MSS: 1460 SackOK TS: 33651464 0 NOP WS: 0

03/27-20:25:23.461096 8:0:3E:7:DB:F7 -> xx:xx:xx:xx:xx:xx type:0x800 len:0x4A
210.218.62.14:1528 -> my.firewall.com:111 TCP TTL:44 TOS:0x0 ID:9855  DF
S***** Seq: 0x28C4BC6E   Ack: 0x0   Win: 0x7D78
TCP Options => MSS: 1460 SackOK TS: 33651764 0 NOP WS: 0
```

Analysis:
This appears to be two seperate attempts at connecting to the rpc.portmap port (111/tcp). The last two traces appear to be one attempt with a retry.

The source IP is coming from Korea and should therefore be considered a hostile scan/intrusion attempt as we have no business partners there.

As noted above, this service was running on the firewall and has been turned off. There were no filesystems exported via nfs, and tripwire on that machine showed no changed files for the time period in question. So the potential for a compromise was therefore reduced, but not mitigated.

Other actions would be to consider running the dtk/honeypot on that port and tring to gain additional information regarding the attempt should the individual return.

******* Detect 7 *******

Background:
The following trace was detected by 'Snort' running on the firewall connected to a cable modem. The network contains only a single Internet IP address and the hosts behind the firewall are using a private address space that is not Internet routable.

Severity: Low

Summary:
Host Scan: Dial-up customer looking for public news servers. No nntp server is running on the server in question.

Trace:
```
03/28-13:12:10.257877 8:0:3E:7:DB:F7 -> xx:xx:xx:xx:xx:xx type:0x800 len:0x3C
38.27.144.87:2328 -> my.firewall.com:119 TCP TTL:18 TOS:0x0 ID:52259  DF
S***** Seq: 0x15F628   Ack: 0x0   Win: 0x2000
TCP Options => MSS: 1460

03/28-13:12:10.920289 8:0:3E:7:DB:F7 -> xx:xx:xx:xx:xx:xx type:0x800 len:0x3C
38.27.144.87:2328 -> my.firewall.com:119 TCP TTL:18 TOS:0x0 ID:57379  DF
S***** Seq: 0x15F628   Ack: 0x0   Win: 0x2000
TCP Options => MSS: 1460

03/28-13:12:11.649581 8:0:3E:7:DB:F7 -> xx:xx:xx:xx:xx:xx type:0x800 len:0x3C
38.27.144.87:2328 -> my.firewall.com:119 TCP TTL:18 TOS:0x0 ID:62755  DF
S***** Seq: 0x15F628   Ack: 0x0   Win: 0x2000
TCP Options => MSS: 1460
```

© SANS Institute 2000 - 2005 Author retains full rights.

```
03/28-13:12:12.313208 8:0:3E:7:DB:F7 -> xx:xx:xx:xx:xx:xx type:0x800 len:0x3C
```

38.27.144.87:2328 -> my.firewall.com:119 TCP TTL:18 TOS:0x0 ID:2084 DF
S***** Seq: 0x15F628   Ack: 0x0   Win: 0x2000
TCP Options => MSS: 1460

Analysis:
The IP in question appears to be part of the dial-in pool of a local ISP.
It would appear that someone was looking for either a publicly-accessable
or an exploitable NNTP service. This server is not running such a service.
No further action is required.

***** Detect 8 *****

Background:
The following trace was detected by 'Snort' running on the firewall
connected to a cable modem. The network contains only a single Internet
IP address and the hosts behind the firewall are using a private address
space that is not Internet routable.

Severity: Low

Summary: System recon via NULL Scan.

Trace:
[**] NULL Scan [**]
03/28-16:34:31.855408 8:0:3E:7:DB:F7 -> xx:xx:xx:xx:xx:xx type:0x800 len:0x5EA
128.118.205.143:139 -> my.firewall.com:61789 TCP TTL:117 TOS:0x0 ID:59365 DF
****** Seq: 0xFFFA49A   Ack: 0xD1285B3A   Win: 0x5010

Analysis:
This trace appears to be some sort of mapping or recon attempt. The
anomolous code bits (none set) and the low source port (netbios) to
ephemeral destination port would seem to be some sort of attempt to evade
detection or to pass through a firewall. It failed. Snort caught it, the
firewall blocked it. No further action required.

***** Detect 9 *****

Background:
The following trace was detected by 'Snort' running on the firewall
connected to a cable modem. The network contains only a single IP address
and the hosts behind the firewall are using a private address space that
is not Internet routable.

Severity: Low

Summary: IMAP scan.

Trace:
03/29-08:33:41.835637 8:0:3E:7:DB:F7 -> xx:xx:xx:xx:xx:xx type:0x800 len:0x3E
206.244.48.131:2872 -> my.filewall.com:143 TCP TTL:120 TOS:0x0 ID:1381 DF
S***** Seq: 0x8191E46   Ack: 0x0   Win: 0x2000
TCP Options => MSS: 536 NOP NOP SackOK

03/29-08:33:42.993713 8:0:3E:7:DB:F7 -> xx:xx:xx:xx:xx:xx type:0x800 len:0x3E
206.244.48.131:2872 -> my.firewall.com:143 TCP TTL:120 TOS:0x0 ID:1637 DF
S***** Seq: 0x8191E46   Ack: 0x0   Win: 0x2000
TCP Options => MSS: 536 NOP NOP SackOK

03/29-08:33:44.032151 8:0:3E:7:DB:F7 -> xx:xx:xx:xx:xx:xx type:0x800 len:0x3E
206.244.48.131:2872 -> my.firewall.com:143 TCP TTL:120 TOS:0x0 ID:1893 DF
S***** Seq: 0x8191E46   Ack: 0x0   Win: 0x2000
TCP Options => MSS: 536 NOP NOP SackOK

03/29-08:33:45.109762 8:0:3E:7:DB:F7 -> xx:xx:xx:xx:xx:xx type:0x800 len:0x3E
206.244.48.131:2872 -> my.firewall.com:143 TCP TTL:120 TOS:0x0 ID:2149 DF
S***** Seq: 0x8191E46   Ack: 0x0   Win: 0x2000
TCP Options => MSS: 536 NOP NOP SackOK

© SANS Institute 2000 - 2005 Author retains full rights.

Analysis:

Another dial-up account from a local ISP looking for IMAP service, or more likely, known vulnerabilities within various IMAP servers. Another possibility is that, since we have only 1 IP within a class C address space, that someone simply mis-typed the hostname in trying to connect to their own mail server as our ISP has this IP listed as xxx999999.their.domain.

Regardless of the cause, this server is not currently running an IMAP server and no further action is indicated.

***** Detect 10 *****

Background:
The following trace was detected by 'Snort' running on the firewall connected to a cable modem. The network contains only a single IP address and the hosts behind the firewall are using a private address space that is not Internet routable.

Severity: Low

Summary: International night on the Magic NetBus.

Trace:
```
[**] Netbus/GabanBus [**]
03/29-20:54:59.511492 8:0:3E:7:DB:F7 ->xx:xx:xx:xx:xx:xx type:0x800 len:0x3E
210.94.99.64:1241 -> x.x.x.x:12345 TCP TTL:103 TOS:0x0 ID:62723  DF
S***** Seq: 0xFF36A   Ack: 0x0   Win: 0x2000
TCP Options => MSS: 1460 NOP NOP SackOK


[**] Netbus/GabanBus [**]
03/30-03:49:28.417442 8:0:3E:7:DB:F7 ->xx:xx:xx:xx:xx:xx type:0x800 len:0x3E
210.183.223.22:1723 -> x.x.x.x:12345 TCP TTL:112 TOS:0x0 ID:44327  DF
S***** Seq: 0x13CA849   Ack: 0x0   Win: 0x2000
TCP Options => MSS: 1460 NOP NOP SackOK

[**] Netbus/GabanBus [**]
03/30-03:49:29.116905 8:0:3E:7:DB:F7 ->xx:xx:xx:xx:xx:xx type:0x800 len:0x3E
210.183.223.22:1723 -> x.x.x.x:12345 TCP TTL:112 TOS:0x0 ID:44839  DF
S***** Seq: 0x13CA849   Ack: 0x0   Win: 0x2000
TCP Options => MSS: 1460 NOP NOP SackOK
```

Analysis:
The preceeding traces were all attempts from various dial-up and cable modem users to scan for the Netbus or GabanBus trojans.

The first was from an ISP in Korea, then Mexico, Halifax and Kentucky. Two more from Korea, San Diego, and lastly, another from Korea.

While most of the traces are unremarkable scans, some of them have anomolies that make them stand out. For example:

Two of the connections attempts have 2 byte data payloads that vary within the (apparent) retries, as a detailed dump with tcpdump shows; though the inital values are '0000' for both.

```
21:58:47.541212 du-148-233-110-89.prodigy.net.mx.2465 >
my.filewall.com.12345: S 6209666:6209666(0) win 8192 <mss 1460> (DF)
                         4500 002c 651d 4000 1106 3dc6 94e9 6e59
                         xxxx xxxx 09a1 3039 005e c082 0000 0000
                         6002 2000 b682 0000 0204 05b4 0000
21:58:48.273609 du-148-233-110-89.prodigy.net.mx.2465 >
my.firewall.com.12345: S 6209666:6209666(0) win 8192 <mss 1460> (DF)
                         4500 002c 661d 4000 1106 3cc6 94e9 6e59
                         xxxx xxxx 09a1 3039 005e c082 0000 0000
                         6002 2000 b682 0000 0204 05b4 687e
21:58:48.993502 du-148-233-110-89.prodigy.net.mx.2465 >
my.firewall.com.12345: S 6209666:6209666(0) win 8192 <mss 1460> (DF)
                         4500 002c 671d 4000 1106 3bc6 94e9 6e59
                         xxxx xxxx 09a1 3039 005e c082 0000 0000
                         6002 2000 b682 0000 0204 05b4 0101
21:58:49.663049 du-148-233-110-89.prodigy.net.mx.2465 >
```

© SANS Institute 2000 - 2005 Author retains full rights.

```
my.firewall.com.12345: S 6209666:6209666(0) win 8192 <mss 1460> (DF)
                         4500 002c 681d 4000 1106 3ac6 94e9 6e59
                         xxxx xxxx 09a1 3039 005e c082 0000 0000
                         6002 2000 b682 0000 0204 05b4 061c

... and ...

03:34:32.486679 210.105.120.61.4830 > my.firewall.com.12345: S
18086129:18086129(0) win 8192 <mss 1460> (DF)
                         4500 002c c32b 4000 1006 9953 d269 783d
                         xxxx xxxx 12de 3039 0113 f8f1 0000 0000
                         6002 2000 2cbd 0000 0204 05b4 0000
03:34:33.236642 210.105.120.61.4830 > my.firewall.com.12345: S
18086129:18086129(0) win 8192 <mss 1460> (DF)
                         4500 002c c42b 4000 1006 9853 d269 783d
                         xxxx xxxx 12de 3039 0113 f8f1 0000 0000
                         6002 2000 2cbd 0000 0204 05b4 0ad9
03:34:33.999761 210.105.120.61.4830 > my.firewall.com.12345: S
18086129:18086129(0) win 8192 <mss 1460> (DF)
                         4500 002c c52b 4000 1006 9753 d269 783d
                         xxxx xxxx 12de 3039 0113 f8f1 0000 0000
                         6002 2000 2cbd 0000 0204 05b4 a93d
03:34:34.737363 210.105.120.61.4830 > my.firewall.com.12345: S
18086129:18086129(0) win 8192 <mss 1460> (DF)
                         4500 002c c62b 4000 1006 9653 d269 783d
                         xxxx xxxx 12de 3039 0113 f8f1 0000 0000
                         6002 2000 2cbd 0000 0204 05b4 1a06

This would tend to indicate that the same tool was used in both scans.

The trace coming from a cable modem in San Diego also has some anomolies:

Snort:
03/30-01:01:29.953423 8:0:3E:7:DB:F7 ->xx:xx:xx:xx:xx:xx type:0x800 len:0x4E
204.210.39.80:1213 -> xx.xx.xx.xx:12345 TCP TTL:113 TOS:0x5 ID:14406  DF
S***** Seq: 0x1124595   Ack: 0x0   Win: 0x2000
TCP Options => MSS: 1460 NOP WS: 0 NOP NOP TS: 0 0 Opt 49 Opt 49 Opt 49 Opt 49 Opt 49
Opt 49 Opt 49 Opt 49 Opt 49 Opt 49 Opt 49 Opt 49 Opt 49 Opt 49 Opt 49 Opt 49 Opt 49
Opt 49 Opt 49 Opt 49 Opt 49 Opt 49 Opt 49 Opt 49 Opt 49 Opt 49 Opt 49 Opt 49 Opt 49
Opt 49 Opt 49 Opt 49 Opt 49 Opt 49

And the same from tcpdump -x:
01:01:29.953423 dt0f0n50.san.rr.com.1213 > my.firewall.com.12345: S
17974677:17974677(0) win 8192 <mss 1460,nop,wscale 0,nop,nop,timestamp[|tcp]>
(DF) [tos 0x5]
                         4505 0040 3846 4000 7106 19a4 ccd2 2750
                         xxxx xxxx 04bd 3039 0112 4595 0000 0000
                         b002 2000 e29a 0000 0204 05b4 0103 0300
                         0101 080a 0000

The TCP header length is set to 0x0b (11 decimal) and indicates that
the header should be 44 bytes in length (11 32-bit words). However,
the packet is only 34 bytes in length. This is an illegal value (as it
does not fall on a 4 byte boundry) and could indicate anything
from a poorly-crafted packet to an attempt to subvert a broken IP
stack in certain OSes.
```

© SANS Institute 2000 - 2005, Author retains full rights.

Last Updated: July 24th, 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 London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
Baltimore Fall 2017 - SEC503: Intrusion Detection In-Depth	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
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
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 Seattle 2017	Seattle, WA	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS Paris November 2017	Paris, France	Nov 13, 2017 - Nov 18, 2017	Live Event
Community SANS Pensacola SEC503	Pensacola, FL	Nov 27, 2017 - Dec 02, 2017	Community SANS
SIEM & Tactical Analytics Summit & Training	Scottsdale, AZ	Nov 28, 2017 - Dec 05, 2017	Live Event
SANS 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