Honeynet Scan of the month #29

Guy Van Sanden
Thu Sep 25 2003

Table of Contents

Guy Van Sanden <guy.van.sanden@pandora.be>

1. Summary

On August 10 2003, the host sbm79 was taken over by an attacker.
He (or they) entered the server via the Apache/OpenSSL server process. After hacking into the box, an IRC bouncer, a password sniffer and a backdoor were installed. The attacker seemed to have gathered account names and passwords.

2. Tools used

The main analysis was done on a Mandrake 9.1 GNU/Linux system. Some parts were done on a FreeBSD 5.0 system.

2.1. Tool list

- VMWare Workstation 4.0.2
- Autopsy and Sleuth http://www.sleuthkit.org
- FIRE 0.4a (Forensics Toolkit) http://fire.dmzs.com
- Knoppix bootable CD 3.2 http://www.knoppix.org
- Clam Antivirus and McAfee Antivirus on FreeBSD

3. Preperation

Download the file using wget and check the signatures:
1db2459dd36ac98fdcf59d1abac0f776 linux-suspended-md5s.gz
d95a8c351e048bd7d5596d6fc49b6d72 linux-suspended.tar.bz2
The signatures of downloaded files match.

Prepare the image for VMWare

```
# bunzip2 linux-suspended.tar.bz2
# tar -xvf linux-suspended.tar
linux-2/
linux-2/linux.vmdk
linux-2/linux.vmx
linux-2/vmware.log
linux-2/nvram
linux-2/linux.vmss
linux-2/linux.png
```

3.1. Precautions

I guessed the IP of the hacked virtual machine to be 192.168.1.79 (using strings and others).
As a precaution, I'm dropping packets originating from that address on my firewall.
Ideally I should run it on an isolated system, but that is not available to me at this time.

4. Questions

4.1. Describe the process you used to confirm that the live host was compromised while reducing the impact to the running system and minimizing your trust in the system.

Since the host might be compromised, it is best to put as little trust as possible in the

installed system, therefor, I used the staticly-linked binaries on the FIRE cd as much as possible. The output of commands was saved to floppy.

The first thing I did is to check for the presence of a rootkit using the chkrootkit script on the FIRE cd (it uses the secure binaries).
The complete output is in the chkrootkit.txt file.

```
Checking `ifconfig'... INFECTED
Checking `ls'... INFECTED
Checking `netstat'... INFECTED
Checking `ps'... INFECTED
Checking `top'... INFECTED
Checking `bindshell'... INFECTED (PORTS:  3049)
Checking `lkm'... You have     4 process hidden for ps command
Warning: Possible LKM Trojan installed
Checking `sniffer'...
eth0 is PROMISC
Checking `z2'...
```

Chkrootkit reports several key system components to be infected, and eth0 is in promiscues mode (which makes me suspect the presence of a sniffer).

The modifications of the files becomes obvious when comparing the output of the local binaries like ps with the 'safe' ones on the CD. Clearly, some processes and files are hidden from the systems administrators.

These processes where hidden by the ps binary on the system:

```
USER       PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root         5  0.0  0.0      0     0 ?        SW   Aug09   0:00 [kswapd]
root       845  0.0  0.0   3260     4 ?        S    Aug09   0:00 smbd -D
root      3137  0.0  0.0   1900    60 ?        S    13:33   0:04 smbd -D
root      3153  0.0  0.0   1664    16 ?        S    13:33   0:00 (swapd)
```

At this point it is safe to assume that the system is indeed hacked.
I proceeded to collect some information of the live-system (using my secure binaries and an incident-response script on the FIRE CD).
After that, I powered off the system without doing a shutdown, it is possible that the shutdown routine is rigged to destroy evidence.

4.2. Explain the impact that your actions had on the running system.

My actions had little impact on the system beyond what any use of it would have done.
I mounted the CDROM which caused mount tabs to be altered and possibly some modules to load if they hadn't been used before, this was however essential to establish a secure environment on an untrusted system.
I did not copy any files or binaries to the system, and I did not modify any files on it.

4.3. List the PID(s) of the process(es) that had a suspect port(s) open (i.e. non Red Hat 7.2 default ports).

There are a number of non default ports open, in addition a number of 'normal' ports where openend by a process or more processes that do not belong on that particular port.

Ports 80 and 443 (http and https) are opened by several processes that do not belong

there.
Additionally there are some 'highports' open (LISTEN) that shouldn't be there.
The system had these ports open:

```
identd     677 ident    4u  IPv4    836       TCP *:113 (LISTEN)
identd     685 ident    4u  IPv4    836       TCP *:113 (LISTEN)
identd     686 ident    4u  IPv4    836       TCP *:113 (LISTEN)
identd     695 ident    4u  IPv4    836       TCP *:113 (LISTEN)
identd     696 ident    4u  IPv4    836       TCP *:113 (LISTEN)
sshd       699  root    3u  IPv4    860       TCP *:22 (LISTEN)
xinetd     732  root    3u  IPv4    881       TCP *:79 (LISTEN)
xinetd     732  root    4u  IPv4    882       TCP *:23 (LISTEN)
xinetd     732  root    5u  IPv4    883       TCP *:21 (LISTEN)
sendmail   759  root    4u  IPv4    925       TCP 127.0.0.1:25 (LISTEN)
smbd       845  root    9u  IPv4   1015       TCP *:139 (LISTEN)
nmbd       850  root    6u  IPv4   1025       UDP *:137
nmbd       850  root    7u  IPv4   1026       UDP *:138
nmbd       850  root    8u  IPv4   1028       UDP 192.168.1.79:137
nmbd       850  root    9u  IPv4   1029       UDP 192.168.1.79:138
smbd      3137  root    6u  IPv4   4571       TCP *:2003 (LISTEN)
smbd      3137  root   16u  IPv4    976       TCP *:443 (LISTEN)
smbd      3137  root   17u  IPv4    977       TCP *:80 (LISTEN)
(swapd)   3153  root   16u  IPv4    976       TCP *:443 (LISTEN)
(swapd)   3153  root   17u  IPv4    977       TCP *:80 (LISTEN)
initd    15119  root    3u  IPv4  15617       TCP *:65336 (LISTEN)
initd    15119  root    5u  IPv4  15619       TCP *:65436 (LISTEN)
initd    15119  root    6u  IPv4  16157       TCP 192.168.1.79:65336-
>213.154.118.200:1188 (ESTABLISHED)
initd    15119  root    9u  IPv4  15909       TCP 192.168.1.79:1146-
>199.184.165.133:6667 (ESTABLISHED)
initd    15119  root   12u  IPv4  16593       UDP 192.168.1.79:1029-
>192.168.1.1:53
xopen    25239  root    8u  IPv4   9972       UDP *:3049
xopen    25239  root   16u  IPv4    976       TCP *:443 (LISTEN)
xopen    25239  root   17u  IPv4    977       TCP *:80 (LISTEN)
xopen    25241  root    8u  IPv4  12302       TCP *:3128 (LISTEN)
xopen    25241  root   16u  IPv4    976       TCP *:443 (LISTEN)
xopen    25241  root   17u  IPv4    977       TCP *:80 (LISTEN)
lsn      25247  root   16u  IPv4    976       TCP *:443 (LISTEN)
lsn      25247  root   17u  IPv4    977       TCP *:80 (LISTEN)
```

I consider ports 2003 (PID 3137), 65336 and 65436 (PID 15119), 3049 (PID 25239) suspicious because they shouldn't be open at all.
In addition ports 443 and 80 (PIDS 3137, 3153, 25239, 25247) are open by non-standard programs, port 3128 (sometimes used for a proxy) is open by the xopen (PID 25241) program.

4.4. Were there any active network connections? If so, what address(es) was the other end and what service(s) was it for?

The secure netstat reports these connections to be up:

```
tcp        0      0 192.168.1.79:65336      213.154.118.200:1188    ESTABLISHED
15119/initd
tcp        0      0 192.168.1.79:1146       199.184.165.133:6667    ESTABLISHED
15119/initd
```

The firt connection (192.168.1.79:65336 to 213.154.118.200:1188) is used by the psyBNC program that was installed on the system by the attacker.
PsyBNC[1] is an IRC bouncer.

In this instance, it is used by the host at 213.154.118.200 to connect to an IRC channel. Going through the bouncer leaves only a trail to the IP address of the hacked machine on the IRC server. This makes a person more anonymous and protects against attacks from other list members.

The second connection is linked to the first, it is the connection of the hacked machine to the IRC host (199.184.165.133 / undernet.irc.rcn.net).
Our machine acts as a relay between the attacker (213.154.118.200) and the IRC host (199.184.165.133).

I would like to note that I did a rudimentary live-analysis on the system (using the FIRE tookit), before powering down and examining the data. Had I not done this, some of the information, like active networking connections would have been lost.

4.5. How many instances of an SSH server were installed and at what times?

I found 3 instances of SSHd on the server, one of them was legitimate.
The binaries are located as follows:

- /usr/sbin/sshd (legitimate sshd, bound to port 22)
  installed on 2003.07.14 13:54:37 PDT – RPM datatase shows install date
  the md5 list provided still matches the file.
- /usr/bin/smbd -D on port 2003
  ID string: SSH-1.5-By-ICE_4_All (Hackers Not Allowed!)
  installed on 2003.08.10 20:33:33 PDT
- /lib/.x/xopen/s/xopen on port 3128
  ID string: SSH-1.5-1.2.32
  installed on 2003.08.10 22:32:16 PDT

4.6. Which instances of the SSH servers from question 5 were run?

All of them are running on the system.

4.7. Did any of the SSH servers identified in question 5 appear to have been modified to collect unique information? If so, was any information collected?

Due to time-contraints, I have not looked into this thouroghly.
As far as I can see the ssh servers do not collect any special information. It may be possible that they do send data to the linsniffer process, which did capture authentication information. Most of the recovered linsniffer data shows POP3 accounts however, so this is unlikely.

```
- [FIN]

cgomez => mir-serv.ez-closet.com [110]
USER carlos
PASS eduardo
STAT
QUIT
```

```
----- [FIN]

cgomez => mir-serv.ez-closet.com [110]
USER carlos
PASS eduardo
STAT
QUIT

----- [FIN]
```

4.8. Which system executables (if any) were trojaned and what configuration files did they use?

Apart from the system commands that were modified to hide the precence of the rootkit (listed by chkrootkit), there was other malware installed on the system.

/usr/bin/sl2 contains the DDoS-Blitz trojan.

```
Troj/Blitz is a TCP SYN flooder for Linux. It sends a target machine continual
TCP connect packets in the hope of crashing the machine or making it unable to
service legitimate requests.
```

/usr/lib/sp0 contains the Linux/Rst.b virus , which is a by-effect of the ATD mass exploiter (ATD itself is infected).

/usr/bin/(swapd) seems to contain linsiffer, possibly modified

/lib/.x/log
/lib/.x/cl
/lib/.x/s/xopen
Are part of the SuckIT rootkit.
/lib/.x/s/sshd_config is the configuration file for the hacked ssh daemon.

4.9. How and from where was the system likely compromised?

The system was compromised through a vulnerability in Apache/OpenSSL using the ATD mass exploiter[2].
One of the logs I recovered (through the /proc file descriptors) lists the address of the attacker:

```
213.154.118.219 - - [10/Aug/2003:13:16:27 -0700] "GET / HTTP/1.1" 400 385 "-" "-
"
213.154.118.219 - - [10/Aug/2003:13:16:37 -0700] "GET / HTTP/1.1" 400 385 "-" "-
"
213.154.118.219 - - [10/Aug/2003:13:23:17 -0700] "GET /sumthin HTTP/1.0" 404 279
"-" "-"
```

This address is most likely real, the attack should spawn a shell back to it, making spoofing rather unlikely. It is also in the same address space as the address that had the IRC bounce connection open in question x (213.154.118.200).

A whois of the address reveals that both addresses belong to an ADSL provider in Romania.
The difference in address could be explained by the use of a proxy or a DHCP address, there is no further evidence to prove this.

```
% This is the RIPE Whois server.
% The objects are in RPSL format.
%
% Rights restricted by copyright.
% See http://www.ripe.net/ripencc/pub-services/db/copyright.html

inetnum:      213.154.96.0 - 213.154.127.255
netname:      PCNET
descr:        PCNET Data Network S.A.
descr:        PROVIDER ADSL Network
country:      RO
admin-c:      BT17-RIPE
tech-c:       PDNN1-RIPE
status:       ASSIGNED PA
notify:       tudor@pcnet.ro
mnt-by:       AS8503-MNT
changed:      tudor@pcnet.ro 20030704
source:       RIPE

route:        213.154.116.0/22
descr:        PCNET
origin:       AS8503
notify:       tudor@pcnet.ro
mnt-by:       AS8503-MNT
changed:      tudor@pcnet.ro 20020912
source:       RIPE

role:         PCNET Data Network NOC
address:      Splaiul Unirii, nr. 10
address:      Bucharest, ROMANIA
```

After a succesful ATD attack, the cracker will have an interactive shell to the system as the apache user. Unfortunately all platforms targeted by the exploiter are also vulnerable to the 'ptrace local root exploit'[4] which allows the attacker to get root.

The attacker installed the suckit rootkit[3] to open a backdoor to the system and to hide his traces (clean log files etc.).

4.10. Bonus Question
What nationality do you believe the attacker(s) to be, and why?

I suspect that the attacker or attackers are Romanian.
The Romanian ADSL account is Romanian and the ATD exploiter is believed to have romanian roots too.

5. Reference

1. PsyBNC – http://www.psychoid.lam3rz.de/
2. Analysis of the ATD OpenSSL Mass Exploiter – http://www.lurhq.com/atd.htm
3. SuckIT rootkit – http://hysteria.sk/sd/f/suckit/readme
4. Ptrace local root - http://bugtraq.underattack.co.kr/xploit.php3?line_1=270&line_2=280