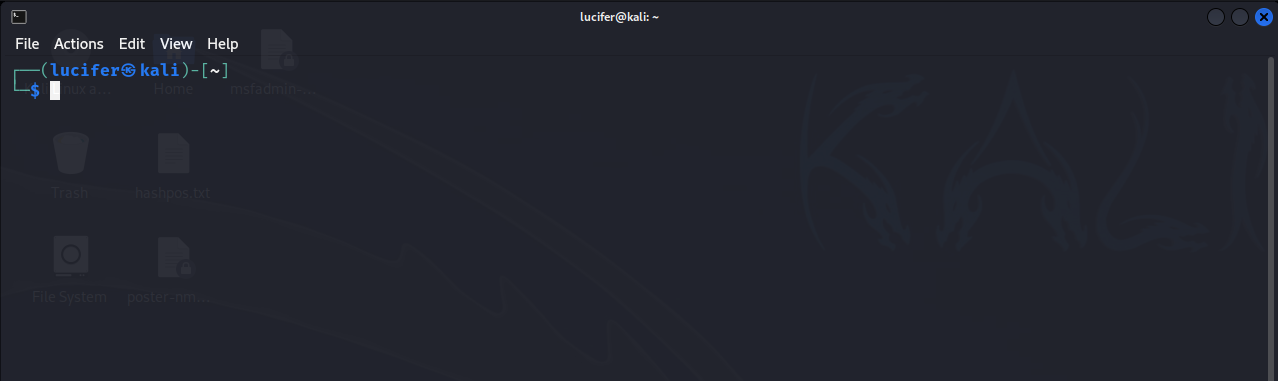
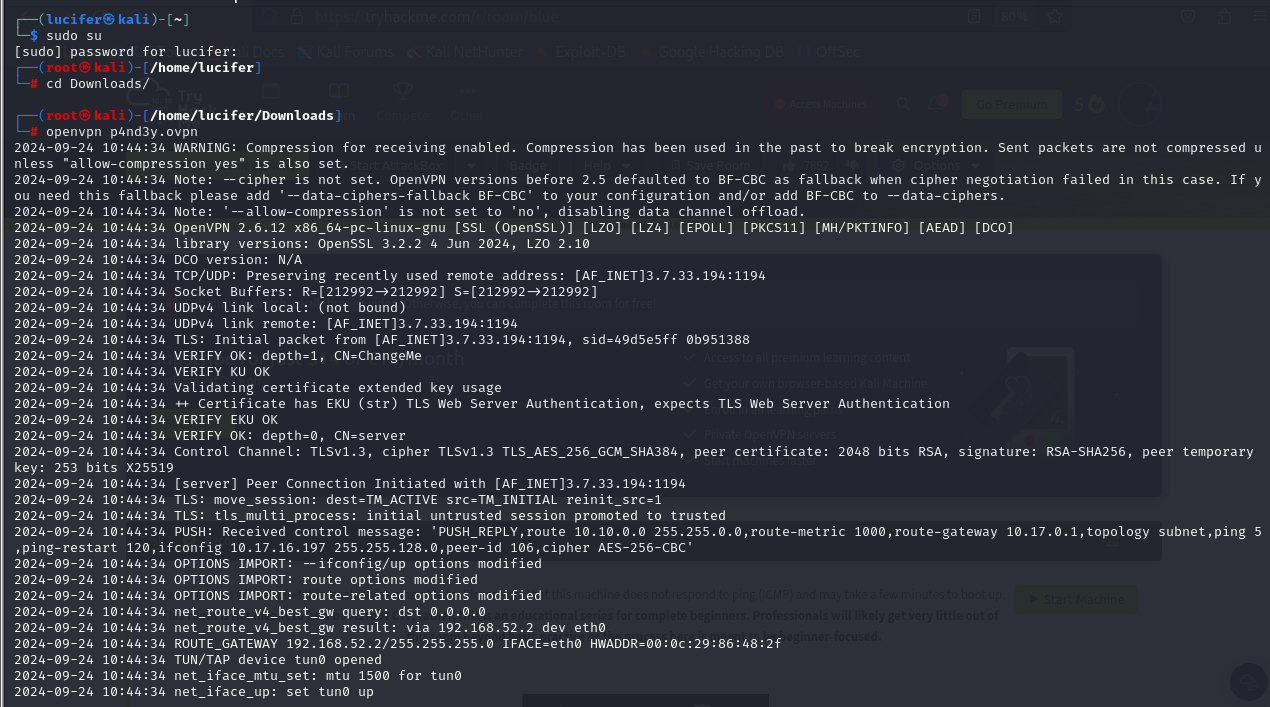
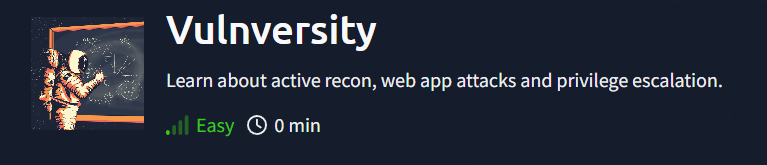
Vulnversity is a box on tryhackme (<https://tryhackme.com/r/room/vulnversity> ) created by **tryhackme, Security Nomad and 1337rce**.

Here our **terminal**  is opened.

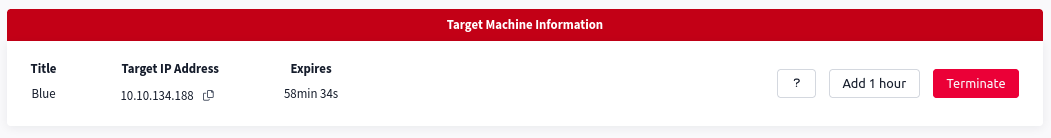


Now we will connect our **vpn** with tryhackme with the help of **openvpn** from vpn’s file downloaded path after doing **sudo**.



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.

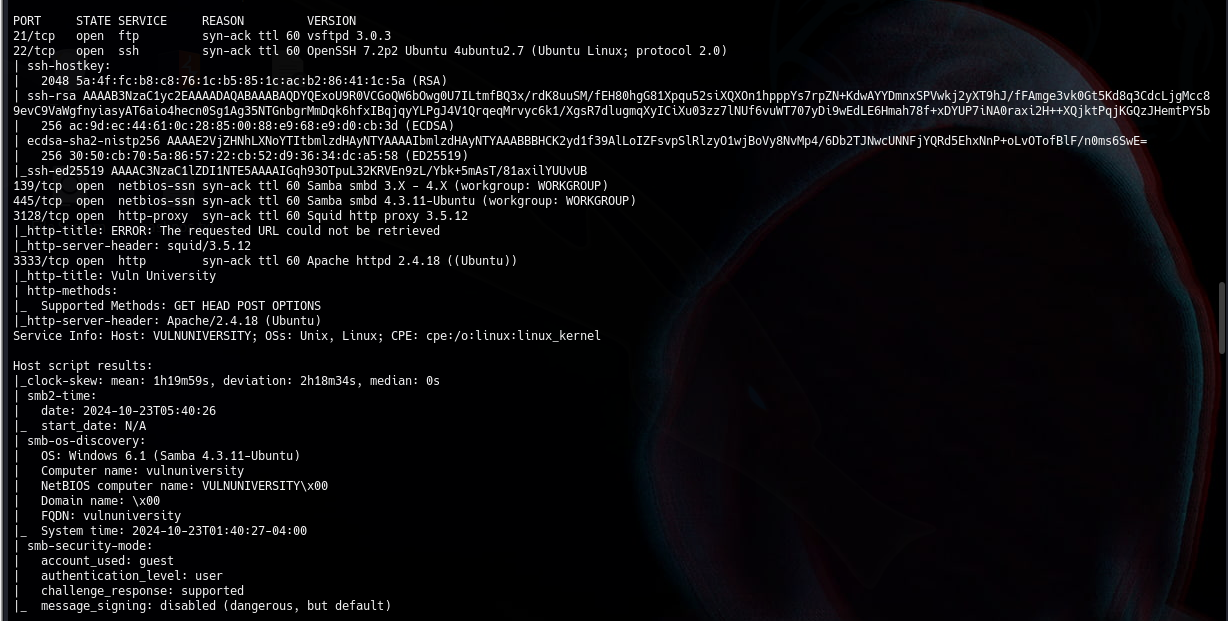


After getting the target ip first thing we’ll do is **nmap** scan to see the open ports and more machine’s info.



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

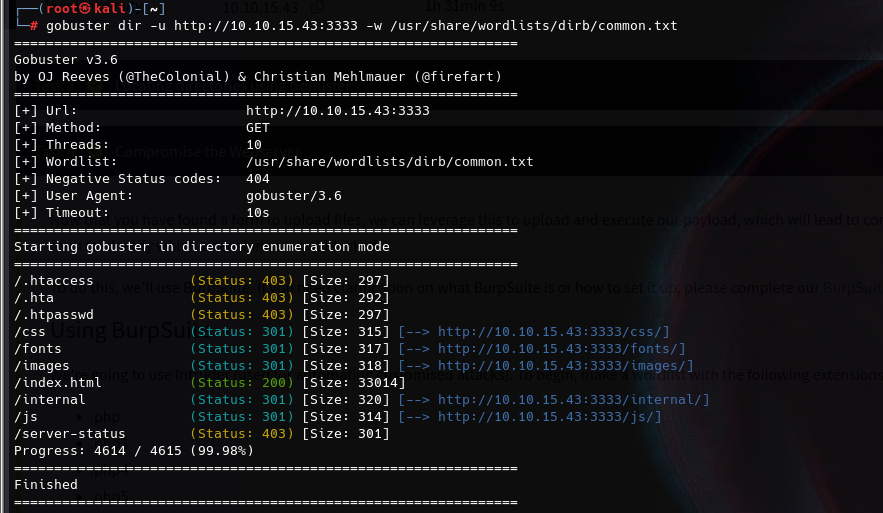
Seems like our scan is completed. Looks like there are total 6 ports open and 2 under 5000.

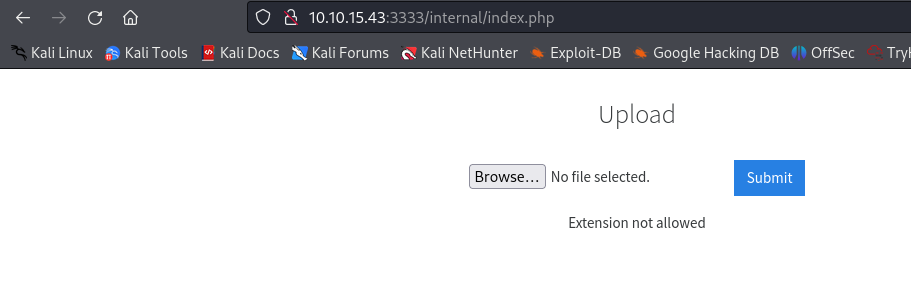


Now that we have know the information from port 3333 using rustscan and it is running http. So we will now explore the web server and try directory bruteforcing using gobuster.

We will use gobuster following command:

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

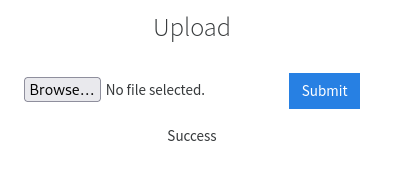


After further recon, we get a upload page on **internal** directory, We will try to get a reverse shell by uploading php reverse shell by **pentestmonkey.** 

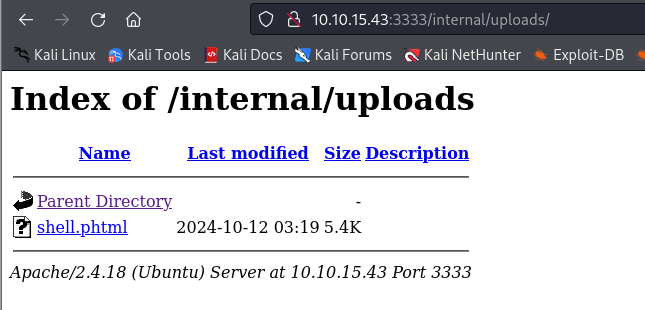
We get that php files can’t be uploaded. So we will try to upload files with different extensions until we get success. Extensions are:

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

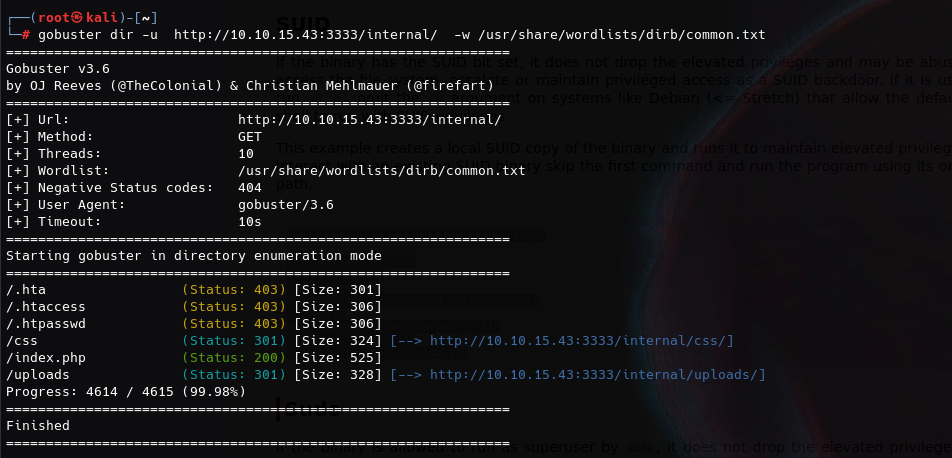
We get a successful uploading from **phtml** file.



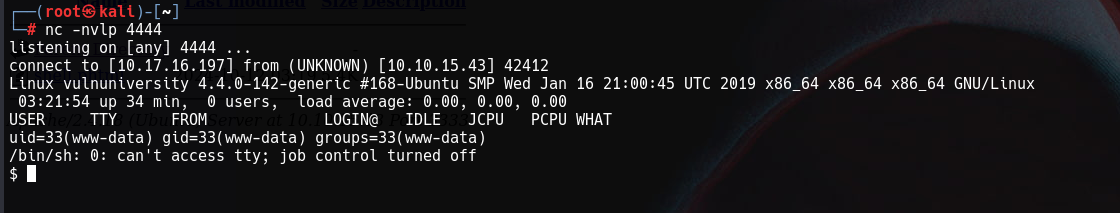
We will now start a listener using netcat on our local machine and execute the shell file we have uploaded. It is in **uploads** directory.



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



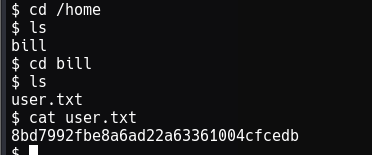
On our machine, after executing the shell file, we get a reverse shell.



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

**python -c ‘import pty;pty.spawn(“/bin/bash”);’**

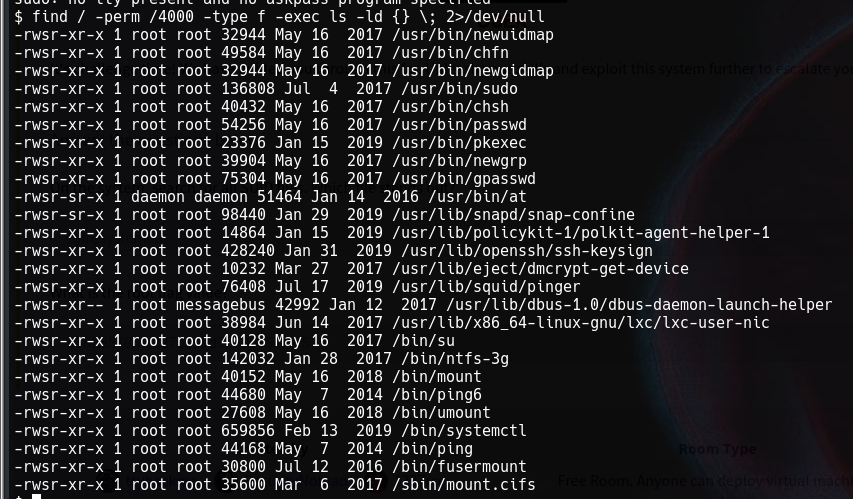
And we will explore the machine.



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

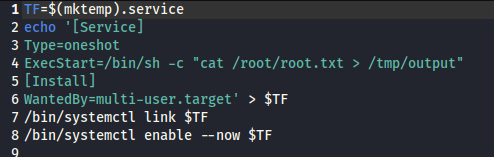
For that we need to escalate privileges.

We will now run command to get SUID permissions files.



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

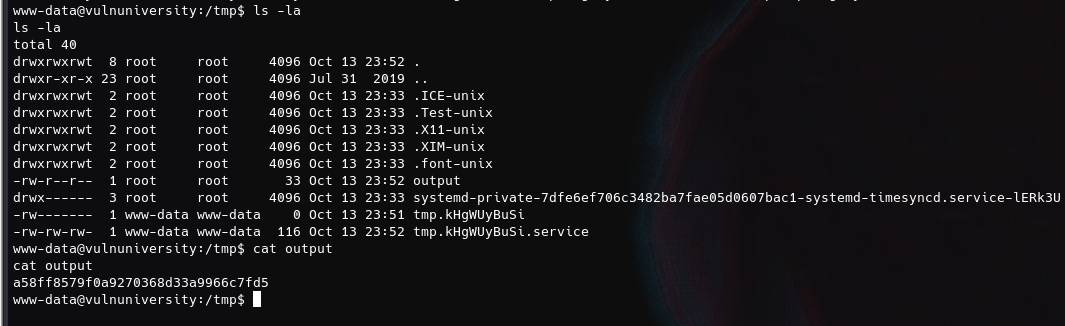
We will go in the **/tmp** folder and run the following commands there because as we know our system files and running processes can be executed or made from there.



We will now execute the commands line by line.



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



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.