



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, 72 *

Detects submitted to SANS by R.J. (Bob) Long, for IDIC Intrusion Detection certification

Source: Sanitized and abbreviated Firewall-1 logs from our company's main Internet connection.

Note: Most detects have been abbreviated to show only representative events, except where pattern was interesting.

Detect #1:

Sequential port scan of our complete Class C, firewall, and probably the ISP subnet it's on.

From: CIMAGNET Communication Information Management, Germany (Small German ISP: www.cimag.de [195.145.171.19])

Does not currently respond to ping. Registration for TCP 1524 is ingreslock. Possibly dial-up, or compromised machine.

No.	Date	Time	I/F	Action	Service	Source	Destination	Proto.
28554	08-Apr-00	22:54:17	Internet	drop	1524	195.145.171.21	ISP.SUBNET.OUR.FW	tcp
28560	08-Apr-00	22:54:39	Internet	drop	1524	195.145.171.21	OUR.CLASS-C.LEASE.0	tcp
28561	08-Apr-00	22:54:39	Internet	drop	1524	195.145.171.21	OUR.CLASS-C.LEASE.1	tcp
...
28818	08-Apr-00	22:54:49	Internet	drop	1524	195.145.171.21	OUR.CLASS-C.LEASE.254	tcp

Detect #2:

Semi-sequential imap scan of our complete class C, plus firewall and likely our ISP's subnet.

From Korea Telecom-PUBNET. Note odd stepping countdown order. Possible tool signature? (full record)

No.	Date	Time	I/F	Action	Service	Source	Destination	Proto.
9421	9-Apr-00	13:56:23	Internet	drop	imap	210.99.10.189	ISP.SUBNET.OUR.FW	tcp
9424	9-Apr-00	13:56:30	Internet	drop	imap	210.99.10.189	OUR.CLASS-C.LEASE.12	tcp
9425	9-Apr-00	13:56:30	Internet	drop	imap	210.99.10.189	OUR.CLASS-C.LEASE.13	tcp
9426	9-Apr-00	13:56:30	Internet	drop	imap	210.99.10.189	OUR.CLASS-C.LEASE.11	tcp
9427	9-Apr-00	13:56:30	Internet	drop	imap	210.99.10.189	OUR.CLASS-C.LEASE.10	tcp
9428	9-Apr-00	13:56:30	Internet	drop	imap	210.99.10.189	OUR.CLASS-C.LEASE.9	tcp
9429	9-Apr-00	13:56:30	Internet	drop	imap	210.99.10.189	OUR.CLASS-C.LEASE.7	tcp
9430	9-Apr-00	13:56:30	Internet	drop	imap	210.99.10.189	OUR.CLASS-C.LEASE.8	tcp
9431	9-Apr-00	13:56:30	Internet	drop	imap	210.99.10.189	OUR.CLASS-C.LEASE.6	tcp
9432	9-Apr-00	13:56:30	Internet	drop	imap	210.99.10.189	OUR.CLASS-C.LEASE.5	tcp
9433	9-Apr-00	13:56:30	Internet	drop	imap	210.99.10.189	OUR.CLASS-C.LEASE.4	tcp
9434	9-Apr-00	13:56:30	Internet	drop	imap	210.99.10.189	OUR.CLASS-C.LEASE.3	tcp
9435	9-Apr-00	13:56:30	Internet	drop	imap	210.99.10.189	OUR.CLASS-C.LEASE.2	tcp
9436	9-Apr-00	13:56:30	Internet	drop	imap	210.99.10.189	OUR.CLASS-C.LEASE.1	tcp
9437	9-Apr-00	13:56:30	Internet	drop	imap	210.99.10.189	OUR.CLASS-C.LEASE.0	tcp
9438	9-Apr-00	13:56:30	Internet	drop	imap	210.99.10.189	OUR.CLASS-C.LEASE.32	tcp
9439	9-Apr-00	13:56:30	Internet	drop	imap	210.99.10.189	OUR.CLASS-C.LEASE.31	tcp
9440	9-Apr-00	13:56:30	Internet	drop	imap	210.99.10.189	OUR.CLASS-C.LEASE.30	tcp
9441	9-Apr-00	13:56:30	Internet	drop	imap	210.99.10.189	OUR.CLASS-C.LEASE.29	tcp
9442	9-Apr-00	13:56:30	Internet	drop	imap	210.99.10.189	OUR.CLASS-C.LEASE.27	tcp
9443	9-Apr-00	13:56:30	Internet	drop	imap	210.99.10.189	OUR.CLASS-C.LEASE.28	tcp
9444	9-Apr-00	13:56:30	Internet	drop	imap	210.99.10.189	OUR.CLASS-C.LEASE.26	tcp
9445	9-Apr-00	13:56:30	Internet	drop	imap	210.99.10.189	OUR.CLASS-C.LEASE.25	tcp
9446	9-Apr-00	13:56:30	Internet	drop	imap	210.99.10.189	OUR.CLASS-C.LEASE.24	tcp

9647	9-Apr-00	13:56:39	Internet	drop	imap	210.99.10.189	OUR.CLASS-C.LEASE.216	tcp
9648	9-Apr-00	13:56:39	Internet	drop	imap	210.99.10.189	OUR.CLASS-C.LEASE.215	tcp
9649	9-Apr-00	13:56:40	Internet	drop	imap	210.99.10.189	OUR.CLASS-C.LEASE.225	tcp
9650	9-Apr-00	13:56:40	Internet	drop	imap	210.99.10.189	OUR.CLASS-C.LEASE.238	tcp
9651	9-Apr-00	13:56:40	Internet	drop	imap	210.99.10.189	OUR.CLASS-C.LEASE.237	tcp
9652	9-Apr-00	13:56:40	Internet	drop	imap	210.99.10.189	OUR.CLASS-C.LEASE.236	tcp
9653	9-Apr-00	13:56:40	Internet	drop	imap	210.99.10.189	OUR.CLASS-C.LEASE.235	tcp
9654	9-Apr-00	13:56:40	Internet	drop	imap	210.99.10.189	OUR.CLASS-C.LEASE.234	tcp
9655	9-Apr-00	13:56:40	Internet	drop	imap	210.99.10.189	OUR.CLASS-C.LEASE.233	tcp
9656	9-Apr-00	13:56:40	Internet	drop	imap	210.99.10.189	OUR.CLASS-C.LEASE.232	tcp
9657	9-Apr-00	13:56:40	Internet	drop	imap	210.99.10.189	OUR.CLASS-C.LEASE.230	tcp
9658	9-Apr-00	13:56:40	Internet	drop	imap	210.99.10.189	OUR.CLASS-C.LEASE.231	tcp
9659	9-Apr-00	13:56:40	Internet	drop	imap	210.99.10.189	OUR.CLASS-C.LEASE.229	tcp
9660	9-Apr-00	13:56:40	Internet	drop	imap	210.99.10.189	OUR.CLASS-C.LEASE.228	tcp
9661	9-Apr-00	13:56:40	Internet	drop	imap	210.99.10.189	OUR.CLASS-C.LEASE.227	tcp
9662	9-Apr-00	13:56:40	Internet	drop	imap	210.99.10.189	OUR.CLASS-C.LEASE.226	tcp
9663	9-Apr-00	13:56:41	Internet	drop	imap	210.99.10.189	OUR.CLASS-C.LEASE.255	tcp
9664	9-Apr-00	13:56:41	Internet	drop	imap	210.99.10.189	OUR.CLASS-C.LEASE.254	tcp
9665	9-Apr-00	13:56:41	Internet	drop	imap	210.99.10.189	OUR.CLASS-C.LEASE.253	tcp
9666	9-Apr-00	13:56:41	Internet	drop	imap	210.99.10.189	OUR.CLASS-C.LEASE.252	tcp
9667	9-Apr-00	13:56:41	Internet	drop	imap	210.99.10.189	OUR.CLASS-C.LEASE.251	tcp
9668	9-Apr-00	13:56:41	Internet	drop	imap	210.99.10.189	OUR.CLASS-C.LEASE.250	tcp
9669	9-Apr-00	13:56:41	Internet	drop	imap	210.99.10.189	OUR.CLASS-C.LEASE.249	tcp
9670	9-Apr-00	13:56:41	Internet	drop	imap	210.99.10.189	OUR.CLASS-C.LEASE.248	tcp
9671	9-Apr-00	13:56:41	Internet	drop	imap	210.99.10.189	OUR.CLASS-C.LEASE.247	tcp
9672	9-Apr-00	13:56:41	Internet	drop	imap	210.99.10.189	OUR.CLASS-C.LEASE.246	tcp
9673	9-Apr-00	13:56:41	Internet	drop	imap	210.99.10.189	OUR.CLASS-C.LEASE.245	tcp
9674	9-Apr-00	13:56:41	Internet	drop	imap	210.99.10.189	OUR.CLASS-C.LEASE.244	tcp
9675	9-Apr-00	13:56:41	Internet	drop	imap	210.99.10.189	OUR.CLASS-C.LEASE.243	tcp
9676	9-Apr-00	13:56:41	Internet	drop	imap	210.99.10.189	OUR.CLASS-C.LEASE.242	tcp
9677	9-Apr-00	13:56:41	Internet	drop	imap	210.99.10.189	OUR.CLASS-C.LEASE.241	tcp
9678	9-Apr-00	13:56:41	Internet	drop	imap	210.99.10.189	OUR.CLASS-C.LEASE.240	tcp
9679	9-Apr-00	13:56:41	Internet	drop	imap	210.99.10.189	OUR.CLASS-C.LEASE.239	tcp

Detect #3:

Some kind of probe? (mapping? fingerprinting? mutant packets? -not enough data captured by firewall to tell)
 From the variable intervals (from 1 sec. To 30min.) appears to be over a broad and randomized IP address range.
 Then again, some (4) of our IP's were revisited (many are not even active addresses).
 Destination ports are all over the ephemeral road. Pinging source yields "Destination host unreachable."
 Possibly bounced off an intermediate host? Apparent source: BTinternet dynamic pool, in Britain. (full record)

No.	Date	Time	I/F	Action	Service	Source	Destination	Proto.
24529	15-Apr-00	18:54:30	Internet	drop	51443	195.99.43.46	OUR.CLASS-C.LEASE.112	tcp
25337	15-Apr-00	19:31:10	Internet	drop	46208	195.99.43.46	OUR.CLASS-C.LEASE.89	tcp
26058	15-Apr-00	20:01:14	Internet	drop	27304	195.99.43.46	OUR.CLASS-C.LEASE.37	tcp
26404	15-Apr-00	20:16:37	Internet	drop	22989	195.99.43.46	OUR.CLASS-C.LEASE.24	tcp
26405	15-Apr-00	20:16:38	Internet	drop	34716	195.99.43.46	OUR.CLASS-C.LEASE.110	tcp
27221	15-Apr-00	20:54:10	Internet	drop	46078	195.99.43.46	OUR.CLASS-C.LEASE.22	tcp
27837	15-Apr-00	21:19:12	Internet	drop	21177	195.99.43.46	OUR.CLASS-C.LEASE.69	tcp

28440	15-Apr-00	21:48:39	Internet	drop	19466	195.99.43.46	OUR.CLASS-C.LEASE.76	tcp
28664	15-Apr-00	21:59:53	Internet	drop	20819	195.99.43.46	OUR.CLASS-C.LEASE.84	tcp
28824	15-Apr-00	22:07:42	Internet	drop	23180	195.99.43.46	OUR.CLASS-C.LEASE.93	tcp
29467	15-Apr-00	22:32:48	Internet	drop	60766	195.99.43.46	OUR.CLASS-C.LEASE.94	tcp
30001	15-Apr-00	22:52:45	Internet	drop	59154	195.99.43.46	OUR.CLASS-C.LEASE.104	tcp
30085	15-Apr-00	22:55:46	Internet	drop	51070	195.99.43.46	OUR.CLASS-C.LEASE.42	tcp
30378	15-Apr-00	23:06:19	Internet	drop	23483	195.99.43.46	OUR.CLASS-C.LEASE.109	tcp
30607	15-Apr-00	23:16:36	Internet	drop	34771	195.99.43.46	OUR.CLASS-C.LEASE.107	tcp
30660	15-Apr-00	23:18:57	Internet	drop	52590	195.99.43.46	OUR.CLASS-C.LEASE.29	tcp
254	16-Apr-00	0:11:32	Internet	drop	56102	195.99.43.46	OUR.CLASS-C.LEASE.57	tcp
1368	16-Apr-00	1:06:11	Internet	drop	13978	195.99.43.46	OUR.CLASS-C.LEASE.37	tcp
1523	16-Apr-00	1:13:43	Internet	drop	43963	195.99.43.46	OUR.CLASS-C.LEASE.112	tcp
2324	16-Apr-00	1:53:10	Internet	drop	27920	195.99.43.46	OUR.CLASS-C.LEASE.56	tcp
2627	16-Apr-00	2:08:27	Internet	drop	35492	195.99.43.46	OUR.CLASS-C.LEASE.26	tcp
3571	16-Apr-00	2:55:08	Internet	drop	60254	195.99.43.46	OUR.CLASS-C.LEASE.121	tcp
4115	16-Apr-00	3:22:01	Internet	drop	37579	195.99.43.46	OUR.CLASS-C.LEASE.64	tcp
4871	16-Apr-00	3:59:40	Internet	drop	26145	195.99.43.46	OUR.CLASS-C.LEASE.87	tcp
5474	16-Apr-00	4:29:38	Internet	drop	56910	195.99.43.46	OUR.CLASS-C.LEASE.59	tcp
5588	16-Apr-00	4:35:23	Internet	drop	10785	195.99.43.46	OUR.CLASS-C.LEASE.53	tcp
6121	16-Apr-00	5:02:14	Internet	drop	37143	195.99.43.46	OUR.CLASS-C.LEASE.64	tcp
6314	16-Apr-00	5:11:49	Internet	drop	56556	195.99.43.46	OUR.CLASS-C.LEASE.15	tcp
7401	16-Apr-00	6:05:54	Internet	drop	47213	195.99.43.46	OUR.CLASS-C.LEASE.23	tcp
9047	16-Apr-00	7:28:05	Internet	drop	11611	195.99.43.46	OUR.CLASS-C.LEASE.69	tcp

Detect #4:

Sequential scan of complete Class C and firewall for proxy port 1080
From TELE2-BACKBONE Modempools in Norway

No.	Date	Time	I/F	Action	Service	Source	Destination	Proto.
15483	20-Apr-00	16:13:04	Internet	drop	1080	193.217.227.10	ISP.SUBNET.OUR.FW	tcp
15495	20-Apr-00	16:13:52	Internet	drop	1080	193.217.227.10	OUR.CLASS-C.LEASE.1	tcp
...
15780	20-Apr-00	16:16:05	Internet	drop	1080	193.217.227.10	OUR.CLASS-C.LEASE.254	tcp

Detect #5:

Semi-sequential scan of most (201 addr's) of our Class C, but not firewall, using undetermined icmp type.
From Exodus Commun. (NETBLK-EC21-1)

No.	Date	Time	I/F	Action	Service	Source	Destination	Proto.
17000	20-Apr-00	17:40:56	Internet	drop		64.28.74.182	OUR.CLASS-C.LEASE.1	icmp
...
17220	20-Apr-00	17:40:58	Internet	drop		64.28.74.182	OUR.CLASS-C.LEASE.254	icmp

Note: verbosity of logs increased from this point on.

Detect #6:

Probe of our firewall on common UDP port for Hack 'a Tack trojan. From MobilCom City LINE GmbH Dialpool in Germany.

Note source and dest. ports one number different. This is the only traffic seen from/to 213.6.x.x today, and it's destined for firewall. Address currently responds to ping. Source could be either compromised machine or dial-up.

No.	Date	Time	I/F	Action	Service	Source	Destination	Proto	S_Port
6804	21-Apr-00	10:01:33	Internet	drop	UDP31789_HackaTack	213.6.174.21	OUR.CLASS-C.LEASE.49	udp	
UDP31790_HackaTack									
6805	21-Apr-00	10:01:33	Internet	drop	UDP31789_HackaTack	213.6.174.21	OUR.CLASS-C.LEASE.169	udp	
UDP31790_HackaTack									

Detect #7:

Sequential scan of most (216 addr's) of our Class C (not firewall) on TCP53 (DNS). Responds to ping. Compromised?
From Connected Networks (NETBLK-CONNECTED-CA) in B.C., Canada

No.	Date	Time	I/F	Action	Service	Source	Destination	Proto	S_Port
13439	21-Apr-00	22:08:41	Internet	reject	nameserver	209.53.123.202	OUR.CLASS-C.LEASE.1	tcp	nameserver
...
13655	21-Apr-00	22:08:46	Internet	reject	nameserver	209.53.123.202	OUR.CLASS-C.LEASE.247	tcp	nameserver

Detect #8a:

Scan of our complete Class-C and firewall on Sub-7 2.1 default port. Does not currently respond to ping (weekday).
From TimeWarnerCable-Road-Runner-TAMPA-mcr23d-24-26-82-0-to-84-0 (NETBLK-RRTAMPA82-84).

No.	Date	Time	I/F	Action	Service	Source	Destination	Proto	S_Port
10733	21-Apr-00	16:07:32	Internet	drop	27374	24.26.82.129	ISP.SUBNET.OUR.FW	tcp	22812
10734	21-Apr-00	16:07:40	Internet	drop	27374	24.26.82.129	OUR.CLASS-C.LEASE.0	tcp	27085
10735	21-Apr-00	16:07:40	Internet	drop	27374	24.26.82.129	OUR.CLASS-C.LEASE.1	tcp	27086
...
10992	21-Apr-00	16:08:09	Internet	drop	27374	24.26.82.129	OUR.CLASS-C.LEASE.254	tcp	30978
10993	21-Apr-00	16:08:09	Internet	drop	27374	24.26.82.129	OUR.CLASS-C.LEASE.255	tcp	31041

Detect #8b:

Another Sub-7 scan next day from another location, of most of our Class-C (234 addr's) and firewall.
From PSInet (NET-PSINET-B2-5). Address responds to ping. Could be either dial-up or compromised.

No.	Date	Time	I/F	Action	Service	Source	Destination	Proto	S_Port
1187	22-Apr-00	3:24:01	Internet	drop	27374	154.5.156.181	ISP.SUBNET.OUR.FW	tcp	1778
1189	22-Apr-00	3:24:16	Internet	drop	27374	154.5.156.181	OUR.CLASS-C.LEASE.21	tcp	2002
...
1422	22-Apr-00	3:24:29	Internet	drop	27374	154.5.156.181	OUR.CLASS-C.LEASE.254	tcp	2236

Detect #9:

DNS scan of most of our class C (216 addr's), not firewall. Address does not currently respond to ping.
From TimeWarnerCable-Road-Runner-Memphis-HUBD-East-104-106 (NETBLK-TWCMEMEAST).

No.	Date	Time	I/F	Action	Service	Source	Destination	Proto	S_Port
3654	22-Apr-00	9:35:38	Internet	reject	nameserver	24.95.106.210	OUR.CLASS-C.LEASE.2	tcp	4813

3655	22-Apr-00	9:35:38	Internet	reject	nameserver	24.95.106.210	OUR.CLASS-C.LEASE.3	tcp	4814
3656	22-Apr-00	9:35:38	Internet	reject	nameserver	24.95.106.210	OUR.CLASS-C.LEASE.1	tcp	4812
3657	22-Apr-00	9:35:38	Internet	reject	nameserver	24.95.106.210	OUR.CLASS-C.LEASE.6	tcp	4817
...
3865	22-Apr-00	9:35:41	Internet	reject	nameserver	24.95.106.210	OUR.CLASS-C.LEASE.247	tcp	1385
3866	22-Apr-00	9:35:41	Internet	reject	nameserver	24.95.106.210	OUR.CLASS-C.LEASE.240	tcp	1378
3867	22-Apr-00	9:35:41	Internet	reject	nameserver	24.95.106.210	OUR.CLASS-C.LEASE.241	tcp	1379
3868	22-Apr-00	9:35:41	Internet	reject	nameserver	24.95.106.210	OUR.CLASS-C.LEASE.244	tcp	1382
3869	22-Apr-00	9:35:41	Internet	reject	nameserver	24.95.106.210	OUR.CLASS-C.LEASE.245	tcp	1383

Detect #10:

Sunrpc scan of most of our class C (201 addr's), and firewall.

From Lesjofors AB on TELIANET-BLK in Sweden. Responds to ping. Likely compromised machine, or possibly dial-up.

No.	Date	Time	I/F	Action	Service	Source	Destination	Proto	S_Port
3884	23-Apr-00	11:25:52	Internet	drop	sunrpc	195.198.109.16	ISP.SUBNET.OUR.FW	tcp	3326
3887	23-Apr-00	11:25:56	Internet	drop	sunrpc	195.198.109.16	OUR.CLASS-C.LEASE.0	tcp	3548
3888	23-Apr-00	11:25:56	Internet	drop	sunrpc	195.198.109.16	OUR.CLASS-C.LEASE.1	tcp	3549
3889	23-Apr-00	11:25:56	Internet	drop	sunrpc	195.198.109.16	OUR.CLASS-C.LEASE.9	tcp	3557
3890	23-Apr-00	11:25:56	Internet	drop	sunrpc	195.198.109.16	OUR.CLASS-C.LEASE.2	tcp	3550
3891	23-Apr-00	11:25:56	Internet	drop	sunrpc	195.198.109.16	OUR.CLASS-C.LEASE.10	tcp	3558
3892	23-Apr-00	11:25:56	Internet	drop	sunrpc	195.198.109.16	OUR.CLASS-C.LEASE.4	tcp	3552
...
4087	23-Apr-00	11:26:06	Internet	drop	sunrpc	195.198.109.16	OUR.CLASS-C.LEASE.249	tcp	3797
4088	23-Apr-00	11:26:06	Internet	drop	sunrpc	195.198.109.16	OUR.CLASS-C.LEASE.252	tcp	3800
4089	23-Apr-00	11:26:06	Internet	drop	sunrpc	195.198.109.16	OUR.CLASS-C.LEASE.250	tcp	3798

Upcoming Training

Click Here to
{Get CERTIFIED!}



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
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
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
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
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 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