

Forum:[Hack Forums](#)

Thread: [# can't ReaD -> \[/etc/named.conf \] \(any bypass?\)](#)

AntiHacker - September 4, 2014, 3:23 am

(after shelling a site)

hey all how you all doin?
hope you guys are in a good life and good moods

my question is that after i uploaded my shell

problem #1

i uploaded my tools as usual to get the configs and domain names

so here is what i did step by step

cat /etc/passwd ok that command worked good then after it shows all the passwds i copied them and paste them into

config.php and i used other tools such as config fucker in Webr00t shell but the result is that i don't get the config files

such as wordpress~~1.txt you know what i am saying

also problem #2

is that i used php script such as d0mains.php

and users.perl and other perl tools to grab the domains and the usernames

but it said can't ReAD etc/named.conf ...

.- now i dont really care about that all i need is to slove the problem #1 which is to get the config files

[+] more info about the server for those who asks

the server has only 3 sites and its linux and for those who say root it i cant because i cant find the

local root exploit for this version

```
id : seiha (user)
$ id
uid=3423253(seiha) gid=1188990(pg2314236) groups=3138390(pg2314236)
id in this server is (user) meaning its not (nobody) , (apache) etc...
```

i tried most popular symlink tools to grab the configs commands that i tried but it Fails!

```
cat /etc/valiases/domain.com
```

```
ls -a /etc/valiases/domain.com
```

```
cat etc/named.conf
```

using webroot cgi shell i tried

```
cat /etc/named.conf | grep zone > users.txt but the file users.txt was empty :(
```

i went to the etc folder

```
cd /
```

```
cd etc
```

```
then
```

```
dir
```

then it displays the folders and files but i cant find named.conf also or the folder valiases
i downloaded some files like userlist.conf from /etc

but still some files from /etc useless at the moment - _____ -

even the folder mail in /etc

long story short i'm trying to get the configs (symlink the configs for other sites on the same server)
but i CAN'T like i said i tried to symlink the root and lots of things etc... do it any help is appreciated!

anybody can help me in any way i will appreciate just comment or pm me ..

Sky - September 4, 2014, 5:07 am

What year is the server? There's a Symlink bypass for all 2014 servers.

~Arcane ?

AntiHacker - September 6, 2014, 1:31 am

2011 x86_64 first serve

2014 x86_64 the second one

but i need the first one for now 2011 x86_64

Nitai - September 6, 2014, 5:54 am

Try to use netcat and than run a rootkit exploit to get full access .

tmp2 - September 6, 2014, 10:09 am

playchu is right, since the server is 2011 , most chances that you can root it with a root exploit kit.

0x77d718fc - September 6, 2014, 11:14 am

check uname -a, cat /etc/issue => search for a corresponding local exploit.

AntiHacker - September 6, 2014, 12:18 pm

(Sep 6, 2014 11:14 AM)0x77d718fc Wrote: [\[CITE\]](#) check uname -a, cat /etc/issue => search for a corresponding local exploit.

thats what it is Linux james-rock 2.6.32.45-grsec-2.2.2-r3 #8 SMP Mon Oct 10 13:33:17 PDT 2011 x86_64 GNU/Linux

josue - September 6, 2014, 12:30 pm

Now Google linux kernel exploit 2.6.32 to verify whether it exists

SaxyMadaFaka - September 7, 2014, 2:00 pm

(Sep 4, 2014 05:07 AM)Sky Wrote: [\[CITE\]](#) What year is the server? There's a Symlink bypass for all 2014 servers.

~Arcane ?

LOL really???

~ Bad Boy ?

AntiHacker - September 24, 2014, 12:35 am

(Sep 7, 2014 02:00 PM)Anti Terrorist Wrote: [\[CITE\]](#) LOL really???

~ Bad Boy ?

What year is the server? There's a Symlink bypass for all 2014 servers.

i h8 2014 servers

i got more than 5 shells on diff. servers its all 2014

fuuuuck!

133720 - September 24, 2014, 7:22 am

Use Server to bypass or try using the base64 .

AntiHacker - September 28, 2014, 4:45 am

ppl seem to give up on 2014 servers!

WPA2 - October 8, 2017, 6:53 pm

evan though this thread is old and the op is closed&@HF

I would like to bring this up as I Have found a solution if you want to read try using sec-war script it works phenomenal

LD_PRELOAD - October 9, 2017, 12:23 am

(Oct 8, 2017 06:53 PM)WPA2 Wrote: [\[CITE\]](#) evan though this thread is old and the op is closed&@HF

I would like to bring this up as I Have found a solution if you want to read try using sec-war script it works phenomenal"a solution"

a solution is to use common sense. You don't need named.conf. it's simply used as an automatic template to lay out symlink destination, you can symlink just fine without it assuming you actually know where to go. How do we know where to go? file descriptors, php/mysql/tomcat/cron/any other form of logging, even catting /etc/passwd on most cases will be enough. The only reason this thread exists is because skids can't privesc without their little spoonfeeding tools