



Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permitted without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Intrusion Detection In-Depth (Security 503)"
at <http://www.giac.org/registration/gcia>

*** Northcutt, OK, solid use of an analysis process. Might be nice to show which trojans in one. 4 could be linuxconf! Named in 5, 7 could be the demonnet pattern. If your source is not your own ports might want to give source. Little research or correlation wouldn't hurt. 72 *

Jerry Fazio - IDIC-1 Practical

Detect #1: trojan scan

```
Mar 20 17:31:04.613318 216.234.161.19,3661 -> 10.0.2.29,113 PR tcp len 20 44 -S
Mar 20 17:31:07.220407 216.234.161.19,3661 -> 10.0.2.29,113 PR tcp len 20 44 -S
Mar 20 17:31:25.162906 216.234.161.19,3661 -> 10.0.2.29,113 PR tcp len 20 44 -S
Mar 20 17:31:35.181965 216.234.161.19,3871 -> 10.0.2.29,1080 PR tcp len 20 44 -S
Mar 20 17:31:37.659888 216.234.161.19,3871 -> 10.0.2.29,1080 PR tcp len 20 44 -S
Mar 20 17:31:43.644366 216.234.161.19,3871 -> 10.0.2.29,1080 PR tcp len 20 44 -S
Mar 20 17:31:54.090547 195.94.0.167,1684 -> 10.0.2.29,20034 PR tcp len 20 48 -S
Mar 20 17:31:54.094325 195.94.0.167,1685 -> 10.0.2.29,5742 PR tcp len 20 48 -S
Mar 20 17:31:54.094619 195.94.0.167,2255 -> 10.0.2.29,31337 PR udp len 20 47
Mar 20 17:31:55.297325 195.94.0.72,2542 -> 10.0.2.29,20034 PR tcp len 20 48 -S
Mar 20 17:31:55.303421 195.94.0.72,2543 -> 10.0.2.29,5742 PR tcp len 20 48 -S
Mar 20 17:31:55.304521 195.94.0.72,4571 -> 10.0.2.29,31337 PR udp len 20 47
Mar 20 17:31:55.635438 216.234.161.19,3871 -> 10.0.2.29,1080 PR tcp len 20 44 -S
Mar 20 17:31:57.078202 195.94.0.167,1683 -> 10.0.2.29,1080 PR tcp len 20 48 -S
Mar 20 17:31:57.079255 195.94.0.167,1685 -> 10.0.2.29,5742 PR tcp len 20 48 -S
Mar 20 17:31:57.080972 195.94.0.167,1684 -> 10.0.2.29,20034 PR tcp len 20 48 -S
Mar 20 17:31:57.083383 195.94.0.167,1681 -> 10.0.2.29,12345 PR tcp len 20 48 -S
Mar 20 17:31:58.381033 195.94.0.72,2543 -> 10.0.2.29,5742 PR tcp len 20 48 -S
Mar 20 17:31:58.382596 195.94.0.72,2542 -> 10.0.2.29,20034 PR tcp len 20 48 -S
Mar 20 17:31:58.396060 195.94.0.72,2540 -> 10.0.2.29,12345 PR tcp len 20 48 -S
Mar 20 17:32:03.096930 195.94.0.167,1683 -> 10.0.2.29,1080 PR tcp len 20 48 -S
Mar 20 17:32:03.097204 195.94.0.167,1685 -> 10.0.2.29,5742 PR tcp len 20 48 -S
Mar 20 17:32:03.098918 195.94.0.167,1684 -> 10.0.2.29,20034 PR tcp len 20 48 -S
Mar 20 17:32:03.101040 195.94.0.167,1681 -> 10.0.2.29,12345 PR tcp len 20 48 -S
Mar 20 17:32:04.246954 195.94.0.72,2543 -> 10.0.2.29,5742 PR tcp len 20 48 -S
Mar 20 17:32:04.247309 195.94.0.72,2542 -> 10.0.2.29,20034 PR tcp len 20 48 -S
Mar 20 17:32:04.247818 195.94.0.72,2540 -> 10.0.2.29,12345 PR tcp len 20 48 -S
Mar 20 17:32:15.249709 195.94.0.167,1683 -> 10.0.2.29,1080 PR tcp len 20 48 -S
Mar 20 17:32:15.250372 195.94.0.167,1685 -> 10.0.2.29,5742 PR tcp len 20 48 -S
Mar 20 17:32:15.250762 195.94.0.167,1684 -> 10.0.2.29,20034 PR tcp len 20 48 -S
Mar 20 17:32:15.251558 195.94.0.167,1681 -> 10.0.2.29,12345 PR tcp len 20 48 -S
Mar 20 17:32:16.208632 195.94.0.72,2543 -> 10.0.2.29,5742 PR tcp len 20 48 -S
Mar 20 17:32:16.209136 195.94.0.72,2542 -> 10.0.2.29,20034 PR tcp len 20 48 -S
Mar 20 17:32:16.209829 195.94.0.72,2540 -> 10.0.2.29,12345 PR tcp len 20 48 -S
Mar 20 17:32:19.639008 216.234.161.19,3871 -> 10.0.2.29,1080 PR tcp len 20 44 -S
```

Summary: Definite evidence of active targeting (10.0.2.29 is the obvious target; 195.94.0.167 and 195.94.0.72 are the probers)

Intent: Intent is a scan of known "trojan" TCP ports (5742,20034,12345)

Technique: The pattern is to alternate between the 2 Source addresses and query the same sequence of ports 1 second apart

Severity: Low to medium; firewall or packet filter would block this

Actions: The network administrator should keep a "watch" on the 195.94.0.0 network.

Detect #2: rexec attempt

```
Mar 18 23:51:35 4C:workstation rexecd[14591]:
refused connect from svstud.win.tue.nl
Mar 19 01:03:14 4C:workstation rexecd[14635]:
refused connect from svstud.win.tue.nl
Mar 19 01:49:15 4C:workstation rexecd[14655]:
```

```
refused connect from svstud.win.tue.nl
Mar 19 04:28:21 4C:workstation rexecd[14731]:
refused connect from svstud.win.tue.nl
Mar 19 05:36:30 4C:workstation rexecd[14774]:
refused connect from svstud.win.tue.nl
Mar 19 05:39:34 4C:workstation rexecd[14775]:
refused connect from svstud.win.tue.nl
Mar 19 08:20:00 4C:workstation rexecd[14857]:
refused connect from svstud.win.tue.nl
Mar 19 09:23:25 4C:workstation rexecd[14897]:
refused connect from svstud.win.tue.nl
```

Summary: There is evidence of intent here since the connection is refused. The password is probably not known or the rexec service is not active.

Technique: If svstud.win is up to no good, rexec leaves a low chance of being detected unless a network or host based IDS is being used.

Intent: Possibly malicious

Severity: Since the connection is not made, the danger here seems low.

Action: If possible, svstud.win could be contacted to see what they are up to.

Detect#3: ping + ftp request

```
Feb 24 23:00:47 aeon icmplogd: ping
from pF2s12a01.client.global.net.uk [195.147.140.243]
Feb 24 23:00:47 aeon icmplogd: ping
from pF2s12a01.client.global.net.uk [195.147.140.243]
Feb 24 23:00:47 aeon tcplogd: ftp connection attempt
from unknown@pF2s12a01.client.global.net.uk [195.147.140.243]
```

Summary: 195.147.140.243 is the target

Technique: Open, not trying to hide anything

Intent: The probber first "pings" to see if the host is "alive", then tries to connect to ftp port.

Severity: Low, this technique would not work if the site blocked ICMP echo requests

Action: None

Detect#4: host scan for tcp port 98

```
-----
Mar 31 19:09:34 203.85.30.129:1542 -> A.B.C.30:98 SYN **S*****
Mar 31 19:09:34 203.85.30.129:1545 -> A.B.C.33:98 SYN **S*****
Mar 31 19:09:38 203.85.30.129:1710 -> A.B.C.197:98 SYN **S*****
Mar 31 19:09:38 203.85.30.129:1714 -> A.B.C.201:98 SYN **S*****
Mar 31 19:09:38 203.85.30.129:1717 -> A.B.C.204:98 SYN **S*****
Mar 31 19:09:38 203.85.30.129:1720 -> A.B.C.207:98 SYN **S*****
Mar 31 19:09:38 203.85.30.129:1727 -> A.B.C.214:98 SYN **S*****
Mar 31 19:09:38 203.85.30.129:1728 -> A.B.C.215:98 SYN **S*****
Mar 31 19:09:38 203.85.30.129:1731 -> A.B.C.218:98 SYN **S*****
Mar 31 19:09:36 203.85.30.129:1748 -> A.B.C.235:98 SYN **S*****
Mar 31 19:09:36 203.85.30.129:2021 -> A.B.D.252:98 SYN **S*****
Mar 31 19:09:37 203.85.30.129:1531 -> A.B.C.19:98 SYN **S*****
Mar 31 19:09:39 203.85.30.129:2006 -> A.B.D.237:98 SYN **S*****
Mar 31 19:09:39 203.85.30.129:2073 -> A.B.E.48:98 SYN **S*****
```

Summary: 203.85.30.129 is scanning a.b.c network to see if tcp port 98 is active.

Technique: Certainly not "low and slow"; 14 hosts in 5 seconds;
however, fast scans can elude IDS

Intent: Possibly malicious

Severity: Medium risk, port 98 offers no known signature or risk

Action: Collect more data on 203.85.30.129

Detect #5: portmapper request

Feb 21 17:26:44 dns3 named[378]: security: notice:
unapproved AXFR from [210.92.138.152].2490 for "VT.edu" (acl)

Feb 21 17:26:43 dns1 named[506979]: security: notice:
unapproved AXFR from [210.92.138.152].2489 for "VT.edu" (acl)

Feb 21 21:44:11 dns3 rpcbind:
refused connect from 210.92.138.152 to dump()
Feb 21 21:44:11 dns3 /usr/local/bin/snort[8374]:
MISC-Source Port Traffic2 <1023: 210.92.138.152:53 -> x.x.x.z:111

[**] MISC-Source Port Traffic2 <1023 [**]
02/21-21:44:10.794608 210.92.138.152:53 -> x.x.x.z:111
TCP TTL:237 TOS:0x0 ID:62128
S* Seq: 0x64 Ack: 0x0 Win: 0x200

[**] MISC-Source Port Traffic2 <1023 [**]
02/21-21:44:11.082608 210.92.138.152:53 -> x.x.x.z:111
TCP TTL:237 TOS:0x0 ID:54238
****R*** Seq: 0x65 Ack: 0x0 Win: 0x0

[**] MISC-Source Port Traffic2 <1023 [**]
02/21-21:44:11.084727 210.92.138.152:53 -> x.x.x.z:111
TCP TTL:237 TOS:0x0 ID:16726
****R*** Seq: 0x65 Ack: 0x0 Win: 0x200

Summary: Target is being scanned to see if port 111 is open.

Technique: Port 111 tcp or udp is an attempt to access portmapper, a
known vulnerability of Sun solaris Systems.

Intent: Malicious

Severity: High

Action: Verify that the portmapper on x.x.x.x.z is secure.
Collect more data on 210.92.138.152

Detect#6: Invalid TCP Flags/Source Port of Zero

-*> Snort! <*-
Version 1.5
By Martin Roesch (roesch@clark.net, www.clark.net/~roesch)
snaplen = 68
Entering readback mode....
02/21-00:01:59.837203 192.0.218.166:4618 -> 152.163.244.9:5190
TCP TTL:126 TOS:0x0 ID:18646 DF
SFRP*U21 Seq: 0x179E86B2 Ack: 0x4460D Win: 0x5011
TCP Options => Opt 32 (32): 2020 2000 3C84 3647 9D6B 36BA
0000 0000 0000 0000 0000 0000 0000 0000 0000 0000

02/21-00:18:35.175490 192.0.205.118:21 -> 216.229.234.199:3547
TCP TTL:126 TOS:0x0 ID:35117
SFRPAU1 Seq: 0x10000 Ack: 0x147 Win: 0x5014
00 01 00 00 00 00 01 47 16 BF 50 14 00 00 76 61G..P...va
20 20 20 20 20 00 .

02/21-00:42:12.071193 24.24.195.129:0 -> 192.0.213.22:2809
TCP TTL:106 TOS:0x0 ID:17275
SF****2 Seq: 0x1A2010DD Ack: 0xE0F90080 Win: 0x5010
TCP Options => EOL EOL CC 3035487176

02/21-00:42:48.444625 24.24.195.129:2809 -> 192.0.213.22:6688
TCP TTL:106 TOS:0x0 ID:59782
SF****2 Seq: 0x10E1 Ack: 0xBB110080 Win: 0x5010
TCP Options => EOL EOL Opt 87 (40): AC9E B567 4D54 8AED CA40
0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000

02/21-00:43:48.845467 24.24.195.129:2809 -> 192.0.213.22:6688
TCP TTL:106 TOS:0x0 ID:16026
SF****2 Seq: 0x10E718F9 Ack: 0x80 Win: 0x5010
TCP Options => EOL EOL Opt 188 (40): BA74 1C80 D986 5563 E1EE
0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000

02/21-00:48:26.937096 192.0.205.114:1185 -> 207.172.3.46:119
TCP TTL:126 TOS:0x0 ID:56339 DF
SFRP**21 Seq: 0x46 Ack: 0xABD78022 Win: 0x5010
TCP Options => Opt 32 (32): 2020 2000 D02A 1E61 0494 000A
0000 0000 0000 0000 0000 0000 0000 0000 0000 0000

02/21-00:52:55.936207 192.0.205.114:1185 -> 207.172.3.46:119
TCP TTL:126 TOS:0x0 ID:18735 DF
SF*PA*1 Seq: 0xE60046 Ack: 0xB32C80D0 Win: 0x5010
00 00 0D 3C 20 20 20 20 20 00 ...< .

02/21-00:54:32.449459 192.0.207.230:0 -> 140.103.41.60:6688
TCP TTL:126 TOS:0x0 ID:51393 DF
SF*PA*2 Seq: 0xA6B02B6 Ack: 0x7E274B2E Win: 0x5018
TCP Options => EOL EOL Opt 87 (40): EE78 AEA3 E9BF BD19 01D7
0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000

02/21-01:03:55.421558 192.0.205.114:1275 -> 207.172.3.46:119
TCP TTL:126 TOS:0x0 ID:26952 DF
SF**P**1 Seq: 0x52E78E Ack: 0x321012 Win: 0x5010
00 52 E7 8E 00 32 10 12 1B 8B 50 10 11 1C 63 26
.R...2....P...c&20 20 20 20 20 00 .

02/21-01:14:50.180395 192.0.205.118:195 -> 216.229.234.199:21
TCP TTL:126 TOS:0x0 ID:15045
SF****21 Seq: 0x83C0000 Ack: 0x17A Win: 0x5014
TCP Options => Opt 32 (32): 2020 2000 0402 13BA 040A 7879
0000 0000 0000 0000 0000 0000 0000 0000 0000 0000

02/21-01:26:15.520937 192.0.205.114:1794 -> 206.132.8.211:20
TCP TTL:126 TOS:0x0 ID:20880 DF
SF**AU Seq: 0x6A Ack: 0xF7BFDDEC Win: 0x5010
TCP Options => Opt 32 (32): 2020 2000 FAC8 E7E9 82B8 0014
0000 0000 0000 0000 0000 0000 0000 0000 0000 0000

02/21-01:27:29.791569 192.0.205.114:1275 -> 207.172.3.46:119
TCP TTL:126 TOS:0x0 ID:39845 DF
SF**A*21 Seq: 0x52 Ack: 0xFA6A1193 Win: 0x5010
FA 6A 11 93 23 D3 50 10 22 38 35 65 20 20 20 20 .j..#.P."85e
20 00 .

02/21-01:27:38.969005 192.0.219.146:1526 -> 129.210.184.178:20

TCP TTL:126 TOS:0x0 ID:49375 DF
SFRP*U21 Seq: 0x189DA5B Ack: 0x168 Win: 0x5010
16 D0 61 B4 00 00 C2 48 97 BA D7 DB 3E 33 7F 6F ..a....H....>3.o
83 C7 ..

02/21-01:35:46.383817 192.0.207.114:213 -> 141.219.85.55:6688
TCP TTL:126 TOS:0x0 ID:48581 DF
SFR*A*2 Seq: 0x46A02E2 Ack: 0xD28C023A Win: 0x5018
00 00 65 63 A9 6C 22 27 49 14 68 A8 F2 19 ..ec.l"'I.h...

02/21-01:36:07.885789 192.0.207.114:6688 -> 141.219.85.55:1130
TCP TTL:126 TOS:0x0 ID:19154 DF
SFR*A*2 Seq: 0x3D02F1 Ack: 0x928C023A Win: 0x5018
00 00 CF 90 90 CF D0 EE 65 08 DD FB 7E 5Fe...~_

02/21-01:36:16.756601 192.0.207.114:6688 -> 141.219.85.55:1130
TCP TTL:126 TOS:0x0 ID:63445 DF
SFR*A*2 Seq: 0x2F6ECD8 Ack: 0xD5023A Win: 0x5010
00 00 FF FB 92 04 09 00 03 4A 90 5E 6E 08J.^n.

02/21-01:37:15.223007 192.0.207.114:6688 -> 141.219.85.55:1130
TCP TTL:126 TOS:0x0 ID:63217 DF
SFR*A*2 Seq: 0x308 Ack: 0x4BA8023A Win: 0x5018
00 00 2A A2 88 18 2E 03 59 C6 94 5A 16 E7 ..*.....Y..Z..

Summary: Evidence of targeting:source ips and dest ips are repeated.

Technique: Evidence of crafted packets:
a.source ports and destination ports rotated and repeated.
b.every packet has the Syn and the Fin flag on which is not normal network traffic
c.source port 0 shows up on 2 packets which is invalid

Intent: This possibly is an OS fingerprinting attempt using "crafted" packets.

Severity: Risk is medium

Action: Use packet filtering to "drop" this kind of traffic

Detect#7: badly formed packets

badly formed ICMP packet (type=0, code=23)
217.133.0.4 -> 117.139.80.16 (IPv12) was ''
badly formed ICMP packet (type=114, code=58)
216.181.0.4 -> 117.139.80.16 (IPv12) was ''
badly formed ICMP packet (type=9, code=218)
223.57.0.4 -> 117.139.80.16 (IPv12) was ''
badly formed ICMP packet (type=100, code=198)
228.237.0.4 -> 117.139.80.16 (IPv12) was ''
badly formed ICMP packet (type=55, code=45)
234.161.0.4 -> 117.139.80.16 (IPv12) was ''
badly formed ICMP packet (type=251, code=210)
240.85.0.4 -> 117.139.80.16 (IPv12) was ''
badly formed ICMP packet (type=55, code=45)
234.161.0.4 -> 117.139.80.16 (IPv12) was ''
badly formed ICMP packet (type=251, code=210)
240.85.0.4 -> 117.139.80.16 (IPv12) was ''
badly formed ICMP packet (type=57, code=161)
246.9.0.4 -> 117.139.80.16 (IPv12) was ''
badly formed ICMP packet (type=91, code=125)
251.189.0.4 -> 117.139.80.16 (IPv12) was ''
badly formed ICMP packet (type=231, code=23)
1.113.0.4 -> 117.139.80.16 (IPv12) was ''

Summary: Host is receiving garbage packets.

Technique: Evidence that packets position have been offset:
a. source ip addresses with 1st octet between 224 & 240
are usually reserved for multicasting
b. ip address with 1st octet above 240 are unusual
c. The types being reported are unusual for icmp; which are usually
low numbers (echo request(8), echo reply(0), dest unreachable(3),
source quench(4))
Intent: Possibly malicious

Severity: medium to high, chewing up cycles on the target

Action: Use a network based IDS to track down the source of the packets.
Could be malfunctioning hardware.

Detect#8: pattern port attack

Jan 22 19:03:23 cybernet portsentry[18767]: attackalert: SYN/Normal
scan from host: 207.236.111.226/207.236.111.226 to TCP port: 110
Jan 22 19:03:23 cybernet portsentry[18767]: attackalert: SYN/Normal
scan from host: 207.236.111.226/207.236.111.226 to TCP port: 109
Jan 22 19:03:23 cybernet portsentry[18767]: attackalert: SYN/Normal
scan from host: 207.236.111.226/207.236.111.226 to TCP port: 143

Summary: Scan from GIAC shows outbound packets from host 207.236.111.226
to ports 110 (pop), 109 (pop) and 143 (IMAP)

Technique: Historical data shows that this pattern 110/109/143 usually
indicates an attacking system

Intent: Malicious

Severity: High

Action: This host/user should be removed from the network

Detect #9: dos attack/echo port of a broadcast address

Feb 12 05:17:28.515591 172.16.0.1,26758 -> 10.11.6.255,7 PR udp len 20 1052
Feb 12 05:17:33.612045 172.16.0.1,3617 -> 10.11.6.255,7 PR udp len 20 1052
Feb 12 05:17:38.712856 172.16.0.1,20151 -> 10.11.6.255,7 PR udp len 20 1052
Feb 12 05:17:43.812900 172.16.0.1,16726 -> 10.11.6.255,7 PR udp len 20 1052

Summary: The spoofed source ip address is sending data to the udp echo port
of a broadcast address.

Technique: Flood the Network and fake source address with replies from broadcast
addresses.

They may be trying to block or silence a router.

Intent: Malicious, denial of service

Severity: Low if firewall or packet filter in place

Action: Use a network based IDS to track down the source.

Detect #10: SYN/FIN Scan

[**] IDS198/SYN FIN Scan [**]
02/16-05:43:22.491486 216.25.99.40:109 -> 172.16.1.11:109
TCP TTL:31 TOS:0x0 ID:39426
SF**** Seq: 0x734EB1D6 Ack: 0xDF0CDA6 Win: 0x404
[**] IDS198/SYN FIN Scan [**]

02/16-05:43:22.511381 216.25.99.40:109 -> 172.16.1.12:109
TCP TTL:31 TOS:0x0 ID:39426
SF**** Seq: 0x734EB1D6 Ack: 0xDF0CDA6 Win: 0x404

Summary: Syn/Fin scan of a private network. Destination ips are incrementing.

Intent: Information gathering, port 109 (pop2) was used with old E-mail systems and not widely used any more. This port could have been left open from a legacy E-mail program.

Technique: Probably crafted packets, since the source port repeats. Syn/Fin scans could go undetected by older IDS.

Severity: Low if packet filtering is in place.

Action: Packet filter in router should drop packets with TCP flags Syn and Fin set.

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

Upcoming Training

Click Here to
{Get CERTIFIED!}



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
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
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
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 Munich December 2017	Munich, Germany	Dec 04, 2017 - Dec 09, 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 London February 2018	London, United Kingdom	Feb 05, 2018 - Feb 10, 2018	Live Event
SANS Dallas 2018	Dallas, TX	Feb 19, 2018 - Feb 24, 2018	Live Event
SANS Northern VA Spring - Tysons 2018	Tysons, VA	Mar 17, 2018 - Mar 24, 2018	Live Event
SANS Secure Canberra 2018	Canberra, Australia	Mar 19, 2018 - Mar 24, 2018	Live Event
SANS 2018	Orlando, FL	Apr 03, 2018 - Apr 10, 2018	Live Event
SANS Baltimore Spring 2018	Baltimore, MD	Apr 21, 2018 - Apr 28, 2018	Live Event
SANS OnDemand	Online	Anytime	Self Paced
SANS SelfStudy	Books & MP3s Only	Anytime	Self Paced