Global Information Assurance Certification Paper

*** Northcutt, Good process, it will serve you well as you continue to practice the craft. Number one is one of those common errors I tell students not to make! Higher probability is that is a traceroute/traceroute like. Three, five and ten might be worth a second look as well. 78 ***

These detects are from the GIAC web page and are for Level 2 Certification
GCIA Candidate: Geoffrey Catron

Detect One

Summary:	This is a Snort detect of a fast port scan.
Source Host:	Single host, 208.185.54.22 AboveNet Communications, San Jose, CA (noc@above.net)
Target Host:	Single target, a.b.c.34
Scan Target:	High UDP Ports
Scan Increment:	Single port positive
Speed:	Fast
Proto:	UDP
Active Targeting:	Yes
Intent:	Determine service ports available for exploit
Technique:	Fast scan of high udp ports
History:	Unknown
Existence:	Unknown
Analysis:	This is a scan of a group of high udp ports used to search for ports that may be open and susceptible to attack. Quick and dirty, the attacker is in and out in just a second or so.

```
Apr 3 08:49:22 dns1 snort[4415]: spp_portscan:
PORTSCAN DETECTED from 208.185.54.22
Apr 3 08:49:28 dns1 snort[4415]: spp_portscan: portscan status
from 208.185.54.22: 14 connections across 1 hosts: TCP(0), UDP(14)
Apr 3 08:49:34 dns1 snort[4415]: spp_portscan: End of portscan
from 208.185.54.22
Apr 3 08:49:22 208.185.54.22:33161 -> a.b.c.34:33512 UDP
Apr 3 08:49:22 208.185.54.22:33161 -> a.b.c.34:33513 UDP
Apr 3 08:49:22 208.185.54.22:33161 -> a.b.c.34:33514 UDP
Apr 3 08:49:22 208.185.54.22:33161 -> a.b.c.34:33515 UDP
Apr 3 08:49:22 208.185.54.22:33161 -> a.b.c.34:33516 UDP
Apr 3 08:49:22 208.185.54.22:33161 -> a.b.c.34:33517 UDP
Apr 3 08:49:22 208.185.54.22:33161 -> a.b.c.34:33518 UDP
Apr 3 08:49:22 208.185.54.22:33161 -> a.b.c.34:33519 UDP
Apr 3 08:49:22 208.185.54.22:33161 -> a.b.c.34:33520 UDP
Apr 3 08:49:22 208.185.54.22:33161 -> a.b.c.34:33521 UDP
Apr 3 08:49:22 208.185.54.22:33161 -> a.b.c.34:33522 UDP
Apr 3 08:49:22 208.185.54.22:33161 -> a.b.c.34:33523 UDP
Apr 3 08:49:22 208.185.54.22:33161 -> a.b.c.34:33524 UDP
Apr 3 08:49:22 208.185.54.22:33161 -> a.b.c.34:33525 UDP
```

Detect Two

Summary:	A scan of known Ring 0 ports.
Source Host:	Single host, 1Cust219.tnt1.bryan.oh.da.uu.net UUnet Technologies, Fairfax, VA (help@uunet)
Target Host:	Single host, @.home.com
Scan Target:	Web and Proxy Ports (Ring 0 ports - 8080, 80, 3128) 8050, 8002
Scan Increment:	Repeating w/ variation
Speed:	Fast
Proto:	TCP/UDP
Active Targeting:	Yes
Intent:	Determine ports available for exploit / Ring 0
Technique:	Scan of ports 8080, 80, 3128, 8050, 8002
History:	Unknown
Existence:	Unknown
Analysis:	This is a scan of known Ring 0 (8080, 80, 3128) ports to determine if the trojan is available for use on the target system. This is a fast scan, over in a couple of seconds.

```
16:55:35.440651 1Cust219.tnt1.bryan.oh.da.uu.net.1865 > @.home.com.8080:
S 12492586:12492586(0) win 8192 (DF)
16:55:35.465692 1Cust219.tnt1.bryan.oh.da.uu.net.1866 > @.home.com.www:
S 12492589:12492589(0) win 8192 (DF)
16:55:35.484070 1Cust219.tnt1.bryan.oh.da.uu.net.1868 > @.home.com.3128:
S 12492595:12492595(0) win 8192 (DF)
16:55:35.484222 1Cust219.tnt1.bryan.oh.da.uu.net.1870 > @.home.com.8050:
S 12492601:12492601(0) win 8192 (DF)
16:55:35.484367 1Cust219.tnt1.bryan.oh.da.uu.net.1869 > @.home.com.8002:
S 12492598:12492598(0) win 8192 (DF)
16:55:36.664311 1Cust219.tnt1.bryan.oh.da.uu.net.1865 > @.home.com.8080:
S 12492586:12492586(0) win 8192 (DF)
16:55:36.666792 1Cust219.tnt1.bryan.oh.da.uu.net.1868 > @.home.com.3128:
S 12492595:12492595(0) win 8192 (DF)
16:55:36.706460 1Cust219.tnt1.bryan.oh.da.uu.net.1869 > @.home.com.8002:
S 12492598:12492598(0) win 8192 (DF)
16:55:36.758762 1Cust219.tnt1.bryan.oh.da.uu.net.1870 > @.home.com.8050:
S 12492601:12492601(0) win 8192 (DF)
16:55:37.625224 1Cust219.tnt1.bryan.oh.da.uu.net.1865 > @.home.com.8080:
S 12492586:12492586(0) win 8192 (DF)
16:55:37.939332 1Cust219.tnt1.bryan.oh.da.uu.net.1868 > @.home.com.3128:
S 12492595:12492595(0) win 8192 (DF)
16:55:37.949391 1Cust219.tnt1.bryan.oh.da.uu.net.1869 > @.home.com.8002:
S 12492598:12492598(0) win 8192 (DF)
16:55:37.985345 1Cust219.tnt1.bryan.oh.da.uu.net.1870 > @.home.com.8050:
S 12492601:12492601(0) win 8192 (DF)
16:55:38.396403 1Cust219.tnt1.bryan.oh.da.uu.net.1866 > @.home.com.www:
S 12492589:12492589(0) win 8192 (DF)
16:55:38.786750 1Cust219.tnt1.bryan.oh.da.uu.net.1865 > @.home.com.8080:
S 12492586:12492586(0) win 8192 (DF)
```

Detect 3

Summary:	Information recon through crafted anomalous TCP flags
Source Host:	Single host, 24.113.9.242 Rogers@Home BC
Target Host:	Multiple hosts
Scan Target:	Various ports
Scan Increment:	Same port at least twice, different flags set
Speed:	Moderate
Proto:	TCP
Active Targeting:	Yes
Intent:	Recon - determine OS by response characteristics
Technique:	Anomalous TCP flags in crafted packets, scan for results from different sets of flag combinations
History:	Unknown
Existence:	Unknown
Analysis:	This is a recon scan which could provide the attacker with information about the target operating systems by analyzing their responses to various invalid TCP flag combinations.

```
12/31-00:04:02.270745 24.113.9.242:6699 -> 192.0.201.78:1149
TCP TTL:110 TOS:0x0 ID:14470 DF
SFR*A*21 Seq: 0x1D4 Ack: 0x2C850531 Win: 0x5010
TCP Options => EOL EOL WS: 151 Opt 153 (40): C3F2 5971 43E7 AB00 0000 0000 0000
0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000

12/31-00:05:24.578272 24.113.9.242:0 -> 192.0.201.78:6699
TCP TTL:111 TOS:0x0 ID:53909 DF
SFR*A*21 Seq: 0x47D01FA Ack: 0xD4850531 Win: 0x5010
TCP Options => EOL EOL Opt 54 (8): 0099 DE50 C103 Opt 46 (40): B9C8 0000 0000
0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000

12/31-00:09:59.342618 24.113.9.242:0 -> 192.0.201.78:6699
TCP TTL:110 TOS:0x0 ID:17345 DF
SFRP**2 Seq: 0x48201D7 Ack: 0xD4330536 Win: 0x5010
TCP Options => EOL EOL Opt 215 (40): B0C2 0B73 F919 C9CE F958 0000 0000 0000
0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000

12/31-00:10:15.367874 24.113.9.242:6699 -> 192.0.201.78:1154
TCP TTL:110 TOS:0x0 ID:10693 DF
SFRP**2 Seq: 0x1DBDC33 Ack: 0x536 Win: 0x5010
TCP Options => EOL EOL Opt 255 (40): B064 8B00 067E 6957 6B38 0000 0000 0000
0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000

12/31-00:10:25.472756 24.113.9.242:6699 -> 192.0.201.78:1154
TCP TTL:111 TOS:0x0 ID:35271 DF
SFRP**2 Seq: 0x1DEB1E7 Ack: 0x536 Win: 0x5018
TCP Options => EOL EOL Opt 173 (40): B4EE 3B29 B285 8A93 3068 0000 0000 0000
0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
```

Detect 4

Summary:	Search to locate DNS servers for exploit
Source Host:	Single host, 194.133.144.6 Comm 2000, Milan, Italy (ivan@comm2000.it)
Target Host:	Multiple hosts, multiple subnets all belonging to same .EDU
Scan Target:	DNS, port 53
Scan Increment:	Single increment pattern, up or down
Speed:	Fast
Proto:	TCP
Active Targeting:	Yes
Intent:	Recon - determine active DNS servers for exploit
Technique:	Incremental scan of hosts on several subnets of port 53 (DNS)
History:	Unknown
Existence:	Unknown
Analysis:	This is a scan of several USC subnets looking for DNS servers by a host in Italy. The first six packets are all SYNs, but the last two are Resets. Attacker may have found two active hosts. Note that attacker is scanning lower numbered hosts in each subnet. Many times resource servers are placed in the lower addresses of a subnet. The source port of 65535 is interesting as the new RC trojan is known to use this port. Perhaps this is a scan being performed remotely by an innocent victim.

```
13:40:26.850467 194.133.144.6.65535 > 192.168.72.5.53: S 253493248:253493248(0)
win 512
13:40:26.856988 194.133.144.6.65535 > 192.168.72.6.53: S 253493248:253493248(0)
win 512
13:40:26.887870 194.133.144.6.65535 > 192.168.72.8.53: S 253493248:253493248(0)
win 512
...
13:51:46.167005 194.133.144.6.65535 > 192.168.247.4.53: S 253493248:253493248(0)
win 512
13:51:46.258822 194.133.144.6.65535 > 192.168.247.5.53: S 253493248:253493248(0)
win 512
13:51:46.264693 194.133.144.6.65535 > 192.168.247.6.53: S 253493248:253493248(0)
win 512
...
13:51:46.801018 194.133.144.6.65535 > 192.168.247.78.53: R
253493249:253493249(0) win 0
13:52:32.005928 194.133.144.6.65535 > 192.168.247.77.53: R
253493249:253493249(0) win 0
```

Detect 5

Summary:	Detects of several hosts searching for Back Orifice, SubSeven, and Secure Shell ports over a several hour period.
Source Host:	Multiple hosts, multiple subnets @Home Network (24.8.162.206,24.3.21.225), UUNet (63.20.110.44), SplitRock Services (209.252.119.188)
Target Host:	Single host (from sensor's point of view, anyway), 24.3.21.199
Scan Target:	Back Orifice, SubSeven, Secure Shell ports
Scan Increment:	Various
Speed:	Slow
Proto:	TCP/UDP
Active Targeting:	Yes
Intent:	Locate hosts with installed Trojans and/or secure shell ports open for exploit
Technique:	SYN or Reset Scan directed at known trojan ports
History:	Unknown
Existence:	Unknown
Analysis:	These detects occurred over a 9 hour period and are evidence of scans for Back Orifice (31337), SubSeven (37374), and Secure Shell (22) ports. They appear to be unrelated other than the fact that they were all targeted at the same host.

```
Jan 3 01:09:33 cc1014244-a kernel: securityalert: tcp if=ef0 from
24.8.162.206:2832 to 24.3.21.199 on unserved port 27374
Jan 3 07:47:56 cc1014244-a kernel: securityalert: udp if=ef0 from
63.20.110.44:1289 to 24.3.21.199 on unserved port 31337
Jan 3 08:31:42 cc1014244-a kernel: securityalert: tcp if=ef0 from
209.252.119.188:4144 to 24.3.21.199 on unserved port 1243
Jan 3 08:32:02 cc1014244-a kernel: securityalert: tcp if=ef0 from
209.252.119.188:4398 to 24.3.21.199 on unserved port 27374
Jan 3 09:48:35 cc1014244-a kernel: securityalert: udp if=ef0 from
24.3.21.225:1174 to 24.3.21.199 on unserved port 22
Jan 3 09:49:52 cc1014244-a kernel: securityalert: tcp if=ef0 from
209.86.206.244:4906 to 24.3.21.199 on unserved port 31337
Jan 3 09:54:41 cc1014244-a kernel: securityalert: udp if=ef0 from
24.3.21.225:1190 to 24.3.21.199 on unserved port 22
Jan 3 10:26:27 cc1014244-a kernel: securityalert: udp if=ef0 from
24.3.21.225:1224 to 24.3.21.199 on unserved port 22
Jan 3 10:27:37 cc1014244-a kernel: securityalert: udp if=ef0 from
24.3.21.225:1228 to 24.3.21.199 on unserved port 5632
Jan 3 10:27:37 cc1014244-a kernel: securityalert: udp if=ef0 from
24.3.21.225:1228 to 24.3.21.199 on unserved port 22
Jan 3 10:29:57 cc1014244-a kernel: securityalert: udp if=ef0 from
24.3.21.225:1233 to 24.3.21.199 on unserved port 22
```

Detect Six

Summary: SYN/FIN scan of FTP and POP3 ports

Source Host: Single host, gojome.caramelpot.co.jp
(note port 0, identical crafted packets)
Caramelpot, Inc, Fukuoka, Japan (info@ddi.ad.jp)

Target Host: Single host, hostx
Scan Target: FTP and POP3 ports
Scan Increment: 2 identical packets POP3, 2 identical packets FTP
Speed: Moderately Fast
Proto: TCP
Active Targeting: Yes
Intent: Recon - Determine Active FTP Control and POP3 ports for exploit, evade some IDS and firewalls, locate linux hosts
Technique: Crafted packet SYN/FIN scan of ports 110 and 21
History: Unknown
Existence: Unknown

Analysis: This crafted SYN/FIN scan packets to the FTP and POP3 ports can serve several purposes, including circumventing some IDS systems or firewalls which check for SYN only connection attempts, identifying linux machines, and locating hosts with active FTP and POP3 services. Note source port 0 and identical crafted packets.

```
12:04:04.195852 gojome.caramelpot.co.jp.0 > hostx.110: SF
1093402624:1093402624(0) win 512
12:04:04.195852 gojome.caramelpot.co.jp.0 > hostx.110: SF
1093402624:1093402624(0) win 512
12:04:15.035216 gojome.caramelpot.co.jp.0 > hostx.21: SF
1110179840:1110179840(0) win 512
12:04:15.035216 gojome.caramelpot.co.jp.0 > hostx.21: SF
1110179840:1110179840(0) win 512
```

Detect Seven

Summary:	Various scans for SunRPC, Deep Throat, FTP, SubSeven, Back Orifice, Hack 'a' Tack, SMTP ports
Source Host:	Multiple hosts, Multiple subnets UCLA Campus Network Svcs (164.67.204.8), UUNet(63.20.34.254, 63.23.231.160), Bowling Green State Univ (129.1.9.146), Level 3 Communications (209.244.70.162, 209.245.41.65, 209.245.41.65), Alphalink Australia (203.62.183.163), Golden Triangle Online, Ontario, Canada (209.183.132.79, 209.183.132.79), Bell Nexxia Canada (216.209.56.193, 216.209.52.62), Rogers@home (24.114.172.74, 24.112.173.121, 24.112.33.11), ANS Co+re Systems (152.166.212.218), Internet Direct Canada (209.161.228.232) Internet Gateway Corp (209.52.160.154)
Target Host:	Single host
Scan Target:	Sun RPC ports, Trojan ports, Telnet and SMTP ports
Scan Increment:	Various over 2 days
Speed:	Slow
Proto:	TCP/UDP
Active Targeting:	Yes
Intent:	Locate trojan and/or Telnet/SMTP ports for exploit
Technique:	Scans to known trojan ports (2140, 27374, 31337, 1243, 31789) to a single host over a couple of days Also scans to ports 21 (ftp) and 25 (SMTP) and 111 (Sun RPC)
History:	Unknown
Existence:	Unknown
Analysis:	This is a great bunch of packets! Scans for Deep Throat, SubSeven, Back Orifice, Hack 'a' Tack, as well as SunRPC, FTP and SMTP ports coming from what appears to be all over North America. If we knew the target subnet we could do some figuring on TTL to set a baseline for possible spoofing. Tim

```
Jan 4 01:42:28 input REJECT eth1 PROTO=TCP
164.67.204.8:39555 <target ip>:111 L=44 S=0x00 I=21806 F=0x0000 T=41 SYN (#13)
Jan 4 01:53:51 input REJECT eth1 PROTO=UDP 63.20.34.254:60000 <target ip>
:2140 L=30 S=0x00 I=15066 F=0x0000 T=111 (#16)
Jan 4 02:09:19 input REJECT eth1 PROTO=TCP 129.1.9.146:5720 <target ip>
:111 L=44 S=0x00 I=1859 F=0x0000 T=40 SYN (#13)
Jan 4 04:02:59 input REJECT eth1 PROTO=UDP 63.20.34.254:60000 <target ip>
:2140 L=30 S=0x00 I=5360 F=0x0000 T=111 (#16)
Jan 4 05:04:56 input REJECT eth1 PROTO=TCP 209.244.70.162:4625 <target ip>
:23 L=48 S=0x00 I=54330 F=0x4000 T=111 SYN (#13)
Jan 4 05:23:19 input REJECT eth1 PROTO=TCP 209.245.41.65:1438 <target ip>
:23 L=48 S=0x00 I=42865 F=0x4000 T=111 SYN (#13)
Jan 4 14:54:45 input REJECT eth1 PROTO=UDP 206.186.146.18:60000 <target ip>
:2140 L=30 S=0x00 I=51090 F=0x0000 T=20 (#16)
```

```
Jan 4 15:55:07 input REJECT eth1 PROTO=UDP 203.62.183.163:60000 <target ip>
:2140 L=30 S=0x00 I=11108 F=0x0000 T=105 (#16)
Jan 4 16:03:38 input REJECT eth1 PROTO=TCP 209.183.132.79:4810 <target ip>
:27374 L=48 S=0x00 I=65022 F=0x4000 T=115 SYN (#13)
Jan 4 16:39:48 input REJECT eth1 PROTO=TCP 216.209.56.193:4799 <target ip>
:20 L=48 S=0x00 I=55189 F=0x0000 T=117 SYN (#13)
Jan 4 18:04:37 input REJECT eth1 PROTO=TCP 216.209.52.62:2286 <target ip>
:21 L=48 S=0x00 I=37406 F=0x0000 T=117 SYN (#13)
Jan 4 20:59:40 input REJECT eth1 PROTO=UDP 24.114.172.74:3764 <target ip>
:31337 L=47 S=0x00 I=65460 F=0x0000 T=123 (#16)
Jan 5 01:48:26 input REJECT eth1 PROTO=UDP 24.141.96.196:60000 <target ip>
:2140 L=30 S=0x00 I=12200 F=0x0000 T=117 (#16)
Jan 5 02:56:39 input REJECT eth1 PROTO=TCP 152.166.212.218:2102 <target ip>
:1243 L=48 S=0x00 I=38494 F=0x4000 T=108 SYN (#13)
Jan 5 05:19:28 input REJECT eth1 PROTO=TCP 24.112.173.121:1491 <target ip>
:27374 L=48 S=0x00 I=22815 F=0x4000 T=124 SYN (#13)
Jan 5 12:59:21 input REJECT eth1 PROTO=TCP 209.161.228.232:2579 <target ip>
:25 L=48 S=0x00 I=50954 F=0x4000 T=119 SYN (#13)
Jan 5 14:07:19 input REJECT eth1 PROTO=TCP 24.112.33.11:3170 <target ip>
:27374 L=48 S=0x00 I=16319 F=0x0000 T=128 SYN (#13)
Jan 5 18:42:32 input REJECT eth1 PROTO=TCP 209.52.160.154:2915 <target ip>
:1243 L=48 S=0x00 I=57182 F=0x4000 T=106 SYN (#13)
Jan 5 23:42:04 input REJECT eth1 PROTO=UDP 63.23.231.160:31790 <target ip>
:31789 L=29 S=0x00 I=24470 F=0x0000 T=110 (#16)
```

Detect 8

Summary:	Probe of host for proxy – Ring 0 server
Source Hosts:	208.146.45.12 (Cable and Wireless) 161.184.149.29 (Edmonton Telephones, Canada)
Target Host:	Single
Scan Target:	Ring 0 proxy ports (8080, 3128) + 81
Scan Increment:	N/A
Speed:	Fast
Proto:	TCP
Active Targeting:	Yes
Intent:	Locate Ring 0 proxy servers
Technique:	Scan Ring 0 service ports 8080, 3128, 80
History:	Unknown
Existence:	Unknown
Analysis:	Packets one, two and four are from the same host and are searching for Ring 0 services on the target. Packet three, from a different host appears to be an unrelated (except for its untimely arrival) attempt to locate www services for unknown reasons.

```
Jan 6 21:23:23 input REJECT eth1 PROTO=TCP 208.146.45.12:1645 <victim ip>:8080
L=44 S=0x00 I=40575 F=0x4000 T=46 SYN (#13)
Jan 6 21:23:28 input REJECT eth1 PROTO=TCP 208.146.45.12:1655 <victim ip>:3128
L=44
S=0x00 I=41428 F=0x4000 T=46 SYN (#13)
Jan 6 21:23:38 input REJECT eth1 PROTO=TCP 161.184.149.29:2946 <victim ip>:80
L=44
S=0x10 I=41780 F=0x4000 T=106 SYN (#13)
Jan 6 21:23:45 input REJECT eth1 PROTO=TCP 208.146.45.12:1672 <victim ip>:81
L=44
S=0x00 I=43553 F=0x4000 T=46 SYN (#13)
```

Detect 9

Summary:	Scan of multiple hosts for proxy – Ring 0 server, Socks, WinHole
Source Hosts:	Single Host, 172.20.20.136 University of Southern California (iana@iana.org)
Target Hosts:	Multiple hosts, multiple ports
Scan Target:	Ring 0 ports (8080, 3128), Socks/WinHole port (1080)
Scan Increment:	Interleaved, three probes per host
Speed:	Fast
Proto:	TCP
Active Targeting:	Yes
Intent:	Locate Ring 0/Socks/and/or WinHole servers
Technique:	Incremental interleaved scan of Ring 0 and WinHole ports on target hosts beginning with host 1 on the subnet
History:	Unknown
Existence:	Unknown
Analysis:	This is yet another fast scanning search of multiple hosts on a subnet by an attacker looking for Ring 0 / socks proxy / WinHole servers to exploit. The attacker will never know the results of his scan as the incoming packets were dropped.

```
14:28:15 drop 172.20.20.136  192.168.16.1      tcp  3128
14:28:15 drop 172.20.20.136  192.168.16.1      tcp  http-proxy
14:28:15 drop 172.20.20.136  192.168.16.2      tcp  http-proxy
14:28:15 drop 172.20.20.136  192.168.16.1      tcp  1080
14:28:15 drop 172.20.20.136  192.168.16.3      tcp  3128
14:28:15 drop 172.20.20.136  192.168.16.2      tcp  3128
14:28:15 drop 172.20.20.136  192.168.16.2      tcp  1080
14:28:15 drop 172.20.20.136  192.168.16.3      tcp  http-proxy
14:28:15 drop 172.20.20.136  192.168.16.3      tcp  1080
14:28:15 drop 172.20.20.136  192.168.16.4      tcp  3128
```

Detect 10

Summary: Evidence of spoofed addresses possibly used for mapping

Source Hosts: Unknown - spoofed

Target Hosts: 192.168.190.226
Scan Target: N/A
Scan Increment: N/A
Speed: Slow
Proto: ICMP
Active Targeting: Yes
Intent: Hide identity of attacker
Technique: Spoof source addresses for ping sweep or other mapping activity
History: Unknown
Existence: Unknown

Analysis: These packets are the result of an attacker spoofing unused addresses, possibly for mapping purposes. The tip-off is that we are receiving ttl exceeded messages for traffic that did not originate with us. Therefore, someone has used our addresses as the "source" of their packets.

```
00:16:12.795227 192.68.190.226 > 172.16.119.11: icmp: time exceeded in-transit
[tos 0xc0]
00:14:16.481616 192.68.190.226 > 172.16.0.53: icmp: time exceeded in-transit
[tos 0xc0]
00:16:12.795227 192.68.190.226 > 172.16.119.11: icmp: time exceeded in-transit
[tos 0xc0]
00:07:24.020358 a.sanitised.net > 172.16.163.35: icmp: time exceeded in-transit
00:07:24.020358 a.sanitised.net > 172.16.163.35: icmp: time exceeded in-transit
00:00:46.446119 b.sanitised.net > 172.16.181.107: icmp: time exceeded in-transit
[tos 0xc0]
00:00:46.446119 b.sanitised.net > 172.16.181.107: icmp: time exceeded in-transit
[tos 0xc0]
```

Last Updated: May 30th, 2017

Upcoming Training

Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANSFIRE 2017 - SEC503: Intrusion Detection In-Depth	Washington, DC	Jul 24, 2017 - Jul 29, 2017	vLive
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
SANS vLive - SEC503: Intrusion Detection In-Depth	SEC503 - 201709,	Sep 11, 2017 - Oct 18, 2017	vLive
Baltimore September 2017 - SEC503: Intrusion Detection In-Depth	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	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 Boston SEC503	Boston, MA	Oct 09, 2017 - Oct 14, 2017	Community SANS
Community SANS Ottawa SEC503	Ottawa, ON	Oct 16, 2017 - Oct 21, 2017	Community SANS
SANS Seattle 2017	Seattle, WA	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS San Diego 2017	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	Live Event
San Diego Fall 2017 - SEC503: Intrusion Detection In-Depth	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	vLive
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 OnDemand	Online	Anytime	Self Paced
SANS SelfStudy	Books & MP3s Only	Anytime	Self Paced