

Forum:[Hack Forums](#)

Thread: [It's either not rootable or the exploit is screwed.](#)

Bacardi - August 18, 2012, 8:47 am

Got a shell on a server and this is the uname -a.

Code Linux xxxx.com 2.6.9-78.ELsmp #1 SMP Fri Jul 25 00:04:28 EDT 2008 i686 i686 i386 GNU/Linux

Sec info:

Code Server software: Apache/2.0.52 (Red Hat)

Disabled PHP Functions: system,exec,passthru,escapeshellcmd,pcntl_exec,shell_exec

Open base dir: /www/users/:/tmp/

cURL support: enabled

Supported databases: MySQL (4.1.12), MSSQL

I've tried all of the 2.6.9 exploit listed here <http://localroot.th3-Outl4ws.com/>

Whenever I try to execute one of them it says this.

Code sh: [25065: 2] tcsetattr: Invalid argument

I also tried this one just in case.

http://www.tsirogiannis.com/uncategorized/linux-kernel-2-42-6-sock_sendpage-local-root-exploit/

That just shows:

Code sh: no job control in this shell

Could the disabled PHP functions be the cause?

Any input is appreciated.

HaxOr? - August 18, 2012, 9:09 am

Can you PM me the shell?

I can try...

Bacardi - August 18, 2012, 9:23 am

(Aug 18, 2012 09:09 AM)?? ? x O r ? Wrote: [\[CITE\]](#) Can you PM me the shell?

I can try...

PMed you the shell. Hope you can figure it out.

HaxOr? - August 18, 2012, 9:25 am

Successfully rooted.

Enjoy mate! ?

You can close this now BTW.

Bacardi - August 18, 2012, 9:33 am

I will, but I remember a thread about what you can when you have root. Can't find it anywhere though.

rvltr - August 18, 2012, 11:20 am

i have one giving me the same thing, nothing but sh: [25065: 2] tcsetattr: Invalid argument when

trying to execute any locals ive tried