Global Information Assurance Certification Paper

*** Northcutt, 70 *

Practical Exam for GIAC Intrusion Analyst Certification

Nicco Coltrinari
4/20/00

Detect #1 Network scan for open well known ports

Date Time Port Source Dest SP DP

18Mar2000; 0:05:10;192.168.219.2;log;drop;;hme0;inbound;tcp;161.58.239.94;172.16.132.113;1295;domain-tcp
18Mar2000; 0:05:17;192.168.219.2;log;drop;;hme0;inbound;tcp;161.58.239.94;1.1.231.104;1934;telnet
18Mar2000; 0:05:34;192.168.219.2;log;drop;;hme0;inbound;tcp;161.58.239.94;172.16.17.31;1295;telnet
18Mar2000; 0:05:36;192.168.219.2;log;drop;;hme0;inbound;tcp;161.58.239.94;1.1.152.52;1055;ftp
18Mar2000; 0:05:46;192.168.219.2;log;drop;;hme0;inbound;tcp;161.58.239.94;1.1.137.74;1934;domain-tcp
18Mar2000; 0:05:49;192.168.219.2;log;drop;;hme0;inbound;tcp;161.58.239.94;172.16.32.9;1440;telnet
18Mar2000; 0:05:53;192.168.219.2;log;drop;;hme0;inbound;tcp;161.58.239.94;172.16.194.106;1440;ftp
18Mar2000; 0:06:03;192.168.219.2;log;drop;;hme0;inbound;tcp;161.58.239.94;172.16.179.0;1295;domain-tcp
18Mar2000; 0:06:09;192.168.219.2;log;drop;;hme0;inbound;tcp;161.58.239.94;1.1.22.120;1934;telnet
18Mar2000; 0:06:13;192.168.219.2;log;drop;;hme0;inbound;tcp;161.58.239.94;1.1.184.89;1934;ftp
18Mar2000; 0:06:18;192.168.219.2;log;drop;;hme0;inbound;tcp;161.58.239.94;172.16.194.106;1440;domain-tcp

Active Targeting: Yes

Analysis: This trace is from our Firewall drop log. The traffic was from 1 host going to over 9000 different host addresses in 2 of our class Bs . The source port was always 1 of 4 possible ports 1295,1440,1934,1055 and only looked at destination ports 20(ftp), 53(dns tcp) and 23(telnet). The low and slow scan started at 11pm and continued for well over 24 hours generating only 353 packets a hour and totaled over 13000 packets before it was done.

Intent: This is a attempt at finding open well known ports in our network.

Detect #2 Class C network scan for linuxconf port 98

Date Time Port Source Dest SP DP

18Mar2000;10:19:35;192.168.219.2;log;drop;;hme0;inbound;tcp;210.200.75.51;192.168.218.1;98;98
18Mar2000;10:19:35;192.168.219.2;log;drop;;hme0;inbound;tcp;210.200.75.51;192.168.218.2;98;98
18Mar2000;10:19:35;192.168.219.2;log;drop;;hme0;inbound;tcp;210.200.75.51;192.168.218.3;98;98
18Mar2000;10:19:35;192.168.219.2;log;drop;;hme0;inbound;tcp;210.200.75.51;192.168.218.4;98;98
18Mar2000;10:19:35;192.168.219.2;log;drop;;hme0;inbound;tcp;210.200.75.51;192.168.218.5;98;98
18Mar2000;10:19:35;192.168.219.2;log;drop;;hme0;inbound;tcp;210.200.75.51;192.168.218.6;98;98
18Mar2000;10:19:36;192.168.219.2;log;drop;;hme0;inbound;tcp;210.200.75.51;192.168.218.7;98;98
18Mar2000;10:19:36;192.168.219.2;log;drop;;hme0;inbound;tcp;210.200.75.51;192.168.218.8;98;98
18Mar2000;10:19:36;192.168.219.2;log;drop;;hme0;inbound;tcp;210.200.75.51;192.168.218.9;98;98
18Mar2000;10:19:36;192.168.219.2;log;drop;;hme0;inbound;tcp;210.200.75.51;192.168.218.10;98;98

Active Targeting: Yes

Analysis: This trace is from our Firewall drop log. This was a very fast scan(< 1 minute) of 3 of our Class C addresses looking for destination port 98(linuxconf). The automated process always used the source port as 98. The attempt into one of the Class Bs was very focused, which makes me think that they had a list of possible hosts in that address space and not the others.

Intent: This was noisy attempt at finding linux machines on our network.

Detect #3 Network scan for Trojan horse(Devil port 65000)

Date Time Port Source Dest SP DP

14Apr2000; 0:05:34;192.168.219.2;log;drop;;hme0;inbound;tcp;24.114.8.216;1.1.240.79;44161;65000
14Apr2000; 0:06:21;192.168.219.2;log;drop;;hme0;inbound;tcp;24.114.8.216;172.16.93.116;30126;65000
14Apr2000; 0:06:41;192.168.219.2;log;drop;;hme0;inbound;tcp;24.114.8.216;172.16.151.117;64870;65000
14Apr2000; 0:06:47;192.168.219.2;log;drop;;hme0;inbound;tcp;24.114.8.216;172.16.237.63;36433;65000
14Apr2000; 0:07:54;192.168.219.2;log;drop;;hme0;inbound;tcp;24.114.8.216;1.1.80.1;13109;65000
14Apr2000; 0:09:58;192.168.219.2;log;drop;;hme0;inbound;tcp;24.114.8.216;172.16.76.22;53767;65000
14Apr2000; 0:10:14;192.168.219.2;log;drop;;hme0;inbound;tcp;24.114.8.216;172.16.0.0;8745;65000;40
14Apr2000; 0:11:07;192.168.219.2;log;drop;;hme0;inbound;tcp;24.114.8.216;172.16.180.10;7128;65000
14Apr2000; 0:14:00;192.168.219.2;log;drop;;hme0;inbound;tcp;24.114.8.216;1.1.61.61;55528;65000
14Apr2000; 0:14:52;192.168.219.2;log;drop;;hme0;inbound;tcp;24.114.8.216;1.1.128.80;51047;65000
14Apr2000; 0:14:56;192.168.219.2;log;drop;;hme0;inbound;tcp;24.114.8.216;172.16.125.26;24539;65000
14Apr2000; 0:15:13;192.168.219.2;log;drop;;hme0;inbound;tcp;24.114.8.216;1.1.176.42;20011;65000
14Apr2000; 0:15:14;192.168.219.2;log;drop;;hme0;inbound;tcp;24.114.8.216;1.1.73.64;18631;65000
…
…
…
19Apr2000;15:19:37;192.168.219.2;log;drop;;hme0;inbound;tcp;24.114.8.216;1.1.103.11;55623;65000
19Apr2000;15:22:01;192.168.219.2;log;drop;;hme0;inbound;tcp;24.114.8.216;172.16.25.65;46860;65000
19Apr2000;15:30:13;192.168.219.2;log;drop;;hme0;inbound;tcp;24.114.8.216;172.16.171.27;58040;65000
19Apr2000;15:31:35;192.168.219.2;log;drop;;hme0;inbound;tcp;24.114.8.216;1.1.106.57;57593;65000
19Apr2000;15:32:34;192.168.219.2;log;drop;;hme0;inbound;tcp;24.114.8.216;1.1.86.4;60391;65000
19Apr2000;15:34:20;192.168.219.2;log;drop;;hme0;inbound;tcp;24.114.8.216;172.16.183.104;36432;65000
19Apr2000;15:34:23;192.168.219.2;log;drop;;hme0;inbound;tcp;24.114.8.216;172.16.171.107;41392;65000
19Apr2000;15:34:59;192.168.219.2;log;drop;;hme0;inbound;tcp;24.114.8.216;172.16.102.112;55967;6500
0
19Apr2000;15:49:41;192.168.219.2;log;drop;;hme0;inbound;tcp;24.114.8.216;1.1.106.55;13192;65000
19Apr2000;15:59:36;192.168.219.2;log;drop;;hme0;inbound;tcp;24.114.8.216;172.16.35.4;29880;65000

Active Targeting: Yes

Analysis: This trace is from our Firewall drop log. This was a scan of our address space looking for destination port 65000(trojan devil). The traffic show up in 3 separate days logs with most of the scan being done on 19Apr over a 15 hour period. The source ports appear random, but the destination is easy to notice. DNS showed cr642498-a.hnsn1.on.wave.home.com a cable modem user on the @home network.

Intent: This was a attempted network scan for Trojan horse port 65000.

Detect #4 Network Scan for port 109(pop2)

Date Time Port Source Dest SP DP

1Mar2000;13:43:42;192.168.219.2;log;drop;;hme0;inbound;tcp;195.5.241.242;172.16.0.3;pop-2;pop-2
1Mar2000;13:43:42;192.168.219.2;log;drop;;hme0;inbound;tcp;195.5.241.242;172.16.0.4;pop-2;pop-2
1Mar2000;13:43:42;192.168.219.2;log;drop;;hme0;inbound;tcp;195.5.241.242;172.16.0.3;pop-2;pop-2
1Mar2000;13:43:42;192.168.219.2;log;drop;;hme0;inbound;tcp;195.5.241.242;172.16.0.4;pop-2;pop-2
1Mar2000;13:43:42;192.168.219.2;log;drop;;hme0;inbound;tcp;195.5.241.242;172.16.0.5;pop-2;pop-2
1Mar2000;13:43:42;192.168.219.2;log;drop;;hme0;inbound;tcp;195.5.241.242;172.16.0.6;pop-2;pop-2
1Mar2000;13:43:42;192.168.219.2;log;drop;;hme0;inbound;tcp;195.5.241.242;172.16.0.7;pop-2;pop-2
1Mar2000;13:43:42;192.168.219.2;log;drop;;hme0;inbound;tcp;195.5.241.242;172.16.0.8;pop-2;pop-2
1Mar2000;13:43:42;192.168.219.2;log;drop;;hme0;inbound;tcp;195.5.241.242;172.16.0.9;pop-2;pop-2
1Mar2000;13:43:42;192.168.219.2;log;drop;;hme0;inbound;tcp;195.5.241.242;172.16.0.10;pop-2;pop-2
1Mar2000;13:43:42;192.168.219.2;log;drop;;hme0;inbound;tcp;195.5.241.242;172.16.0.2;pop-2;pop-2

Active Targeting: Yes

Analysis: This trace is from our Firewall drop log. This was a scan of our address space looking for destination port 109(pop2). This fast and loud automated scan always had a source and destination port of 109 and generated over 21000 packets in 25 minutes. DNS showed no reverse lookup and the address space is assigned in Europe.

Intent: This was a attempted network scan for Trojan horse port 65000.

Detect #5 Limited Trojan Horse scan

Date Time Port Source Dest SP DP

01Mar2000; 1:23:10;192.168.219.2;log;drop;;hme0;inbound;udp;213.46.18.151;1.1.0.1;2140;60000
01Mar2000; 1:23:10;192.168.219.2;log;drop;;hme0;inbound;udp;213.46.18.151;1.1.0.2;2140;60000
01Mar2000; 1:23:10;192.168.219.2;log;drop;;hme0;inbound;udp;213.46.18.151;1.1.0.3;2140;60000
10Mar2000; 1:23:10;192.168.219.2;log;drop;;hme0;inbound;udp;213.46.18.151;1.1.0.4;2140;60000
10Mar2000; 1:23:10;192.168.219.2;log;drop;;hme0;inbound;udp;213.46.18.151;1.1.0.5;2140;60000
01Mar2000; 1:23:10;192.168.219.2;log;drop;;hme0;inbound;udp;213.46.18.151;1.1.0.6;2140;60000
01Mar2000; 1:23:11;192.168.219.2;log;drop;;hme0;inbound;udp;213.46.18.151;1.1.0.7;2140;60000
01Mar2000; 1:23:11;192.168.219.2;log;drop;;hme0;inbound;udp;213.46.18.151;1.1.0.8;2140;60000
01Mar2000; 1:23:11;192.168.219.2;log;drop;;hme0;inbound;udp;213.46.18.151;1.1.0.9;2140;60000
01Mar2000; 1:23:11;192.168.219.2;log;drop;;hme0;inbound;udp;213.46.18.151;1.1.0.10;2140;60000

Active Targeting: Yes

Analysis: This trace is from our Firewall drop log. This was a scan of part of our address space looking for udp port 60000. This fast process was using trojan horse port udp 2140(deep throat) going for a trojan horse range type port in 60000. DNS showed d18151.dtk.chello.nl a ISP in Europe.

Intent: This was a attempt to find open port 60000(trojan horse?)

Detect #6 Network Map scan

Date Time Port Source Dest SP DP

9Mar2000;19:57:28;192.168.219.2;log;drop;;hme0;inbound;tcp;198.142.66.178;172.16.140.1;12345;4430
9Mar2000;19:57:28;192.168.219.2;log;drop;;hme0;inbound;tcp;198.142.66.178;172.16.140.3;12345;4432
9Mar2000;19:57:28;192.168.219.2;log;drop;;hme0;inbound;tcp;198.142.66.178;172.16.140.5;12345;4434
9Mar2000;19:57:28;192.168.219.2;log;drop;;hme0;inbound;tcp;198.142.66.178;172.16.140.2;12345;4431
9Mar2000;19:57:28;192.168.219.2;log;drop;;hme0;inbound;tcp;198.142.66.178;172.16.140.4;12345;4433
9Mar2000;19:57:28;192.168.219.2;log;drop;;hme0;inbound;tcp;198.142.66.178;172.16.140.7;12345;4436
9Mar2000;19:57:28;192.168.219.2;log;drop;;hme0;inbound;tcp;198.142.66.178;172.16.140.6;12345;4435
9Mar2000;19:57:28;192.168.219.2;log;drop;;hme0;inbound;tcp;198.142.66.178;172.16.140.9;12345;4438
9Mar2000;19:57:28;192.168.219.2;log;drop;;hme0;inbound;tcp;198.142.66.178;172.16.140.8;12345;4437

Active Targeting: Yes

Analysis: This trace is from our Firewall drop log. This was a scan of part of our address space looking for a response to a tcp open on the port. This fast and loud automated process always had a source port of 12345 and incremented the destination port in the 3000 to 4000 range. The scan was looking for a repsonse of some kind for that target address generating a list of available hosts. DNS showed wdcax7-178.dialup.optusnet.com.au a dial up ISP user.

Intent: This was a attempted to map available hosts on our network by a response from a tcp open

Detect #7 Network scan for open IRC(chat) port

Date Time Port Source Dest SP DP

31Jan2000; 0:04:55;192.168..219.2;log;drop;;hme0;inbound;tcp;195.16.97.35;172.16.97.4;1440;6667
31Jan2000; 0:05:40;192.168..219.2;log;drop;;hme0;inbound;tcp;195.16.97.35;1.1.87.115;1934;6667
31Jan2000; 0:06:15;192.168..219.2;log;drop;;hme0;inbound;tcp;195.16.97.35;1.1.102.93;1055;6667
31Jan2000; 0:06:18;192.168..219.2;log;drop;;hme0;inbound;tcp;195.16.97.35;172.16.129.41;1295;6667
31Jan2000; 0:06:53;192.168..219.2;log;drop;;hme0;inbound;tcp;195.16.97.35;172.16.144.19;1440;6667
31Jan2000; 0:07:37;192.168..219.2;log;drop;;hme0;inbound;tcp;195.16.97.35;1.1.134.2;1934;6667
31Jan2000; 0:08:16;192.168..219.2;log;drop;;hme0;inbound;tcp;195.16.97.35;172.16.176.56;1295;6667
31Jan2000; 0:08:50;192.168..219.2;log;drop;;hme0;inbound;tcp;195.16.97.35;172.16.191.34;1440;6667
31Jan2000; 0:09:35;192.168..219.2;log;drop;;hme0;inbound;tcp;195.16.97.35;1.1.181.17;1934;6667
31Jan2000 0:10:10;192.168..219.2;log;drop;;hme0;inbound;tcp;195.16.97.35;1.1.196.123;1055;6667
31Jan2000; 0:10:14;192.168..219.2;log;drop;;hme0;inbound;tcp;195.16.97.35;172.16.223.71;1295;6667

Active Targeting: Yes

Analysis: This trace is from our Firewall drop log. The traffic was from 1 host looking for open port 6667 on our network. The source port was always 1 of 4 ports 1295,1440,1934,1055. These source ports I saw in my first detect, so I have to say that this and the first detect are using the same program. This slower scan appeared in logs for 3 days and totaled over 5400 packets. DNS showed office.portal.ru as the source of the traffic.

Intent: This was a attempt at finding a open IRC(chat) port in our network.

Detect #8 Network Scan

Date Time Port Source Dest SP DP

23Feb2000; 9:46:28;192.168..219.2;log;drop;;hme0;inbound;tcp;141.53.36.17;172.16.1.0;8080;42625
23Feb2000; 9:46:28;192.168..219.2;log;drop;;hme0;inbound;tcp;141.53.36.17;172.16.1.4;8080;42629
23Feb2000; 9:46:28;192.168..219.2;log;drop;;hme0;inbound;tcp;141.53.36.17;172.16.1.5;8080;42630
23Feb2000; 9:46:28;192.168..219.2;log;drop;;hme0;inbound;tcp;141.53.36.17;172.16.1.6;8080;42631
23Feb2000; 9:46:28;192.168..219.2;log;drop;;hme0;inbound;tcp;141.53.36.17;172.16.1.7;8080;42632
23Feb2000; 9:46:28;192.168..219.2;log;drop;;hme0;inbound;tcp;141.53.36.17;172.16.1.8;8080;42633
23Feb2000; 9:46:28;192.168..219.2;log;drop;;hme0;inbound;tcp;141.53.36.17;172.16.1.9;8080;42634
23Feb2000; 9:46:28;192.168..219.2;log;drop;;hme0;inbound;tcp;141.53.36.17;172.16.1.10;8080;42635
23Feb2000; 9:46:28;192.168..219.2;log;drop;;hme0;inbound;tcp;141.53.36.17;172.16.1.11;8080;42636
23Feb2000 9:46:28;192.168..219.2;log;drop;;hme0;inbound;tcp;141.53.36.17;172.16.1.12;8080;42637
23Feb2000; 9:46:28;192.168..219.2;log;drop;;hme0;inbound;tcp;141.53.36.17;172.16.1.13;8080;42638

Active Targeting: Yes

Analysis: This trace is from our Firewall drop log. The traffic was from 1 host looking for open responses to tcp open requests. The source port was crafted to always be port 8080 possible helping to hide the attempt to scan the network for available hosts. This faster scan generated over 14000 packets in 30 minutes trying to get a response. DNS showed microbio7.biologie.uni-greifswald.de a University in Germany.

Intent: This was a attempt at a network scan using proxy port 8080 to hide.

Detect #9 DNS Load Balancing

Date Time Port Source Dest SP DP

22Apr2000; 0:30:59;192.56.219.2;log;drop;;hme0;inbound;tcp;216.34.196.73;192.56.220.12;domain-tcp;2200
22Apr2000; 0:30:59;192.56.219.2;log;drop;;hme0;inbound;tcp;216.34.196.73;192.56.220.12;domain-tcp;2201
22Apr2000; 0:30:59;192.56.219.2;log;drop;;hme0;inbound;tcp;216.34.196.73;192.56.220.12;domain-tcp;2202

22Apr2000; 0:31:11;192.56.219.2;log;drop;;hme0;inbound;tcp;216.32.193.135;192.56.220.12;domain-tcp;2000
22Apr2000; 0:31:11;192.56.219.2;log;drop;;hme0;inbound;tcp;216.32.193.135;192.56.220.12;domain-tcp;2002
22Apr2000; 0:31:11;192.56.219.2;log;drop;;hme0;inbound;tcp;216.32.193.135;192.56.220.12;domain-tcp;2001

Active Targeting: Yes

Analysis: This trace is from our Firewall drop log. The destination of these packets is one of our DNS forwarders. Looking up the DNS names for these IP address revealed la3dns.tunes.com and nj3dns.tunes.com, so this must be a DNS load balancer attempt to a traceroute for latency from the East and West Coasts to our DNS box.

Intent: DNS load balancing for Web Site

Detect #10 Network Scan for open IMAP(143) port

19Apr2000; 0:16:03;192.168.219.2;log;drop;;hme0;inbound;tcp;206.251.12.170;1.1.86.111;27327;143
19Apr2000; 0:38:43;192.168.219.2;log;drop;;hme0;inbound;tcp;206.251.12.170;1.1.19.142;36051;143
19Apr2000; 0:56:55;192.168.219.2;log;drop;;hme0;inbound;tcp;206.251.12.170;1.1.69.152;64596;143
19Apr2000; 1:22:58;192.168.219.2;log;drop;;hme0;inbound;tcp;206.251.12.170;172.16.69.110;3153;143
19Apr2000; 2:21:34;192.168.219.2;log;drop;;hme0;inbound;tcp;206.251.12.170;172.16.65.184;39248;143
19Apr2000; 3:28:31;192.168.219.2;log;drop;;hme0;inbound;tcp;206.251.12.170;1.1.238.106;22038;143
19Apr2000; 4:14:47;192.168.219.2;log;drop;;hme0;inbound;tcp;206.251.12.170;1.1.178.122;33388;143
19Apr2000; 5:58:19;192.168.219.2;log;drop;;hme0;inbound;tcp;206.251.12.170;1.1.203.238;59117;143
19Apr2000; 6:03:15;192.168.219.2;log;drop;;hme0;inbound;tcp;206.251.12.170;1.1.123.236;3479;143

Active Targeting: Yes

Analysis: This trace is from our Firewall drop log. The traffic was from 1 host looking for open requests to tcp port 143. This appears to be a automated network scan which ran very slow in a attempt not to be seen. I will be looking for a return of this address on upcoming days to see if he continues his probe. DNS showed vital.bleeding.com

Intent: This was a slow attempt to find open IMAP ports on our network

Last Updated: May 27th, 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 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**
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**
Baltimore September 2017 - SEC503: Intrusion Detection In-Depth	**Baltimore, MD**	**Sep 25, 2017 - Sep 30, 2017**	**vLive**
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 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 Seattle 2017	**Seattle, WA**	**Oct 30, 2017 - Nov 04, 2017**	**Live Event**
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**