Global Information Assurance Certification Paper

*** Northcutt, Very interesting, Bill is making use of BlackIce while I get three to four messages a day from my students telling me why they can't detect anything. That has to be worth a few points! Good use of an analysis process. A little attention for formatting would improve clarity. 82 ***

Certification Exercise
Submitted by Bill Connett
4/06/2000

Unfortunately, I dont yet have sophisticated sensors in place. As a result
of the Sans IDIC course we are now working on developing security policies,
additional protection to our networks and putting IDS in place. All of
these traces are from BlackIce Defender on my work PC (using a program
called "ethereal" to format the traces). A big problem using BlackIce is
that the Detect traces are only "incoming" and you have to look in separate
logs if you want to try to find both incoming and outgoing packets -- not
nice at all. As you can see, other than being behind a switch, we are
pretty open to the world. We do have limited ingress and egress router
(routers not under our control) filtering in place to prevent address
spoofing but at this point that's about it. Hopefully we will be in much
better shape in the near future. I should add that I couldn't figure out
why so few people from the previous class did this assignment until I tried
to do it. For those who have been doing this as part of their jobs for
awhile it is clearly a piece of cake. For those of us who haven't and who
don't have IDS systems in place it is a pretty daunting exercise. I've
been struggling with this assignment for several days and am biting the
bullet today and will finish it before I sleep, if I sleep. :-)

Detect 1:

```
    No. Time      Source        Destination
Protocol Info

2 22:40:34.0920   mapper   xxx.xxx.146.169 TCP  0 > 111
[FIN, SYN]
Seq=3729129472 Ack=0 Win=512 Len=0
3 23:23:35.5820   mapper   xxx.xxx.146.169 TCP  0 > 143
[FIN, SYN] Seq=
508624896 Ack=0 Win=512 Len=0
4 00:06:03.4229   mapper   xxx.xxx.146.169 TCP  0 > 53
[FIN, SYN]
Seq=3679911936 Ack=0 Win=512 Len=0
```

This is a Syn,Fin port scan scanning Sun RPC, IMAP and DNS (Zone transfer because it is TCP instead of UDP) ports. The source port of 0 is not normal and is an indication of crafting and perhaps indicates the use of the program "linux portz 0.1" (Northcutt, Intrusion Analysts Handbook, p98) which sets the default source port to 0. Because this is logged on a machine behind several switches it is not possible to see the other addresses that are being scanned. The lag of several minutes between scans to this address is probably due to the sequential scanning of all of the ports of the same number in the Class C network. The sequence numbers also are not in order and may be crafted as well. Mapper was a single address but could not be located in whois.

Active Targeting: Yes
Intent: Mapping well known potentially vulnerable assets
Technique: Syn/Fin scan of RPC, DNS, and IMAP ports for potential revisit
Severity: (C4+L1)-(CM4+N1)= 0 Explanation- Desktop machine but with critical system access (C4),

attack not likely to succeed on this machine (L1), Running two
personal firewalls and current
patches (CM4), Network countermeasures weak N1)
Please Note: The
utility of the severity formula is limited in this set of
examples due to most of the detects being on the same machine and
network. If the sensor was able to detect exploits
on more than one machine I would be able to see a broader range of
exploits or more importantly exploits on a broader range of
equipment, then the formula results would vary and demonstrate a
greater degree of usefulness.
Source: BlackIce Detect

Detect 2:

```
 No. Time            Source                Destination           Protocol
Info

 54 05:45:55.7050   xxx.xxx.72.120  xxx.xxx.146.169 TCP
23 > 23 [ACK]
Seq=1675637262 Ack=1761221395 Win=1028 Len=0
 55 05:49:17.2159   xxx.xxx.72.120  xxx.xxx.146.169 TCP
4 > 80 [FIN,
SYN] Seq=963161181 Ack=95514272 Win=1028 Len=0
 56 05:49:17.3099   xxx.xxx.72.120  xxx.xxx.146.169 TCP
5 > 80 [PSH]
Seq=963161181 Ack=95514272 Win=1028 Len=0
 57 05:49:17.3489   xxx.xxx.72.120  xxx.xxx.146.169 TCP
5578 > 139
[SYN] Seq=1534610384 Ack=0 Win=512 Len=0
 58 05:49:20.0249   xxx.xxx.72.120  xxx.xxx.146.169 TCP
5578 > 139
[SYN] Seq=1534610384 Ack=0 Win=32120 Len=0
```

This is an interesting set of port probes to one dest address ports 23
(telnet), 80 (http), and 139 (Netbios). The interesting thing is the variety
of source ports and the variety of flags used. The sequence numbers in

pairs indicate crafting as do the ack numbers. The attempt to probe port 80
and 139 twice each indicates a less than stealth approach and may be some
indication of the talent of the prober. It isn't clear to me what the 3
minute gap is between the first and second probe. This could be waiting for
a response before running a script as the subsequent probes are pretty fast.

Active Targeting: Yes
Intent: Probing selected well known ports
Technique: Random anomalous flag sets
Severity: (C4+L1)-(CM4+N1)= 0 Low. Probably a script kiddie with limited
skills. No evidence of system compromise.
Source: BlackIce Detect

Detect 3:

```
6044 15:09:34.5640   xxx.xxx.146.253  xxx.xxx.146.169  TCP
33120 > 61 [FIN,
PSH, URG] Seq=0 Ack=0 Win=3072 Urg=0 Len=0
6045 15:09:34.5789   xxx.xxx.146.253  xxx.xxx.146.169  TCP
33120 > 101 [FIN,
PSH, URG] Seq=0 Ack=0 Win=3072 Urg=0 Len=0
6046 15:09:34.5989   xxx.xxx.146.253  xxx.xxx.146.169  TCP
33120 > 873 [FIN,
PSH, URG] Seq=0 Ack=0 Win=3072 Urg=0 Len=0
6047 15:09:34.6139   xxx.xxx.146.253  xxx.xxx.146.169  TCP
33120 > 370 [FIN,
PSH, URG] Seq=0 Ack=0 Win=3072 Urg=0 Len=0
6048 15:09:34.6339   xxx.xxx.146.253  xxx.xxx.146.169  TCP
33120 > 42 [FIN,
PSH, URG] Seq=0 Ack=0 Win=3072 Urg=0 Len=0
6049 15:09:34.6490   xxx.xxx.146.253  xxx.xxx.146.169  TCP
33120 > 465 [FIN,
PSH, URG] Seq=0 Ack=0 Win=3072 Urg=0 Len=0
6050 15:09:34.6649   xxx.xxx.146.253  xxx.xxx.146.169  TCP
33121 > 405 [FIN,
PSH, URG] Seq=0 Ack=0 Win=3072 Urg=0 Len=0
6051 15:09:34.6840   xxx.xxx.146.253  xxx.xxx.146.169  TCP
33121 > 816 [FIN,
```

PSH, URG] Seq=0 Ack=0 Win=3072 Urg=0 Len=0
6052 15:09:34.6990 xxx.xxx.146.253 xxx.xxx.146.169 TCP
33121 > 224 [FIN,
PSH, URG] Seq=0 Ack=0 Win=3072 Urg=0 Len=0
6053 15:09:34.7139 xxx.xxx.146.253 xxx.xxx.146.169 TCP
33121 > 802 [FIN,
PSH, URG] Seq=0 Ack=0 Win=3072 Urg=0 Len=0
6054 15:09:34.7339 xxx.xxx.146.253 xxx.xxx.146.169 TCP
33121 > 203 [FIN,
PSH, URG] Seq=0 Ack=0 Win=3072 Urg=0 Len=0

This is a contrived Detect. One of my co-workers scanned my PC with nmap
because we wanted to see what BlackIce would do and what the Detect would
look like. BlackIce identified this scan as the TCP xmas scan although not
all the flags are turned on.

Active Targeting: Yes for sure
Intent: Testing, non malicious hopefully
Technique: nmap with random dst port numbers and three anomalous flags set.
Seq numbers crafted and ttl also set arbitrarily to 62 (not shown)
Severity: (C4+L1)-(CM4+N1)= 0 Low
Source: BlackIce Detect

We also did a Syn Scan and a Null Scan. Nothing interesting to report as
far as differences between them except for flags. BlackIce did correctly
detect and identify them.

Detect 4:

15 11:01:44.6679 xxx.xxx.72.167 xxx.xxx.146.169 TCP
2882 > 1 [SYN]
Seq=3403969300 Ack=0 Win=32120 Len=0
16 11:01:56.6330 xxx.xxx.72.167 xxx.xxx.146.169 TCP
2879 > 21 [SYN]
Seq=3408068459 Ack=0 Win=32120 Len=0
17 11:02:20.6480 xxx.xxx.72.167 xxx.xxx.146.169 TCP
2876 > 111 [SYN]

```
Seq=3402534135 Ack=0 Win=32120 Len=0
18 11:03:08.6829   xxx.xxx.72.167  xxx.xxx.146.169  TCP
2873 > 23 [SYN]
Seq=3409999887 Ack=0 Win=32120 Len=0
19 11:03:08.6829   xxx.xxx.72.167  xxx.xxx.146.169  TCP
2883 > 515 [SYN]
Seq=3408648014 Ack=0 Win=32120 Len=0
20 11:04:44.7130   xxx.xxx.72.167  xxx.xxx.146.169  TCP
2882 > 1 [SYN]
Seq=3403969300 Ack=0 Win=32120 Len=0
21 11:06:44.7230   xxx.xxx.72.167  xxx.xxx.146.169  TCP
2879 > 21 [SYN]
Seq=3408068459 Ack=0 Win=32120 Len=0
22 11:08:44.7430   xxx.xxx.72.167  xxx.xxx.146.169  TCP
2876 > 111 [SYN]
Seq=3402534135 Ack=0 Win=32120 Len=0
23 11:10:44.7779   xxx.xxx.72.167  xxx.xxx.146.169  TCP
2873 > 23 [SYN]
Seq=3409999887 Ack=0 Win=32120 Len=0
24 11:10:44.7779   xxx.xxx.72.167  xxx.xxx.146.169  TCP
2883 > 515 [SYN]
Seq=3408648014 Ack=0 Win=32120 Len=0

Date: 2/22/2000
Active Targeting: Yes
Intent: A combination of OS fingerprint (port 1 - SGI) and
scan for open
ports -- particular concern
     is the RPC port (111).  Not sure what the importance
of 515 (printer
spooler port) is?
Technique: Standard Syn scan with crafted src ports and Seq
# (note matches
between them) and Ack=0 on all.
     Timing is erratic and may have something to do with
the stealthing
on the attacked machine on some
     ports causing the attacker to wait for a timeout on
that port before
moving on to the next one? Or
     interleaved scanning?
     Repeated scanning of same ports is low stealth - this
repeated
additional times
Severity: (C4+L1)-(CM4+N1)= 0 Low
Source: BlackIce Detect
```

Detect 5:

```
38 17:29:10.1380   xxx.xxx.218.150 xxx.xxx.146.169 TCP
20 > 1762 [SYN]
Seq=4001384687 Ack=0 Win=512 Len=0
39 17:29:56.2680   xxx.xxx.218.150 xxx.xxx.146.169 TCP
20 > 1769 [SYN]
Seq=936374699 Ack=0 Win=512 Len=0
40 17:29:56.2730   xxx.xxx.218.150 xxx.xxx.146.169 TCP
20 > 1769 [SYN]
Seq=936374699 Ack=0 Win=16060 Len=0
41 17:29:56.2779   xxx.xxx.218.150 xxx.xxx.146.169 TCP
20 > 1772 [SYN]
Seq=2517046452 Ack=0 Win=512 Len=0
42 17:29:56.2829   xxx.xxx.218.150 xxx.xxx.146.169 TCP
20 > 1772 [SYN]
Seq=2517046452 Ack=0 Win=16060 Len=0
43 17:29:56.2829   xxx.xxx.218.150 xxx.xxx.146.169 TCP
20 > 1772 [SYN]
Seq=2517046452 Ack=0 Win=16060 Len=0
44 17:29:56.2879   xxx.xxx.218.150 xxx.xxx.146.169 TCP
20 > 1769 [SYN]
Seq=936374699 Ack=0 Win=16060 Len=0
45 17:30:29.3839   xxx.xxx.218.150 xxx.xxx.146.169 TCP
20 > 1774 [SYN]
Seq=8415158 Ack=0 Win=512 Len=0
46 17:30:29.3880   xxx.xxx.218.150 xxx.xxx.146.169 TCP
20 > 1774 [SYN]
Seq=8415158 Ack=0 Win=16060 Len=0
47 17:30:29.3930   xxx.xxx.218.150 xxx.xxx.146.169 TCP
20 > 1774 [SYN]
Seq=8415158 Ack=0 Win=16060 Len=0
48 17:30:29.3980   xxx.xxx.218.150 xxx.xxx.146.169 TCP
20 > 1776 [SYN]
Seq=1907674164 Ack=0 Win=512
```

Date: 4/01/2000
Active Targeting: Yes, port mapping by web server (www.trinux.org)
Intent: Not clear what the intent of this is. It is not targeted at a
netbios port

or,as far as I know, a known trojan port. This occurs when you
attempt to see the list of
downloadable files.
Technique: Very fast scan of ephemeral ports in three with some variation.
Interesting that the window size
changes. Do sequence numbers indicate a very busy server?
Severity: (C4+L1)-(CM4+N1)=0 Low
Source: BlackIce Detect

Detect 6:

```
43 18:59:14.5049   xxx.xxx.126.41  xxx.xxx.146.169 TCP
4560 > 139 [SYN]
Seq=248663655 Ack=0 Win=8192 Len=0
44 19:00:21.1349   xxx.xxx.126.41  xxx.xxx.146.169 TCP
4560 > 139 [SYN]
Seq=248663655 Ack=0 Win=8192 Len=0
45 19:00:21.1390   xxx.xxx.126.41  xxx.xxx.146.169 TCP
4560 > 139 [SYN]
Seq=248663655 Ack=0 Win=8192 Len=0
46 19:00:21.1490   xxx.xxx.126.41  xxx.xxx.146.169 TCP
4560 > 139 [SYN]
Seq=248663655 Ack=0 Win=8192 Len=0
47 19:00:58.7100   xxx.xxx.126.41  xxx.xxx.146.169 TCP
4576 > 139 [SYN]
Seq=248663916 Ack=0 Win=8192 Len=0
48 23:57:58.6799   xxx.xxx.216.42  xxx.xxx.146.169 TCP
1986 > 139 [SYN]
Seq=1791183030 Ack=0 Win=32120 Len=0
49 23:58:01.6890   xxx.xxx.216.42  xxx.xxx.146.169 TCP
1986 > 139 [SYN]
Seq=1791183030 Ack=0 Win=32120 Len=0
```

Date: 3/08/2000
Active Targeting: Yes Netbios port probe from a residence hall
Intent: Two bored students putting off studying or one with two machines?
Technique: This looks like they were browsing the network neighborhood for
open shares. No packet crafting,

just poking around.
Severity: (C4+L1)-(CM4+N1)=0 Low
Source: BlackIce Detect

Detect 7:

264 06:37:38.8760 xxx.xxx.10.102 xxx.xxx.146.169 UDP
Source port: 60000
Destination port: 2140

Date: April 1, 2000 (happy April fools day present)
Active Targeting: Yes
Intent: A trojan (Deep Throat) Scan. Note from San website writeup on Deep
Throat: "Using outbound source port 60000,
the DT client sends UDP to port 2140. If successful in finding the
DT server (compromised box) the DT
client initiates a back door, BO-like remote session using ports
2140 and 3150"
Technique: A single packet to the dst address. Address is traceable to a UK
AOL address with 17 hops from the
victim. This is reasonably consistent with a ttl of 113 found on
the incoming Detect.
Severity: (C4+L1)-(CM4+N1)=0 Low -- no indication of client/server
connection or outgoing packets to http which is
characteristic of an infected machine. BlackIce would not detect
this but the second personal firewall (AtGuard)
running on this host would detect outgoing attempts.
Source: Human Scanning a BlackIce Trace -- BlackIce did not detect this
probe.
I noticed it as I looked through a trace that BlackIce had triggered
for a false positive UDP Scan

Detect 8:

84 13:46:33.4550 xxx.xxx.64.137 xxx.xxx.146.169
UDP Source
port: 19220 Destination port: 51200
85 13:46:33.4550 xxx.xxx.64.137 xxx.xxx.146.169
UDP Source
port: 19220 Destination port: 51200
86 13:46:33.4550 xxx.xxx.64.137 xxx.xxx.146.169
UDP Source
port: 19220 Destination port: 51200
87 13:46:33.4550 xxx.xxx.64.137 xxx.xxx.146.169
UDP Source
port: 19220 Destination port: 51200
88 13:46:33.4600 xxx.xxx.64.137 xxx.xxx.146.169
UDP Source
port: 19221 Destination port: 51201
89 13:46:36.4149 xxx.xxx.64.137 xxx.xxx.146.169
UDP Source
port: 19221 Destination port: 51201
90 13:47:26.7309 xxx.xxx.64.139 xxx.xxx.146.169
UDP Source
port: 18068 Destination port: 51200
91 13:47:26.7309 xxx.xxx.64.139 xxx.xxx.146.169
UDP Source
port: 18068 Destination port: 51200
92 13:47:26.8049 xxx.xxx.64.139 xxx.xxx.146.169
UDP Source
port: 18068 Destination port: 51200
93 13:47:26.8300 xxx.xxx.64.139 xxx.xxx.146.169
UDP Source
port: 18068 Destination port: 51200
94 13:47:26.8550 xxx.xxx.64.139 xxx.xxx.146.169
UDP Source
port: 18068 Destination port: 51200

Date:2/24/2000
Active Targeting: No
Intent: At first blush this looked really interesting. Two high UDP ports
getting pounded by lots of incoming packets. After looking at the
trojan lists and not finding any identified with these ports, I did a net
search and found a reference to the internet telephony program DialPad using

destination port 51200 and realized this was around the time I was
experimenting with DialPad! My assumption at this point is that this was one
of the dialpad hosts trying to respond to a request from my machine for a
connection. When I have a little time I will try to recreate this.
Technique: Normal function
Severity: (C4+L1)-(CM4+N1)=0 to None
Source: BlackIce UDP scan trace

Detect 9: taken from Sans -- I realized at the last minute that I had
duplicated two detects, uggg

Brian Friday from .edu has a close encounter with Brazil, I deleted about 60
of the attempts)
Mar 31 05:08:28 myhost portsentry[172]: attackalert:
Connect from host: 150.183.91.134/150.183.91.134
to TCP port: 111
Mar 31 10:36:38 myhost portsentry[173]: attackalert:
Connect from host: dgt048.cpunet.com.br/200.254.53.48
to UDP port: 111
Mar 31 10:38:36 myhost portsentry[173]: attackalert:
Connect from host: dgt048.cpunet.com.br/200.254.53.48
to UDP port: 111

Mar 31 12:34:44 myhost portsentry[173]: attackalert:
Connect from host: user-
33qs1hs.dialup.mindspring.com/199.174.6.60
to UDP port: 31337
Mar 31 12:35:10 myhost2 portsentry[8311]: attackalert:
Connect from host: user-
33qs1hs.dialup.mindspring.com/199.174.6.60
to UDP port: 31337

Date: 3/09/2000
Active Targeting: Yes
Intent: 3 RPC probes (port 111), two from Brazil and one self inflicted?
Weird (sometimes when I feel

completely inadequate a sense of humor is all I have to fall back
on). and two back orifice
probes.
Technique: Low stealth scan -- fast and twice on same port. 30 second
interval on the BO so might be
manual.
Severity: Don't have all the info but I would judge low on both
Source: Sans Web site

Detect 10:

59 18:06:15.9110 xxx.xxx.235.11 xxx.xxx.146.169 UDP
Source port: 1512
Destination port: 31337

Date: 3/27/2000
Active Targeting: Likely a broad scan
Intent: Scanning for Back Orifice (port 31337) trojan
Technique: Insufficient information. UDP TTL was 53 and backtrace to IP
address was to an existing dns.
Could have been (likely?) a spoofed address.
Severity: Low
Source: BlackIce Scan

Last Updated: May 28th, 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
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
Community SANS Boston SEC503	Boston, MA	Oct 09, 2017 - Oct 14, 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 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