Global Information Assurance Certification Paper

*** Northcutt, very solid analysis, you can see the evidence of home field advantage, did research brought several to ground and has a signature I hadn't seen the IP ID of zero. Heck, I will stick that in tomorrow's GIAC. This one will be in the running for top score, I'll stick a 95 on it and let the panel sort it out! 95 *

SANS 2000

Practical Exam

Kevin Peterson

Traces from March 29 – April 11, 2000

April 11, 2000

Detect 1

Apr 4 13:57:17 unix: securityalert: tcp if=hme1 from 152.1.192.116:1963 to a.b.90.1 on unserved port 6000

ANALYSIS

Active Targeting
Yes, these packets were sent to our firewall machine.
Intent
Someone was trying to connect to an X Server.
History
Researching this, I went back into our firewall logs to see if someone had connected to the host 152.1.192.116 from inside the firewall.

Apr 4 13:56:52 tn-gw[12260]: permit host=dharbour-pc.bbt.com/a.b.81.49 destination=152.1.192.116 port=23

Looks like someone connected to the machine 152.1.192.116 and attempted to display X back through the firewall. Since this is disallowed at the firewall communication was not possible.

Severity
Low. This appears to be an engineer who did not realize that X is not allowed through the firewall

Detect 2

[**] MISC-DNS-version-query [**]
04/06-08:22:54.626552 0:60:5C:F3:69:9B -> 8:0:20:A8:73:16 type:0x800 len:0x48 144.92.98.76:2839 -> a.b.90.1:53 UDP TTL:44 TOS:0x0 ID:20842 Len: 38

08:22:54.626552 0:60:5c:f3:69:9b 8:0:20:a8:73:16 0800 72: 144.92.98.76.2839 > a.b.90.1.53: 15501+ [b2&3=0x180] TXT CHAOS)? version.bind. (30) (ttl 44, id 20842)

```
  4500 003a 516a 0000 2c11 3005 905c 624c      E..:Qj..,.0..\bL
  c09a 5a01 0b17 0035 0026 875f 3c8d 0180      ..Z....5.&._<...
  0001 0000 0000 0000 0776 6572 7369 6f6e      .........version
  0462 696e 6400 0010 0003 .... .... ....      .bind.....
```

08:22:54.626552 0:60:5c:f3:69:9b 8:0:20:a8:73:16 ip 72: orson.lis.wisc.edu.2839 > a.b.com.domain: 15501+ [b2&3=0x180] TXT CHAOS)? version.bind. (30) (ttl 44, id 20842)

```
4500 003a 516a 0000 2c11 3005 905c 624c    E..:Qj..,0..\bL
c09a 5a01 0b17 0035 0026 875f 3c8d 0180    ..Z....5.&._<...
0001 0000 0000 0000 0776 6572 7369 6f6e    .........version
0462 696e 6400 0010 0003 .... .... ....    .bind.....
```

ANALYSIS

Active Targeting
Yes.
Intent
Information gathering about our DNS server
Technique
Single query to find out the version of named we are running.
History
No other activity from this IP or Class C address space in the messages logs on the firewall.
No activity in the WEB logs from this IP or Class C address space.
In the past couple of days I have been seeing a probe or two per day for this information. We have changed the setup of Bind so that it does not return any useful information when queried for its version number.
Severity
(5 + ?) - (4 + 4) = 2 -> -2; Depends on the security holes the version of bind "provides".

Medium. Since this was against our DNS server a heightened level of surveillance is in order.

Detect 3

```
09:26:59.450743 0:e0:16:98:ed:85 8:0:20:a8:73:16 ip 88: htp-0b.bbt.com.snmp > w.x.54.5.snmp-trap:
|30|2c|02|01|04|09C=SNMP_trap |a4|1cTrap(28) |06|09E:1770.3.1 |40|04[w.x.54.209]|02|01 coldStart|02|01 |43|010|30|00 (ttl 63, id
17090)
  4500 004a 42c2 0000 3f11 2957 c09a 5883    E..JB...?.)W..X.
  c067 3605 00a1 00a2 0036 0000 302c 0201    .g6......6..0,..
  0004 0953 4e4d 505f 7472 6170 a41c 0609    ...SNMP_trap....
  2b06 0104 018d 6a03 0140 04c0 6736 d102    +.....j..@..g6..
  0100 0201 0043 0100 3000 .... .... ....    .....C..0.
09:26:59.453618 0:e0:16:98:ed:85 8:0:20:a8:73:16 ip 111: htp-0b.bbt.com.snmp > w.x.54.5.snmp-trap: |30|43|02|01[version(1)!=0]
(ttl 63, id 17091)
  4500 0061 42c3 0000 3f11 293f c09a 5883 E..aB...?.)?..X.
  c067 3605 00a1 00a2 004d 0000 3043 0201    .g6......M..0C..
  0104 0953 4e4d 505f 7472 6170 a733 0201    ...SNMP_trap.3..
  0002 0100 0201 0030 2830 0d06 082b 0601    .......0(0...+..
  0201 0103 0043 0100 3017 060a 2b06 0106    .....C..0...+...
  0301 0104 0100 0609 2b06 0106 0301 0105    ........+.......
  01.. .... .... .... .... .... .... ....    .
```

ANALYSIS

Active Targeting
Yes. It was coming from mutliple sources from inside our network.
Intent
It ended up being misconfigured software. It could have been an attempt to gather information from the inside, similar to a trojan sending out information.
Technique
Used snmp traps.
History
These packets and many others like it were picked up after seeing log messages in our firewall about an inside machine trying to send snmp trap messages to a machine out on the internet. After investigating the destination address, I found that it belonged to a company that happened to be a supplier of some snmp code that we were using. After talking to the developer, he indicated that there were some default addresses in the code that he did not change because he didn't know what to change them to. I suggested 127.0.0.1.
Severity

Low(-1). The snmp traps were being stopped at the firewall so the information was not getting out into the wild.

Detect 4

A snippet of the log file:

Mar 29 13:19:57 unix: securityalert: tcp if=hme1 from w.x.y.z:1385 to a.b.90.1 on unserved port 1
Mar 29 13:19:57 unix: securityalert: tcp if=hme1 from w.x.y.z:1386 to a.b.90.1 on unserved port 2
Mar 29 13:19:57 unix: securityalert: tcp if=hme1 from w.x.y.z:1387 to a.b.90.1 on unserved port 3
Mar 29 13:19:57 unix: securityalert: tcp if=hme1 from w.x.y.z:1388 to a.b.90.1 on unserved port 5
Mar 29 13:19:57 unix: securityalert: tcp if=hme1 from w.x.y.z:1389 to a.b.90.1 on unserved port 7
Mar 29 13:19:57 unix: securityalert: tcp if=hme1 from w.x.y.z:1390 to a.b.90.1 on unserved port 9
Mar 29 13:19:57 unix: securityalert: tcp if=hme1 from w.x.y.z:1391 to a.b.90.1 on unserved port 11
Mar 29 13:19:57 unix: securityalert: tcp if=hme1 from w.x.y.z:1392 to a.b.90.1 on unserved port 13
Mar 29 13:19:57 unix: securityalert: tcp if=hme1 from w.x.y.z:1393 to a.b.90.1 on unserved port 15

ANALYSIS

Active Targeting
Yes.
Intent
To determine open ports on our firewall machine
Technique
Brute force port mapping attempt. Automated tool: timestamps close together.
History
No other activity had been seen from this IP. This is probably due to the fact that this is a dialup connection from one of the local ISP's.
Severity
Medium (1). An increased level of scrutiny is warranted here since this attack was on the firewall machine.

Detect 5

Apr 4 06:18:03 212.240.128.169:1427 -> 192.154.90.4:80 SYN **S*****
Apr 4 06:18:00 212.240.128.169:27960 -> 192.154.90.4:27960 NOACK 2*S*RP*U RESERVEDBITS

ANALYSIS

Active Targeting
Yes.
Intent
Apparently nothing hostile (if you believe the ISP).
History
This is one of the demon.net packets (which actually came from demon.net). They have a broken router which they are going to replace "tomorrow". It was interesting to actually catch one of these after talking about it at SANS 2000.
Severity
Low. This is a known problem coming from a known network.

Detect 6

[**] Source Port traffic [**]
04/11-07:15:21.367810 0:60:5C:F3:69:9B -> 8:0:20:A8:73:16 type:0x800 len:0x3C 167.216.248.60:53 -> 192.154.90.1:53 TCP
TTL:245 TOS:0x0 ID:0
S*A* Seq: 0x1908F84 Ack: 0x1908F83 Win: 0x1020
TCP Options => MSS: 556

07:15:21.367834 0:60:5c:f3:69:9b 8:0:20:a8:73:16 0800 60: 167.216.248.60.53 > a.b.90.1.53: S 26251140:26251140(0) ack 26251139 win 4128 <mss 556> (ttl 245,id 0)
4500 002c 0000 0000 f506 0b1b a7d8 f83c E..,.....<
c09a 5a01 0035 0035 0190 8f84 0190 8f83 ..Z..5.5.....

```
  6012 1020 ae3b 0000 0204 022c aae1 ....      `.. .;.....,..
07:15:21.369308 8:0:20:a8:73:16 0:60:5c:f3:69:9b 0800 60: a.b.90.1.53 > 167.216.248.60.53: R 26251139:26251139(0) win 0 (DF)
(ttl 245, id 61739)
  4500 0028 f12b 4000 f506 d9f2 c09a 5a01      E..(.+@.......Z.
  a7d8 f83c 0035 0035 0190 8f83 0000 0000      ...<.5.5........
  5004 0000 63b2 0000 5555 5555 5555 ....      P...c...UUUUUU
```

ANALYSIS

Active Targeting
Yes.
Intent
Spoofed source address possibility or is it some type of information gathering?
Technique
Looks like someone spoofed one of our addresses and Digital Island responded back to us with the second part of a three-way handshake.
The one piece of information that make me wonder about the spoofed source address is that the IP ID is zero. In the last day I have seen ten of these packets, each of which have an IP ID of zero.
History
I was running tcpdump and capturing all the packets going across the wire when this packet was flagged. I checked the log file for any other activity destined for this host of originating from this host and did not find any. Obviously, our host did not know anything about the connection and sent a Reset for the connection.
Severity
Medium: Since the firewall is performing a Reset on the connection, no information other than possible OS fingerprinting is being gathered. Will keep an eye on this since this is a new type of pattern I am seeing.

Detect 7

```
[**] SNMP public access [**]
04/01-01:10:38.898495 0:60:5C:F3:69:9B -> 8:0:20:A8:73:16 type:0x800 len:0x5A 193.82.112.220:1115 -> a.b.90.1:161 UDP
TTL:51 TOS:0x0 ID:17818
Len: 56

02:10:38.898495 0:60:5c:f3:69:9b 8:0:20:a8:73:16 0800 90: 193.82.112.220.1115 >
a.b.90.1.161: |30|82|00|2c|02|01|04|06|a1|82|00|1dGetNextRequest(29)|02|04|0
2|01|02|01|30|82|00|0d |30|82|00|09|06|05.1.3.6.1.2.1|05|00 (ttl 51, id 17818)
  4500 004c 459a 0000 3311 f53c c152 70dc      E..LE...3..<.Rp.
  c09a 5a01 045b 00a1 0038 c8cc 3082 002c      ..Z..[...8..0..,
  0201 0004 0670 7562 6c69 63a1 8200 1d02      .....public.....
  0466 575a 3c02 0100 0201 0030 8200 0d30      .fWZ<......0...
  8200 0906 052b 0601 0201 0500 .... ....      .....+.....
```

ANALYSIS

Active Targeting
Yes.
Intent
Information gathering.
Technique
Trying to use SNMP against our firewall to see if it will give up any secrets…They only tried the public community string so I suspect this was a passing attempt in a wider sweep.
History
I have not seen any other suspicious activity from this IP address in my log files.
Severity
Low(-1). The firewall does not provide snmp information.

Detect 8

```
[**] Happy 99 Virus [**]
04/11-09:25:04.589604 0:60:5C:F3:69:9B -> 8:0:20:A8:73:16 type:0x800 len:0x5EA
```

209.42.192.246:3733 -> 192.154.90.1:25 TCP TTL:121 TOS:0x0 ID:41393 DF
*****PA* Seq: 0x1F731864 Ack: 0x76591B6A Win: 0x20E0

09:25:04.589604 0:60:5c:f3:69:9b 8:0:20:a8:73:16 0800 1514: 209.42.192.246.3733
> 192.154.90.1.25: P 527636580:527638040(1460) ack 1985551210 win 8416 (DF) (ttl 121, id 41393)
4500 05dc a1b1 4000 7906 adad d12a c0f6 E.....@.y....*..
c09a 5a01 0e95 0019 1f73 1864 7659 1b6a ..Z.....s.dvY.j
<..stuff deleted..>
202d 3034 3030 0d0a 0d0a 6265 6769 6e20 -0400....begin
3634 3420 4861 7070 7939 392e 6578 650d 644 Happy99.exe.
0a4d 3335 4930 6060 2860 6060 6024 6060 .M35I0``(```$``

ANALYSIS

Active Targeting
Yes.
Intent
An attempt to infect machines with the Happy99 virus.
Technique
Using good old email. Hoping that the receiver would open it up.
History
This virus has been around for awhile and all the major virus software will protect the users. All machines here are running virus protection so this should not be an issue.
Severity
Low. Protections are in place so that this would not become an infestation problem.

Detect 9

Apr 10 10:07:23 unix: securityalert: udp if=hme1 from 216.59.125.58:35264 to a.b.90.1 on unserved port 500
Apr 10 10:07:24 unix: securityalert: udp if=hme1 from 216.59.125.58:35264 to a.b.90.1 on unserved port 500
Apr 10 10:07:26 unix: securityalert: udp if=hme1 from 216.59.125.58:35264 to a.b.90.1 on unserved port 500
Apr 10 10:07:30 unix: securityalert: udp if=hme1 from 216.59.125.58:35264 to a.b.90.1 on unserved port 500
Apr 10 10:07:38 unix: securityalert: udp if=hme1 from 216.59.125.58:35264 to a.b.90.1 on unserved port 500
Apr 10 10:07:54 unix: securityalert: udp if=hme1 from 216.59.125.58:35264 to a.b.90.1 on unserved port 500

ANALYSIS

Active Targeting
Yes.
Intent
Information gathering
Technique
A series of probes to see if our firewall was running the isakmp protocol. The time between probes is increasing 2x times for each probe.
History
The only other activity from this host that made it into the log files was a piece of mail sent in the middle of these probes.
The Internet Security Association & Key Management Protocol (ISAKMP) provides a framework for Internet key management and provides the specific protocol support for negotiation of security attributes. By itself, it does not establish session keys, however it can be used with various session key establishment protocols, such as Oakley, to provide a complete solution to Internet key management. The ISAKMP specification is also available in postscript

Severity
Low. It was stopped by the firewall.

Detect 10

[**] IIS-_vti_inf [**]
03/30-15:51:38.172519 0:60:5C:F3:69:9B -> 8:0:20:78:2E:56 type:0x800 len:0x12F 212.162.0.153:1059 -> a.b.90.4:80 TCP TTL:16 TOS:0x0 ID:1028 DF
*****PA* Seq: 0xECCDF7 Ack: 0xC525C00B Win: 0x2180

47 45 54 20 2F 5F 76 74 69 5F 69 6E 66 2E 68 74 GET /_vti_inf.ht
6D 6C 20 48 54 54 50 2F 31 2E 31 0D 0A 44 61 74 ml HTTP/1.1..Dat

ANALYSIS

Active Targeting
Yes.
Intent
To gain information about an IIS server
Technique
The user did a get on this file.
History
The _vti_inf.html file contains configuration information that the FrontPage Explorer and FrontPage Editor need to communicate with the FrontPage server extensions installed on this web server. One of the more interesting pieces of information is the version of the IIS server extensions in use on the server. This could provide valuable information to an intruder.
Severity
Low. Since we are not running an IIS server, this is not a problem for us.

Last Updated: July 21st, 2017

Upcoming Training

SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
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
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 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