***** Northcutt, student put his name on the report, had some of his own traces, analysis is good, clear, concise. There is a bit of humor, some will find fault with this, but I do it myself to give the folks in the CERTs a bit of a break. I rank this 85 as the first scoring *****

SANS Intrusion Detection Certification
Practical Trace Analysis

Martin C. Walker

<u>TRACE #1</u>

```
   DATE       TIME ACTION  PROTO  SOURCE          DEST               DST PRT   SRC PRT
27-Mar-00  13:49:52 drop   tcp    195.121.113.65  my.host.extrn.adr  ftp-data     1062
27-Mar-00  13:49:52 drop   tcp    195.121.113.65  my.host.extrn.adr  ftp          1063
27-Mar-00  13:49:52 drop   tcp    195.121.113.65  my.host.extrn.adr        22     1064
27-Mar-00  13:49:52 drop   tcp    195.121.113.65  my.host.extrn.adr  telnet       1065
27-Mar-00  13:49:52 drop   tcp    195.121.113.65  my.host.extrn.adr        29     1069
27-Mar-00  13:49:52 drop   tcp    195.121.113.65  my.host.extrn.adr        31     1070
27-Mar-00  13:49:52 drop   tcp    195.121.113.65  my.host.extrn.adr  ftp-data     1062
27-Mar-00  13:49:52 drop   tcp    195.121.113.65  my.host.extrn.adr  ftp          1063
27-Mar-00  13:49:52 drop   tcp    195.121.113.65  my.host.extrn.adr        22     1064
27-Mar-00  13:49:52 drop   tcp    195.121.113.65  my.host.extrn.adr  telnet       1065
27-Mar-00  13:49:52 drop   tcp    195.121.113.65  my.host.extrn.adr        29     1069
27-Mar-00  13:49:52 drop   tcp    195.121.113.65  my.host.extrn.adr        31     1070
27-Mar-00  13:49:55 drop   tcp    195.121.113.65  my.host.extrn.adr        24     1066
27-Mar-00  13:49:55 drop   tcp    195.121.113.65  my.host.extrn.adr        27     1068
27-Mar-00  13:49:55 drop   tcp    195.121.113.65  my.host.extrn.adr        24     1066
27-Mar-00  13:49:55 drop   tcp    195.121.113.65  my.host.extrn.adr        27     1068
27-Mar-00  13:50:56 drop   tcp    195.121.113.65  my.host.extrn.adr        22     1064
27-Mar-00  13:50:56 drop   tcp    195.121.113.65  my.host.extrn.adr        22     1064
27-Mar-00  13:51:05 drop   tcp    195.121.113.65  my.host.extrn.adr  ftp          1063
27-Mar-00  13:51:05 drop   tcp    195.121.113.65  my.host.extrn.adr  ftp          1063
27-Mar-00  13:51:20 drop   tcp    195.121.113.65  my.host.extrn.adr        24     1066
27-Mar-00  13:51:20 drop   tcp    195.121.113.65  my.host.extrn.adr        24     1066
```

This trace appears to be a quick and not very “stealthy” port scan of the external (i.e. advertised public) address of our sites MX server. The repetitive and sequential nature of the source ports and target ports indicates that these are crafted packets coming from a scan that tries multiple ports simultaneously for a few packets each. Possibly a better data capture from a sensor located outside the firewall would show some differences between the apparently duplicated packets such as different invalid flags. The RIPE whois database shows this IP address belongs to a Netherlands ISP, quite possibly it is part of a dialup pool.

Classification: Definitely targeted towards this machine and malicious in intent. This is a recon operation that could be the prelude to an attack if a weakness was found. There was no history of targeting from this IP or any others in the same range.

Follow Up: Notify administrator, watch IP addresses from that block

TRACE #2, 3 AND 4

```
12-Mar-00  10:17:05 drop     Tcp     203.229.230.14   x.y.z.1       sunrpc    Domain
12-Mar-00  19:51:23 drop     Tcp     203.229.230.14   x.y.z.3       sunrpc    Domain
13-Mar-00  0:37:02  drop     Tcp     203.229.230.14   x.y.z.4       sunrpc    Domain
13-Mar-00  7:00:13  drop     Tcp     203.229.230.14   x.y.z.5       sunrpc    domain
18-Mar-00  0:30:22  drop     Tcp     198.109.185.2    x.y.z.1       sunrpc         638
18-Mar-00  0:30:23  drop     Tcp     198.109.185.2    x.y.z.2       sunrpc         639
18-Mar-00  0:30:24  drop     Tcp     198.109.185.2    x.y.z.3       sunrpc         640
18-Mar-00  0:30:25  drop     Tcp     198.109.185.2    x.y.z.4       sunrpc         641
18-Mar-00  0:30:26  drop     Tcp     198.109.185.2    x.y.z.5       sunrpc         642
18-Mar-00  16:31:35 drop     Tcp     207.79.139.5     x.y.z.1       sunrpc    sunrpc
18-Mar-00  16:31:35 drop     Tcp     207.79.139.5     x.y.z.2       sunrpc    sunrpc
18-Mar-00  16:31:35 drop     Tcp     207.79.139.5     x.y.z.3       sunrpc    sunrpc
18-Mar-00  16:31:35 drop     Tcp     207.79.139.5     x.y.z.4       sunrpc    sunrpc
18-Mar-00  16:31:35 drop     Tcp     207.79.139.5     x.y.z.5       sunrpc    sunrpc
```

Here we see the trace of three distinct host scans against the rpc portmapper of the IP addresses that appear in the DMZ network of the target site. Each of these scans has a different signature. These are recon attempts and the possible prelude to an attack. There is no history of attack from any of these IP ranges.

The first group is from ns.neo-com.net. This is almost certainly a name server and probably one that has been compromised. The cracker is using it to launch attacks while remaining anonymous. This is a “low and slow” scan, there is a large pause between the probe of each host. The cracker is hoping to pass under the threshold of whatever IDS the target site is running, unfortunately for him I personally inspect each dropped connection attempt. Note also the source port is port 53 (DNS). Monitoring of DNS is frequently turned off on IDS and firewalls due to the high level of traffic and high rate of false positives. State insensitive devices may leave this port open. The cracker is hoping that his traffic will go ignored and/or be allowed through whatever firewall or screening router exists based on the source port.

Classification: Targeted, malicious and high risk. The risk is high because the fact it is a low and slow scan coupled with the possibility of an already compromised machine as the source indicates a cracker who knows his trade.

Follow up: Notify name server administrator.

The second trace is this group is from a Michigan educational network (darn kids). This scan is by no means “low and slow”, it completes in 4 seconds. Interesting here is the incremental number of the source ports. This would indicate an extremely lightly loaded box (probably a PC) or more likely a set of crafted packets coming from a scan tool.

Classification: Targeted, malicious and medium risk.

Follow Up: Watch addresses from that netblock

The third trace comes from an IP range belonging to UUNet and servicing Chile. South America is becoming well known for its cracking community as well as the value of its red table wines. Again this host scan is far from “low and slow”. This time the cracker is using the same source port as the target port. This is possibly an attempt to pass unnoticed through a firewall or screening router, or to appear innocuous in the logs.

Classification: Targeted, malicious and medium risk.

Follow up: Watch IP address from that netblock

TRACE #5

```
22-Mar-00  16:50:12 drop    tcp    207.71.92.221    x.y.z.1        ftp           2040
22-Mar-00  16:50:57 drop    tcp    207.71.92.221    x.y.z.1        telnet        2218
22-Mar-00  16:52:27 drop    tcp    207.71.92.221    x.y.z.1        finger        2593
22-Mar-00  16:53:57 drop    tcp    207.71.92.221    x.y.z.1        pop-3         2978
22-Mar-00  16:55:29 drop    tcp    207.71.92.221    x.y.z.1        imap          3240
```

This trace shows a port scan targeted against our machine. In this case cracker probes several ports that often run services known to have security problems. Looking at the time of each probe and the deltas in port number I would guess that these are not “crafted” packets but that the cracker is actually attempting a connect to each service by hand. This would indicate either a half hearted attempt at gaining information or more likely a very unsophisticated attacker.

Classification: targeted, malicious but low risk.
Follow Up: Notify Mom and Dad

TRACE #6

```
27-Mar-00  4:21:10   drop   tcp    209.235.11.254   x.y.z.1        exec         50325
27-Mar-00  4:21:10   drop   tcp    209.235.11.254   x.y.z.2        exec         50326
27-Mar-00  4:21:10   drop   tcp    209.235.11.254   x.y.z.3        exec         50327
27-Mar-00  4:21:10   drop   tcp    209.235.11.254   x.y.z.5        exec         50329
```

This is a host scan targeted against the exec port (512) of the machines in the DMZ. It originates from an ISP and web hosting service based in NY. The exec service is used to execute commands on a host remotely or to provide shell access. Obviously if it is not secured it provides a huge security hole. Judging by the sequential source port numbers on these packets they are crafted by the scanning application. There is no history of probes from this block of network numbers.

Classification: Targeted, malicious, medium risk.
Follow Up: Watch IP netblock

TRACE #7

From GIAC web site:

I noticed these 2 packets from teamcast.com. This occurred during a HTTP request outbound from our network. The source on their side is port 0 destined for 137 UDP on our side.

```
Mar 24 10:16:17.938 host kernel: 226 IP packet dropped
(www.teamcast.com[209.87.230.50]->host[x.x.x.x]: Protocol=UDP Port 0->137):
Bad IP Header (received on interface x.x.x.x)
Mar 24 10:16:20.851 host kernel: 226 IP packet dropped
(www.teamcast.com[209.87.230.50]->host[x.x.x.x]: Protocol=UDP Port 0->137):
Bad IP Header (received on interface x.x.x.x) [1 duplicates suppressed]
```

The source port is 0, which is not a valid port. Attempts to connect with invalid header information can often be OS fingerprinting exercises. However I would discount OS fingerprinting because this typically uses multiple packets with different kinds of problems in them such as different invalid flag combinations. The questions I would ask immediately are “Was the outbound connection to teamcast.com?” and “Can it be duplicated?” If the two answers are “yes” then my analysis would be that this is either some sort of attempt to gather “marketing data” or a misconfigured web server/firewall at the teamcast site. The target port, 137, is the netbios service which could provide some information such as computer name, users name, machine details or operating system.

Classification: Non-malicious, low risk.
Follow Up: Query web site administrator

TRACE #8

From the GIAC web site:

```
-*> Snort! <*-
Version 1.5
By Martin Roesch (roesch@clark.net, www.clark.net/~roesch)
snaplen = 68
Entering readback mode....
03/25-08:12:22.688347 24.200.89.143:0 -> MY.NET.97.80:1105
TCP TTL:114 TOS:0x0 ID:26854 DF
SF*P*U21 Seq: 0x1A200045 Ack: 0x19205F1C Win: 0x5010
TCP Options => EOL EOL EOL EOL EOL EOL Opt 140 (9): BCCE 82B3
0014 0000 EOL EOL EOL EOL EOL EOL EOL EOL EOL

03/25-08:12:23.539724 24.200.89.143:1105 -> MY.NET.97.80:6688
TCP TTL:114 TOS:0x0 ID:50662 DF
SF**A*21 Seq: 0x451920 Ack: 0x5F1C Win: 0x5010
TCP Options => EOL EOL EOL EOL EOL EOL SackOK Opt 141 (40):
82C1 0014 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
0000 0000 0000 0000 0000 0000 0000

03/25-08:12:32.906576 24.200.89.143:1105 -> MY.NET.97.80:6688
TCP TTL:114 TOS:0x0 ID:53480 DF
SF*PA*21 Seq: 0x45 Ack: 0x19205F1D Win: 0x5010
19 20 5F 1D 20 DB 50 10 21 80 80 89 00 00 00 00 . _. .P.!.......
00 00 ..

03/25-08:14:10.442604 24.200.89.143:1105 -> MY.NET.97.80:6688
TCP TTL:114 TOS:0x0 ID:33274 DF
SF*P*U21 Seq: 0x45 Ack: 0x19205F20 Win: 0x5010
TCP Options => EOL EOL EOL EOL EOL EOL SackOK Opt 20 (21):
1617 1819 0000 0000 0000 0000 0000 0000 0000 0000 EOL EOL
EOL EOL EOL EOL EOL EOL EOL EOL EOL

03/25-08:14:32.936127 24.200.89.143:1105 -> MY.NET.97.80:6688
TCP TTL:114 TOS:0x0 ID:59390 DF
SF***U2 Seq: 0x45 Ack: 0x19205F21 Win: 0x5010
TCP Options => EOL EOL EOL EOL EOL EOL SackOK Opt 20 (21):
1617 1819 0000 0000 0000 0000 0000 0000 0000 0000 EOL EOL
EOL EOL EOL EOL EOL
```

Here we see a variety of packets all from the same source address (a Canadian telecommunications company) all targeted at the same destination. These packets are anomalous for several reasons:

- They have invalid flag combinations such as SYN and FIN or SYN, FIN and PSH
- The last three packets all have a sequence number of 45, which is unlikely in the extreme except in crafted packets (interestingly the other packets have 45 in the sequence number)
- They have what looks like some pad data
- The first packet has an invalid source port of 0

- They are coming in very slowly

My first reaction is that perhaps this is an OS fingerprinting exercise since sending packets with invalid flags is a common method of achieving OS fingerprinting. On examining the target port I note that 6688 is close to the IRC port of 6668, an easy keystroke error to make. This could also be an attempt to probe IRC services for some exploit such as a buffer overrun.

Classification: A malicious probe attempt and assign a medium or high risk depending on whether there is a service running on 6688 or IRC 6668.
Follow Up: Watch IP netblock

TRACE #9

From the GIAC web site:

```
Mar 27 02:53:36 myhost portsentry[178]: attackalert:
Connect from host: 203.228.92.135/203.228.92.135 to UDP port: 111
Mar 27 02:53:36 myhost portsentry[178]: attackalert:
Connect from host: 203.228.92.135/203.228.92.135 to UDP port: 111
Mar 27 02:53:41 myhost portsentry[178]: attackalert:
Connect from host: 203.228.92.135/203.228.92.135 to UDP port: 111
Mar 27 02:53:46 myhost portsentry[178]: attackalert:
Connect from host: 203.228.92.135/203.228.92.135 to UDP port: 111
Mar 27 02:53:51 myhost portsentry[178]: attackalert:
Connect from host: 203.228.92.135/203.228.92.135 to UDP port: 111
Mar 27 02:54:00 myhost portsentry[178]: attackalert:
Connect from host: 203.228.92.135/203.228.92.135 to UDP port: 111
Mar 27 02:54:01 myhost portsentry[178]: attackalert:
Connect from host: 203.228.92.135/203.228.92.135 to UDP port: 111
Mar 27 02:54:07 myhost portsentry[178]: attackalert:
Connect from host: 203.228.92.135/203.228.92.135 to UDP port: 111
Mar 27 02:54:11 myhost portsentry[178]: attackalert:
Connect from host: 203.228.92.135/203.228.92.135 to UDP port: 111
Mar 27 02:54:16 myhost portsentry[178]: attackalert:
Connect from host: 203.228.92.135/203.228.92.135 to UDP port: 111
Mar 27 02:54:21 myhost portsentry[178]: attackalert:
Connect from host: 203.228.92.135/203.228.92.135 to UDP port: 111
Mar 27 02:54:26 myhost portsentry[178]: attackalert:
Connect from host: 203.228.92.135/203.228.92.135 to UDP port: 111
Mar 27 02:54:31 myhost portsentry[178]: attackalert:
Connect from host: 203.228.92.135/203.228.92.135 to UDP port: 111
Mar 27 02:54:40 myhost portsentry[178]: attackalert:
Connect from host: 203.228.92.135/203.228.92.135 to UDP port: 111
Mar 27 02:54:41 myhost portsentry[178]: attackalert:
Connect from host: 203.228.92.135/203.228.92.135 to UDP port: 111
Mar 27 02:54:47 myhost portsentry[178]: attackalert:
Connect from host: 203.228.92.135/203.228.92.135 to UDP port: 111
Mar 27 02:54:51 myhost portsentry[178]: attackalert:
Connect from host: 203.228.92.135/203.228.92.135 to UDP port: 111
Mar 27 02:54:57 myhost portsentry[178]: attackalert:
Connect from host: 203.228.92.135/203.228.92.135 to UDP port: 111
Mar 27 02:55:01 myhost portsentry[178]: attackalert:
Connect from host: 203.228.92.135/203.228.92.135 to UDP port: 111
```

Here we see a large number of packets coming to the targets UDP port 111, the RPC portmapper. This is a common port for probes because it can provide an attacker with information about the services running on the host. Unfortunately with the trace provided we cannot see much information about each packet. They are coming in fairly rapidly so we can conclude it is not a low and slow attempt. We cannot see any header information such as flag combinations or source ports so there is no way to tell if the packets are fabricated or if there are invalid flag combinations. If there were this could potentially be an OS fingerprinting exercise or and attempt to exploit some sort of porttmapper flaw such as a buffer overrun. There are several possible conclusions which need more data to support them.

- OS fingerprinting
- Portmapper exploit attempt
- Unsophisticated attempt to access portmapper
- The packets could have a spoofed source address in an attempt to cause trouble for the ostensible source address or to deflect attention from some other less obvious activity directed towards the target machine.

Classification: Targeted, malicious and medium risk.
Follow Up: Collect more data.

TRACE #10

From the GIAC web site:

```
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
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
```

Here we see a number of packets inbound to a variety of TCP ports on the target machine. The packets are well spaced out over time. This low and slow technique is intended to pass under the trigger level of IDS. We can also see that the source ports of the packets are all identical, this indicates a crafted packet. Unfortunately we cannot see any other information such as flags, sequence numbers etc which might give us more information about the source or help us create a signature for this scan. The packets appear to originate from the Brazilian Research Network which has become a frequent source of crack attempts (I guess its all that cheap Chilean Cabernet). There seems to be a pattern in the target ports selected i.e. the ports are offset a multiple of 2560 from each other. In fact only 10437 and 12997 are missing from the series. However, the received packets are not transmitted exactly in sequence (18117 is out of order and there are a couple of repeats). There are no well known trojans on any of these ports or on 2560. This is probably not an OS fingerprinting exercise because the packets are not going to ports with services. Neither is the attacker looking for open services because the probes are not coming on ports with well known services. Perhaps this is a search for an as yet unknown trojan.

Classification: Targeted, unknown intent, low risk.
Follow Up: Collect more data.

Last Updated: July 20th, 2017

Upcoming Training

SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
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 Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 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
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
SANS Baltimore Fall 2017	Baltimore, MD	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
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