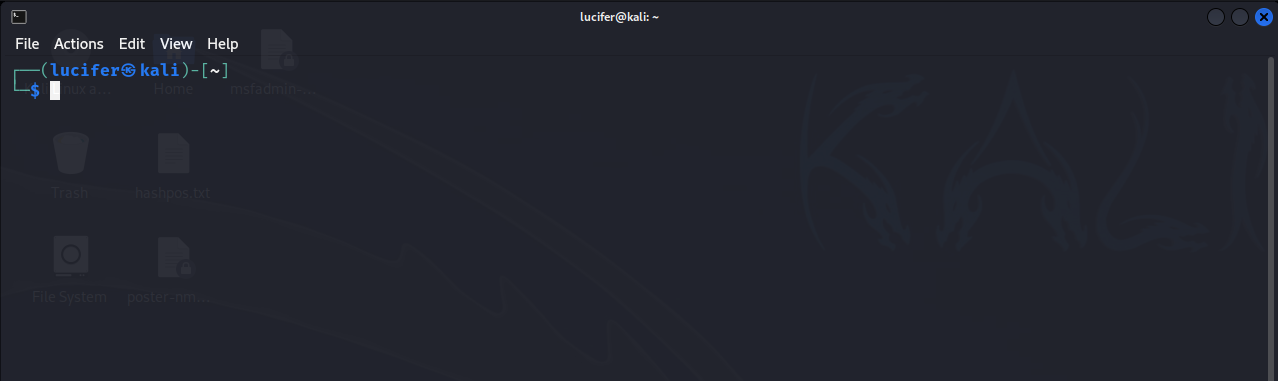
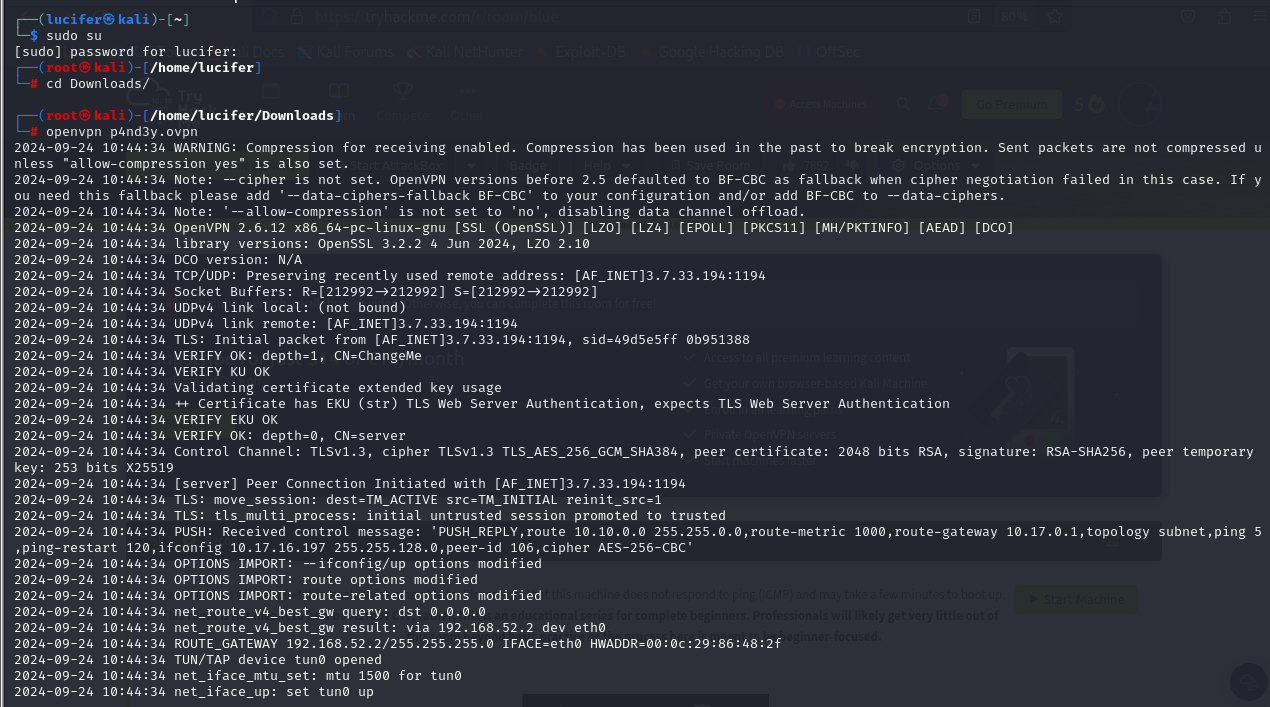
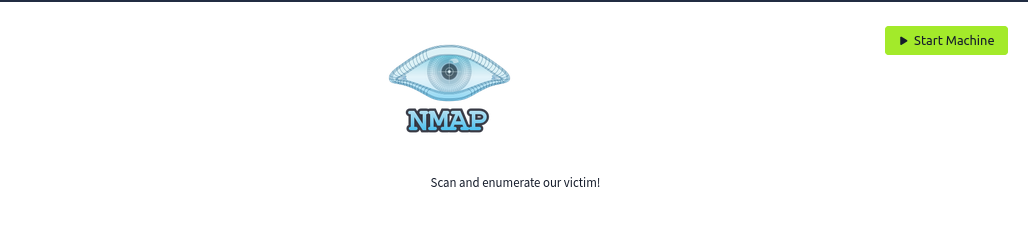
Blue is a box on tryhackme (<https://tryhackme.com/r/room/ice>) created by DarkStar7471.

Here our **terminal**  is opened.

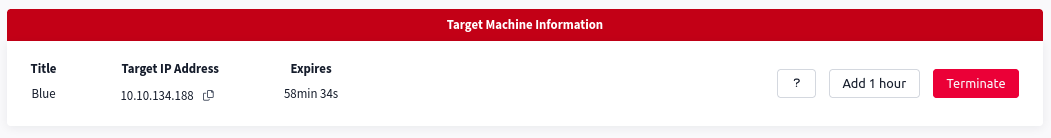


Now we will connect our **vpn** with tryhackme with the help of **openvpn** from vpn’s file downloaded path after doing **sudo**.

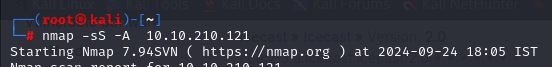


Now, we will check the ip of the target machine from tryhackme website which will be shown after pressing the **start machine** button. ****

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

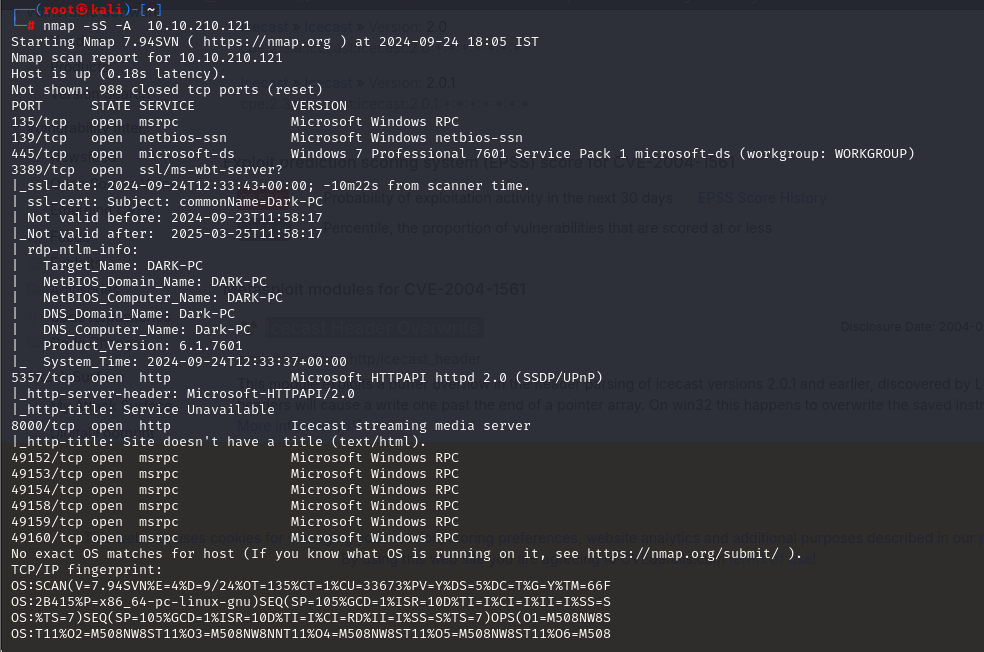


After getting the target ip first thing we’ll do is **nmap** scan to see the open ports and more machine’s info.



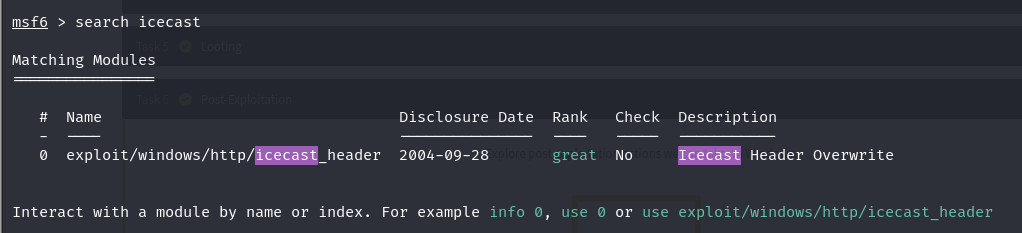
Here I am using **nmap -sS -A <IP>** (SYN Scan to see all the hidden ports)**.**

Seems like our scan is completed. Looks like there are total 12 ports open and 3 under 1000.



Now that we have know the information from port 8000 using nmap and there lies a severe Icecast Header Overwrite vulnerability. We can use **searchsploit** or google it about the previous exploits in it. Guess what we found it using searchsploit. Seems that it has severe vulnerability CVE-2004-1561 with impact score of 6.1.

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.

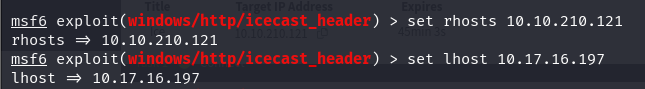


We found an exploit. Now we’ll use it.

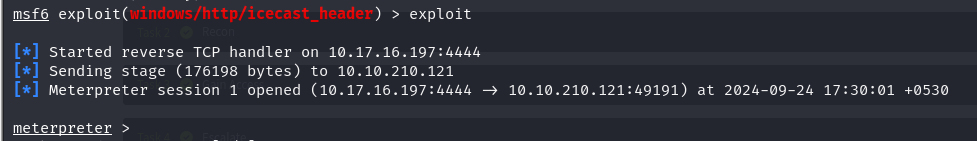
We’ll set the required options needed to exploit the target machine.



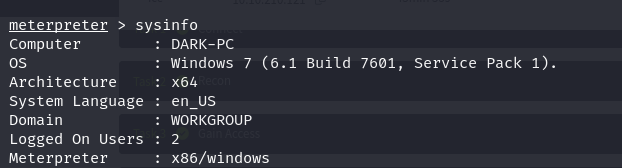
We’ll set **RHOSTS** as the target ip and **LHOST** as our local machine’s address ip and rest will be default.



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

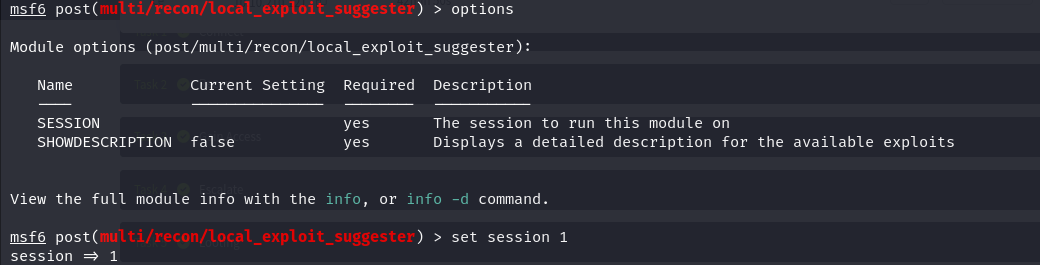


See, we gained the **meterpreter** session. Now we’ll see what privileges we got after typing sysinfo.



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 .

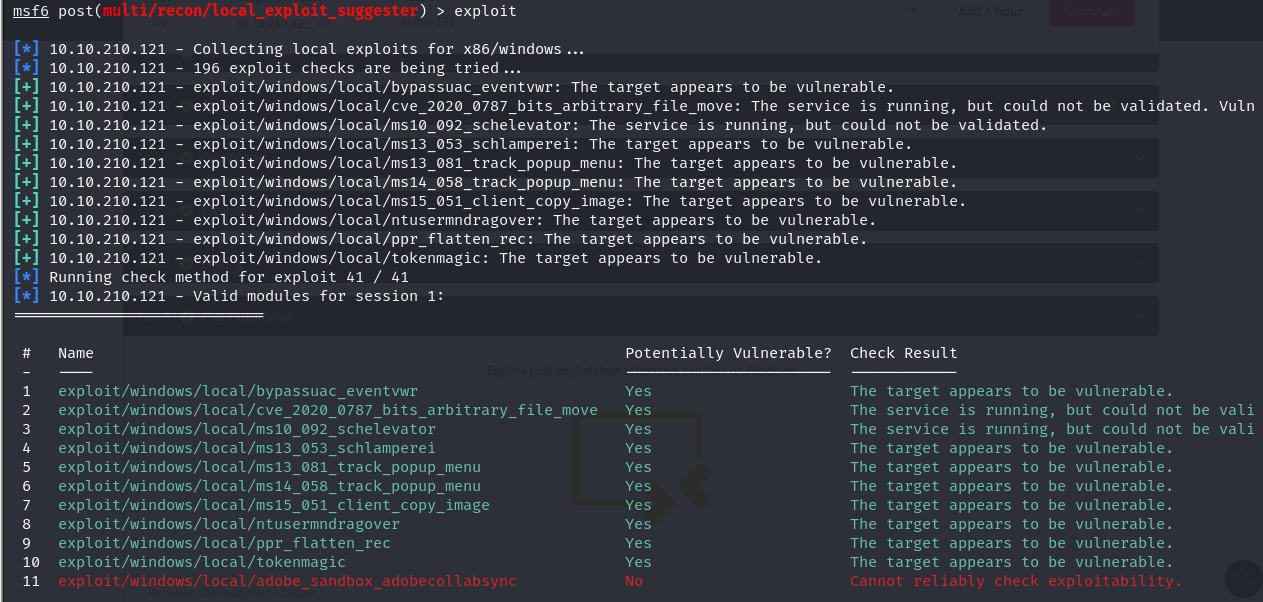
We’ll background the meterpreter session using CTRL+Z and use the post module on which we are using local exploit suggestor to see the that the target machine is vulnerable to which exploits.



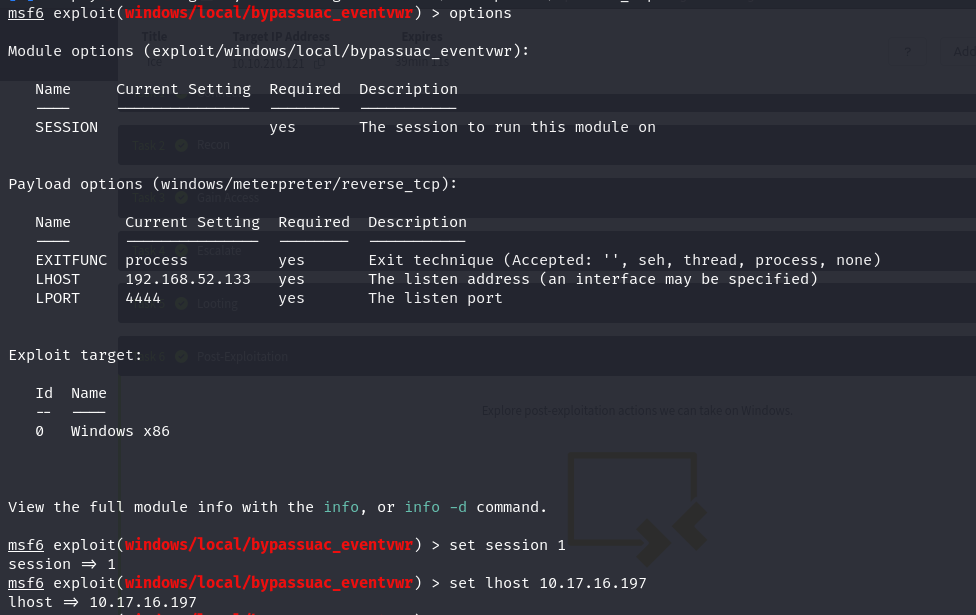
SESSION option in the options menu.

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

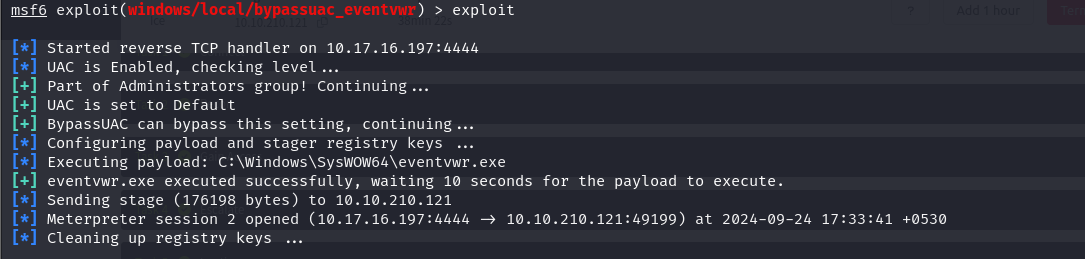
We’ll now exploit the module.



After completion we will select the first exploit and modify their options.

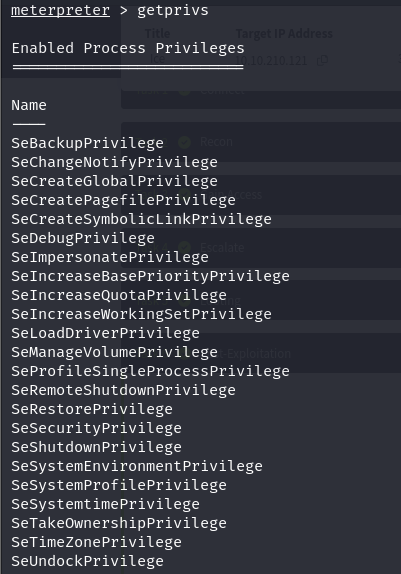


We will now start the exploit.

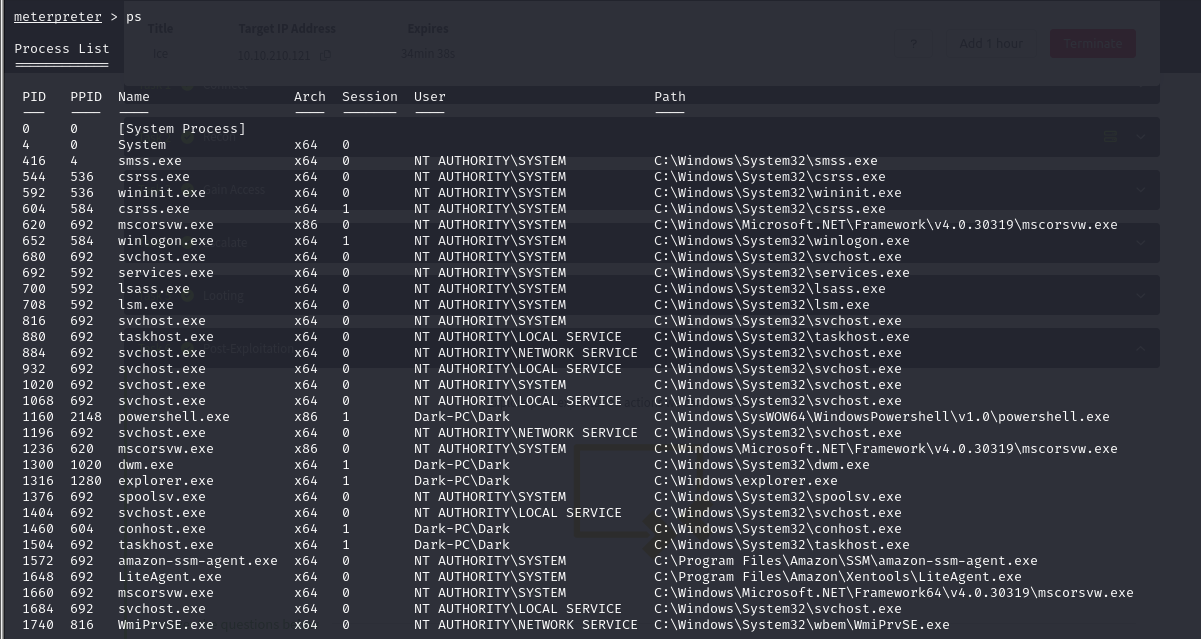


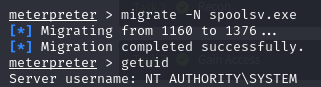
Again we entered the meterpreter session. But we have NT AUTHORITY\SYSTEM.

We can see and modify the privileges using **getprivs** to take ownership of the target machine**.**

****

We will now see the processes running on the target machine using **ps** command to execute the exploit.

We will migrate to the **spoolsv.exe** process using **migrate -N <process name>** and check the userid of the process running which will help us know whether we can run the exploit in it or not.

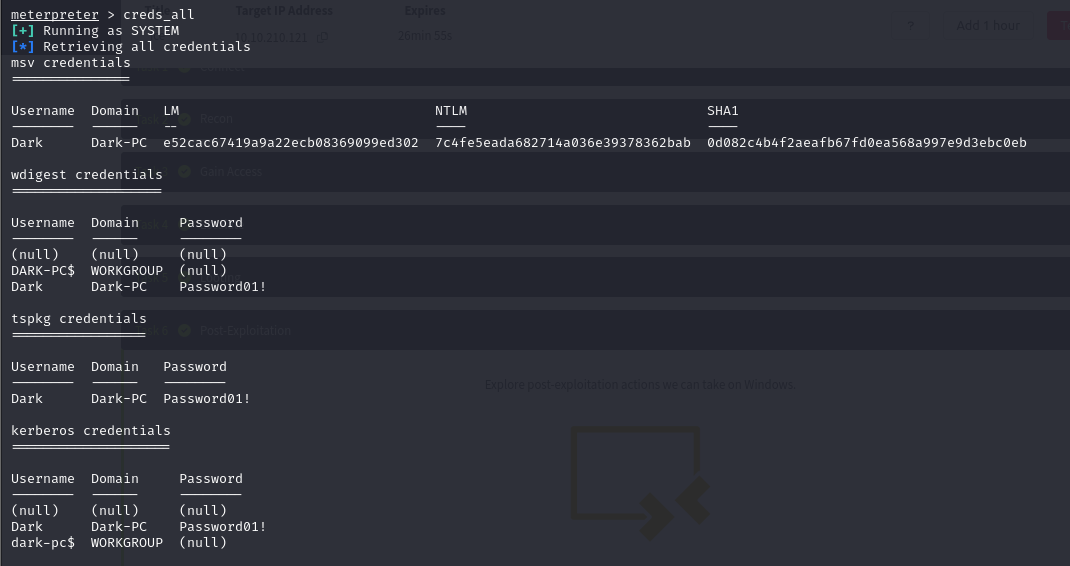


We will now load **kiwi** which is pre-installed tool with Metasploit to dump the password hashes in the target system.



As we see **kiwi**  is now loaded in target machine and we can now execute kiwi related commands there.

So we will use **creds\_all**  to dump all the credentials in the target machine.



We can see the user **Dark’s** password is listed which was our motive to find.