SCAN OF THE MONTH 28

HAPPYCACTUS <HAPPYCACTUS@VENE.WS>

1. 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.

2. Forensic Environment and set-up

"Ethereal" was the main tool used for this analysis. Many other tools was used from the standard linux installation.

The system where the analysis was performed is a standard GNU/Debian linux woody, running on a i386 platform. A unprivileged account was created for that task.

The logs was downloaded from the main honeynet.org site, and checked with the published md5 sums:

```
[forensic@braverabbit] scan28$ md5sum day?.log.gz
   79e5871791542c8f38dd9cee2b2bc317 day1.log.gz
   af8ab95f41530fe3561b506b422ed636 day3.log.gz
```

3. The attack analysis

The very first things we did, was to search for a tcp packet with SYN flag originating from the honeypot, since we can easily imagine that no tcp connection should start from the honeypot (except for the DNS query) unless the system is compromised. So we performed the following query to the "frame search" menu in ethereal:

```
(ip.src == 192.168.100.28) && (tcp.flags == 0x02)
```

We found the frame number 620, where a FTP session was initiated by the honeypot, directed to the 62.611.66.16 system (—).

Since there are no reasons for the system to initiate such a communication, we imagine that the system was compromised, so we searched backward for the reason; the previous frame (619) is part of a telnet session directed to the port 1524 on the honeypot.

We searched backward many times for other tcp packet with syn flag set, from the internet directed to the honeypot; we found the frame 561, where the remote system 61.219.90.180 connected to the honeypot port 6112. Immediately after the completion of the three-way handshake, that system tried a connection (failed) with the tcp port 1524 (frame 564), and after this one, again with the 6112 (frame 566).

Following the tcp stream with ethereal, we can see that with this tcp session the remote system exploited the vulnerable CDE with a buffer overflow that executed the following shell code:

```
/bin/ksh -c echo "ingreslock stream tcp nowait root /bi n/sh sh
-i">/tmp/x;/usr/sbin/inetd -s /tmp/x;sleep 10;/bin/rm -f /tmp/x
```

it opens a backdoor on the ingreslock (1524/tcp) port that execute on a connection a shell with root privileges.

So the following telnet session on the port 1524/tcp is a root shell that the attacker used to complete the intrusion.

We can follow the stream that starts on the frame 588.

By decoding that stream, we can retrieve the tools downloaded by the attacker on the honeypot: wget and some other tools (sol.tar.gz). We used dd on the saved tcp stream.

The compromised machine was used, on the following days, as a bouncer for some irc sessions (psyBNC), and to launch a DDoS against 195.130.233.20 (javairc.tiscali.it). The DDoS was a mix of a TCP SYN flood, ping flood, UDP flood a other malformed packets flood. before the beginning of the DDoS, we can see four similar packets:

```
0000 08 00 20 d1 76 19 00 07 ec b2 d0 0a 08 00 45 00 .. .v... ......E.
   0010 04 14 ed 74 40 00 ed 01 ab cd 3d 86 03 0b c0 a8 ...t@...
..=.....
   0020 64 1c 00 00 2c 9a 26 ce 00 00 00 00 00 00 00 00 d...,.&.
........
   0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ........ ........
   0040 00 00 c3 82 e9 14 00 00 00 00 00 00 00 00 00 00 ........ ........
   0050 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ........ ........
   0060 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ........ ........
```

Note the four bytes at the offset 0x42 (c3 82 e9 14), decoded to a ip address we obtain the target of the DDoS (195. 130.233.20)

4. Answers to questions

4.1. What is the operating system of the honeypot? How did you determine that? (see day1). The honeypot runs a

```
SunOS zoberius 5.8 Generic_108528-09 sun4u sparc SUNW,Ultra-
5_10
```

as we can see from the telnet session on the honeypot port 1524/tcp. The same string can be found on day3, in the syslogd stream following a reboot of the machine, probably performed by the attacker as command in the ssh session (the backdoor was bound to port 5001 and downloaded in the sol.tar.gz archive downloaded from the xoom free page site).

4.2. **How did the attacker(s) break into the system? (see day1).** He exploited a buffer overflow-vulnerable cde server running on port 6112/TCP. http://www.cert.org/advisories/CA-2001-31.html

After that, the attacker installed a rootkit, a bouncer, and joined the compromised machine 'Stacheldraht' zombies network.

By analizing the sol.tar.gz 'setup' script, we can find that the installation at a certain point failed, and not all the tools was downloaded to the honeypot; on day3 the attacker completed the installation by connecting to the backdoor ssh server bound to 5001/tcp port.

4.3. **Which systems were used in this attack, and how?(see day1).** For the compromisation of the system, the attacker used another, probably compromised, machine (61.219.90.180).

To download the tool he used to cover his tracks and bind the server with the irc botnet, he used an ftp server (62.211.66.16 - services.xoom.virgilio.it), a free service, and an http server (62.211.66.53 - xoom.virgilio.it).

When connecting with the irc net, the attacker used the installed bouncer (psyBNC) from the ip 80.117.14.22 (host222-14.pool80117.interbusiness.it). It is most probably the attacker's ip.

4.4. **Create a diagram that demonstrates the sequences involved in the attack. (see day1).**

4.5. **What is the purpose/reason of the ICMP packets with 'skillz' in them? (see day1).** With sol.tar.gz, the 'Stacheldraht' DDoS zombie was installed on the system.

As we can see in the iss advisory (http://www.iss.net/issEn/delivery/xforce/alertdetail.jsp?id=advise43), this tool uses some icmp packets (icmp-echo-reply) to syncronize the 'agent' machines (zombies) with the master machine. The use of the ICMP protocol instead of the normal UDP or TCP stream, permit the communication inside some firewalled LANs, and some NIDS cannot detect this communication.

Stacheldraht uses the payload and the IDs of the icmp-echo-reply to send queries, commands and hearthbeat signals. The 'skillz' payload is a requests to the master of a hearthbeat reply, that contains the 'ficken' string on the payload.

4.6. **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).** He used a tunnel for the IPv6 net 6bone.net, ovet the normal IPv4 network. It was installed on day3, maybe because during day1 the installation script failed and the rootkit wasn't installed properly.

4.7. **Can you identify the nationality of the attacker? (see day3) What is the operating system of the honeypot? How did you determine that? (see day1).** The attacker is an italian script kiddy, from the interbusinnes.it network. His nick on the irc network is *'dj* bobz', he is from Paestum, Naples. We can determine that from many sources:

- In the irc sessions, the attacker directely connected to the honeypot, ignoring the presence of a sniffer on the system. When attacking the vulnerable system he never connected directely, instead he used a proxy or another compromised machine, thinking that the communication was not monitored.
- Following the irc conversation, he spoke italian or an italian dialect from the south regions (Naples).
- While authenticating on the irc bouncer, he used the password 'fargetta', the name of an italian DJ.
- Following the irc conversation with another used, we read:

  ```
  :|AnDr34z|!~OmBr4@vhost.irc6.server.tb.ngnet.it PRIVMSG #bobz :bob
  :|AnDr34z|!~OmBr4@vhost.irc6.server.tb.ngnet.it PRIVMSG #bobz :ma tu di dove sei ,)
  :|AnDr34z|!~OmBr4@vhost.irc6.server.tb.ngnet.it PRIVMSG #bobz :che non ho ancora capito
  :bobz`!~ahaa@irc6.vhost.la PRIVMSG #bobz :Salerno
  :bobz`!~ahaa@irc6.vhost.la PRIVMSG #bobz :Salerno
  :bobz`!~ahaa@irc6.vhost.la PRIVMSG #bobz :PAESTUM
  ```

  (AnDr34a: bob, where are you from, that I did not understand? bobz: Salerno, Paestum)
- Chanses are that the ip 80.117.14.22 is the real attacker's IP. It is owned by the italian ISP interbusiness.

5. Bonus Questions

5.1. **What are the implications of using the unusual IP protocol to the Intrusion Detection industry?** Many NIDS did not yet support the IPv6 protocol, so they are not able to decode/detect many activities.

5.2. **What tools exist that can decode this protocol?** Ethereal, tcpdump