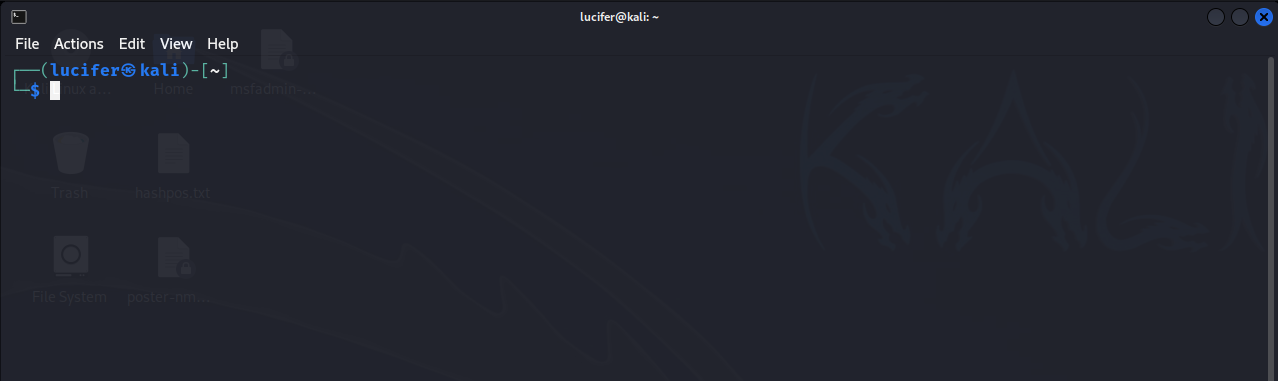
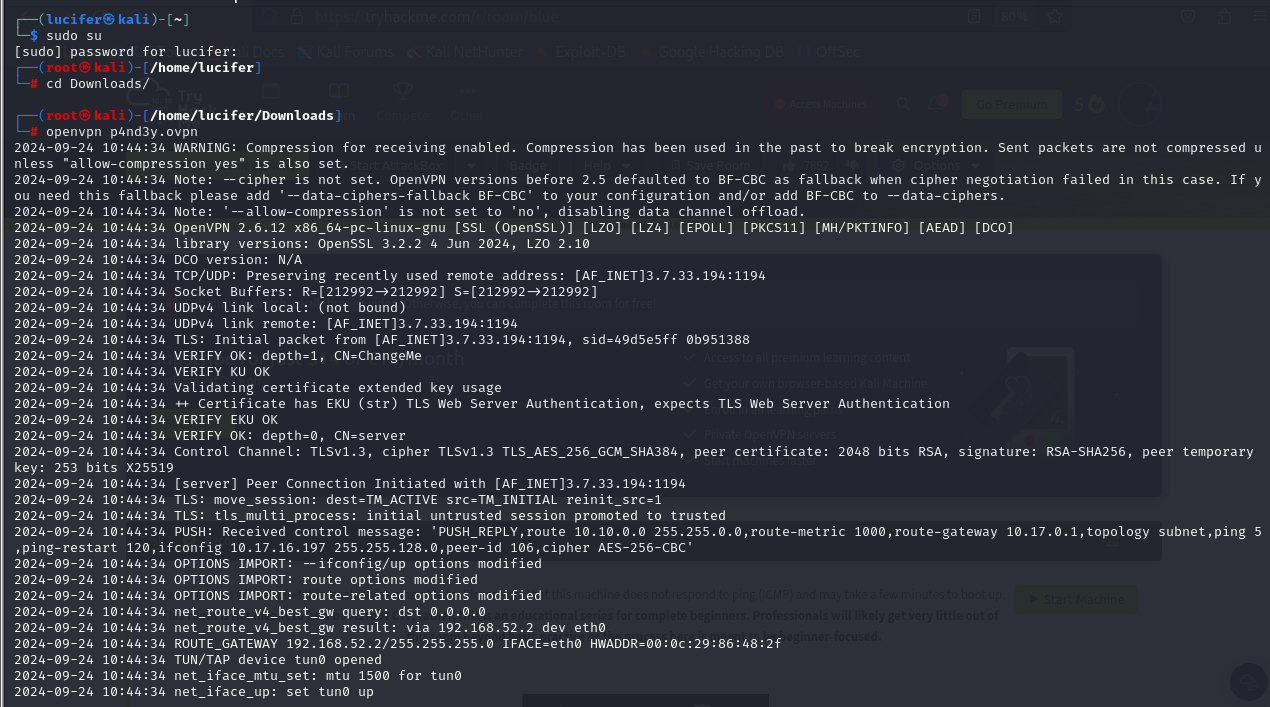
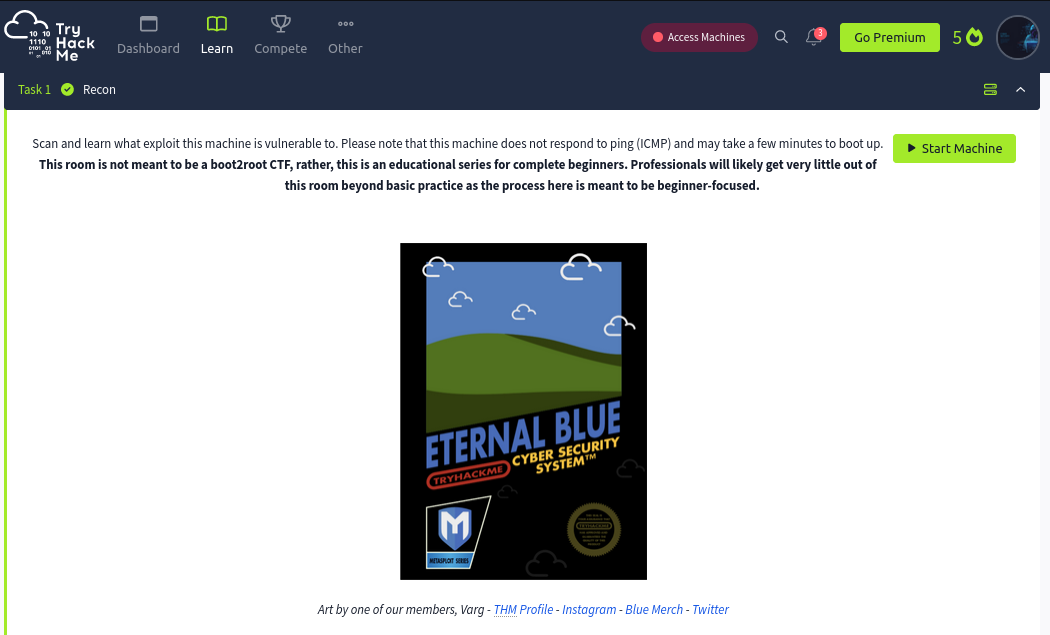
Blue is a box on tryhackme (<https://tryhackme.com/r/room/blue>) created by DarkStar7471. You can download it from: <https://download.vulnhub.com/basicpentesting/basic_pentesting_1.ova>

Here our **terminal**  is opened.

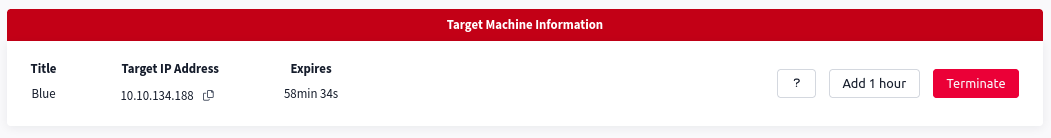


Now we will connect our **vpn** with tryhackme with the help of **openvpn** from vpn’s file downloaded path after doing **sudo**.

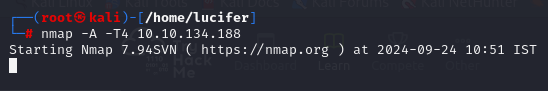


Now, we will check the ip of the target machine from tryhackme website which will be shown after pressing the **start machine** button.****

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

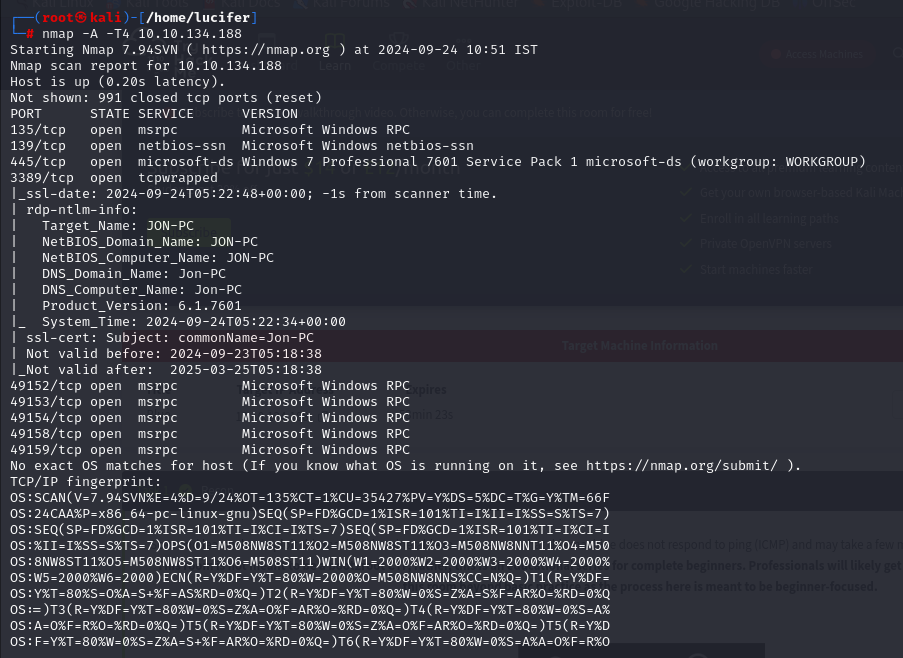


After getting the target ip first thing we’ll do is **nmap** scan to see the open ports and more machine’s info.



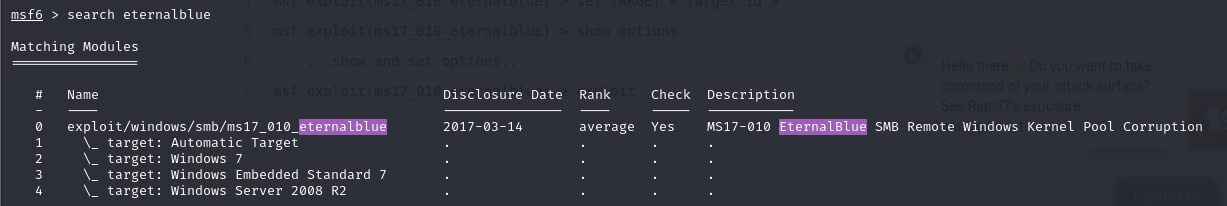
Here I am using **nmap -A -T4 <IP>.** You can also use different scripts like **nmap -sCv -T4 <IP>** or many more as you like.

We Seems like our scan is completed. Looks like there are total 9 ports open and 3 under 1000.



Now that we have know the OS info from port 445 we can use **searchsploit** or google it about the previous exploits in it. Guess what we found it using google. Seems that it has severe vulnerability **MS17-010 (EternalBlue)** with impact score of 8.8 which is really high.

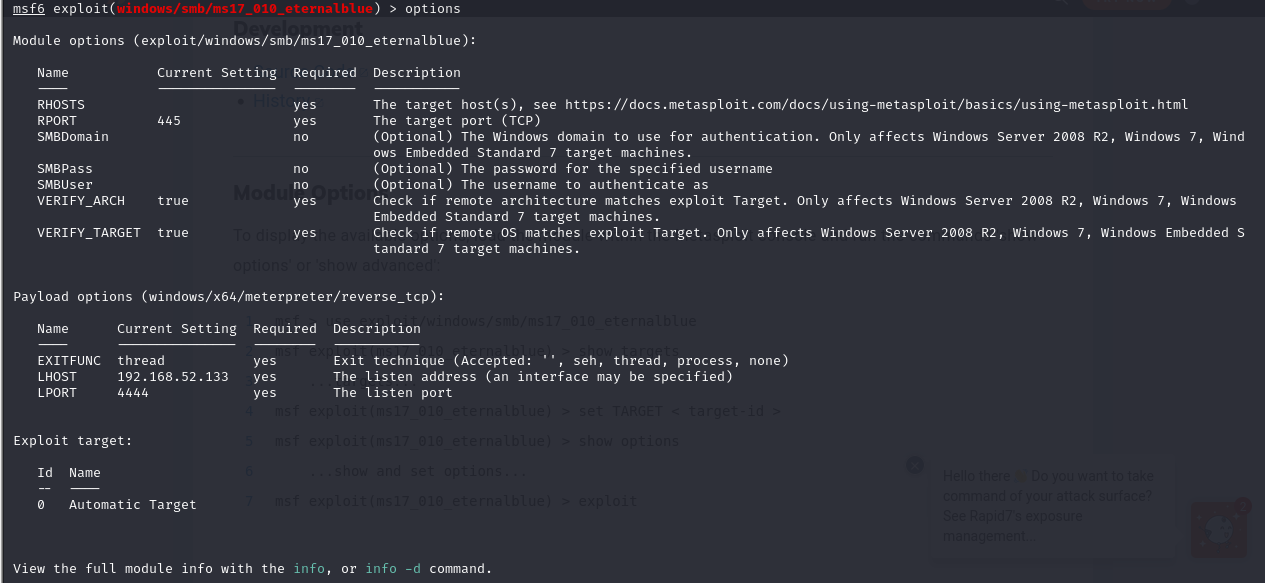
Now we’ll use **msfconsole(metasploit)**  to exploit this machine as we know the vulnerability after further research. We’ll search the exploit on metasploit.



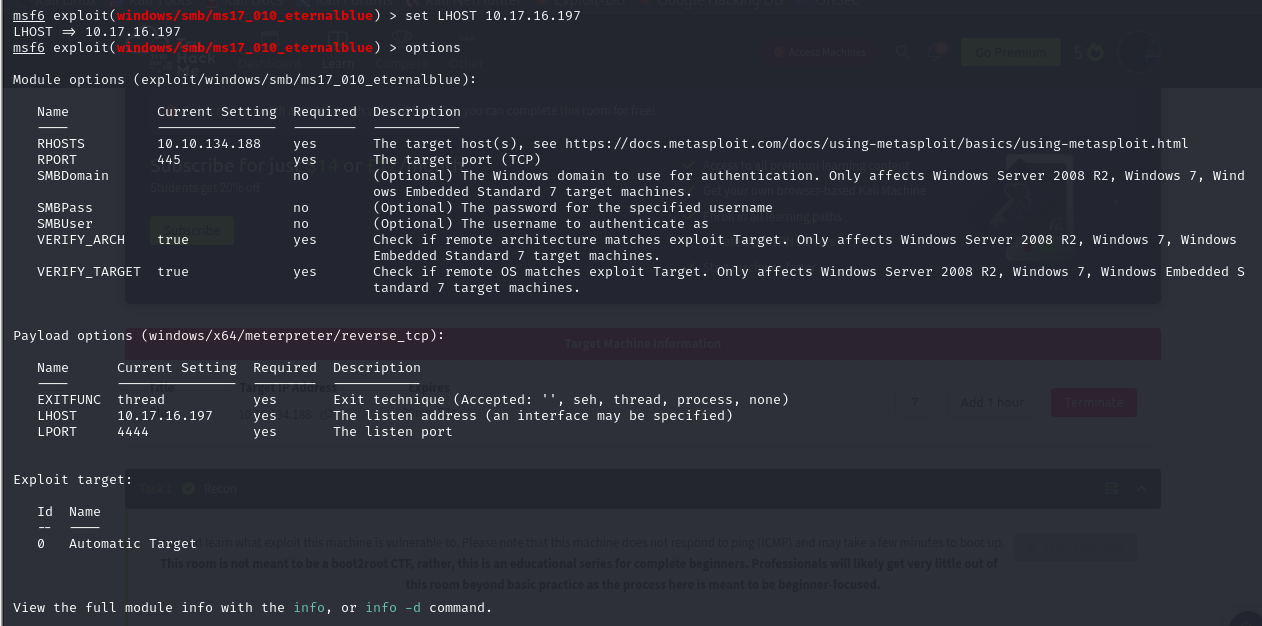
We found an exploit. Now we’ll use it.



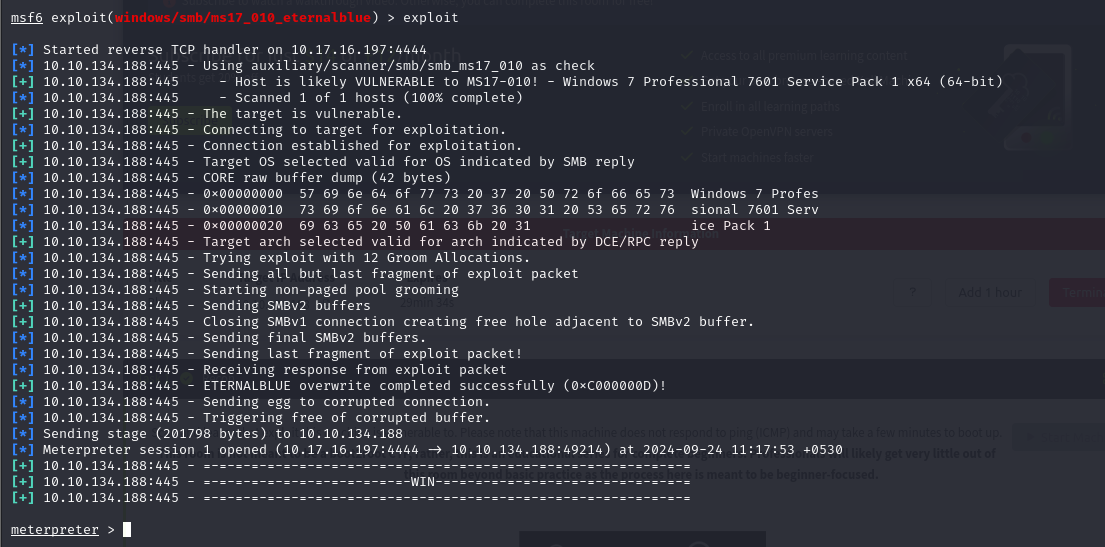
We’ll set the required options needed to exploit the target machine.



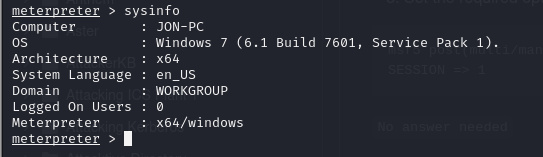
We’ll set **RHOSTS** as the target ip and **LHOST** as our local machine’s address ip and rest will be default.



We can see RHOSTS and LHOST is now modified and now we can start the exploit.

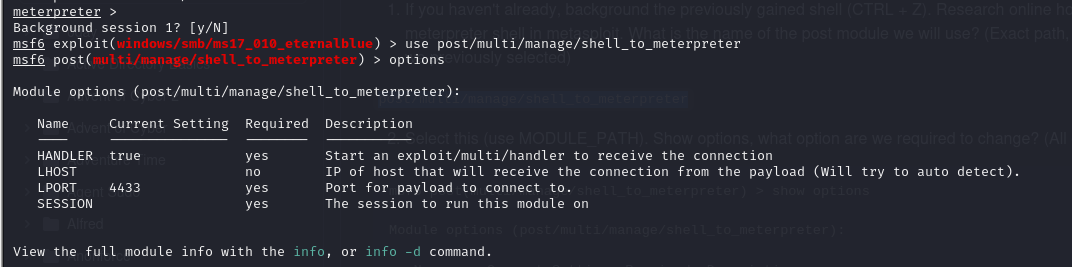


See, we gained the **meterpreter** session. Now we’ll see what privileges we got after typing sysinfo.



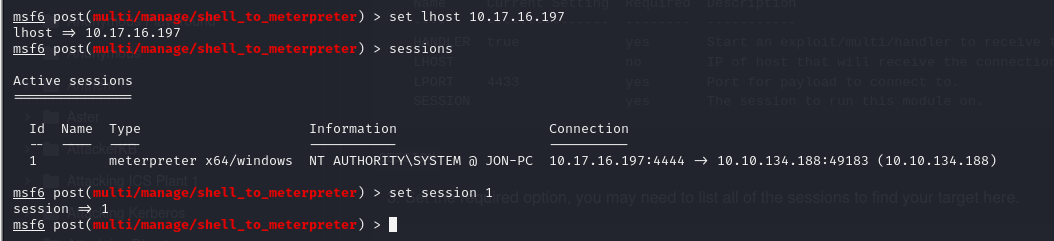
We can see that we don’t have much privileges as **meterpreter** . We need to **escalate privileges** using a post module which is in Metasploit .

We’ll background the meterpreter session using CTRL+Z and use the post module.



We need to change the LHOST and SESSION option in the options menu.

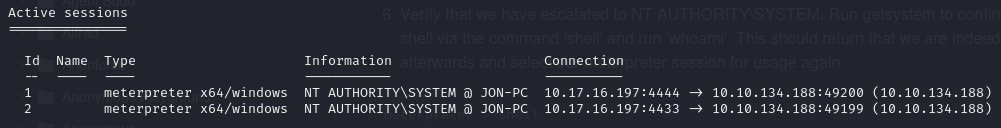
We can see the session after typing sessions in msfconsole and set it to 1.



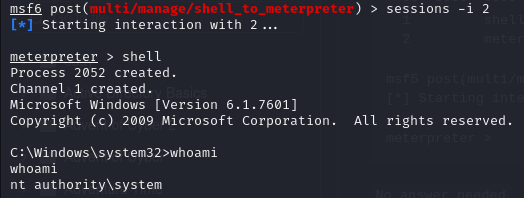
We’ll now run the module.



After completion we can see there are two sessions now.



Now we’ll open session 2 with **session -i 2**  and type shell.



We can see we’re now **nt authority\system (root).**

Now we’ll explore the target machine. After going into the **C:\**  directory we can find the flag.

