Global Information Assurance Certification Paper

Northcutt, 4/12/00 was asked to re-grade by panel. Panel, please keep in mind that Sean's was one of the first submissions of his class and should get some "pioneer grace".

Starts out with 100 has own detects.
1 -3 incorrect description
2 -3 incorrect, -1 clarity
3 ok
4 nice job actually
5 seems fine
6 -4 incorrect description
7 seems fine
8 this doesn't match the standard pattern for DOS, so do we mark the student wrong? I don't think so.
9 seems fine
10 -3 incorrect

- 8 overall limited history, research, draft score 79

Sean M. Dickens
****
* Detect #1   *
****

```
12:00:13.111559 server1.com > 10.1.227.3: icmp: address mask is 0xfffffe00
12:15:26.806311 server1.com > 192.168.95.89: icmp: address mask is 0xfffffe00
12:16:24.373946 server1.com > 10.1.62.62: icmp: address mask is 0xfffffe00
12:33:32.136320 server1.com > 10.1.69.76: icmp: address mask is 0xfffffe00
12:43:58.795005 server1.com > 192.168.43.40: icmp: address mask is 0xfffffe00
12:44:53.971457 server1.com > 10.1.124.47: icmp: address mask is 0xfffffe00
12:49:18.361727 server1.com > 172.16.12.95: icmp: address mask is 0xfffffe00
12:53:48.520128 server1.com > 172.21.1.123: icmp: address mask is 0xfffffe00
12:53:48.521803 server1.com > 172.21.1.123: icmp: address mask is 0xfffffe00
12:56:19.578767 server1.com > 172.16.60.71: icmp: address mask is 0xfffffe00
12:58:39.737127 server1.com > 10.1.221.50: icmp: address mask is 0xfffffe00
12:59:35.207796 server1.com > 192.168.208.76: icmp: address mask is 0xfffffe00
```

Active Targeting: Yes
Techniques: Fairly slow (really slow in specific subnets).
Randomly scanned IPs even though there is one repeated IP Address, probably would have escaped detection if we would only be monitoring a single Class C range (IDS is set for higher number of requests threshold than the number of requests from each individual IP range is being scanned).

Source address range is valid however no determination concerning spoofing (unable to tcpdump output for TTL's to detect possible spoofing).

Intent: Probable Efficient Network Mapping

History: This source was identified performing the same type of scans every day, every hour over a period of about 2 weeks.

Analysis: Source is performing initial network mapping (recon) slowly to avoid detection. CERT should be notified.

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

07:11:28.976343 ns.foreign-net.1664 > 10.1.91.21.domain: S 2105728000:2105728000(0) win 4096
07:11:34.628642 ns.foreign-net.1664 > 10.1.91.21.domain: S 2105728000:2105728000(0) win 4096
07:11:34.645795 ns.foreign-net.1661 > 10.1.91.21.domain: S 2105536000:2105536000(0) win 4096
07:11:46.633523 ns.foreign-net.1664 > 10.1.91.21.domain: S 2105728000:2105728000(0) win 4096
07:11:46.646801 ns.foreign-net.1661 > 10.1.91.21.domain: S 2105536000:2105536000(0) win 4096
07:12:10.633264 ns.foreign-net.1664 > 10.1.91.21.domain: S 2105728000:2105728000(0) win 4096
07:12:10.633267 ns.foreign-net.1661 > 10.1.91.21.domain: S 2105536000:2105536000(0) win 4096
07:31:45.837604 ns.foreign-net.1917 > 10.1.91.21.domain: S 144448000:144448000(0) win 4096
07:31:57.819165 ns.foreign-net.1917 > 10.1.91.21.domain: S 144448000:144448000(0) win 4096
07:32:21.823601 ns.foreign-net.1917 > 10.1.91.21.domain: S 144448000:144448000(0) win 4096
07:32:53.529853 ns.foreign-net.1923 > 10.1.91.21.domain: S 155776000:155776000(0) win 4096
07:33:11.323822 ns.foreign-net.1923 > 10.1.91.21.domain: S 155776000:155776000(0) win 4096
07:39:31.823055 ns1.mysite.1034 > ns.foreign-net.domain: 33703+ (33)
07:39:31.827618 ns1.mysite.1034 > ns.foreign-net.domain: 22512+ (33)
07:39:31.961189 ns.foreign-net.domain > ns1.mysite.1034: 22512* 2/0/0 (74)
07:39:31.974523 ns.foreign-net.domain > ns1.mysite.1034: 33703* 2/0/0 (74)

Active Targeting: Yes
Techniques:  Not very subtle.
             Packets are crafted (based on recurring seq numbers, and src ports).
             Packets w/ src port 1664 have seq # of 2105728000, 1661 are 2105536000, 1917 are 144448000 and 1923 are
              155776000.
             This part of the trace doesn't show it but the src host changed the src ports to a similar pattern as above
              every hour.
             Packets sent in pattern (5-8 packets, within 40 seconds twice an hour).
             No SYN/ACK & FIN packets detected.  Incomplete 3-way handshake.
Intent:  Possible SYN flood of DNS trying a known DNS exploit.  Also, possible DNS zone transfer attempts.
History:  During this one day, this site hit us with this same pattern every hour.  They also continued to perform these
          hits for over 8 hours then no more traffic was seen.
Analysis:  Considering the number of packets and the length of history and the dst host addr it seems to be a SYN flood.
           At the end of every hours scanning, a different IDS performed the DNS lookup.  This leads me to believe that
           it is a SYN flood, however the DNS did not show visible signs Denial of Service.  There were no reports about
           the DNS not working.  There's so many of these packets that fall into a pattern and that are crafted, a DOS
           seems likely.  Again, this analysis was performed without the use of TCPDump raw data, so src host-spoofing
           determination cannot be performed.
```

```
***************
*  Detect #3   *
***************

14:01:45.208038 foreign-host.4851 > server1.mysite.telnet: S 3513843160:3513843160(0) win 16060  (DF)
14:01:47.622683 foreign-host.4852 > server1.mysite.ftp: S 3511786092:3511786092(0) win 16060  (DF)
14:02:03.213520 foreign-host.4852 > server1.mysite.ftp: F 3511786093:3511786093(0) ack 575816481 win 16060 (DF)
14:02:03.213563 foreign-host.4853 > server1.mysite.imap2: S 3536796329:3536796329(0) win 16060  (DF)
14:02:04.261318 foreign-host.4854 > server1.mysite.pop-3: S 3528261018:3528261018(0) win 16060  (DF)
14:03:51.436943 foreign-host.4851 > server1.mysite.telnet: F 3513843161:3513843161(0) ack 575676979 win 16060 (DF)

Active Targeting: Yes
Techniques:  Appears to have crafted src ports or possibly a really idle machine.
             Hit four services with known vulnerabilities.
             Not stealthy, times for the 6 packets are fairly close although this could be so slow that it was not
               detected before or after because it didn't "break" the intrusion parameters of our IDS.
Intent:  Possible host scan for services with vulnerabilities.  Possible determination of server software (based on the
         reply of the SYN & F/ACK packets) being run for those services to be used later for a more directed attack.
History:  No other traffic from this host was found during the previous 5 days and one day after.  The source address
          (if not spoofed) is from a known information gathering & attacking entity.
Analysis:  Slow host/service scan.  This may have been a second or third tier scan to narrow their attack hosts.  This
           scan may have been used to gather more detailed information about the host to help determine what type of
           exploit to use.
```

```
****************
*  Detect #4   *
****************

22:15:03.971577 foreign-host.country.98 > 10.1.2.1.98: SF 920391737:920391737(0) win 1028
22:15:03.986650 foreign-host.country.98 > 10.1.2.2.98: SF 920391737:920391737(0) win 1028
22:15:04.003814 foreign-host.country.98 > 10.1.2.3.98: SF 920391737:920391737(0) win 1028
22:15:04.026751 foreign-host.country.98 > 10.1.2.4.98: SF 920391737:920391737(0) win 1028
22:15:04.046412 foreign-host.country.98 > 10.1.2.5.98: SF 920391737:920391737(0) win 1028
22:15:04.064436 foreign-host.country.98 > 10.1.2.6.98: SF 920391737:920391737(0) win 1028
22:15:04.084466 foreign-host.country.98 > 10.1.2.7.98: SF 920391737:920391737(0) win 1028
22:15:04.106646 foreign-host.country.98 > 10.1.2.8.98: SF 609686485:609686485(0) win 1028
22:15:04.123953 foreign-host.country.98 > 10.1.2.9.98: SF 609686485:609686485(0) win 1028
22:15:04.145048 foreign-host.country.98 > 10.1.2.10.98: SF 609686485:609686485(0) win 1028

Active Targeting: Yes
Techniques:  Sloppy work.  Times very close together and over an extended period of time.
             Crafted packets based on src port always 98 and seq numbers being the same two.
             Sequential dst hosts scanned.
             Hosts scanned for Linux Configuration ports.
             Anomalous SYN/FIN bits set.
Intent:  Probable Information Gathering about the LinuxConf service.
History:  Scan performed over 2 days in the same manner on every class C address in our network.  The above techniques
          were noted on all the scans.  This src addr was never before nor after seen.
Analysis:  Information gathering about the LinuxConf service by a script kiddie.  The sloppiness and speed of the scan
           indicate lack of caring if he's caught, unknowledgeable or having fun.
```

```
****************
*  Detect #5   *
****************

12:33:44.624498 server.net.netbios-ns > 172.16.160.2.netbios-ns: udp 50
12:33:55.283115 server.net.netbios-ns > 172.16.160.3.netbios-ns: udp 50
12:34:05.869114 server.net.netbios-ns > 172.16.160.4.netbios-ns: udp 50
12:34:07.332534 server.net.netbios-ns > 172.16.160.4.netbios-ns: udp 50
12:34:19.364950 server.net.netbios-ns > 172.16.160.5.netbios-ns: udp 50
12:34:26.733039 server.net.netbios-ns > 172.16.160.6.netbios-ns: udp 50
12:34:28.539262 server.net.netbios-ns > 172.16.160.6.netbios-ns: udp 50
12:34:29.787635 server.net.netbios-ns > 172.16.160.6.netbios-ns: udp 50
12:34:37.584627 server.net.netbios-ns > 172.16.160.7.netbios-ns: udp 50
12:34:39.135623 server.net.netbios-ns > 172.16.160.7.netbios-ns: udp 50
12:34:48.267294 server.net.netbios-ns > 172.16.160.8.netbios-ns: udp 50
12:35:13.606019 server.net.netbios-ns > 172.16.160.10.netbios-ns: udp 50
12:35:27.368513 server.net.netbios-ns > 172.16.160.11.netbios-ns: udp 50
12:35:28.956166 server.net.netbios-ns > 172.16.160.11.netbios-ns: udp 50
12:35:46.917256 server.net.netbios-ns > 172.16.160.13.netbios-ns: udp 50
12:35:49.726370 server.net.netbios-ns > 172.16.160.13.netbios-ns: udp 50

Active Targeting: Yes
Techniques:  Continuous scan of sequentially incremented IP Addresses.
             Scan Time very close together.
             Src port is static.
             Single Service port scanned.
             Sloppy, easily detected.
Intent:  Probable host scan for NetBIOS (Windows OS), Information Gathering.
History:  Conducted scan for 42 minutes of entire Class C Subnet.  Src Addr never seen before.  Similar IP Address
          detected performing similar scans after this one was detected.
Analysis:  Service scan for OS determination for follow-up supplemental information gathering and Windows-based
           exploits.
```

```
****************
*  Detect #6   *
****************

01:17:45.217720 isphost.net > 172.16.93.30: icmp: host ThirdHost1 unreachable
01:18:10.248452 isphost.net > 10.1.225.120: icmp: host ThirdHost1 unreachable
01:18:38.823551 isphost.net > 10.1.149.95: icmp: host ThirdHost2 unreachable
01:20:32.419783 isphost.net > 172.16.12.93: icmp: host ThirdHost3 unreachable
01:21:17.938372 isphost.net > 192.168.128.87: icmp: host ThirdHost4 unreachable
01:24:56.635578 isphost.net > 10.1.111.53: icmp: host ThirdHost5 unreachable
01:32:24.615536 isphost.net > 10.1.75.11: icmp: host ThirdHost6 unreachable
01:32:49.628331 isphost.net > 172.16.202.19: icmp: host ThirdHost3 unreachable
01:35:29.377552 isphost.net > 10.1.152.43: icmp: host ThirdHost7 unreachable
01:36:37.843302 isphost.net > 10.1.134.120: icmp: host ThirdHost3 unreachable
01:36:52.798988 isphost.net > 192.168.157.100: icmp: host ThirdHost6 unreachable
01:38:18.866023 isphost.net > 192.168.91.82: icmp: host ThirdHost6 unreachable
01:38:25.377858 isphost.net > 10.1.53.109: icmp: host ThirdHost6 unreachable
01:39:15.196911 isphost.net > 172.16.125.110: icmp: host ThirdHost3 unreachable
01:39:51.463735 isphost.net > 10.1.149.77: icmp: host ThirdHost6 unreachable
01:42:07.175664 isphost.net > 172.16.31.95: icmp: host ThirdHost3 unreachable
02:01:14.571289 isphost.net > 10.1.61.109: icmp: host ThirdHost6 unreachable
02:01:39.923279 isphost.net > host1.mysite: icmp: host ThirdHost6 unreachable
02:01:43.578323 isphost.net > host2.mysite: icmp: host ThirdHost6 unreachable
02:03:34.382767 isphost.net > 172.16.76.18: icmp: host ThirdHost6 unreachable
02:04:29.281495 isphost.net > 172.16.200.6: icmp: host ThirdHost6 unreachable
02:06:55.924470 isphost.net > 172.16.39.98: icmp: host ThirdHost6 unreachable
02:07:34.872114 isphost.net > 10.1.38.92: icmp: host ThirdHost6 unreachable
02:08:04.026117 isphost.net > 10.1.61.103: icmp: host ThirdHost6 unreachable
02:08:15.568636 isphost.net > 10.1.41.30: icmp: host ThirdHost6 unreachable
02:12:54.917524 isphost.net > 172.16.128.120: icmp: host ThirdHost6 unreachable
02:13:53.664915 isphost.net > host3.mysite: icmp: host ThirdHost6 unreachable
02:14:04.478203 isphost.net > 172.16.162.122: icmp: host ThirdHost6 unreachable
02:16:24.342714 isphost.net > 172.16.50.63: icmp: host ThirdHost6 unreachable

Active Targeting: Yes
Techniques:  Single host is sending packets from same src port.
             Multiple local IP's being "borrowed", none used twice.
             All ICMP messages are unreachable.
             Not very stealthy.  Not trying to be undetected.
Intent:  Possible Denial of Service or network mapping.
History:  This traffic occurred approximately 2.5 hours early in the morning.  Traffic was not seen prior nor after this
          detect.
```

Analysis: Possible Denial of Service, however the time between packets are too far apart. Also, there are many "victims", not very concentrated. Thirdhost6 is the most likely target with the others being possible camouflage. I think that It may be a new "hacker" trying out a DoS script but didn't configure it well enough to affect the desired outcome.

```
****************
*  Detect #7   *
****************

01:19:08.219877 host.country.1075 > myhost.mysite.www: S 56031:56031(0) win 8192  (DF)
01:19:08.222532 myhost.mysite.www > host.country.1075: R 0:0(0) ack 56032 win 0
01:19:08.833843 host.country.1075 > myhost.mysite.www: S 56031:56031(0) win 8192  (DF)
01:19:08.835025 myhost.mysite.www > host.country.1075: R 0:0(0) ack 56032 win 0
01:19:09.449081 host.country.1075 > myhost.mysite.www: S 56031:56031(0) win 8192  (DF)
01:19:09.450294 myhost.mysite.www > host.country.1075: R 0:0(0) ack 56032 win 0
01:19:10.053625 host.country.1075 > myhost.mysite.www: S 56031:56031(0) win 8192  (DF)
01:19:10.054684 myhost.mysite.www > host.country.1075: R 0:0(0) ack 56032 win 0
01:19:10.235370 host.country.1090 > myhost.mysite.webcache: S 58048:58048(0) win 8192  (DF)
01:19:13.172774 host.country.1090 > myhost.mysite.webcache: S 58048:58048(0) win 8192  (DF)
01:19:19.225969 host.country.1090 > myhost.mysite.webcache: S 58048:58048(0) win 8192  (DF)
01:19:31.268378 host.country.1090 > myhost.mysite.webcache: S 58048:58048(0) win 8192  (DF)
01:19:55.421395 host.country.1155 > myhost.mysite.3128: S 103248:103248(0) win 8192  (DF)
01:19:58.441540 host.country.1155 > myhost.mysite.3128: S 103248:103248(0) win 8192  (DF)
01:20:04.534060 host.country.1155 > myhost.mysite.3128: S 103248:103248(0) win 8192  (DF)
01:20:16.604157 host.country.1155 > myhost.mysite.3128: S 103248:103248(0) win 8192  (DF

Active Targeting: Yes
Techniques:  Single host, multiple src ports.
             Src ports for each given service remain the same (80 for 80, 1090 for 8080, 1155 for 3128).
             Myhost responded on the WWW port.
             Pattern of 4 packets to each port on the site.
             Seq numbers are the same for each set of packets.
             Scan done extremely quickly.
Intent:  Probable sweep for squid proxy vulnerability on this host.  Most likely a followup scan to a previous web
         server scan.
History:  This host was not seen before nor after this small scan was detected.  The host was found with personal web
          services.  During this one day, other sites from the same country was found scanning multiple local hosts for
          multiple ports.  This host was not on any of the other scans.  Scanning hosts were from ISP's so the IP
          Addresses are valid, in-use IPs.
Analysis:  Squid Proxy vulnerability scan.  Appears to be very directed.  Probable follow-up scan to a web service scan
           done previously.  Since the IP Address is from an ISP and no other traffic was found from these addresses
           before or after this scan, the scanner probably "borrowed" the IP address either by using a machine hacked
           within the ISP or by spoofing (but if he spoofed it makes more difficult to gather the info).
```

```
****************
*  Detect #8   *
****************

00:04:11.965100 isp.20859 > 172.16.106.199.24844: R 0:0(0) ack 1435102413 win 0
00:05:17.370712 isp.21538 > 10.1.86.93.8232: R 0:0(0) ack 1427836337 win 0
04:54:20.909069 isp.20976 > 172.16.45.95.13170: R 0:0(0) ack 288441842 win 0
04:54:27.086171 isp.28899 > 172.16.171.225.41242: R 0:0(0) ack 1284361888 win 0
04:54:32.623339 isp.1538 > 172.16.213.64.47627: R 0:0(0) ack 1179694190 win 0
04:54:42.020516 isp.32420 > 10.1.152.168.35129: R 0:0(0) ack 974441611 win 0
04:54:42.265574 isp.24216 > 10.1.22.142.50756: R 0:0(0) ack 1757805074 win 0
04:54:46.863847 isp.8921 > 10.1.96.176.18539: R 0:0(0) ack 1687367606 win 0
04:54:49.286001 isp.1803 > 172.16.203.169.41435: R 0:0(0) ack 1459687649 win 0
04:54:51.783608 isp.3370 > 10.1.88.218.58441: R 0:0(0) ack 920654057 win 0
04:54:51.932583 router.mysite > isp: icmp: time exceeded in-transit

Active Targeting: Yes
Techniques:  Active scanning detected for 2+ hours.
             Src ports for the entire scan never duplicated.
             Dst ports repeated for a small number of IP Addresses.  (not incl. In this excerpt)
             Most dst ports are over 10,000.
             One IP Address responded on 7 high ports (not incl. in this excerpt)
             Scanned appeared to begin around midnight local time for 2 packets then pick up again at 04:54.
             RST/Ack bits set.
             Not subtle at all.
             Router.mysite sent time exceeded in transit on several occasions. (not incl. In this excerpt)
Intent:  Possible network mapping or Trojan port scan.
History:  This ISP is known for it's network mapping.  We've seen it hundreds of times, in different forms.
Analysis:  The IDS sensor had a hardware failure for the 4+ hours between 00-04.  Scanning may have continued.  This ISP
           has a long history of allowing users to perform any operation they want and will not respond to queries.
           This is a RST scan hoping for RST responses for information gathering purposes.  If an IP Address is invalid
           my routers politely tell them the IP Address is inactive.  Several local systems responded to the high port
           RSTs indicating the high port is active.  Further investigation using nmap and a phone call revealed that the
           systems that responded were HP LJ printers.  The high ports are not listed in any "known Trojan" list.
```

```
****************
*  Detect #9   *
****************

02:44:48.230251 friendly-host.1028 > 172.16.170.238.snmp: GetRequest(11)
02:44:48.230997 router.mysite > 55.192.6.152: icmp: host 172.16.170.238 unreachable - admin prohibited filter
02:44:48.338889 friendly-host.1028 > 172.16.170.237.snmp: GetRequest(11)
02:44:48.359272 friendly-host.1028 > 172.16.170.236.snmp: GetRequest(11)
02:44:48.390383 friendly-host.1028 > 172.16.170.235.snmp: GetRequest(11)
02:44:48.418781 friendly-host.1028 > 172.16.170.234.snmp: GetRequest(11)
02:44:48.449705 friendly-host.1028 > 172.16.170.233.snmp: GetRequest(11)
02:44:48.485357 friendly-host.1028 > 172.16.170.232.snmp: GetRequest(11)
02:44:48.515834 friendly-host.1028 > 172.16.170.231.snmp: GetRequest(11)
02:44:48.539502 friendly-host.1028 > 172.16.170.230.snmp: GetRequest(11)
02:44:48.570299 friendly-host.1028 > 172.16.170.229.snmp: GetRequest(11)
02:44:48.599136 friendly-host.1028 > 172.16.170.228.snmp: GetRequest(11)
02:44:48.630919 friendly-host.1028 > 172.16.170.227.snmp: GetRequest(11)
02:44:48.677692 friendly-host.1028 > 172.16.170.226.snmp: GetRequest(11)
02:44:48.693260 friendly-host.1028 > 172.16.170.225.snmp: GetRequest(11)
02:44:48.741503 friendly-host.1028 > 172.16.170.224.snmp: GetRequest(11)
02:44:48.742233 router.mysite > friendly-host: icmp: host 172.16.170.224 unreachable - admin prohibited filter
02:44:49.321522 friendly-host.1028 > 172.16.170.223.snmp: GetRequest(11)
02:44:49.322202 router.mysite > friendly-host: icmp: host 172.16.170.223 unreachable - admin prohibited filter

Active Targeting: Yes
Techniques:  Not subtle, however scanned for only 2 minutes (twice within one day)
             Same src port on every packet.
             Scanned sequential IPs in one Class C range.
             Scanned dst SNMP port only.
             Sent 11 bytes of in data every packet.
             Router blocked some requests using ACL.
             Src IP static.
Intent:  Possible querying for SNMP enabled hosts.  Querying for SNMP enable or community strings.  Possbile spoofed src
         addresses.
History:  Src site is a partnered site.  Scans were done daily, four times a day until offending source found.
Analysis:  Friendly-host is a HP Printer (or some other snmp managing device) scanning for SNMP manageable equipment.
           By default the equipment is set up to scan 255.255.255.255 for devices every 6 hours.  Determined that
           friendly-host was not spoofed.
```

```
****************
*  Detect #10  *
****************

12:03:17.764663 foreign-host.country.auth > 172.16.243.13.1142: S 8331218:8331218(0) ack 674711610 win 32736
12:04:43.789575 foreign-host.country.auth > 10.1.103.25.1243: S 8917010:8917010(0) ack 674711610 win 32736
12:04:55.997424 foreign-host.country.auth > 172.16.81.44.1142: S 7079850:7079850(0) ack 674711610 win 32736
12:05:18.268642 foreign-host.country.auth > 10.1.135.62.1098: S 12335402:12335402(0) ack 674711610 win 32736
12:05:32.714976 foreign-host.country.auth > 10.1.150.40.1243: S 4184298:4184298(0) ack 674711610 win 32736
12:05:59.111635 foreign-host.country.auth > 172.16.143.37.1287: S 12878346:12878346(0) ack 674711610 win 32736
12:06:21.134630 foreign-host.country.auth > 10.1.197.55.1243: S 12652434:12652434(0) ack 674711610 win 32736
12:06:22.272309 foreign-host.country.auth > 172.21.1.24.1619: S 6289986:6289986(0) ack 674711610 win 32736
12:06:22.274043 foreign-host.country.auth > 172.21.1.24.1619: S 6289986:6289986(0) ack 674711610 win 32736
12:07:09.395393 foreign-host.country.auth > 10.1.244.70.1243: S 16225882:16225882(0) ack 674711610 win 32736
12:07:44.307870 foreign-host.country.auth > 172.16.237.67.1287: S 12826730:12826730(0) ack 674711610 win 32736
12:09:52.897742 foreign-host.country.auth > 172.16.60.120.1142: S 2725146:2725146(0) ack 674711610 win 32736
12:10:09.098030 foreign-host.country.auth > 172.16.75.98.1287: S 5100586:5100586(0) ack 674711610 win 32736
12:10:09.138897 172.16.75.1 > foreign-host.country: icmp: time exceeded in-transit

Active Targeting: Yes
Techniques:  Static src port.
             Continuous scan for 4 dst ports.
             Rarely duplicated dst IP Addresses.
             At least one dst port is listening port for a Trojan.
             SYN/ACKs sent fairly slowly especially to the same IP Range.  (roughly 30 sec apart)
             Seq numbers appear to be fairly random across the scanned IP Ranges.
             Router notified foreign-host of invalid IP numbers.
Intent:  Probable Trojan scan with clutter added.  Other dst addresses may be "unregistered" Trojan service ports.
History:  IP Addresses similar to Foreign-host has conducted scans of local network in the past.  The scans were RST
          scans across our IP Ranges.  This scan may have not been detected if the scan didn't cross over to 2 different
          class B ranges and 1 class C range and the threshold broken.
Analysis:  Trojan Port scan nested within clutter.
```

Last Updated: July 25th, 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 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