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!

Subject: Re: "hidden processes" in OpenVZ
Posted by vaverin on Tue, 20 Nov 2007 10:43:50 GMT
View Forum Message <> Reply to Message

Hi floogy,

Please do not worry, I believe it's falshe alerts.

Let me explain:
each process inside VE have 2 pids -- "virtualized" and system".
Inside VE "virtualized" pids are used, "system" are used in hardware node conext. As an example: init process in each VE have pid=1 visible inside VE and "real" pid on HW node.

Proc inside VE shows "virtualized" pids, but allows to use "system" pids too, therefore "system" pids looks as hidden.

Also I would note that you can find some more details in
"PID namespaces in the 2.6.24 kernel" article on LWN
http://lwn.net/Articles/259217/

Currently this article is available to LWN subscribers only and will become freely available on November 29, 2007.

thank you,
Vasily Averin

Subject: Re: "hidden processes" in OpenVZ
Posted by floogy on Tue, 20 Nov 2007 12:59:36 GMT
View Forum Message <> Reply to Message

Hi vaverin,

thank you so much! It's nice to hear, that I shouldn't bother about hidden processes in VPS or OpenVZ, because these messages of unhide/rkhunter/chkrootkit are really scary!

How can I investigate them further?
Though, it might be still necessary to investigate the server further, don't it? And if so, how to do so?

Or is it almost impossible to install such rootkits or other hidden processes into a OpenVZ guest operating system?

Thank you in advance!

Subject: Re: "hidden processes" in OpenVZ
Posted by vaverin on Tue, 20 Nov 2007 13:56:00 GMT
View Forum Message <> Reply to Message

Sorry, I do not understand your question.
"hidden" processes inside VE -- is not a problem, it is false alerts.
If you want to be sure that hidden pid is "system" pid for some process -- /proc/<pid>/status file

should have correct "envID:" field

thank you,
Vasily Averin

Subject: Re: "hidden processes" in OpenVZ
Posted by floogy on Tue, 20 Nov 2007 14:03:01 GMT
View Forum Message <> Reply to Message

Hi Vasily,
Quote:"hidden" processes inside VE -- is not a problem, it is false alerts.

Is this alltimes true, in every case? You see: Due to rkhunter I became a paranoid person

I'm sorry, but I think I do not understand, for example:
./unhide sys
[...]
Found HIDDEN PID: 30849
cat /proc/30849/status
cat: /proc/30849/status: No such file or directory
cat /proc/30849
cat: /proc/30849: No such file or directory

That makes sure, that it's a false positive?

Subject: Re: "hidden processes" in OpenVZ
Posted by vaverin on Tue, 20 Nov 2007 14:17:26 GMT
View Forum Message <> Reply to Message

You can check pid from HW node.

Subject: Re: "hidden processes" in OpenVZ
Posted by floogy on Tue, 20 Nov 2007 14:24:57 GMT
View Forum Message <> Reply to Message

My Google search for define:"HW-node" remained without result. (?)
I guess it's a term for the Host-Computer on which OpenVZ runs the Guest-VE's. I guess I need a break, and an good introduction to OpenVZ

The problem is: I rent a vserver which is virtualized by virtuozzo, which based on OpenVZ.
"Unfortunately" I don't have access to the host-system (the hw-node). No, instead I'm happy to be

not responsable for that system

Though, in the VZPP:System Prozesses I can not find these hidden processes neither their envID.

My question is: how can I decide, that all hidden processes are system processes of the hardwarenode, if I'm not able to compare the PIDs numbers in VE with the pids in hw-node?

Oh jesus, I think I'm getting completly paranoid... It's time to switch either to managed webspace or to a rootserver, with access to the hw-node, isn't it?

nmap, logcheck etc. didn't report anything unusual, I'm sorry but this hidden stuff makes me nervous...

Subject: Re: "hidden processes" in OpenVZ
Posted by floogy on Tue, 20 Nov 2007 21:11:56 GMT
View Forum Message <> Reply to Message

"floogy"I'm sorry but this hidden stuff makes me nervous...
Is there maybe a plan, to integrate some code, that compares the hw-node pids with the ve hidden pids, and show the different processes as an alert in the VZPP:System Prozesses, or provide a method to tools like chkrootkit/rkhunter/unhide, to give them the capability to detect these hidden hw-node processes as harmless?

Subject: Re: "hidden processes" in OpenVZ
Posted by vaverin on Wed, 21 Nov 2007 05:18:06 GMT
View Forum Message <> Reply to Message

You can find some definition in openVZ wiki:
http://wiki.openvz.org/HW

"Hardware Node (otherwise known as host system) is a term used in OpenVZ documentation. Basically it means the physical server on which OpenVZ is installed and running.

Sometimes Hardware Node is abbreviated as HW or HN."

Subject: Re: "hidden processes" in OpenVZ
Posted by vaverin on Wed, 21 Nov 2007 06:01:58 GMT
View Forum Message <> Reply to Message

I would note that you cannot make process "hidden" from userspace. It can be done from kernel-space only, i.e. by using loadable kernel modules.
However nobody inside VE have such permissions, nobody is able to load any kernel modules from inside VE, only HW-node admin is able to do it.

Therefore "hidden" proccesses detected inside VE is not mean that your VE has been hacked. All that yo can do is just report to HW-node admin and he can check your "hidden" pids.

However you can make some checks inside VE too. Usually "virtual" pids visible inside VE = "system" Pid + 1024 (i.e bit 10 is used to mark pid as Virtual). Therefore if you found "hidden" pid with this number, it makes sense to search according "virtual" pid inside VE.

Of course we'll make "system" pids to be more "invisible" inside VE -- to prevent chkrootkit's false alerts.

Thank you,
Vasily Averin

Subject: Re: "hidden processes" in OpenVZ
Posted by vaverin on Wed, 21 Nov 2007 06:50:45 GMT
View Forum Message <> Reply to Message

FYI: I've added bug #736 added into our bugzilla:
http://bugzilla.openvz.org/show_bug.cgi?id=736

Subject: Re: "hidden processes" in OpenVZ
Posted by floogy on Wed, 21 Nov 2007 10:22:47 GMT
View Forum Message <> Reply to Message

Hello Vasily,

thank you very much for your efforts. It's now much more clearer that these hidden processes are harmless, and one can check that by the pid number "structur". Maybe rkhunter and chkrootkit could have some code, enabled by an extra '--ve'-option, that checks only for hidden processes that aren't hw-node system processes, but instead "virtual" hidden.

I don't know much about rootkits etc. but I understand, that loadeable modules (LKM) aren't possible in ve's. I can't think of hidden processes that are working different, but that's because I don't have the knowledge.

I'm not sure that I did understand everything right, that you were so kind to explain to me, but I understand this sentence, and that eases my mind:
Quote:I would note that you cannot make process "hidden" from userspace.

Again I'm sorry for my poor english, I think, that this will bring up "virtual" issues ...

Please, would you be so kind, to have also a look into my still unanswered question about my "lockedpage issue"?

Problem with lockedpages failcnt 192, limit 344:

http://forum.openvz.org/index.php?t=msg&goto=22868&# msg_22868

Subject: Re: "hidden processes" in OpenVZ
Posted by vaverin on Wed, 21 Nov 2007 12:53:57 GMT
View Forum Message <> Reply to Message

As you know each process has a directory on proc filesystem:
/proc/<pid>/...

Usually /proc/<pid> are visible by any filesystem system calls. "Hidden" pids are not visible directly -- for example readdir() system call does not show it. However some other system calls still can use this pid: for exmaple you can change directory to "hidden" or something else. (I would note -- it is not usual "cd" shell command, but syscall chdir() used by chkproc).

Procfs -- is virtual filesystem, its content created by kernel an the fly and even root is not able to change its content. On the other hand root is able to load some kernel modules that will change kernel code and by this way will be able to change proc output too. Some rootkits uses this ability and changes kernel code to make itself invisible.

That's why chkrootkit tries detect these "invisible" processes by using some unusual ways. Such "hidden" processes really looks suspect.

Unfortunately our "system" pids are visible inside VE for some system call, chkrootkit is able to detect it and report about suspected pids.

However nobody inside VE hav permissions to load kernel modules, and therefore any rootkits inside VE are not able to make the processes "hidden".

thank you,
Vasily Averin

Subject: Re: "hidden processes" in OpenVZ
Posted by dev on Thu, 06 Mar 2008 20:48:20 GMT
View Forum Message <> Reply to Message

fixed in 028stab054

Subject: Re: "hidden processes" in OpenVZ
Posted by sara3 on Fri, 07 Mar 2008 12:26:10 GMT
View Forum Message <> Reply to Message

where is 028stab054 lcoated ???

Subject: Re: "hidden processes" in OpenVZ
Posted by dev on Fri, 07 Mar 2008 13:16:26 GMT
View Forum Message <> Reply to Message

not available yet. I post such comment when commit is fixed to the kernel and specify the version where it will appear. The actual version will be built/tested and finally released later actually.
It's just a notice where you'll be able to find the fix.
Or you can apply the patch from the bug in question.