# Global Information Assurance Certification Paper

***** Northcutt, I loved number 4, Andrew gets a full 10 point bonus for a signature I had never seen before, small nit on 1 source is fixed at 60000, not 6000, if you still have the content dump 1 and let me know what you get. 92 ***

**GIAC Practical Submission**
**Andrew J. Korty**

**All detects in this submission were personally collected. The tcpdump program was used on a FreeBSD 3.4 system to collect and analyze all detects. Our own IP addresses have been changed, but foreign addresses have been left as they were found, complete with hostnames if possible.**

**1. Deep Throat Trojan Scan**

**UDP traffic to port 2140 indicates the attacker is scanning for the Deep Throat trojan. The attacker used crafted packets to keep the source port fixed at 6000, perhaps in an attempt to disguise the scan as legitimate X11 window system traffic. The scan was fast, spanning the entire subnet in only a few seconds.**

**Many of the IPs in the address space were skipped, which could mean we do not have full source, meaning we are not seeing all the traffic from the attacker. It could also indicate this attacker has already done reconnaissance on this subnet and has narrowed the target list.**

**Using WHOIS and the World Wide Web, it was determined the attacker appears to be a customer of the PIPEX Dial Service in the UK.**

```
08:23:39.830437 userbu51.aol.uk.uudial.com.60000 > 192.168.67.11.2140: udp 2
08:23:39.880126 userbu51.aol.uk.uudial.com.60000 > 192.168.67.15.2140: udp 2
08:23:39.951929 userbu51.aol.uk.uudial.com.60000 > 192.168.67.22.2140: udp 2
08:23:39.983435 userbu51.aol.uk.uudial.com.60000 > 192.168.67.27.2140: udp 2
08:23:39.999510 userbu51.aol.uk.uudial.com.60000 > 192.168.67.30.2140: udp 2
08:23:40.000673 userbu51.aol.uk.uudial.com.60000 > 192.168.67.31.2140: udp 2
08:23:40.092103 userbu51.aol.uk.uudial.com.60000 > 192.168.67.43.2140: udp 2
08:23:40.106437 userbu51.aol.uk.uudial.com.60000 > 192.168.67.46.2140: udp 2
08:23:40.110901 userbu51.aol.uk.uudial.com.60000 > 192.168.67.47.2140: udp 2
08:23:40.152773 userbu51.aol.uk.uudial.com.60000 > 192.168.67.52.2140: udp 2
08:23:40.153908 userbu51.aol.uk.uudial.com.60000 > 192.168.67.51.2140: udp 2
08:23:40.159301 userbu51.aol.uk.uudial.com.60000 > 192.168.67.54.2140: udp 2
08:23:40.187662 userbu51.aol.uk.uudial.com.60000 > 192.168.67.56.2140: udp 2
08:23:40.202133 userbu51.aol.uk.uudial.com.60000 > 192.168.67.58.2140: udp 2
08:23:40.208379 userbu51.aol.uk.uudial.com.60000 > 192.168.67.60.2140: udp 2
08:23:40.288612 userbu51.aol.uk.uudial.com.60000 > 192.168.67.69.2140: udp 2
08:23:40.307150 userbu51.aol.uk.uudial.com.60000 > 192.168.67.72.2140: udp 2
08:23:40.341321 userbu51.aol.uk.uudial.com.60000 > 192.168.67.77.2140: udp 2
08:23:40.419522 userbu51.aol.uk.uudial.com.60000 > 192.168.67.83.2140: udp 2
08:23:40.454346 userbu51.aol.uk.uudial.com.60000 > 192.168.67.90.2140: udp 2
08:23:40.510595 userbu51.aol.uk.uudial.com.60000 > 192.168.67.95.2140: udp 2
08:23:40.520048 userbu51.aol.uk.uudial.com.60000 > 192.168.67.96.2140: udp 2
08:23:40.587004 userbu51.aol.uk.uudial.com.60000 > 192.168.67.106.2140: udp 2
08:23:40.649680 userbu51.aol.uk.uudial.com.60000 > 192.168.67.115.2140: udp 2
08:23:40.677038 userbu51.aol.uk.uudial.com.60000 > 192.168.67.117.2140: udp 2
08:23:40.741468 userbu51.aol.uk.uudial.com.60000 > 192.168.67.130.2140: udp 2
08:23:40.749098 userbu51.aol.uk.uudial.com.60000 > 192.168.67.132.2140: udp 2
08:23:40.818842 userbu51.aol.uk.uudial.com.60000 > 192.168.67.139.2140: udp 2
08:23:40.868515 userbu51.aol.uk.uudial.com.60000 > 192.168.67.142.2140: udp 2
08:23:40.874842 userbu51.aol.uk.uudial.com.60000 > 192.168.67.144.2140: udp 2
08:23:40.883001 userbu51.aol.uk.uudial.com.60000 > 192.168.67.145.2140: udp 2
08:23:40.918964 userbu51.aol.uk.uudial.com.60000 > 192.168.67.151.2140: udp 2
08:23:40.919786 userbu51.aol.uk.uudial.com.60000 > 192.168.67.152.2140: udp 2
08:23:40.924176 userbu51.aol.uk.uudial.com.60000 > 192.168.67.153.2140: udp 2
08:23:41.029434 userbu51.aol.uk.uudial.com.60000 > 192.168.67.163.2140: udp 2
```

```
08:23:41.037476 userbu51.aol.uk.uudial.com.60000 > 192.168.67.165.2140: udp 2
08:23:41.065154 userbu51.aol.uk.uudial.com.60000 > 192.168.67.170.2140: udp 2
08:23:41.072420 userbu51.aol.uk.uudial.com.60000 > 192.168.67.171.2140: udp 2
08:23:41.084455 userbu51.aol.uk.uudial.com.60000 > 192.168.67.172.2140: udp 2
08:23:41.098736 userbu51.aol.uk.uudial.com.60000 > 192.168.67.176.2140: udp 2
08:23:41.106518 userbu51.aol.uk.uudial.com.60000 > 192.168.67.178.2140: udp 2
08:23:41.158190 userbu51.aol.uk.uudial.com.60000 > 192.168.67.185.2140: udp 2
08:23:41.159013 userbu51.aol.uk.uudial.com.60000 > 192.168.67.186.2140: udp 2
08:23:41.172506 userbu51.aol.uk.uudial.com.60000 > 192.168.67.187.2140: udp 2
08:23:41.210718 userbu51.aol.uk.uudial.com.60000 > 192.168.67.189.2140: udp 2
08:23:41.218905 userbu51.aol.uk.uudial.com.60000 > 192.168.67.190.2140: udp 2
08:23:41.259169 userbu51.aol.uk.uudial.com.60000 > 192.168.67.198.2140: udp 2
08:23:41.274693 userbu51.aol.uk.uudial.com.60000 > 192.168.67.203.2140: udp 2
08:23:41.316696 userbu51.aol.uk.uudial.com.60000 > 192.168.67.205.2140: udp 2
08:23:41.449203 userbu51.aol.uk.uudial.com.60000 > 192.168.67.224.2140: udp 2
08:23:41.500719 userbu51.aol.uk.uudial.com.60000 > 192.168.67.227.2140: udp 2
08:23:41.502749 userbu51.aol.uk.uudial.com.60000 > 192.168.67.228.2140: udp 2
08:23:41.553494 userbu51.aol.uk.uudial.com.60000 > 192.168.67.233.2140: udp 2
08:23:41.631664 userbu51.aol.uk.uudial.com.60000 > 192.168.67.242.2140: udp 2
08:23:41.686274 userbu51.aol.uk.uudial.com.60000 > 192.168.67.246.2140: udp 2
08:23:41.716656 userbu51.aol.uk.uudial.com.60000 > 192.168.67.248.2140: udp 2
```

**2. Fallout from Spoofing or Operating System Fingerprinting**

The only source we have for this detect is three TCP resets spaced about 40 minutes apart. Perhaps the attacker is slowly trying several exploits on vital.bleeding.com and spoofing our IP addresses. Since vital.bleeding.com is not listening on any of these ports, we're seeing the TCP reset packets. The source addresses for the resets are for the following services:

```
isi-gl           55/tcp    #ISI Graphics Language
netbios-ssn     139/tcp    #NETBIOS Session Service
iso-tp0         146/tcp
```

The NetBIOS session port is a common target, but the other two services seem pretty obscure. The high destination ports for the resets could indicate that the attacker's machine is very busy trying these exploits on our machines and others.

Another possibility is that vital.bleeding.com is initiating a low and slow scan against our network, crafting packets to have unusual source ports. The destination ports are not those of known trojans, so perhaps the attacker is attempting to perform operating system fingerprinting by sending unsolicited RST-ACK packets to ports that probably won't be listening, hoping it will evoke different responses on different systems. This scenario is disturbing, since we see the attacker only targeting these three machines, which he or she may be very determined to compromise.

```
21:48:43.393260 vital.bleeding.com.146 > 192.168.67.117.46016: R 0:0(0) ack 0 win 0
22:30:14.285649 vital.bleeding.com.55 > 192.168.67.112.52230: R 0:0(0) ack 0 win 0
23:12:46.068500 vital.bleeding.com.139 > 192.168.67.151.22436: R 0:0(0) ack 0 win 0
```

**3. Scan for FTP Servers**

This scan for FTP servers involves most of the subnet. The attacker could be looking for vulnerabilities or just an anonymous drop area for pirated software or password files from other systems. The scan is most likely automated, judging by the speed, but the packets are probably not crafted, since the source ports are increasing and the sequence numbers are changing.

As in previous detects in this report, some IPs are being skipped,

which could have been an indication the attacker had already mapped the network and now knows which IPs to target. However, in this case, the intervals by which the source port numbers and the destination IPs increase correspond, indicating we probably do not have full source.

The attacker appears to be the typical abuser of a dial-in service provider, Verio.

```
16:27:03.790754 209-107-87-034.chicago.verio.net.2360 > 192.168.67.11.21: S
3674146652:3674146652(0) win 32120 <mss 1460,sackOK,timestamp 243771545 0,nop,wscale 0>
(DF)
16:27:03.794728 209-107-87-034.chicago.verio.net.2364 > 192.168.67.15.21: S
3678742278:3678742278(0) win 32120 <mss 1460,sackOK,timestamp 243771545 0,nop,wscale 0>
(DF)
16:27:03.908417 209-107-87-034.chicago.verio.net.2369 > 192.168.67.20.21: S
3682818394:3682818394(0) win 32120 <mss 1460,sackOK,timestamp 243771558 0,nop,wscale 0>
(DF)
16:27:03.967357 209-107-87-034.chicago.verio.net.2371 > 192.168.67.22.21: S
3679985817:3679985817(0) win 32120 <mss 1460,sackOK,timestamp 243771565 0,nop,wscale 0>
(DF)
16:27:04.492339 209-107-87-034.chicago.verio.net.2385 > 192.168.67.30.21: S
3679996600:3679996600(0) win 32120 <mss 1460,sackOK,timestamp 243771617 0,nop,wscale 0>
(DF)
16:27:04.515237 209-107-87-034.chicago.verio.net.2397 > 192.168.67.42.21: S
3674099790:3674099790(0) win 32120 <mss 1460,sackOK,timestamp 243771617 0,nop,wscale 0>
(DF)
16:27:04.519524 209-107-87-034.chicago.verio.net.2402 > 192.168.67.47.21: S
3682577695:3682577695(0) win 32120 <mss 1460,sackOK,timestamp 243771617 0,nop,wscale 0>
(DF)
16:27:04.521326 209-107-87-034.chicago.verio.net.2398 > 192.168.67.43.21: S
3672735298:3672735298(0) win 32120 <mss 1460,sackOK,timestamp 243771617 0,nop,wscale 0>
(DF)
16:27:04.523902 209-107-87-034.chicago.verio.net.2401 > 192.168.67.46.21: S
3682119392:3682119392(0) win 32120 <mss 1460,sackOK,timestamp 243771617 0,nop,wscale 0>
(DF)
16:27:04.533960 209-107-87-034.chicago.verio.net.2406 > 192.168.67.51.21: S
3678952634:3678952634(0) win 32120 <mss 1460,sackOK,timestamp 243771617 0,nop,wscale 0>
(DF)
16:27:04.941718 209-107-87-034.chicago.verio.net.2449 > 192.168.67.94.21: S
3669694749:3669694749(0) win 32120 <mss 1460,sackOK,timestamp 243771662 0,nop,wscale 0>
(DF)
16:27:04.951860 209-107-87-034.chicago.verio.net.2457 > 192.168.67.102.21: S
3681220051:3681220051(0) win 32120 <mss 1460,sackOK,timestamp 243771662 0,nop,wscale 0>
(DF)
16:27:04.959772 209-107-87-034.chicago.verio.net.2450 > 192.168.67.95.21: S
3682967424:3682967424(0) win 32120 <mss 1460,sackOK,timestamp 243771662 0,nop,wscale 0>
(DF)
16:27:05.128642 209-107-87-034.chicago.verio.net.2464 > 192.168.67.109.21: S
3681832322:3681832322(0) win 32120 <mss 1460,sackOK,timestamp 243771681 0,nop,wscale 0>
(DF)
16:27:05.145675 209-107-87-034.chicago.verio.net.2467 > 192.168.67.112.21: S
3681736912:3681736912(0) win 32120 <mss 1460,sackOK,timestamp 243771682 0,nop,wscale 0>
(DF)
16:27:05.150733 209-107-87-034.chicago.verio.net.2468 > 192.168.67.113.21: S
3683542211:3683542211(0) win 32120 <mss 1460,sackOK,timestamp 243771682 0,nop,wscale 0>
(DF)
16:27:05.608484 209-107-87-034.chicago.verio.net.2487 > 192.168.67.117.21: S
3686343904:3686343904(0) win 32120 <mss 1460,sackOK,timestamp 243771728 0,nop,wscale 0>
(DF)
16:27:05.619000 209-107-87-034.chicago.verio.net.2500 > 192.168.67.130.21: S
3684145903:3684145903(0) win 32120 <mss 1460,sackOK,timestamp 243771728 0,nop,wscale 0>
(DF)
16:27:05.619802 209-107-87-034.chicago.verio.net.2499 > 192.168.67.129.21: S
3674794748:3674794748(0) win 32120 <mss 1460,sackOK,timestamp 243771728 0,nop,wscale 0>
(DF)
```

```
16:27:05.801081 209-107-87-034.chicago.verio.net.2505 > 192.168.67.135.21: S
3670774022:3670774022(0) win 32120 <mss 1460,sackOK,timestamp 243771748 0,nop,wscale 0>
(DF)
16:27:06.075963 209-107-87-034.chicago.verio.net.2512 > 192.168.67.139.21: S
3671536548:3671536548(0) win 32120 <mss 1460,sackOK,timestamp 243771774 0,nop,wscale 0>
(DF)
16:27:06.078316 209-107-87-034.chicago.verio.net.2517 > 192.168.67.144.21: S
3683915758:3683915758(0) win 32120 <mss 1460,sackOK,timestamp 243771774 0,nop,wscale 0>
(DF)
16:27:06.083402 209-107-87-034.chicago.verio.net.2518 > 192.168.67.145.21: S
3679458575:3679458575(0) win 32120 <mss 1460,sackOK,timestamp 243771774 0,nop,wscale 0>
(DF)
16:27:06.090199 209-107-87-034.chicago.verio.net.2524 > 192.168.67.151.21: S
3685402670:3685402670(0) win 32120 <mss 1460,sackOK,timestamp 243771774 0,nop,wscale 0>
(DF)
16:27:07.366406 209-107-87-034.chicago.verio.net.2658 > 192.168.67.227.21: S
3685915888:3685915888(0) win 32120 <mss 1460,sackOK,timestamp 243771901 0,nop,wscale 0>
(DF)
16:27:07.503727 209-107-87-034.chicago.verio.net.2397 > 192.168.67.42.21: S
3674099790:3674099790(0) win 32120 <mss 1460,sackOK,timestamp 243771917 0,nop,wscale 0>
(DF)
16:27:07.510215 209-107-87-034.chicago.verio.net.2409 > 192.168.67.54.21: S
3675453232:3675453232(0) win 32120 <mss 1460,sackOK,timestamp 243771917 0,nop,wscale 0>
(DF)
16:27:07.526228 209-107-87-034.chicago.verio.net.2419 > 192.168.67.64.21: S
3671858631:3671858631(0) win 32120 <mss 1460,sackOK,timestamp 243771917 0,nop,wscale 0>
(DF)
16:27:07.527197 209-107-87-034.chicago.verio.net.2424 > 192.168.67.69.21: S
3671597070:3671597070(0) win 32120 <mss 1460,sackOK,timestamp 243771917 0,nop,wscale 0>
(DF)
16:27:07.531208 209-107-87-034.chicago.verio.net.2423 > 192.168.67.68.21: S
3684438214:3684438214(0) win 32120 <mss 1460,sackOK,timestamp 243771917 0,nop,wscale 0>
(DF)
16:27:07.535022 209-107-87-034.chicago.verio.net.2427 > 192.168.67.72.21: S
3680322744:3680322744(0) win 32120 <mss 1460,sackOK,timestamp 243771918 0,nop,wscale 0>
(DF)
16:27:07.874144 209-107-87-034.chicago.verio.net.2755 > 192.168.67.242.21: S
3687271100:3687271100(0) win 32120 <mss 1460,sackOK,timestamp 243771950 0,nop,wscale 0>
(DF)
16:27:07.992745 209-107-87-034.chicago.verio.net.2457 > 192.168.67.102.21: S
3681220051:3681220051(0) win 32120 <mss 1460,sackOK,timestamp 243771962 0,nop,wscale 0>
(DF)
16:27:08.123053 209-107-87-034.chicago.verio.net.2464 > 192.168.67.109.21: S
3681832322:3681832322(0) win 32120 <mss 1460,sackOK,timestamp 243771981 0,nop,wscale 0>
(DF)
16:27:08.137107 209-107-87-034.chicago.verio.net.2467 > 192.168.67.112.21: S
3681736912:3681736912(0) win 32120 <mss 1460,sackOK,timestamp 243771982 0,nop,wscale 0>
(DF)
16:27:08.142345 209-107-87-034.chicago.verio.net.2468 > 192.168.67.113.21: S
3683542211:3683542211(0) win 32120 <mss 1460,sackOK,timestamp 243771982 0,nop,wscale 0>
(DF)
16:27:08.246772 209-107-87-034.chicago.verio.net.2764 > 192.168.67.251.21: S
3686368041:3686368041(0) win 32120 <mss 1460,sackOK,timestamp 243771991 0,nop,wscale 0>
(DF)
16:27:08.271410 209-107-87-034.chicago.verio.net.2761 > 192.168.67.248.21: S
3679604797:3679604797(0) win 32120 <mss 1460,sackOK,timestamp 243771991 0,nop,wscale 0>
(DF)
16:27:09.065164 209-107-87-034.chicago.verio.net.2518 > 192.168.67.145.21: S
3679458575:3679458575(0) win 32120 <mss 1460,sackOK,timestamp 243772074 0,nop,wscale 0>
(DF)
16:27:13.522101 209-107-87-034.chicago.verio.net.2397 > 192.168.67.42.21: S
3674099790:3674099790(0) win 32120 <mss 1460,sackOK,timestamp 243772517 0,nop,wscale 0>
(DF)
16:27:13.525095 209-107-87-034.chicago.verio.net.2407 > 192.168.67.52.21: S
3678507112:3678507112(0) win 32120 <mss 1460,sackOK,timestamp 243772517 0,nop,wscale 0>
```

```
(DF)
16:27:13.525906 209-107-87-034.chicago.verio.net.2411 > 192.168.67.56.21: S
3684766198:3684766198(0) win 32120 <mss 1460,sackOK,timestamp 243772517 0,nop,wscale 0>
(DF)
16:27:13.547944 209-107-87-034.chicago.verio.net.2423 > 192.168.67.68.21: S
3684438214:3684438214(0) win 32120 <mss 1460,sackOK,timestamp 243772517 0,nop,wscale 0>
(DF)
16:27:13.953316 209-107-87-034.chicago.verio.net.2457 > 192.168.67.102.21: S
3681220051:3681220051(0) win 32120 <mss 1460,sackOK,timestamp 243772562 0,nop,wscale 0>
(DF)
16:27:14.127017 209-107-87-034.chicago.verio.net.2464 > 192.168.67.109.21: S
3681832322:3681832322(0) win 32120 <mss 1460,sackOK,timestamp 243772581 0,nop,wscale 0>
(DF)
16:27:14.140573 209-107-87-034.chicago.verio.net.2467 > 192.168.67.112.21: S
3681736912:3681736912(0) win 32120 <mss 1460,sackOK,timestamp 243772582 0,nop,wscale 0>
(DF)
16:27:14.144227 209-107-87-034.chicago.verio.net.2468 > 192.168.67.113.21: S
3683542211:3683542211(0) win 32120 <mss 1460,sackOK,timestamp 243772582 0,nop,wscale 0>
(DF)
16:27:15.060002 209-107-87-034.chicago.verio.net.2518 > 192.168.67.145.21: S
3679458575:3679458575(0) win 32120 <mss 1460,sackOK,timestamp 243772674 0,nop,wscale 0>
(DF)
16:27:37.699185 209-107-87-034.chicago.verio.net.1164 > 192.168.67.68.21: S
3710792078:3710792078(0) win 32120 <mss 1460,sackOK,timestamp 243774937 0,nop,wscale 0>
(DF)
16:27:37.713963 209-107-87-034.chicago.verio.net.1179 > 192.168.67.83.21: S
3703357634:3703357634(0) win 32120 <mss 1460,sackOK,timestamp 243774937 0,nop,wscale 0>
(DF)
16:27:37.727077 209-107-87-034.chicago.verio.net.1173 > 192.168.67.77.21: S
3704974604:3704974604(0) win 32120 <mss 1460,sackOK,timestamp 243774937 0,nop,wscale 0>
(DF)
16:27:37.727893 209-107-87-034.chicago.verio.net.1171 > 192.168.67.75.21: S
3706560582:3706560582(0) win 32120 <mss 1460,sackOK,timestamp 243774937 0,nop,wscale 0>
(DF)
16:27:37.929586 209-107-87-034.chicago.verio.net.1186 > 192.168.67.90.21: S
3717185326:3717185326(0) win 32120 <mss 1460,sackOK,timestamp 243774960 0,nop,wscale 0>
(DF)
16:27:38.360041 209-107-87-034.chicago.verio.net.1198 > 192.168.67.102.21: S
3702753693:3702753693(0) win 32120 <mss 1460,sackOK,timestamp 243775000 0,nop,wscale 0>
(DF)
16:27:39.442289 209-107-87-034.chicago.verio.net.1353 > 192.168.67.172.21: S
3712582809:3712582809(0) win 32120 <mss 1460,sackOK,timestamp 243775108 0,nop,wscale 0>
(DF)
16:27:39.865637 209-107-87-034.chicago.verio.net.1379 > 192.168.67.198.21: S
3712307637:3712307637(0) win 32120 <mss 1460,sackOK,timestamp 243775152 0,nop,wscale 0>
(DF)
16:27:39.879522 209-107-87-034.chicago.verio.net.1384 > 192.168.67.203.21: S
3718663279:3718663279(0) win 32120 <mss 1460,sackOK,timestamp 243775152 0,nop,wscale 0>
(DF)
16:27:40.291208 209-107-87-034.chicago.verio.net.1405 > 192.168.67.224.21: S
3720040841:3720040841(0) win 32120 <mss 1460,sackOK,timestamp 243775197 0,nop,wscale 0>
(DF)
16:27:40.332883 209-107-87-034.chicago.verio.net.1409 > 192.168.67.228.21: S
3705452639:3705452639(0) win 32120 <mss 1460,sackOK,timestamp 243775200 0,nop,wscale 0>
(DF)
16:27:40.391331 209-107-87-034.chicago.verio.net.1160 > 192.168.67.64.21: S
3703914270:3703914270(0) win 32120 <mss 1460,sackOK,timestamp 243775206 0,nop,wscale 0>
(DF)
16:27:40.700858 209-107-87-034.chicago.verio.net.1164 > 192.168.67.68.21: S
3710792078:3710792078(0) win 32120 <mss 1460,sackOK,timestamp 243775237 0,nop,wscale 0>
(DF)
16:27:40.705577 209-107-87-034.chicago.verio.net.1171 > 192.168.67.75.21: S
3706560582:3706560582(0) win 32120 <mss 1460,sackOK,timestamp 243775237 0,nop,wscale 0>
(DF)
16:27:41.326365 209-107-87-034.chicago.verio.net.1205 > 192.168.67.109.21: S
```

```
3709245564:3709245564(0) win 32120 <mss 1460,sackOK,timestamp 243775300 0,nop,wscale 0>
(DF)
16:27:41.335322 209-107-87-034.chicago.verio.net.1208 > 192.168.67.112.21: S
3704317387:3704317387(0) win 32120 <mss 1460,sackOK,timestamp 243775300 0,nop,wscale 0>
(DF)
16:27:41.344989 209-107-87-034.chicago.verio.net.1209 > 192.168.67.113.21: S
3718348926:3718348926(0) win 32120 <mss 1460,sackOK,timestamp 243775300 0,nop,wscale 0>
(DF)
16:27:41.364715 209-107-87-034.chicago.verio.net.1198 > 192.168.67.102.21: S
3702753693:3702753693(0) win 32120 <mss 1460,sackOK,timestamp 243775300 0,nop,wscale 0>
(DF)
16:27:42.398502 209-107-87-034.chicago.verio.net.1326 > 192.168.67.145.21: S
3712825300:3712825300(0) win 32120 <mss 1460,sackOK,timestamp 243775407 0,nop,wscale 0>
(DF)
16:27:42.416121 209-107-87-034.chicago.verio.net.1337 > 192.168.67.156.21: S
3704074624:3704074624(0) win 32120 <mss 1460,sackOK,timestamp 243775407 0,nop,wscale 0>
(DF)
16:27:42.429923 209-107-87-034.chicago.verio.net.1346 > 192.168.67.165.21: S
3712352049:3712352049(0) win 32120 <mss 1460,sackOK,timestamp 243775408 0,nop,wscale 0>
(DF)
16:27:47.319005 209-107-87-034.chicago.verio.net.1198 > 192.168.67.102.21: S
3702753693:3702753693(0) win 32120 <mss 1460,sackOK,timestamp 243775900 0,nop,wscale 0>
(DF)
16:27:47.353710 209-107-87-034.chicago.verio.net.1205 > 192.168.67.109.21: S
3709245564:3709245564(0) win 32120 <mss 1460,sackOK,timestamp 243775900 0,nop,wscale 0>
(DF)
16:27:47.362061 209-107-87-034.chicago.verio.net.1208 > 192.168.67.112.21: S
3704317387:3704317387(0) win 32120 <mss 1460,sackOK,timestamp 243775900 0,nop,wscale 0>
(DF)
16:27:47.366248 209-107-87-034.chicago.verio.net.1209 > 192.168.67.113.21: S
3718348926:3718348926(0) win 32120 <mss 1460,sackOK,timestamp 243775900 0,nop,wscale 0>
(DF)
16:27:48.400953 209-107-87-034.chicago.verio.net.1334 > 192.168.67.153.21: S
3716845305:3716845305(0) win 32120 <mss 1460,sackOK,timestamp 243776007 0,nop,wscale 0>
(DF)
16:27:48.438789 209-107-87-034.chicago.verio.net.1326 > 192.168.67.145.21: S
3712825300:3712825300(0) win 32120 <mss 1460,sackOK,timestamp 243776007 0,nop,wscale 0>
(DF)
```

### 4. ICMP Echo Requests

This detect looks like a conventional ping scan, and it probably is. However, dumping the packets reveals something unlike any ping packet I've ever seen. Most ping packets contain in their 8-byte header an identifier and a sequence number. Following the header is usually a 56-byte payload, consisting of an 8-byte timestamp and a fill pattern. This FreeBSD ping packet follows the convention:

```
23:14:11.295427 localhost > localhost: icmp: echo request
                        4500 0054 5336 0000 ff01 6a70 7f00 0001
                        7f00 0001 0800 1e15 2263 0000 13ca 0339
                        b181 0400 0809 0a0b 0c0d 0e0f 1011 1213
                        1415 1617 1819 1a1b 1c1d 1e1f 2021 2223
                        2425 2627 2829 2a2b 2c2d 2e2f 3031 3233
                        3435 3637
```

Of course, other ping programs are likely to build different packets, but the ones in this detect do seem odd. The payload is only 12 bytes in length. The identifier is always 0xbeef, which would make it difficult for the sending computer to know which process the replies are intended for, and the sequence number is always 0xdead, so there is no way to tell how many pings have succeeded without being dropped or duplicated. It is interesting to note that 0xdeadbeef is often used by programmers as a fill pattern.

The rest of the payload consists of 6 static bytes and 6 bytes that vary slightly. My initial fear that this is a Loki detect can be dismissed, since there is not enough dynamic information contained in the packets. However, it might be worth further investigation to determine the intent of this attack.

```
06:05:24.834566 195.61.132.6 > 128.210.67.55: icmp: echo request (DF)
                        4500 0028 7873 4000 f101 0614 c33d 8406
                        80d2 4337 0800 656a beef dead 3901 885d
                        0008 6f87 80d2 4337 0000 0000 0000
06:05:24.835882 195.61.132.6 > 128.210.67.74: icmp: echo request (DF)
                        4500 0028 7873 4000 f101 0601 c33d 8406
                        80d2 434a 0800 5928 beef dead 3901 885d
                        0008 7bb6 80d2 434a 0000 0000 0000
06:05:24.844607 195.61.132.6 > 128.210.67.34: icmp: echo request (DF)
                        4500 0028 7869 4000 f101 0633 c33d 8406
                        80d2 4322 0800 740a beef dead 3901 885d
                        0008 60fc 80d2 4322 0000 0000 0000
06:05:24.846490 195.61.132.6 > 128.210.67.186: icmp: echo request (DF)
                        4500 0028 7887 4000 f101 057d c33d 8406
                        80d2 43ba 0800 0f00 beef dead 3901 885d
                        0008 c56e 80d2 43ba 0000 0000 0000
06:05:24.848421 195.61.132.6 > 128.210.67.58: icmp: echo request (DF)
                        4500 0028 7873 4000 f101 0611 c33d 8406
                        80d2 433a 0800 6375 beef dead 3901 885d
                        0008 7179 80d2 433a 0000 0000 0000
06:06:14.435792 195.61.132.6 > 128.210.67.112: icmp: echo request (DF)
                        4500 0028 3a29 4000 f101 4425 c33d 8406
                        80d2 4370 0800 9f0a beef dead 3901 888f
                        0002 3582 80d2 4370 0000 0000 0000
06:06:14.436990 195.61.132.6 > 128.210.67.117: icmp: echo request (DF)
                        4500 0028 3a29 4000 f101 4420 c33d 8406
                        80d2 4375 0800 9729 beef dead 3901 888f
                        0002 3d5e 80d2 4375 0000 0000 0000
```

### 5. SYN-FIN Scan from Russia

The attacker is employing a SYN-FIN scan for DNS servers. While there have been many DNS exploits, it is also generally useful to the attacker to gain access a DNS server any way possible. The attacker can spoof hostnames to gain access to other systems or to hide the source of subsequent attacks.

The packets are crafted to have a fixed source port of 53, probably so as to look like legitimate DNS traffic. The sequence numbers are fixed for awhile and then change. Perhaps this technique is used to defeat certain intrusion detection systems.

SYN-FIN scans are often used for operating system fingerprinting, since different operating systems respond differently to this combination of TCP flags. This scan therefore provides the attacker with a network map complete with operating system information.

```
11:49:32.270034 aftn.civilavia.ru.53 > 192.168.67.11.53: SF 388839728:388839728(0) win
1028
11:49:32.317006 aftn.civilavia.ru.53 > 192.168.67.15.53: SF 388839728:388839728(0) win
1028
11:49:32.405861 aftn.civilavia.ru.53 > 192.168.67.20.53: SF 388839728:388839728(0) win
1028
11:49:32.446373 aftn.civilavia.ru.53 > 192.168.67.22.53: SF 388839728:388839728(0) win
1028
11:49:32.466360 aftn.civilavia.ru.53 > 192.168.67.23.53: SF 388839728:388839728(0) win
1028
11:49:32.553077 aftn.civilavia.ru.53 > 192.168.67.27.53: SF 77449084:77449084(0) win 1028
11:49:32.616477 aftn.civilavia.ru.53 > 192.168.67.30.53: SF 77449084:77449084(0) win 1028
```

```
11:49:32.631522 aftn.civilavia.ru.53 > 192.168.67.31.53: SF 77449084:77449084(0) win 1028
11:49:32.851941 aftn.civilavia.ru.53 > 192.168.67.42.53: SF 77449084:77449084(0) win 1028
11:49:32.924784 aftn.civilavia.ru.53 > 192.168.67.46.53: SF 77449084:77449084(0) win 1028
11:49:32.948404 aftn.civilavia.ru.53 > 192.168.67.47.53: SF 77449084:77449084(0) win 1028
11:49:32.965635 aftn.civilavia.ru.53 > 192.168.67.48.53: SF 77449084:77449084(0) win 1028
11:49:32.985815 aftn.civilavia.ru.53 > 192.168.67.49.53: SF 77449084:77449084(0) win 1028
11:49:33.010088 aftn.civilavia.ru.53 > 192.168.67.50.53: SF 77449084:77449084(0) win 1028
11:49:33.031309 aftn.civilavia.ru.53 > 192.168.67.51.53: SF 77449084:77449084(0) win 1028
11:49:33.057281 aftn.civilavia.ru.53 > 192.168.67.52.53: SF 77449084:77449084(0) win 1028
11:49:33.145561 aftn.civilavia.ru.53 > 192.168.67.56.53: SF 77449084:77449084(0) win 1028
11:49:33.221283 aftn.civilavia.ru.53 > 192.168.67.60.53: SF 77449084:77449084(0) win 1028
11:49:33.396310 aftn.civilavia.ru.53 > 192.168.67.69.53: SF 77449084:77449084(0) win 1028
11:49:33.438966 aftn.civilavia.ru.53 > 192.168.67.71.53: SF 77449084:77449084(0) win 1028
11:49:33.470395 aftn.civilavia.ru.53 > 192.168.67.72.53: SF 77449084:77449084(0) win 1028
11:49:33.548493 aftn.civilavia.ru.53 > 192.168.67.77.53: SF 1918378465:1918378465(0) win
1028
11:49:33.603628 aftn.civilavia.ru.53 > 192.168.67.80.53: SF 1918378465:1918378465(0) win
1028
11:49:33.666290 aftn.civilavia.ru.53 > 192.168.67.83.53: SF 1918378465:1918378465(0) win
1028
11:49:33.892460 aftn.civilavia.ru.53 > 192.168.67.94.53: SF 1918378465:1918378465(0) win
1028
11:49:33.912267 aftn.civilavia.ru.53 > 192.168.67.95.53: SF 1918378465:1918378465(0) win
1028
11:49:33.929811 aftn.civilavia.ru.53 > 192.168.67.96.53: SF 1918378465:1918378465(0) win
1028
11:49:34.137682 aftn.civilavia.ru.53 > 192.168.67.106.53: SF 1918378465:1918378465(0) win
1028
11:49:34.179864 aftn.civilavia.ru.53 > 192.168.67.108.53: SF 1918378465:1918378465(0) win
1028
11:49:34.195613 aftn.civilavia.ru.53 > 192.168.67.109.53: SF 1918378465:1918378465(0) win
1028
11:49:34.222383 aftn.civilavia.ru.53 > 192.168.67.110.53: SF 1918378465:1918378465(0) win
1028
11:49:34.258281 aftn.civilavia.ru.53 > 192.168.67.112.53: SF 1918378465:1918378465(0) win
1028
11:49:34.909417 aftn.civilavia.ru.53 > 192.168.67.144.53: SF 1605608465:1605608465(0) win
1028
11:49:34.957813 aftn.civilavia.ru.53 > 192.168.67.147.53: SF 1605608465:1605608465(0) win
1028
11:49:35.040802 aftn.civilavia.ru.53 > 192.168.67.151.53: SF 1605608465:1605608465(0) win
1028
11:49:35.077855 aftn.civilavia.ru.53 > 192.168.67.153.53: SF 1605608465:1605608465(0) win
1028
11:49:35.149269 aftn.civilavia.ru.53 > 192.168.67.157.53: SF 1605608465:1605608465(0) win
1028
11:49:35.463603 aftn.civilavia.ru.53 > 192.168.67.171.53: SF 1605608465:1605608465(0) win
1028
11:49:35.528087 aftn.civilavia.ru.53 > 192.168.67.176.53: SF 1605608465:1605608465(0) win
1028
11:49:35.569554 aftn.civilavia.ru.53 > 192.168.67.178.53: SF 1315007011:1315007011(0) win
1028
11:49:35.719499 aftn.civilavia.ru.53 > 192.168.67.185.53: SF 1315007011:1315007011(0) win
1028
11:49:35.740048 aftn.civilavia.ru.53 > 192.168.67.186.53: SF 1315007011:1315007011(0) win
1028
11:49:35.758728 aftn.civilavia.ru.53 > 192.168.67.187.53: SF 1315007011:1315007011(0) win
1028
11:49:35.800557 aftn.civilavia.ru.53 > 192.168.67.189.53: SF 1315007011:1315007011(0) win
1028
11:49:35.823816 aftn.civilavia.ru.53 > 192.168.67.190.53: SF 1315007011:1315007011(0) win
1028
11:49:36.082353 aftn.civilavia.ru.53 > 192.168.67.203.53: SF 1315007011:1315007011(0) win
1028
11:49:36.165522 aftn.civilavia.ru.53 > 192.168.67.207.53: SF 1315007011:1315007011(0) win
```

```
1028
11:49:36.540283 aftn.civilavia.ru.53 > 192.168.67.224.53: SF 1315007011:1315007011(0) win
1028
11:49:36.561779 aftn.civilavia.ru.53 > 192.168.67.227.53: SF 2078775555:2078775555(0) win
1028
11:49:36.581889 aftn.civilavia.ru.53 > 192.168.67.228.53: SF 2078775555:2078775555(0) win
1028
11:49:36.683241 aftn.civilavia.ru.53 > 192.168.67.233.53: SF 2078775555:2078775555(0) win
1028
11:49:36.858141 aftn.civilavia.ru.53 > 192.168.67.242.53: SF 2078775555:2078775555(0) win
1028
11:49:36.957646 aftn.civilavia.ru.53 > 192.168.67.246.53: SF 2078775555:2078775555(0) win
1028
11:49:36.986395 aftn.civilavia.ru.53 > 192.168.67.248.53: SF 2078775555:2078775555(0) win
1028
```

**6. Portmapper Scan**

This scan turned up one portmapper that was willing to talk, running on 192.168.67.186. We don't have full source, but we can assume the victim host replied to the attacker's SYN with a SYN|ACK because we see the attacker then sending a RST to tear down the connection. (The nmap program, for one, behaves this way.) Soon another connection comes from the attacker to that port and attempts a conversation. We can't see what our host responds with, but if we run "rpcinfo -p 192.168.67.168", we get

```
   program vers proto   port
    100000    2   tcp    111  portmapper
    100000    2   udp    111  portmapper
    300019    1   tcp   1023  amd
    300019    1   udp   1022  amd
```

The Berkeley automounter is the only other RPC service registered, but there is a popular exploit for the Linux version of this service. This system is running FreeBSD, but I know from experience that applying the Linux buffer overflow causes the FreeBSD amd process to crash.

This scan is apparently the work of an automated tool which uses crafted packets to keep the source port fixed at 53 and the sequence number at 100. The destination IPs are scanned in random order to avoid detection. When a willing portmapper is found, the tool automatically connects to it requesting a list of RPC services that host is running. During the time gaps, the tool could be scanning other networks or other hosts on this subnet whose traffic we can't see.

```
00:03:25.504478 155.230.132.202.53 > 192.168.67.77.111: S 100:100(0) win 512
00:03:25.517063 155.230.132.202.53 > 192.168.67.228.111: S 100:100(0) win 512
00:03:25.549767 155.230.132.202.53 > 192.168.67.105.111: S 100:100(0) win 512
00:03:26.419285 155.230.132.202.53 > 192.168.67.163.111: S 100:100(0) win 512
00:03:26.434590 155.230.132.202.53 > 192.168.67.67.111: S 100:100(0) win 512
00:03:26.445889 155.230.132.202.53 > 192.168.67.142.111: S 100:100(0) win 512
00:03:27.330879 155.230.132.202.53 > 192.168.67.43.111: S 100:100(0) win 512
00:03:28.216649 155.230.132.202.53 > 192.168.67.46.111: S 100:100(0) win 512
00:03:29.089743 155.230.132.202.53 > 192.168.67.193.111: S 100:100(0) win 512
00:03:33.556219 155.230.132.202.53 > 192.168.67.22.111: S 100:100(0) win 512
00:03:36.996104 155.230.132.202.53 > 192.168.67.153.111: S 100:100(0) win 512
00:03:39.929777 155.230.132.202.53 > 192.168.67.203.111: S 100:100(0) win 512
00:04:04.444661 155.230.132.202.53 > 192.168.67.90.111: S 100:100(0) win 512
00:04:04.594999 155.230.132.202.53 > 192.168.67.198.111: S 100:100(0) win 512
00:04:04.598190 155.230.132.202.53 > 192.168.67.189.111: S 100:100(0) win 512
00:04:04.621177 155.230.132.202.53 > 192.168.67.60.111: S 100:100(0) win 512
00:04:04.627424 155.230.132.202.53 > 192.168.67.30.111: S 100:100(0) win 512
00:04:04.628844 155.230.132.202.53 > 192.168.67.187.111: S 100:100(0) win 512
```

```
00:04:04.668890 155.230.132.202.53 > 192.168.67.144.111: S 100:100(0) win 512
00:04:04.707868 155.230.132.202.53 > 192.168.67.172.111: S 100:100(0) win 512
00:04:04.737010 155.230.132.202.53 > 192.168.67.186.111: S 100:100(0) win 512
00:04:04.745172 155.230.132.202.53 > 192.168.67.227.111: S 100:100(0) win 512
00:04:05.517258 155.230.132.202.53 > 192.168.67.69.111: S 100:100(0) win 512
00:04:05.551837 155.230.132.202.53 > 192.168.67.186.111: R 101:101(0) win 0
00:04:05.575252 155.230.132.202.53 > 192.168.67.186.111: R 101:101(0) win 512
00:04:05.576257 155.230.132.202.727 > 192.168.67.186.111: S 3104805337:3104805337(0) win
32120 <mss 1460,sackOK,timestamp 105232480 0,nop,wscale 0> (DF)
00:04:06.374642 155.230.132.202.727 > 192.168.67.186.111: . ack 863704318 win 32120 (DF)
00:04:06.389844 155.230.132.202.727 > 192.168.67.186.111: P 0:44(44) ack 1 win 32120 (DF)
00:04:06.488926 155.230.132.202.53 > 192.168.67.96.111: S 100:100(0) win 512
00:04:07.215703 155.230.132.202.727 > 192.168.67.186.111: . ack 113 win 32120 (DF)
00:04:07.217670 155.230.132.202.727 > 192.168.67.186.111: F 44:44(0) ack 113 win 32120
(DF)
00:04:08.041036 155.230.132.202.727 > 192.168.67.186.111: . ack 114 win 32120 (DF)
00:04:08.173779 155.230.132.202.53 > 192.168.67.141.111: S 100:100(0) win 512
00:04:15.277685 155.230.132.202.53 > 192.168.67.151.111: S 100:100(0) win 512
00:04:16.936564 155.230.132.202.53 > 192.168.67.115.111: S 100:100(0) win 512
00:05:18.060688 155.230.132.202.53 > 192.168.67.185.111: S 100:100(0) win 512
00:05:18.061502 155.230.132.202.53 > 192.168.67.170.111: S 100:100(0) win 512
00:05:18.062323 155.230.132.202.53 > 192.168.67.31.111: S 100:100(0) win 512
00:05:18.090703 155.230.132.202.53 > 192.168.67.205.111: S 100:100(0) win 512
00:05:18.097154 155.230.132.202.53 > 192.168.67.171.111: S 100:100(0) win 512
00:05:18.099025 155.230.132.202.53 > 192.168.67.80.111: S 100:100(0) win 512
00:05:18.136148 155.230.132.202.53 > 192.168.67.58.111: S 100:100(0) win 512
00:05:18.140772 155.230.132.202.53 > 192.168.67.63.111: S 100:100(0) win 512
00:05:18.184921 155.230.132.202.53 > 192.168.67.233.111: S 100:100(0) win 512
00:05:18.186223 155.230.132.202.53 > 192.168.67.20.111: S 100:100(0) win 512
00:05:18.189849 155.230.132.202.53 > 192.168.67.47.111: S 100:100(0) win 512
00:05:19.131122 155.230.132.202.53 > 192.168.67.72.111: S 100:100(0) win 512
00:05:19.220121 155.230.132.202.53 > 192.168.67.178.111: S 100:100(0) win 512
00:05:19.229419 155.230.132.202.53 > 192.168.67.73.111: S 100:100(0) win 512
00:05:19.236662 155.230.132.202.53 > 192.168.67.241.111: S 100:100(0) win 512
00:05:20.098758 155.230.132.202.53 > 192.168.67.54.111: S 100:100(0) win 512
00:05:20.712906 155.230.132.202.53 > 192.168.67.26.111: S 100:100(0) win 512
00:05:29.582411 155.230.132.202.53 > 192.168.67.62.111: S 100:100(0) win 512
00:05:54.642855 155.230.132.202.53 > 192.168.67.139.111: S 100:100(0) win 512
00:05:54.647221 155.230.132.202.53 > 192.168.67.152.111: S 100:100(0) win 512
00:05:54.758656 155.230.132.202.53 > 192.168.67.230.111: S 100:100(0) win 512
00:05:54.774796 155.230.132.202.53 > 192.168.67.248.111: S 100:100(0) win 512
00:05:54.785682 155.230.132.202.53 > 192.168.67.157.111: S 100:100(0) win 512
00:05:54.792156 155.230.132.202.53 > 192.168.67.176.111: S 100:100(0) win 512
00:05:54.843402 155.230.132.202.53 > 192.168.67.165.111: S 100:100(0) win 512
00:05:55.744916 155.230.132.202.53 > 192.168.67.174.111: S 100:100(0) win 512
00:05:55.748804 155.230.132.202.53 > 192.168.67.95.111: S 100:100(0) win 512
00:05:56.655347 155.230.132.202.53 > 192.168.67.190.111: S 100:100(0) win 512
00:05:57.178293 155.230.132.202.53 > 192.168.67.112.111: S 100:100(0) win 512
00:05:58.030170 155.230.132.202.53 > 192.168.67.37.111: S 100:100(0) win 512
00:06:01.507729 155.230.132.202.53 > 192.168.67.117.111: S 100:100(0) win 512
00:06:01.637703 155.230.132.202.53 > 192.168.67.242.111: S 100:100(0) win 512
00:06:02.467880 155.230.132.202.53 > 192.168.67.226.111: S 100:100(0) win 512
00:06:03.298547 155.230.132.202.53 > 192.168.67.94.111: S 100:100(0) win 512
00:06:09.488011 155.230.132.202.53 > 192.168.67.51.111: S 100:100(0) win 512
00:06:10.311714 155.230.132.202.53 > 192.168.67.132.111: S 100:100(0) win 512
00:06:11.124183 155.230.132.202.53 > 192.168.67.52.111: S 100:100(0) win 512
00:06:30.043994 155.230.132.202.53 > 192.168.67.122.111: S 100:100(0) win 512
00:06:30.051471 155.230.132.202.53 > 192.168.67.74.111: S 100:100(0) win 512
00:06:30.053452 155.230.132.202.53 > 192.168.67.224.111: S 100:100(0) win 512
00:06:30.054269 155.230.132.202.53 > 192.168.67.234.111: S 100:100(0) win 512
00:06:30.082541 155.230.132.202.53 > 192.168.67.15.111: S 100:100(0) win 512
00:06:30.092512 155.230.132.202.53 > 192.168.67.56.111: S 100:100(0) win 512
00:06:30.137119 155.230.132.202.53 > 192.168.67.251.111: S 100:100(0) win 512
00:06:30.142732 155.230.132.202.53 > 192.168.67.246.111: S 100:100(0) win 512
00:06:30.146896 155.230.132.202.53 > 192.168.67.23.111: S 100:100(0) win 512
00:06:30.211147 155.230.132.202.53 > 192.168.67.27.111: S 100:100(0) win 512
```

```
00:06:30.216509 155.230.132.202.53 > 192.168.67.130.111: S 100:100(0) win 512
00:06:30.222010 155.230.132.202.53 > 192.168.67.83.111: S 100:100(0) win 512
00:06:31.147225 155.230.132.202.53 > 192.168.67.11.111: S 100:100(0) win 512
00:06:32.032886 155.230.132.202.53 > 192.168.67.145.111: S 100:100(0) win 512
```

**7. Scan for rexec**

Here is evidence of a quick scan from the University of Kent at Canterbury. The attacker is trying to connect to rexec, an RPC service with a very weak security model. The source ports and sequence numbers change as would be expected without crafting packets. The source ports are high, indicating the source machine is busy, possibly scanning other machines.

```
06:31:47.363730 sapir.ukc.ac.uk.55492 > 192.168.67.94.512: S 2054957413:2054957413(0) win
8760 <mss 1460> (DF)
06:31:47.369120 sapir.ukc.ac.uk.55491 > 192.168.67.83.512: S 2054857137:2054857137(0) win
8760 <mss 1460> (DF)
06:31:47.372012 sapir.ukc.ac.uk.55499 > 192.168.67.242.512: S 2055560859:2055560859(0)
win 8760 <mss 1460> (DF)
06:31:47.374043 sapir.ukc.ac.uk.55498 > 192.168.67.241.512: S 2055472529:2055472529(0)
win 8760 <mss 1460> (DF)
```

**8. Strange Local UDP Traffic**

Both the source and destination hosts for this detect are inside my organization. The port is not linked to any known trojans. Maybe someone has installed an altered trojan, or maybe we're just seeing traffic for some home-grown service.

When dumped, we see the payload contains the string "HiCMHiCM", which looks human-invented. It could be a magic number or password used to access a trojan, but it could also be a password for a poorly-designed local service.

```
13:56:59.105298 172.16.11.10.1033 > 172.21.11.81.38293: udp 16
                        4500 002c 0fbc 0000 7c11 fcc0 95a5 0b0a
                        8644 0b51 0409 9595 0018 1a44 020a 0020
                        4869 434d 4869 434d 0000 0000 0000
14:01:06.369629 172.16.11.15.1033 > 172.21.11.81.38293: udp 16
                        4500 002c 4f2c 0000 7c11 bd4b 95a5 0b0f
                        8644 0b51 0409 9595 0018 1a3f 020a 0020
                        4869 434d 4869 434d 0000 0000 0000
14:13:38.899322 172.16.11.10.1033 > 172.21.11.81.38293: udp 16
                        4500 002c 9362 0000 7c11 791a 95a5 0b0a
                        8644 0b51 0409 9595 0018 1a44 020a 0020
                        4869 434d 4869 434d 0000 0000 0000
15:26:38.810199 172.30.208.25.1029 > 172.21.11.83.38293: udp 16
                        4500 002c e47d 0000 7c11 7743 814f d019
                        8644 0b53 0405 9595 0018 698c 020a 0020
                        4869 434d 4869 434d 0000 0000 0000
15:28:12.872712 172.30.208.25.1029 > 172.21.11.83.38293: udp 16
                        4500 002c bdce 0000 7c11 0cd4 814f 6138
                        8644 0b53 0405 9595 0018 d86d 020a 0020
                        4869 434d 4869 434d 0000 0000 0000
15:32:05.437463 172.16.11.10.1033 > 172.21.11.83.38293: udp 16
                        4500 002c 60e9 0000 7c11 ab91 95a5 0b0a
                        8644 0b53 0409 9595 0018 1a42 020a 0020
                        4869 434d 4869 434d 0000 0000 0000
15:33:26.332026 172.21.75.77.1032 > 172.21.11.84.38293: udp 16
                        4500 002c 50a8 0000 7e11 88ef 8644 4b4d
                        8644 0b54 0408 9595 0018 e95f 020a 0020
                        4869 434d 4869 434d 0000 0000 0000
```

**9. Ping and SNMP Attempts Against a Router**

**This detect could just indicate an HP OpenView process gone awry. On the other hand, it could be an attacker who has identified the destination host as a router because its IP has a final octet of 1.**

**Whatever it is, it's definitely automated, since the echo requests come in at regular intervals of 2.5 seconds. After a while an SNMP GetRequest comes in and retries every 18 seconds with a community string of "public", as revealed by inspecting the payload.**

**It is important to investigate further and determine whether this detect indicates HP OpenView or someone trying to control our router.**

```
13:51:39.205440 162.1.131.21 > 172.16.240.1: icmp: echo request (DF)
13:51:39.205473 172.16.240.1 > 162.1.131.21: icmp: echo reply (DF)
13:54:09.031881 162.1.131.21 > 172.16.240.1: icmp: echo request (DF)
13:54:09.031917 172.16.240.1 > 162.1.131.21: icmp: echo reply (DF)
13:56:08.080698 162.1.131.21.40393 > 172.16.240.1.snmp: GetRequest(27)
system.sysObjectID.0 (DF)
13:56:26.084402 162.1.131.21.40393 > 172.16.240.1.snmp: GetRequest(27)
system.sysObjectID.0 (DF)
13:56:39.224997 162.1.131.21 > 172.16.240.1: icmp: echo request (DF)
13:56:39.225042 172.16.240.1 > 162.1.131.21: icmp: echo reply (DF)
13:56:44.079425 162.1.131.21.40393 > 172.16.240.1.snmp: GetRequest(27)
system.sysObjectID.0 (DF)
```

**10. TELNET Attempts**

**Though the packets don't appear crafted because of the changing source port numbers and sequence numbers, the close timestamps indicate an automated scan. Connection attempts are retried for the second targeted host, 172.21.11.80, because a firewall is dropping the SYN packets.**

**It is not unreasonable to assume the attacker tried all the IPs between 172.21.11.59 and 172.21.11.80, since the source port numbers jump the same interval.**

**The host mail.ectiplus.com has a webserver running on it with the default root page installed by Debian Linux. The [|tcp] notation would otherwise be strange--a SYN that is bigger than tcpdump's default snarf length, but Linux tends to load up its TCP packets with many options, so it is not too unusual.**

```
23:01:59.828583 mail.ectiplus.com.2214 > 172.21.11.59.telnet: S 681608294:681608294(0)
win 32120 <mss 1460,sackOK,timestamp 139197199[|tcp]> (DF)
23:01:59.967934 mail.ectiplus.com.2235 > 172.21.11.80.telnet: S 674280704:674280704(0)
win 32120 <mss 1460,sackOK,timestamp 139197199[|tcp]> (DF)
23:02:02.429860 mail.ectiplus.com.2235 > 172.21.11.80.telnet: S 674280704:674280704(0)
win 32120 <mss 1460,sackOK,timestamp 139197499[|tcp]> (DF)
23:02:08.428368 mail.ectiplus.com.2235 > 172.21.11.80.telnet: S 674280704:674280704(0)
win 32120 <mss 1460,sackOK,timestamp 139198099[|tcp]> (DF)
```

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 |