Global Information Assurance Certification Paper

SANS 2000 INTRUSION DETECTION

PRACTICALS

By
Sunil K. Panda

June 9, 2000

CONVENTION

Severity is calculated by using the formula:

Severity = (Criticality + Lethality) – (system countermeasures + network countermeasures)

Where each component is rated on a scale of 0 (negligible) – 5 (highest).

DETECT 1

```
TIME STAMP          SRC IP.SRC PORT   DEST IP.DEST PORT    PROTO   LEN
09:51:13.789365 MYHOST.echo  > A.B.C.D.33452:     udp      64
09:51:13.975520 MYHOST.echo  > W.X.Y.Z.21960:     udp      64
09:51:14.129342 MYHOST.echo  > W.X.Y.Z.47148:     udp     512
09:51:14.386437 MYHOST.echo  > W.X.Y.Z.37124:     udp      64
09:51:14.512489 MYHOST.echo  > W.X.Y.Z.42901:     udp      64
09:51:14.758341 MYHOST.echo  > A.B.C.D.33252:     udp     512
09:51:15.889732 MYHOST.echo  > A.B.C.D.31263:     udp     512
09:51:16.031251 MYHOST.echo  > A.B.C.D.41373:     udp     512
09:51:16.573096 MYHOST.echo  > W.X.Y.Z.36391:     udp      64
```

1. SOURCE OF TRACE

Organization's internal network

2. DETECT WAS GENERATED BY

TCPDump. Please note that the IP addresses have been sanitized from the trace for security reasons.

3. PROBABILITY THE SOURCE ADDRESS WAS SPOOFED

Negligible. Organization's stateful firewalls have rules against spoofing.

4. DESCRIPTION OF ATTACK

It seems like there is a lot of response from MYHOST without any stimulus. Could be a

- misconfiguration of the network causing the sensor to see traffic in only one direction
- a backdoor connection
- a probable denial of service with A.B.C.D & W.X.Y.Z as victims

5. ATTACK MECHANISM

ECHO port on MYHOST sending chunks of data to higher ports on hosts A.B.C.D & W.X.Y.Z.

6. CORRELATIONS
This detect is well known and the probable reasons has been explained under the description of attack section. A call to the network-engineering group revealed an operator error, which caused a problem with the VLAN configuration for the switched network.

7. EVIDENCE OF ACTIVE TARGETING
The "all response-no stimulus" activity was never observed before.

8. SEVERITY
Zero or negative since the problem was due to a network misconfiguration.

9. DEFENSIVE RECOMMENDATIONS
A sensor with a single network interface, one that listens in promiscuous mode and also reports to a central analysis server can upset some switched network configuration. It's better to use two network interfaces – one for listening in the promiscuous mode and the other for communicating with the analysis server.

10. TEST QUESTION
The potential reason for the above trace could be:

a) UDP scan
b) VLAN misconfiguration of a switched network
c) Echo scan
d) Trace routing

Answer: b

DETECT 2

```
19:02:11.740314 local-university-host.1820 >
DMZ.MAILSERVER.111: S 7461746:7461746(0) win 8192 (DF)

19:02:14.231892 local-university-host.1821 >
DMZ.NAMESERVER.111: S 7492314:7492314(0) win 8192 (DF)

19:03:45.190321 local-university-host.1822 >
DMZ.MAILSERVER.111: S 7571902:7571902(0) win 8192 (DF)
```

```
19:03:50.601256 local-university-host.1823 >
DMZ.NAMESERVER.111: S 7580218:7580218(0) win 8192 (DF)

19:07:19.301681 local-university-host.1824 >
DMZ.MAILSERVER.111: S 7609034:7609034(0) win 8192 (DF)

19:07:27.701392 local-university-host.1825 >
DMZ.NAMESERVER.111: S 7628419:7628419(0) win 8192 (DF)
```

1. SOURCE OF TRACE

Organization's DMZ ID sensor

2. DETECT WAS GENERATED BY

TCPDump. Please note that the IP addresses have been sanitized from the trace for security reasons. Blank lines have been added for readability.

3. PROBABILITY THE SOURCE ADDRESS WAS SPOOFED

Highly probable. The IP was traced back to a local university, which believed in an open door policy.

4. DESCRIPTION OF ATTACK

TCP port 111 is the portmapper daemon, which handles the RPC services. There is a known vulnerability for exploiting unsecured portmappers, which affected several Sun Solaris systems in late 1997 and early 1998.

5. ATTACK MECHANISM

The attacker is probing the mail server and the name server in the DMZ for portmapper services. The probe is slow and is in pairs.

6. CORRELATIONS

This rpc.statd vulnerability is well known. The CERN warning can be found at http://www.cert.org/advisories/CA-97.26.statd.htm.

7. EVIDENCE OF ACTIVE TARGETING

The probing activity for port 111 in the DMZ servers had not been observed for almost 2 years.

8. SEVERITY

(Criticality + Lethality) - (System + Network) = Severity

(4 + 4) - (4 + 4) = **0**

9. DEFENSIVE RECOMMENDATIONS

These days, most UNIX operating systems have secure portmappers. If the UNIX box does not have a secure portmapper, get the fix from the vendor asap.

10. TEST QUESTION
The above trace could be:

a) Denial of service
b) Sequence number prediction
c) MTU determination
d) Portmapper vulnerability probing

Answer: d

DETECT 3

```
13:21:17.23 badguy.28901 > DMZ-NAMESERVER.23: S
5461790:5461790(0) ack 0
13:21:17.24 badguy.28902 > DMZ-NAMESERVER.23: SF
5461790:5461790(0)
13:21:17.27 badguy.28903 > DMZ-NAMESERVER.23: F
5461790:5461790(0)
13:21:17.29 badguy.28904 > DMZ-NAMESERVER.23: F
5461790:5461790(0) ack 0
13:21:17.32 badguy.28905 > DMZ-NAMESERVER.23: SF
5461790:5461790(0) ack 0
13:21:17.41 badguy.28906 > DMZ-NAMESERVER.23: S
5461790:5461790(0) ack 0
     4500 0028 cf76 0000 fc06 2f62 XXXX XXXX
     YYYY YYYY 70ea 0017 0053 571e 0000 0000
     50c2 1234 c4d5 0000 0000 0000 0000
13:21:17.49 badguy.28907 > DMZ-NAMESERVER.23: S
5461790:5461790(0) ack 0
```

1. SOURCE OF TRACE
Organization's DMZ ID sensor

2. DETECT WAS GENERATED BY
TCPDump. Please note that the IP addresses have been sanitized from the trace for security reasons. Time stamps have been shortened for readability.

3. PROBABILITY THE SOURCE ADDRESS WAS SPOOFED
Zero. Bad guy turned out to be a "script kiddie", whose friend worked in the information security group of a local company. Friend provided script to "script kiddie."

4. DESCRIPTION OF ATTACK
The attacker is most likely trying to determine the behavior of the TCP stack to illegal TCP flag bits. Different operating systems respond differently when probed with impossible packets. In this case, port 23 did not respond back due to restrictive firewall rulesets.

5. ATTACK MECHANISM
Fast scan to telnet port 23 of the DMZ name server by sending packets with illegal TCP flag bits combination. The sequence numbers are the same for every packet. Note that the source port increments by 1 for every packet sent.

6. CORRELATIONS
It can be observed from the trace that one of the packet has the two high-order bits, of the TCP flag (byte 13 of the TCP header), switched on along with the SYN flag (S). The two high-order bits are reserved flags and not used in normal network transmissions. This flag combination (S12) is pretty well known as the QueSO OS fingerprinting technique. The technique is to determine the OS by an a TCP/IP stack analysis.

7. EVIDENCE OF ACTIVE TARGETING
Lookup in the analysis database revealed prior probing to DMZ name server by prober.

8. SEVERITY
(Criticality + Lethality) - (System + Network) = Severity
(4 + 4) - (4 + 4) = **0**

9. DEFENSIVE RECOMMENDATIONS
Restrictive firewall rulesets should be put in place.

10. TEST QUESTION
The above trace could be an indication of:

e) Denial of service
f) Sequence number prediction
g) QueSO OS finger printing
h) NMAP OS finger printing

Answer: c

DETECT 4

```
21:10:21.145219 A.B.C.D:1945 -> W.X.Y.Z:80 TCP TTL:16 TOS:0x0 ID:1132
DF
*****PA* Seq: 0xECEDF7   Ack: 0xC525EE0B   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
```

1. SOURCE OF TRACE
Organization's internal ID sensor

2. DETECT WAS GENERATED BY
Snort. Certain fields have been removed/sanitized for readability and security reasons.

3. PROBABILITY THE SOURCE ADDRESS WAS SPOOFED
Zero. Both A.B.C.D and W.X.Y.Z belong to our organization's class B network.

4. DESCRIPTION OF ATTACK
Attacker seems to be probing host W.X.Y.Z for information about IIS server.

5. ATTACK MECHANISM
Attacker did a GET on the file "_vti_inf.html"

6. CORRELATIONS
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. The attacker can get information about the version of the IIS server extensions in use on the server. This could help the attacker prepare for his attack. Attacker was an internal employee working with the organization's ethical hacking team.

7. EVIDENCE OF ACTIVE TARGETING
No.

8. SEVERITY
Zero. IIS server did not exist on host W.X.Y.Z

9. DEFENSIVE RECOMMENDATIONS
None

10. TEST QUESTION

The above trace shows the following

a) Attempt to access information about a Netscape webserver
b) Attemp to access information about a Microsoft IIS server
c) CGI exploit
d) Password exploit

Answer: b

DETECT 5

```
04/19-16:10:27.721824 SCANNER:4072 -> HOME-FIREWALL:1243
TCP TTL:114 TOS:0x0 ID:32524  DF
S***** Seq: 0xBC6DFD   Ack: 0x0   Win: 0x2000
TCP Options => MSS: 536 NOP NOP SackOK

04/19-16:10:28.517284 SCANNER:4073 -> HOME-FIREWALL:1999
TCP TTL:114 TOS:0x0 ID:32525  DF
S***** Seq: 0xBC6DFD   Ack: 0x0   Win: 0x2000
TCP Options => MSS: 536 NOP NOP SackOK
```

1. SOURCE OF TRACE
Home network.

2. DETECT WAS GENERATED BY
This trace was generated by Snort running on a firewall (non-windows platform on a home network) connected to a cable modem. The home network has been assigned a single static IP address and all the computers behind the firewall are NAT'ed (Network Address Translated) and are not Internet routable.

3. PROBABILITY THE SOURCE ADDRESS WAS SPOOFED
A WHOIS lookup revealed that the packet originated from a small ISP in Germany.

4. DESCRIPTION OF ATTACK
This appears to be a scanning (could be random or in order) in pairs (port 1243 & port 1999) for previously compromised systems. The attacker is searching for the existence of the well known backdoor trojan called SubSeven (aka Sub7 or Backdoor_G).

5. ATTACK MECHANISM
The attack could be either be on a random group of IP addresses or in order. The attacker is scanning for two SubSeven ports on the hosts.

6. CORRELATIONS
SubSeven (aka Sub7 or Backdoor_G) currently affects Windows 95/98 PC's and can be a bit tricky to remove. This is because the server portion can be configured to rerun itself automatically from any of four places each time the system has been rebooted. TCP Ports **6711** and **6776** are used by default but there's a third TCP port, which is the port used in the establishment of the connection between the "client" and "server". This third TCP port can be configured to be anything, although it's commonly seen as TCP port **1243** or TCP port **1999**.

7. EVIDENCE OF ACTIVE TARGETING
There was no previous history of targeting. It was a one-time affair.

8. SEVERITY
Zero. The home network does not have any Windows machines.

9. DEFENSIVE RECOMMENDATIONS
Check for existence of SubSeven server binaries and registry entries on Windows PC. Refer to Bugtraq for more details.

10. TEST QUESTION
The above trace is a scan for

a) Back Orifice
b) SubSeven Windows Trojan
c) PC Anywhere
d) Shivka Burka Trojan

Answer: b

DETECT 6

```
02/23-11:39:31.521927 SCANNER:3021 -> HOME-FIREWALL:10520
TCP TTL:32 TOS:0x0 ID:4235  DF
S***** Seq: 0xF76DB6   Ack: 0x0   Win: 0x2000

02/23-11:39:31.931045 SCANNER:3022 -> HOME-FIREWALL:10521
TCP TTL:32 TOS:0x0 ID:4236  DF
S***** Seq: 0xF76DB6   Ack: 0x0   Win: 0x2000
```

1. SOURCE OF TRACE

Home network mentioned in detect 5.

2. DETECT WAS GENERATED BY

This trace was generated by Snort running on a firewall (non-windows platform on a home network) connected to a cable modem. The home network has been assigned a single static IP address and all the computers behind the firewall are NAT'ed (Network Address Translated) and are not Internet routable.

3. PROBABILITY THE SOURCE ADDRESS WAS SPOOFED

A WHOIS lookup revealed that the packet originated from an IP address, which belonged to a respectable couple who used a cable modem (with a static IP address) but did not deploy a firewall !! They also used the cable modem rather infrequently.

4. DESCRIPTION OF ATTACK

The attacker is doing a fast SYN scan for ports 10520 and 10521. The IP addresses being scanned could be either in random order or in sequence.

5. ATTACK MECHANISM

The attacker could be using an automated script. The IP identifier and the source port get incremented by one.

6. CORRELATIONS

A lookup for port 10520 revealed it to be the default port for the Windows backdoor trojan - Acid Shivers.

7. EVIDENCE OF ACTIVE TARGETING

There was no previous history of targeting. It was a one-time affair.

8. SEVERITY

Zero. The home network does not have any Windows machines.

9. DEFENSIVE RECOMMENDATIONS

Check for existence of Acid Shivers server binaries and registry entries on Windows PC. Refer to Bugtraq for more details.

10. TEST QUESTION
The above trace could be

a) Back Orifice
b) Syn Flood
c) OS Determination
d) Acid Shivers Trojan

Answer: d

DETECT 7

```
19:31:24.020615 HOST.ISP.com.2012 > friend.com.161: GetRequest(11)
19:31:25.173218 HOST.ISP.com.2013 > friend.com.161: GetRequest(11)
19:31:26.542318 HOST.ISP.com.2014 > friend.com.161: GetRequest(11)
19:31:27.256197 HOST.ISP.com.2015 > friend.com.161: GetRequest(11)
19:31:28.239106 HOST.ISP.com.2016 > friend.com.161: GetRequest(11)
19:31:29.976314 HOST.ISP.com.2017 > friend.com.161: GetRequest(11)
19:31:30.753012 HOST.ISP.com.2018 > friend.com.161: GetRequest(11)
```

and more

1. SOURCE OF TRACE
The trace was obtained from a friend's home business network.

2. DETECT WAS GENERATED BY
TCPDump. Please note that the IP addresses have been sanitized from the trace for security reasons.

3. PROBABILITY THE SOURCE ADDRESS WAS SPOOFED
Zero. It was from a local ISP.

4. DESCRIPTION OF ATTACK
A string of SNMP requests to a specific address on my friend's home business network.

5. ATTACK MECHANISM

A series of crafted or scripted packets, about one per second, with the source port incrementing by one for every packet that is sent.

6. CORRELATIONS
A local ISP server doing "information gathering" from "customers" – note that the request was not directed at the broadcast address but rather a host on the home business network

7. EVIDENCE OF ACTIVE TARGETING
Yes. A string of SNMP traffic to a specific address on the home business network.

8. SEVERITY
(Criticality + Lethality) - (System + Network) = Severity
(2 + 2) - (4 + 4) = **-4**

9. DEFENSIVE RECOMMENDATIONS
Block SNMP requests at the firewall or filtering router. Make sure to use a unique SNMP community string rather than using – public, private or organization name.

10. TEST QUESTION
The above trace can be attributed to

a) SNMP exploit
b) Information gathering by ISP
c) Denial of service
d) Back Orifice

Answer: b

DETECT 8

```
21:01:16 ISPHOST.27710 > DMZ-NAMESERVER.113: S 350312783: 350312783 (0)
21:01:16 ISPHOST.29320 > DMZ-NAMESERVER.113: S 468192560: 458192560 (0)
21:01:16 ISPHOST.4035  > DMZ-NAMESERVER.113: S 791064231: 791064231 (0)
21:01:17 ISPHOST.31023 > DMZ-NAMESERVER.113: S 394671803: 394671803 (0)
21:01:17 ISPHOST.23109 > DMZ-NAMESERVER.113: S 192740192: 192740192 (0)
21:01:17 ISPHOST.32453 > DMZ-NAMESERVER.113: S 891668205: 891668205 (0)
21:01:18 ISPHOST.31459 > DMZ-NAMESERVER.113: S 139240123: 139240123 (0)
21:01:18 ISPHOST.3672  > DMZ-NAMESERVER.113: S 219166685: 219166685 (0)
```
and more

1. SOURCE OF TRACE
Organization's DMZ ID sensor

2. DETECT WAS GENERATED BY
TCPDump. Please note that the IP addresses have been sanitized from the trace for security reasons. Time stamps have been shortened for readability.

3. PROBABILITY THE SOURCE ADDRESS WAS SPOOFED
Source IP address belonged to a local ISP provider.

4. DESCRIPTION OF ATTACK
Fast scan (of 2 to 3 packets per second) to port 113 of the DMZ name server. Port 113 is the identd service port, which provide a means to identify the owner of a particular TCP connection.

5. ATTACK MECHANISM
Automated script doing a rapid SYN scan of DMZ name server for port 113. Port 113 is the identd port.

6. CORRELATIONS
The ident service defined in RFCs 931 and 1413 provides a means to determine the identity of the owner of a particular TCP connection. Given a TCP port number, the identd daemon will return a character string, which identifies the owner of that connection on the host. The scanning process can be useful to determine who is running daemons on high ports, which is a security risk. It can also be used to determine misconfigurations - httpd service running as root, etc. The process is well known as the reverse identd scanning.

7. EVIDENCE OF ACTIVE TARGETING
Yes. A series of SYN requests to port 113.

8. SEVERITY
In this case, the identd service is not running on the DMZ name server.

(Criticality + Lethality) - (System + Network) = Severity
(4 + 4) - (4 + 4) = **0**

9. DEFENSIVE RECOMMENDATIONS
The "identd" service should be turned of on hosts (especially DMZ hosts) that do not specifically need it.

10. TEST QUESTION
The above trace is

a) SYN Flood
b) DNS buffer overflow
c) Reverse Identd scanning
d) Portmapper scanning

Answer: c

DETECT 9

```
18:47:31 SCANNER:13100 -> HOME-FIREWALL:1
SF**** Seq: 0x0   Ack: 0x0

18:47:31 SCANNER:13101 -> HOME-FIREWALL:7
SF**** Seq: 0x0   Ack: 0x0

18:47:31 SCANNER:13102 -> HOME-FIREWALL:9
SF**** Seq: 0x0   Ack: 0x0

18:47:32 SCANNER:13103 -> HOME-FIREWALL:13
18:47:32 SCANNER:13104 -> HOME-FIREWALL:17
18:47:33 SCANNER:13105 -> HOME-FIREWALL:19
18:47:33 SCANNER:13106 -> HOME-FIREWALL:21
18:47:33 SCANNER:13107 -> HOME-FIREWALL:22
18:47:34 SCANNER:13108 -> HOME-FIREWALL:23
18:47:34 SCANNER:13109 -> HOME-FIREWALL:25
```
and more

1. SOURCE OF TRACE

Home network mentioned in detect 5.

2. DETECT WAS GENERATED BY

This trace was generated by Snort running on a firewall (non-windows platform on a home network) connected to a cable modem. The home network has been assigned a single static IP address and all the computers behind the firewall are NAT'ed (Network Address Translated) and are not Internet routable.

3. PROBABILITY THE SOURCE ADDRESS WAS SPOOFED

Source IP address belonged to a neighbouring state ISP provider.

4. DESCRIPTION OF ATTACK

A rapid SYN/FIN scan to all well-known service ports on the home network firewall.

5. ATTACK MECHANISM

A rapid scan (2 to 3 packets per second) to all well-known service ports on the firewall. The SYN/FIN flags have been set. Both the sequence and acknowledgement numbers have been set to zero.

6. CORRELATIONS
The intruder is trying to determine the open ports on the firewall. The SYN/FIN flags have been set with the intention of escaping detection.

7. EVIDENCE OF ACTIVE TARGETING
Yes.

8. SEVERITY
(Criticality + Lethality) - (System + Network) = Severity
(4 + 4) - (4 + 4) = **0**

9. DEFENSIVE RECOMMENDATIONS
Tighten firewall rulesets. Drop packets silently.

10. TEST QUESTION
The above trace can be attributed to

a) Denial of service
b) VPN misconfiguration
c) SYN/FIN scan
d) OS finger printing

Answer: c

DETECT 10

```
12/05-23:12:16.101629 SCANNER:31337 -> HOME-FIREWALL:31337
TCP TTL:40 TOS:0x0 ID:10023  DF
SFRP** Seq: 0x0   Ack: 0x0   Win: 0x1560

12/05-23:12:16.961995 SCANNER:31338 -> HOME-FIREWALL:31338
TCP TTL:40 TOS:0x0 ID:10024  DF
SFRP** Seq: 0x0   Ack: 0x0   Win: 0x1560
```

1. SOURCE OF TRACE
The home network mentioned in detect 5.

2. DETECT WAS GENERATED BY

This trace was generated by Snort running on a firewall (non-windows platform on a home network) connected to a cable modem. The home network has been assigned a single static IP address and all the computers behind the firewall are NAT'ed (Network Address Translated) and are not Internet routable.

3. PROBABILITY THE SOURCE ADDRESS WAS SPOOFED
Source IP address belonged to a local ISP provider.

4. DESCRIPTION OF ATTACK
This is an interesting trace because the attacker seems to be scanning the host for ports 31337 (Back Orifice) and 31338 (Deep Back Orifice) with a source port of the 31337 and 31338. The SYN/FIN/RESET/PUSH flags seem to be turned on. Also both the sequence and acknowledgement numbers have been set to zero.

5. ATTACK MECHANISM
A rapid scan for Back Orifice trojans with SFRP flags turned on. Looks like an automated script (nmap?). The attacker is definitely not trying a stealthy approach.

6. CORRELATIONS
The attacker is probably trying to accomplish three things – a) search for Back Orifice, b) determine the OS type & c) Predict the sequence numbers.

Port 31337 and 31338 scan is for finding back orifice. SFRP illegal TCP flags combination is for determining OS type because different OS's respond differently to illegal TCP flags. Doing a TCP stack analysis will help an intruder determine the OS type as well as predict the sequence numbers.

7. EVIDENCE OF ACTIVE TARGETING
No prior scanning history.

8. SEVERITY
Back Orifice is not running. All patches have been applied to firewall. Sequence number generation is truly random.
(Criticality + Lethality) - (System + Network) = Severity
(4 + 4) - (4 + 4) = **0**

9. DEFENSIVE RECOMMENDATIONS
Check host for services on port 31337 and 31338.

10. TEST QUESTION
The above trace could be
a) Search for Back Orifice
b) OS finger printing

c) Sequence number prediction
d) All of the above

Answer: d