Global Information Assurance Certification Paper

***** Northcutt, 73**

Practical Exam for GCIA
2nd submission

10 Detects with Analysis

Kristy Westphal

Student from Orlando IDIC class, March 2000

Capture 1 (from GIAC, 4/18/00)

On 3 machines -- times are EDT (GMT-4)
(don't know why this machine doesn't show a POP2 connect attempt -- this machine DOES run a POP3 server and is our mail server but the other two don't run POP services at all)

```
Apr 16 02:22:06 picard tcplog: pop3 connection attempt from 207.61.128.71
Apr 16 02:23:31 medusa tcplog: pop2 connection attempt from 207.61.128.71
Apr 16 02:24:45 medusa tcplog: pop3 connection attempt from 207.61.128.71
Apr 16 02:22:06 bigfoot tcplog: pop2 connection attempt from 207.61.128.71
Apr 16 02:22:06 bigfoot tcplog: pop3 connection attempt from 207.61.128.71
```

Along with these TCP connect attempts appears to be a LOT of UDP attempts too...but only on medusa (our secondary name server)

```
Apr 16 02:23:32 medusa icmplog: destination
unreachable from medusa.csihq.com to medusa.csihq.com
```

Michael D. Black

Targeting: Yes.
Intent: Appears to be looking for a pop mail server for possible buffer overflow exploit. Possibly scanning for POP2 to exploit older version vulnerabilities.
Techniques: Attempting to connect to specifically three machines. This indicates prior recon effort (as evidenced by the complaint about receiving a lot of UDP traffic to the secondary name server).
History: POP buffer overflow attempts are an easy door in to gaining root access. If the sys admin has failed to keep their patches up to date, it can be easily exploited.
Analysis: It would appear that the attacker is trying to find which servers on this network are running the POP service in order to gain root access to the box. The timing is quick, and early in the morning, which increases suspicion. If I were the poster of this trace, I think I'd look at the machine that does run the POP service a bit closer to see if anything funny has happened to the OS.

Severity Rating:

Criticality: 4 (for an e-mail server)
Lethality: 5 (for possible root access)
System Countermeasures: 4 (don't know enough details about the network, but we'll give it to him that their OS patches are up to snuff)
Network Countermeasures: 4 (caught the trace; again, though, don't know enough about firewall to give it a 5)
Total: 1

Capture 2 (Provided by S. Northcutt-see e-mail text)

[**] PUSH FIN Scan [**]
04/06-00:15:06.303713 150.135.200.75:1810 -> MY.NET.213.150:6688

Targeting: Given the odd time of day, the fact that the source port is 1810 (which is recorded as the Jerand license manager) and that the destination port is to a typically unused port, I believe that there is evidence of targeting.

Intent: This trace only showed up once in the several days worth of logs that were provided me, which indicates either a low and slow scan, or perhaps a one time attempt at a port probe. On the flip side, it could be a totally innocent attempt to connect to the target's license server in the middle of the night.
Techniques: A scan with an unusual signature of the Push Fin.
History: The source IP address is from the University of Arizona, but could possibly be spoofed. Looking throughout the rest of the logs provided indicates several attempts to connect to port 6688 from different source ports, addresses and times. Some other examples:

[**] Queso fingerprint [**]
04/06-11:09:15.202192 194.251.102.43:1644 -> MY.NET.209.42:6688
[**] Watchlist 000220 IL-ISDNNET-990517 [**]
04/01-06:52:41.774941 212.179.101.106:1048 -> MY.NET.10.119:6688
[**] PUSH Scan [**]
04/08-02:55:45.011672 24.10.90.171:6688 -> MY.NET.203.214:1582
[**] Null scan! [**]
04/08-06:08:46.095903 212.198.240.124:6688 -> MY.NET.217.94:2891
[**] Null scan! [**]
04/08-15:34:00.798700 24.68.30.209:1044 -> MY.NET.205.186:6688
[**] URG Scan [**]
04/07-12:23:01.838862 128.211.236.128:6688 -> MY.NET.180.200:1125
[**] FIN Scan [**]
04/07-17:46:16.648291 169.232.69.176:2252 -> MY.NET.208.14:6688

All source addresses are all Teleco companies of one sort or another, spread all over the world.

Analysis: It would appear that port 6688 is used for some type of cable modem connection, possibly just to establish a proprietary link to this University's net.

Severity Rating:

Criticality: 1 (for targeting an infrequently used port)
Lethality: 2 (for completing the scan)
System Countermeasures: 4 (most likely the newest software since using cable modem technology)
Network Countermeasures: 4 (detect picked up)
Total: -5

Capture 3 (from GIAC, 4/19/00)

Hi after looking through my logs from the weekend I found this for Friday eve. After discussing this with my network architect 1 of 2 things could be possible. Either someone has a machine name called router.midcan.com or 2 (more likely) they have a linux machine setup as a router. It is probing for SunRPC's and looks like broadcast for ftp. I was just curious if anyone else had seen this.

```
20:02:25.364937 router.midcan.com.2975 >
```

```
255.255.255.255.21: S 358794685:358794685(0) win 32120 (DF)
20:02:39.897269 router.midcan.com.667 >
mydomain.com.111: S 372237668:372237668(0) win 32120 (DF)
20:02:40.386161 router.midcan.com.4770 >
255.255.255.255.21: S 363105747:363105747(0) win 32120 (DF)
20:02:43.380314 router.midcan.com.4770 >
255.255.255.255.21: S 363105747:363105747(0) win 32120 (DF)
```

Targeting: Yes.
Intent: A broadcast type of scan for machines with ftp ports (21) on that particular domain, as well as open SunRPC ports (111).
Techniques: Sending SYN packets to broadcast addresses for the particular port they are looking for.
History: Typically, when a packet is sent to the address of 255.255.255.255, it means that the attacker is coming from the subnet that the router is on. The ftp service has become an interesting way to do portscanning, utilizing a method called FTP bounce. This type of portscanning can easily scan a network, giving the attacker the information they need, while hiding their identity.

Port 111 is a target for Portmapper. This indicates that the attacker is trying to exploit the rpc service of NFS, to display the mounts available. This usually indicates recon for a later attack.
Analysis: It is suspicious to me that this trace would display the broadcast search for ftp ports, as well as the portmapper. I sense a recon attempt in its early stages. I don't tend to agree with the router theory, because routers (even if they use the RIP protocol) don't typically look for just one type of port. The combination of ports 21 and 111 make me lean even more heavily on a recon mission.

Severity Rating:

Criticality: 3 (for the service that it is looking for ranks low)
Lethality: 4 (for the possibilities it leaves down the road)
System Countermeasures: 3 (unsure as to details of how OS is set up)
Network Countermeasures: 4 (caught the scan)
Total: 0

Capture 4 (from GIAC, 4/21/00)

Logged some more denies from the same subnet as I reported last week from a Taiwan .edu. Complaints to edu.tw admins have gone unanswered so far.
One example log from one of our Cisco devices of a recent incident. Time is US CST (-5 hours UTC).

```
Apr 19 02:02:13 ournet.x.y.z 6329: Apr 19 02:02:12: %SEC-6-IPACCESSLOGP:
list 110 denied tcp 140.126.10.131(1434) -> 0.0.0.0(23), 1 packet
140.126.10.131 resolves to: Class5-46.cc-pc.chu.edu.tw
```

Targeting: Yes.
Intent: Trying to map out the victim's network through what would appear to be a hijacked address. The fact that the admins haven't replied back yet indicates some mischief.

Techniques: By sending a broadcast request to the telnet port (23) to see what comes back with a reply. This can be then used for future reference in a possible attack.
History: Sending packets to broadcast addresses typically indicates some type of denial of service. However, it has also been known as a mapping technique for further activity, which is what I believe to be happening here.
Analysis: I am speculating that the 140.126.10.131 computer has been compromised, and is being used to attempt to map the victim's network. Since it has happened more than once, I feel like whomever the attacker is using a script of some sort, leaving it to run unattended. Otherwise, the attacker probably would have tried it once and moved on after being denied the first time.

My other theory on this one is pretty benign: it could just be a misconfigured SQL server (port 1434 is a SQL Management server). Since it does keep occurring, this is another possible explanation.

Severity Rating:

Criticality: 3 (nothing specific targeted yet, potential threat in future)
Lethality: 1 (just trying to map, no damage yet)
System Countermeasures: 3 (again, no particular system targeted)
Network Countermeasures: 4 (firewall caught it, no problem)
Total: -3

Capture 5 (GIAC- 3/31/00)

```
Site: @home Host lookup: Date: 20000330 Pattern:
src host 63.11.117.219 /usr/local/logger/one_day_pat.pl
-S -d 20000330 -l @home -p 'src host 63.11.117.219 '
/Shadow/@home/Mar30
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)
```

Targeting: Yes.
Intent: Original intent is to impart the RingZero trojan, with perhaps use of some new ports.
Techniques: Utilizing the recognized pattern of ports 8080 and 3128, with ports 8002 and 8050 interesting new additions.
History: RingZero was identified as a trojan that used ports 80, 8080 and 3128 to report ip addresses and proxy ports to a central server (www.rusftpsearch.net). This particular trace highlighted these new ports as possibly a mutation of this trojan.
Analysis: After some extensive searching on the internet, it would appear that these ports are utilized generally for the following:

Port 8002: seems to be linked to Quake 3 (UDP) or Web (TCP).

Port 8050: a lot of disk drives named this, but I can't find anything else!! Have also seen as an alternate web port on occasion.

It would appear that if this is indeed a mutation of RingZero, then the scanning executable that connects back to the central server may have been altered to utilize new web ports to throw off IDS's looking for the generally recognized three port pattern of 80, 8080, and 3128.

Severity Rating:

Criticality: 3
Lethality: 2 (info gathering)
System Countermeasures: 4 (better have the virus scanner up-to-date, didn't sound like it made it through the firewall)
Network Countermeasures: 4 (firewall detected it)
Total: -3

Capture 6 (GIAC-4/1/00)

Mar 31 11:27:43 dns1 snort[4415]: spp_portscan: PORTSCAN DETECTED from 208.185.54.22
Mar 31 11:27:49 dns1 snort[4415]: spp_portscan: portscan status from 208.185.54.22: 14 connections across 1 hosts: TCP(0), UDP(14)
Mar 31 11:27:55 dns1 snort[4415]: spp_portscan: End of portscan from 208.185.54.22
Mar 31 11:27:43 208.185.54.22:33161 -> a.b.c.34:33465 UDP Mar 31 11:27:43 208.185.54.22:33161 -> a.b.c.34:33466 UDP
Mar 31 11:27:43 208.185.54.22:33161 -> a.b.c.34:33467 UDP Mar 31 11:27:43 208.185.54.22:33161 -> a.b.c.34:33468 UDP

Mar 31 11:27:43 208.185.54.22:33161 -> a.b.c.34:33469 UDP Mar 31 11:27:43
208.185.54.22:33161 -> a.b.c.34:33470 UDP
Mar 31 11:27:43 208.185.54.22:33161 -> a.b.c.34:33471 UDP Mar 31 11:27:43
208.185.54.22:33161 -> a.b.c.34:33472 UDP
Mar 31 11:27:43 208.185.54.22:33161 -> a.b.c.34:33473 UDP Mar 31 11:27:43
208.185.54.22:33161 -> a.b.c.34:33474 UDP
Mar 31 11:27:43 208.185.54.22:33161 -> a.b.c.34:33475 UDP Mar 31 11:27:43
208.185.54.22:33161 -> a.b.c.34:33476 UDP
Mar 31 11:27:43 208.185.54.22:33161 -> a.b.c.34:33477 UDP Mar 31 11:27:43
208.185.54.22:33161 -> a.b.c.34:33478 UDP

Targeting: Yes.
Intent: This looks to be a recon effort to map the network.
Techniques: This attack most likely is using traceroute.
History: This range of UDP ports that the attacker is sending to (33465-33477) are typical of this utility. This type of pattern is usually seen during a recon effort of an attacker who is trying to find out what the victim's network looks like. A coordinated traceroute can be most useful if run at various times throughout the day, just to see what may be on the air at different times (i.e. trying to find a user's workstation that gets turned off at 5:00 p.m., versus a Mail server that stays on all the time).
Analysis: This would appear to be a form of coordinated traceroute or network mapping through traceroute. The closeness in timing also tends to point towards the coordinated traceroute.

Severity Rating:

Criticality: 4
Lethality: 3
System Countermeasures: 3
Network Countermeasures: 4
Total: 0

Capture 7 (from GIAC, 4/17/00)

A NetBIOS attack from a RoadRunner user in Tampa FL.
This is a ZoneAlarm log entry Times are EDT
oneAlarm Basic Logging Client v2.1.10
Windows 98-4.10.1998- -SP

```
type,date,time,source,destination,transport
FWIN,2000/04/16,09:20:50 -4:00 GMT,24.26.88.187:137,x.x.x.x:137,UDP
FWIN,2000/04/16,09:20:50 -4:00 GMT,24.26.88.187:61705,x.x.x.x:137,UDP
```

Targeting: Yes.
Intent: NetBIOS scans are tough. I believe that in this case that the attacker is trying to find out some network information through the use of UDP port 137.
Techniques: By using destination port 137, and having such an odd source port of 61705, the attacker can connect and gain network information.

History: If an attacker uses a vulnerable port 137, once connected through that port, can use the utility nbtstat to gain valuable network information. At first, I thought that since the source port was not 137 also, that it might be innocent traffic by the use of Samba. However, Samba typically uses ports 137-139. The use of such a high UDP port to connect to port 137 is unusual.

Analysis: This looks like a possible spoofed source address from a machine at Roadrunner in Tampa, with the intent of finding out more information on the target machine.

Severity Rating:

Criticality: 3 (hard to tell since I don't know the the nature of the destination host)
Lethality: 2
System Countermeasures: 3
Network Countermeasures: 4 (firewall picked up detect)
Total: -2

Capture 8 (from GIAC, 4/10/00)

It's been a relatively quiet week in this neck of the woods - not that I mind at all.
Apart from some boring scans on port 25 for a few boxes, the most exciting thing was the following UDP scan to port 161 on a box running portsentry.
It'll be interesting to see if the network owner acknowledges/replies to the notification.

```
Apr 5 20:13:50 gatekeeper portsentry[1776]: attackalert:
UDP scan from host: router.nastec.com.au/150.101.8.1 to UDP port: 161
Apr 5 20:13:50 gatekeeper portsentry[1776]: attackalert:
Host 150.101.8.1 has been blocked via wrappers with string: "ALL:
150.101.8.1"
Apr 5 20:13:50 gatekeeper portsentry[1776]: attackalert:
UDP scan from host: router.nastec.com.au/150.101.8.1 to UDP port: 161
Apr 5 20:13:50 gatekeeper portsentry[1776]: attackalert:
Host: router.nastec.com.au/150.101.8.1 is already blocked Ignoring
```

Targeting: Yes.
Intent: To connect to this particular host via the SNMP port 161.
Techniques: The host 150.101.8.1 is attempting to connect to UDP port 161 on the victim's network.
History: SNMP services are historically an easy entry point for attackers, if the victim's site has not properly secured them. Many devices on a network run this particular service and if the default admin password is not changed, then the door is wide open for a recon mission.
Analysis: I would guess that the device 150.101.8.1 is either a compromised router or similar network device, due to its low number (.1 is usually reserved for network devices). It is probably being used to attempt recons on other networks through the SNMP port. No other traffic was reported from this host, so most likely no automated script was being used to generate this traffic. Kind of a hit and run type of recon activity.

Severity Rating:

Criticality: 4
Lethality: 4
System Countermeasures: 4
Network Countermeasures: 4 (portsentry caught it and blocked the site from future connection attempts. Very nice!)
Total: 0

Capture 9 (from GIAC, 4/14/00)

(David Hoelzer has recently brought up a new IDS and is seeing some interesting activity to his firewall. There were many repeated connections that were edited from the submission for the sake of brevity.)
This pretty clearly shows that there are multiple sites attempting this connection. The best piece of news from this is that the firewall consistently responds with a RST ACK. I have been unable to find any references to any software that uses port 3412 to establish a connection. Have you seen this type of activity before?

```
01:39:40.090480 pmwino1-14.rconnect.com.1027 >
myfirewall.com.3412: S 928312:928312(0) win 8192 (DF)
01:16:33.296812 host213.2106230.gcn.net.tw.2529 >
myfirewall.com.3412: S 3697304180:3697304180(0) win 32120
<mss 1460,sackOK,timestamp 190620606[|tcp]> (DF)
04:55:30.845172 InternationalTabaccoMachinery.unisrc.net.1204 >
myfirewall.com.3412: S 12265145:12265145(0) win 8192
<mss 1460> (DF)
05:00:36.891080 S67-58.smumn.edu.1134 >
myfirewall.com.3412: S 34581972:34581972(0) win 8192
<mss 1460,nop,nop,sackOK> (DF)
05:22:46.825600 ppp-41.nrw-online.de.58687 >
myfirewall.com.3412: S 11063088:11063088(0) win 8192
<mss 1460> (DF)
```

Targeting: Yes.
Intent: Wow-hard to say. I dug pretty deep to see if I could find anything related to this port, but no luck. I have 2 theories after all of this: 1) It could be some type of DOS or 2) Perhaps it is a twisted new form of an old trojan that uses port 1243 (our friend SubSeven).
Techniques: Using multiple sites to probe this firewall at Port 3412.
History: None yet- but judging from the multiple attempts to reach this port from several differing sites, it looks like a DDOS attack of some sort.
Analysis: I will stick with my two theories mentioned in the Intent section until further use of this scan is seen elsewhere!

Severity Rating:

Criticality: 5
Lethality: 4
System Countermeasures: 4
Network Countermeasures: 4
Total: 1

Capture 10 (GIAC, 4/6/00)

```
Apr 3 23:30:07 gamma kernel: securityalert: no match found in forward screen:
ip_p=255 if=fpa0 srcaddr=63.xxx.252.10 dstaddr=128.xxx.118.47
Apr 3 23:30:12 gamma kernel: securityalert: no match found in forward screen:
ip_p=255 if=fpa0 srcaddr=63.xxx.252.10 dstaddr=128.xxx.94.114
Apr 3 23:30:35 gamma kernel: securityalert: no match found in forward screen:
ip_p=255 if=fpa0 srcaddr=63.xxx.252.10 dstaddr=128.xxx.230.50
Apr 3 23:30:54 gamma kernel: securityalert: no match found in forward screen:
ip_p=255 if=fpa0 srcaddr=63.xxx.252.10 dstaddr=128.xxx.77.45
Apr 3 23:31:08 gamma kernel: securityalert: no match found in forward screen:
ip_p=255 if=fpa0 srcaddr=63.xxx.252.10 dstaddr=128.xxx.171.103
```

Targeting: Yes.
Intent: Looks like an attempted portscan.
Techniques: I can't tell if the attacker intended to use a broadcast to find open ports and mistyped the protocol number, or if they just wanted to be really obvious that they were scanning this person's network!
History: The attempted connection of one server to multiple addresses and ports on someone else's network typically indicates a mapping effort.
Analysis: It would seem to me that someone, going through their ISP or spoofing the ISP (63.xxx.252 appears to belong to one), perhaps mistyped the protocol while attempting to recon the victim's network. Something is definitely wrong here because IP protocol 255 is a reserved protocol for the IANA, not frequently used.

Severity Rating:

Criticality: 3
Lethality: 2
System Countermeasures: 3
Network Countermeasures: 4
Total: -2

Then we have the W.A.G. of the day:

GIAC has seen quite a bit of activity recently coming from that sneaky Roadrunner in Tampa,FL. The post from 4/22/00 then caught my eye:

Greetings,
On Tuesday night 04/19/00 from 2000/04/19 9:21:25 PM GMT -0400 to 2000/04/19 10:42:12 PM GMT -0400 I detected numerous scans of port 37015 and 47015. These scans appear to have originated from several sources, including:
216.161.215.139
216.63.97.39
194.229.103.215
216.103.51.189
128.211.218.115

24.1.97.66
131.215.103.89
208.61.0.233
209.51.167.221
195.197.41.184
141.64.111.90
63.10.148.174
12.77.153.134
63.17.105.92
24.48.150.25
208.14.222.162
24.94.251.83
216.232.96.245
24.66.196.134
24.92.134.35

There were approximately 100 scans in the course of about an hour. They typically are in groups of three or six. Here are some examples:

```
2000/04/19 9:21:25 PM GMT -0400: Linksys LNE100TX ..[0004]
[No matching rule] Blocking incoming UDP: src=216.161.215.139,
dst=24.24.60.246,
sport=3232, dport=37015.
2000/04/19 10:15:25 PM GMT -0400: Linksys LNE100TX ..[0004][No matching
rule] Blocking incoming UDP: src=208.14.222.162, dst=24.24.60.246,
sport=4358, dport=47015.
```

What is port 37015 used for?

Always being curious as to what these mysterious new ports are, I started doing some digging; thus, my W.A.G./W.A.T(heory). You'll have to forgive me if this sounds silly, but the coincidence was really too good to pass up!

I noticed an odd correlation between these IP addresses and some of the ones I mentioned in my analysis of Capture 2. They were very similar in fact, some originated from the same company, just slightly different subnets within their domain.

The ports are very different except for one thing. The ones if have focused in on: 6688, 37015, and 47015 (as well as ports 49431, 48017, 50372, 51621, 51191, 27492, 54640, 46691, 55928, 62894, 50225, 50620, and 32771) are all in the Debian bug database or archive database as report numbers. OK, once you are done snickering, I would just like to add that perhaps the attacker is fond of Debian Linux using this pattern for some odd, massive recon effort. Not that these ports are highly used in Linux or anything else for that matter, just that the bug database give them a lot of interesting numbers to work with.

The W.A.G. is now over. If you think it is worth further pursuit, please let me know. Thanks for your ears and eyes!

Formal Analysis:

Targeting: Yes.
Intent: Looks like an attempted portscan.
Techniques: Using random ports mirrored after the Debian bug database to search for unguarded ports.
History: This is a fairly new detect- history in the making!
Analysis: For some reason, possibly a new type of game, or more likely, a new type of exploit on typically unused ports. The reason it seems so suspicious is the amount of sources that this particular scan came from. It seems to correlate with those of another detect submitted earlier in April at a UMBC, similar sources, and a wide variety of the Debian bug report numbers in the scan.

Severity Rating:

Criticality: 3
Lethality: 2
System Countermeasures: 4
Network Countermeasures: 4
Total: -3

Last Updated: July 24th, 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