Subject: "hidden processes" in OpenVZ
Posted by floogy on Sun, 18 Nov 2007 14:11:25 GMT
View Forum Message <> Reply to Message

Hello,

I got a vserver, and found "hidden processes" by rkhunter, unhide and chkrootkit:

chkrootkit:
Output of: ./chkproc -v -v -p 3
###
PID   482(/proc/482): not in getpriority readdir output
[...]
PID 31564(/proc/31564): not in getpriority readdir output
You have   49 process hidden for readdir command
not found

ossec-rootcheck

./ossec-rootcheck -c rootcheck.conf

** Starting Rootcheck v0.7 by Daniel B. Cid   **
** http://www.ossec.net/hids/aboutus.php#dev-team **
** http://www.ossec.net/rootcheck/   **

Be patient, it may take a few minutes to complete...

[FAILED]: Rootkit 'Showtee' detected by the presence of file '/usr/lib/libfl.so'.

[OK]: No binaries with any trojan detected. Analyzed 57 files

[FAILED]: File '/dev/shm/network/ifstate' present on /dev. Possible hidden file.

[OK]: No problem found on the system. Analyzed 40717 files.

[FAILED]: Process '8329' hidden from ps. Possible trojaned version installed.
[...]
[FAILED]: Excessive number of hidden processes. It maybe a false-positive or something really bad is going on.

[OK]: No kernel-level rootkit hiding any port.
    Netstat is acting correctly. Analyzed 131072 ports.

[OK]: The following ports are open:
    25 (tcp),80 (tcp),3306 (tcp),4949 (tcp),
    12345 (tcp)

[OK]: No problem detected on ifconfig/ifs. Analyzed 3 interfaces.

- Scan completed in 86 seconds.

'/usr/lib/libfl.so' and '/dev/shm/network/ifstate' alerts are known false positives on debian systems.
The open ports are ok.
It's only 25, 80 and ssh open. 25 is postfix, relaying is denied.
4949 is plesk and virtuozzo.

unhide:

/usr/local/sbin/unhide sys
Unhide 02-11-2007
yjesus [at] security-projects.com

[*]Searching for Hidden processes through getpriority() scanning

Found HIDDEN PID: 941
[...]
Found HIDDEN PID: 31564
[*]Searching for Hidden processes through getpgid() scanning
rkhunter.log

[06:54:14] Warning: Hidden processes found: 4309
[..]
 25743
[06:54:14]
[06:54:14]   Performing check of files with suspicious contents

Yesterday there were 329 hidden processes listed in rkhunter.log, today 385.

listps didn't find anything suspicious:
./listps -d
Checking pids from 0 to 33000
/usr/local/sbin/untcp
Unhide 02-11-2007
yjesus [at] security-projects.com

Starting TCP checking

Starting UDP checking

zeppoo-0.0.4 didn't work on the vserver due to permission denied errors on /dev/mem and

/dev/kmem. I take that as a proof that it's maybe not possible to install a rootkit on a virual machine, like its not possible to load kernel modules into the kernel (LKM)?

In the supportforum I found this:

http://forum.openvz.org/index.php?t=search&srch=chkrootk it&btn_submit=Search
http://forum.openvz.org/index.php?t=tree&th=2481

Is it for sure, or at least almost certainly a false positive in vserver environements? I think so, because rkhunter and chkrootkit couldn't find any suspicious files or rootkits.
Can anyone give a hint how to assess this situation?

This is what I found, so far:
http://www.jaguarpc.com/support/kbase/705.html
http://www.ossec.net/ossec-list/2007-May/msg00089.html
http://forums.vpslink.com/showthread.php?t=1898

The tools I used:
http://csl.sublevel3.org/listps/
http://wiki.linuxquestions.org/wiki/Rootkit_Hunter
http://rkhunter.sourceforge.net/
http://sourceforge.net/project/showfiles.php?group_id=155034
http://wiki.linuxquestions.org/wiki/Unhide
http://www.security-projects.com/?Unhide
http://www.chkrootkit.org/

```
# ls -d /proc/* | grep [0-9] | wc -l; ps ax | wc -l
25
25
# ls -d /proc/* | grep [0-9] | wc -l; listps |grep [0-9] | wc -l
24
25
```

As far as I understand, has this got to do with the different process handling in VE's, is this right?

If so: How to get sure there is nothing hidden going on on my vserver? Is it sure to ignore these detected "hidden processes"? How can I investigate them further?

I'm sorry for my poor english, and thank you in advance!