OLD DOMINION UNIVERSITY

CYSE 301 CYBERSECURITY TECHNIQUES AND OPERATIONS

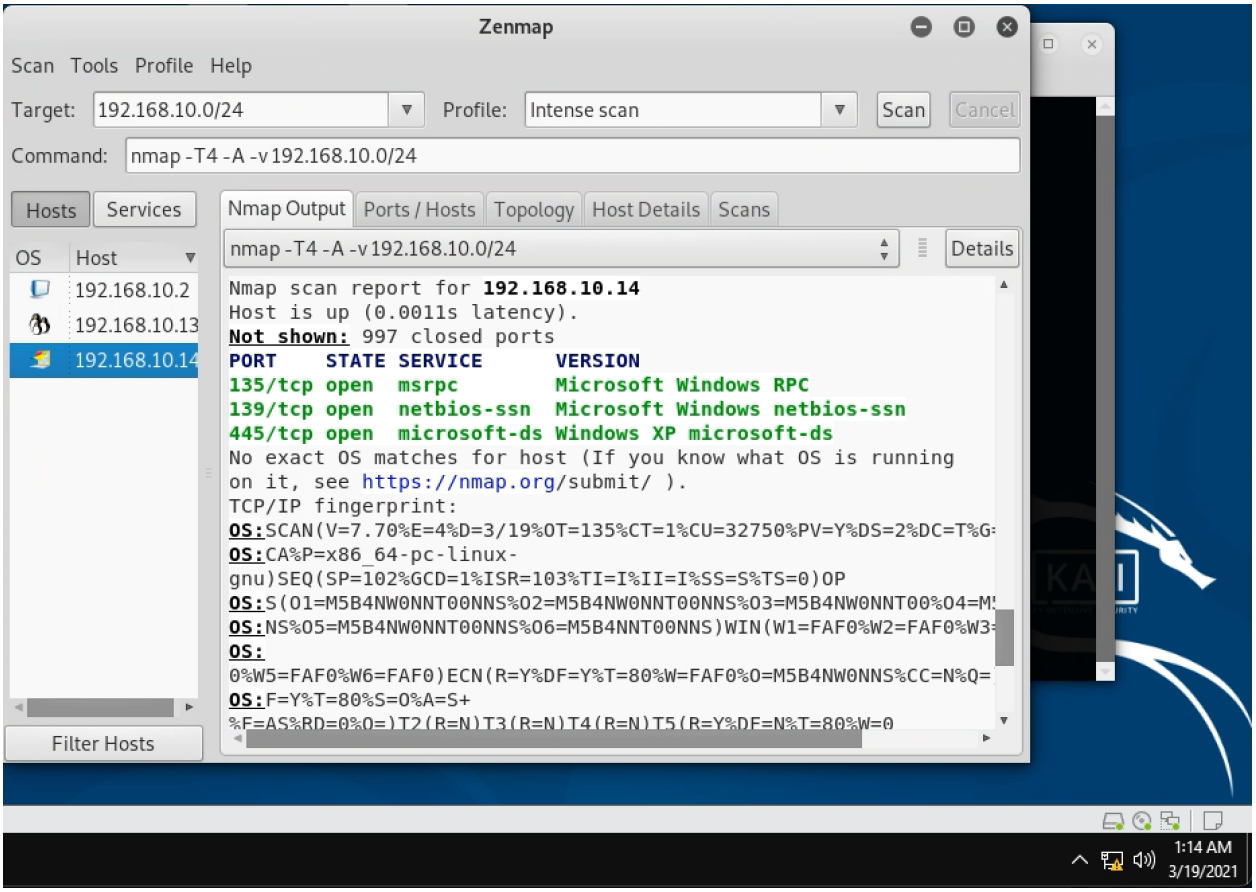
Assignment M3.1:Penetration Test on Windows XP

Joy Diggs

00491693

STEP 1-TASK A

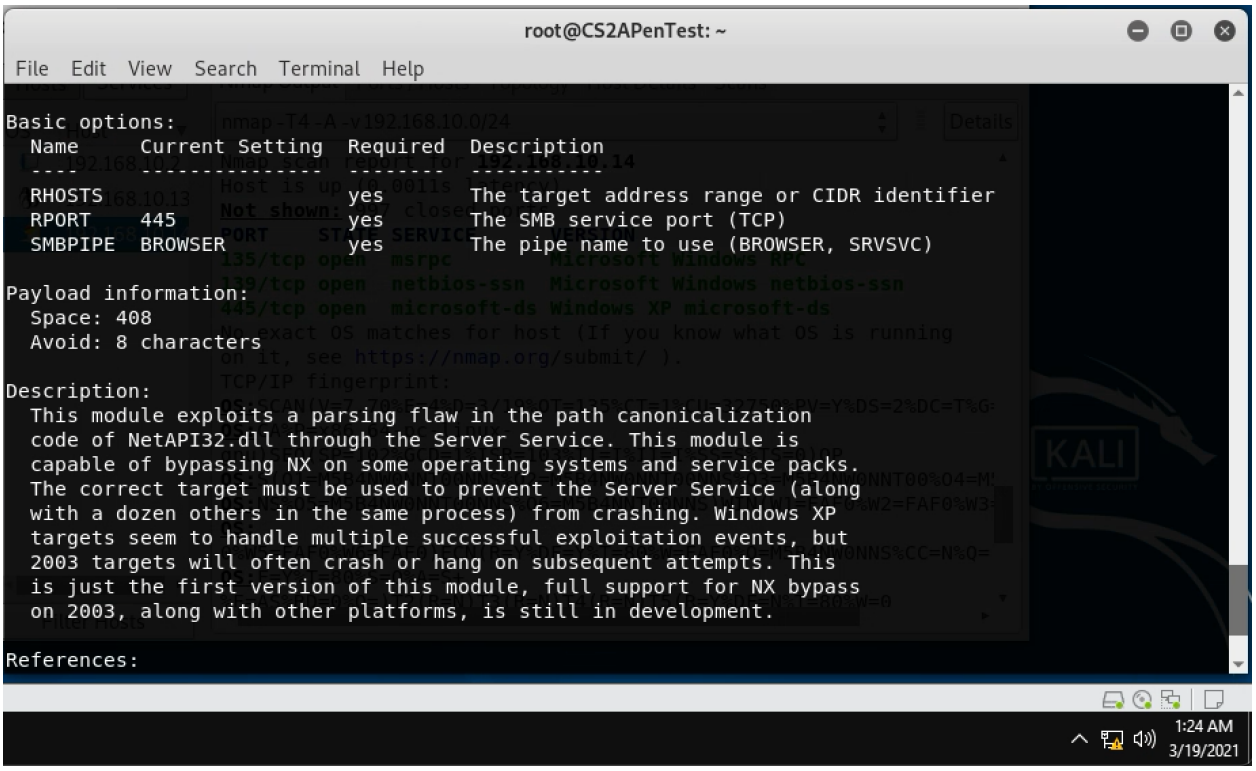
1. Follow the instruction discussed in the class and find all the possible vulnerabilities in Windows XP by using Nmap.



Above is the screenshot of the nmap scan of the network showing the open ports.

STEP 2

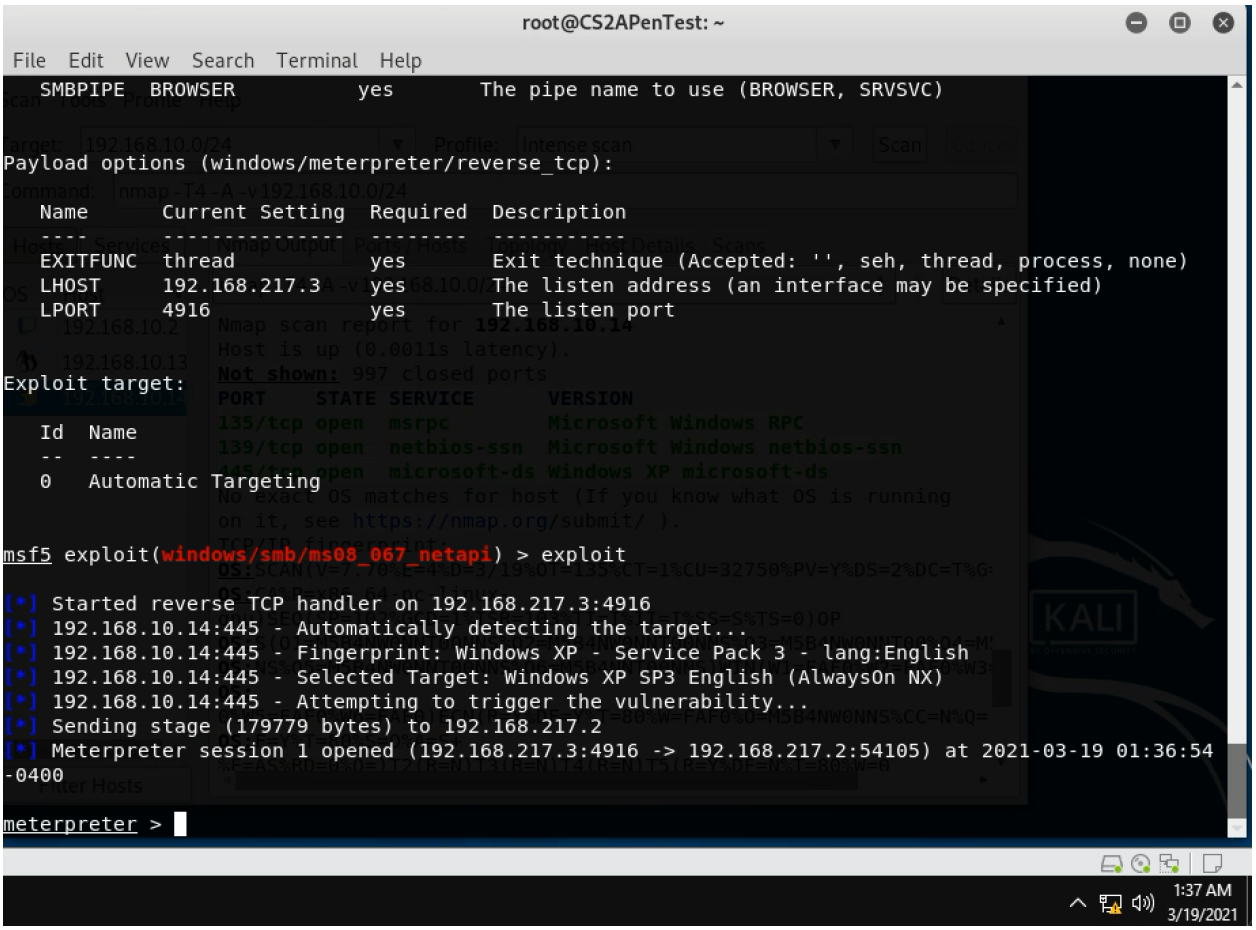
2. In Metasploit, search the detailed information and usage regarding the exploit: ms08_067_netapi. Which port on the target system will be exploited if I use this exploit? Is this port available on the target Windows XP?



Above is the screenshot of the information on the exploit. The port 445 will be exploited on the target machine and it is open and available on the target machine.

STEP 1-TASK B

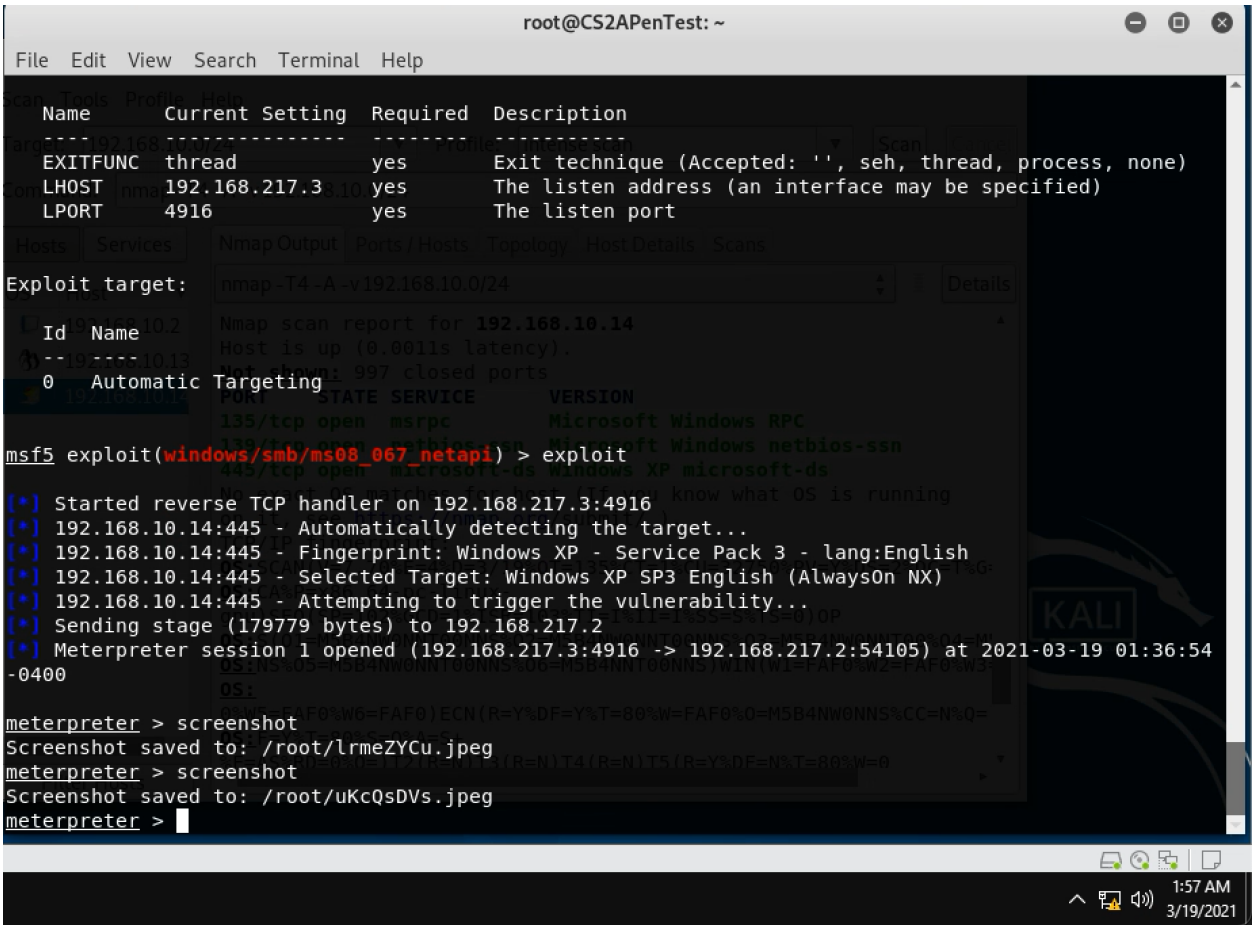
1. Configure Metasploit framework to set up a meterpreter reverse shell connection to the target Windows XP by using the following configurations. Listening Port: UIN without zeros.



Above is the screenshot of the configured framework for the meterpreter reverse shell.

STEP 1-TASK C

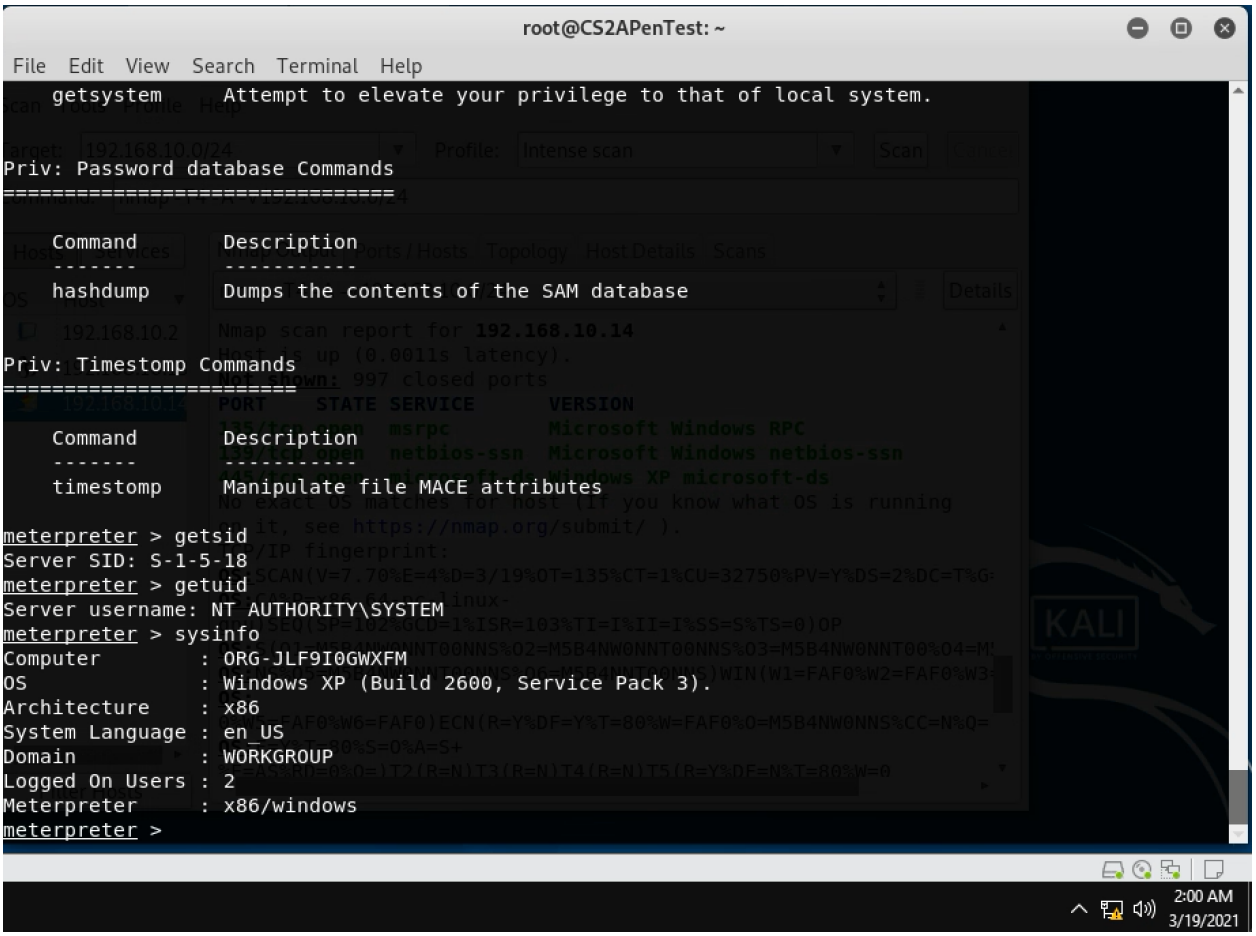
1. Take a screenshot of the target machine.



Above is the screenshot of the screenshot of the target machine using meterpreter shell.

STEP 2

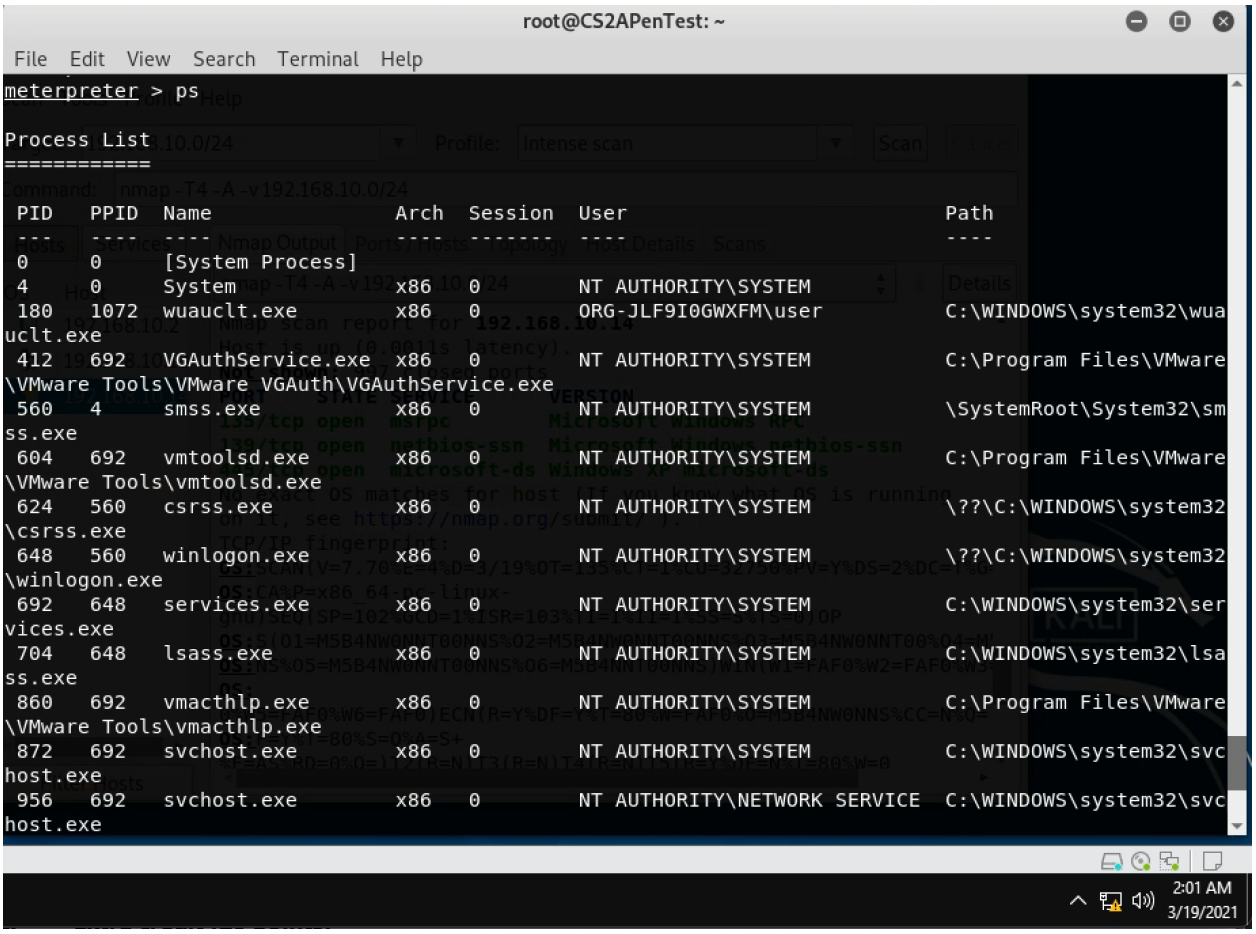
2. Collect the target system info.



Above is the screenshot of the target system info.

STEP 3

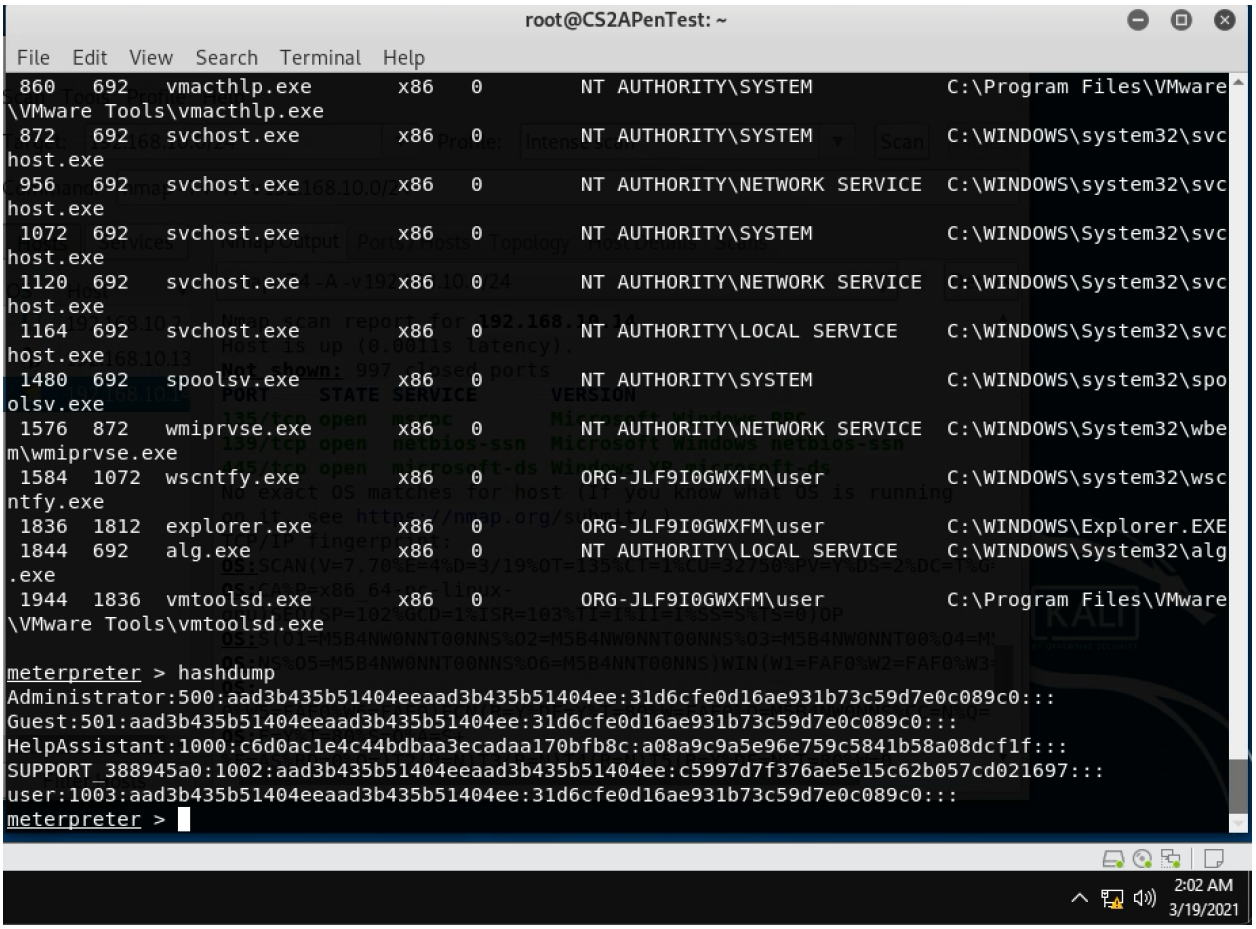
3. Collect the list of the running processes on the target machine.



Above is the screenshot of the running processes on the target machine.

STEP 4

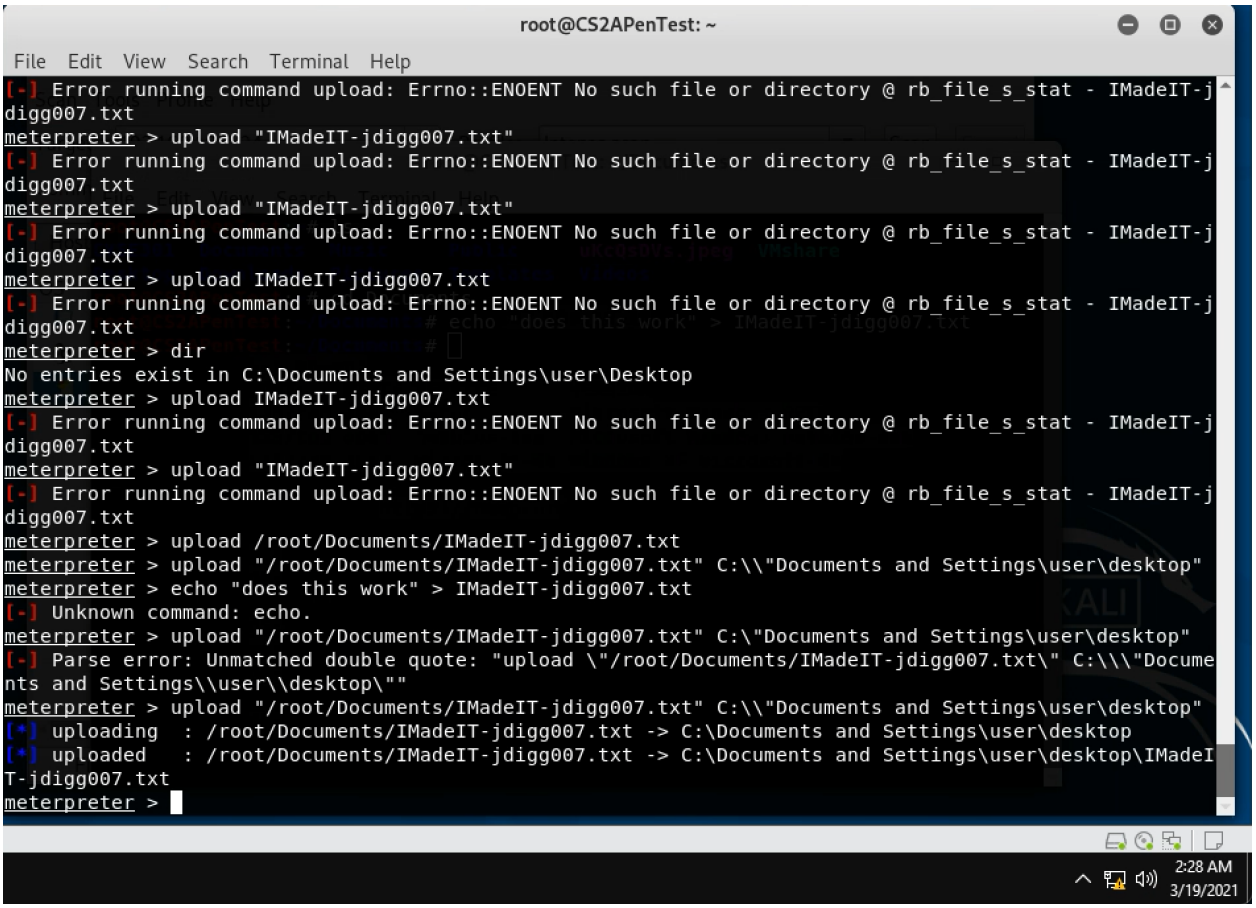
4. Collect the password hashes of the current users.

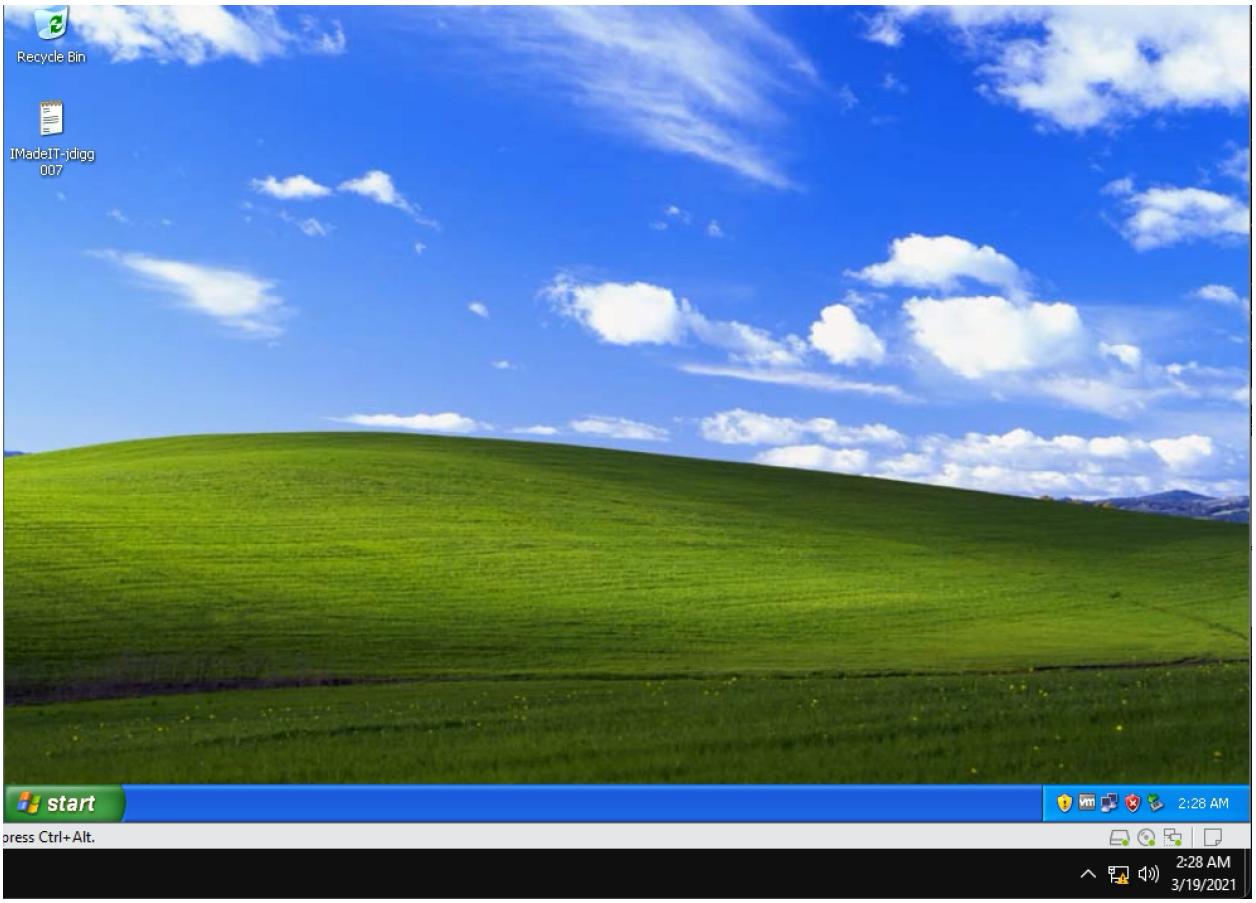


Above is the screenshot of the current users' passwords on the system.

STEP 5

5. Upload a file called "IMadeIT-YourMIDAS.txt" to the target's desktop. Login to the Windows XP and check if the file exist.

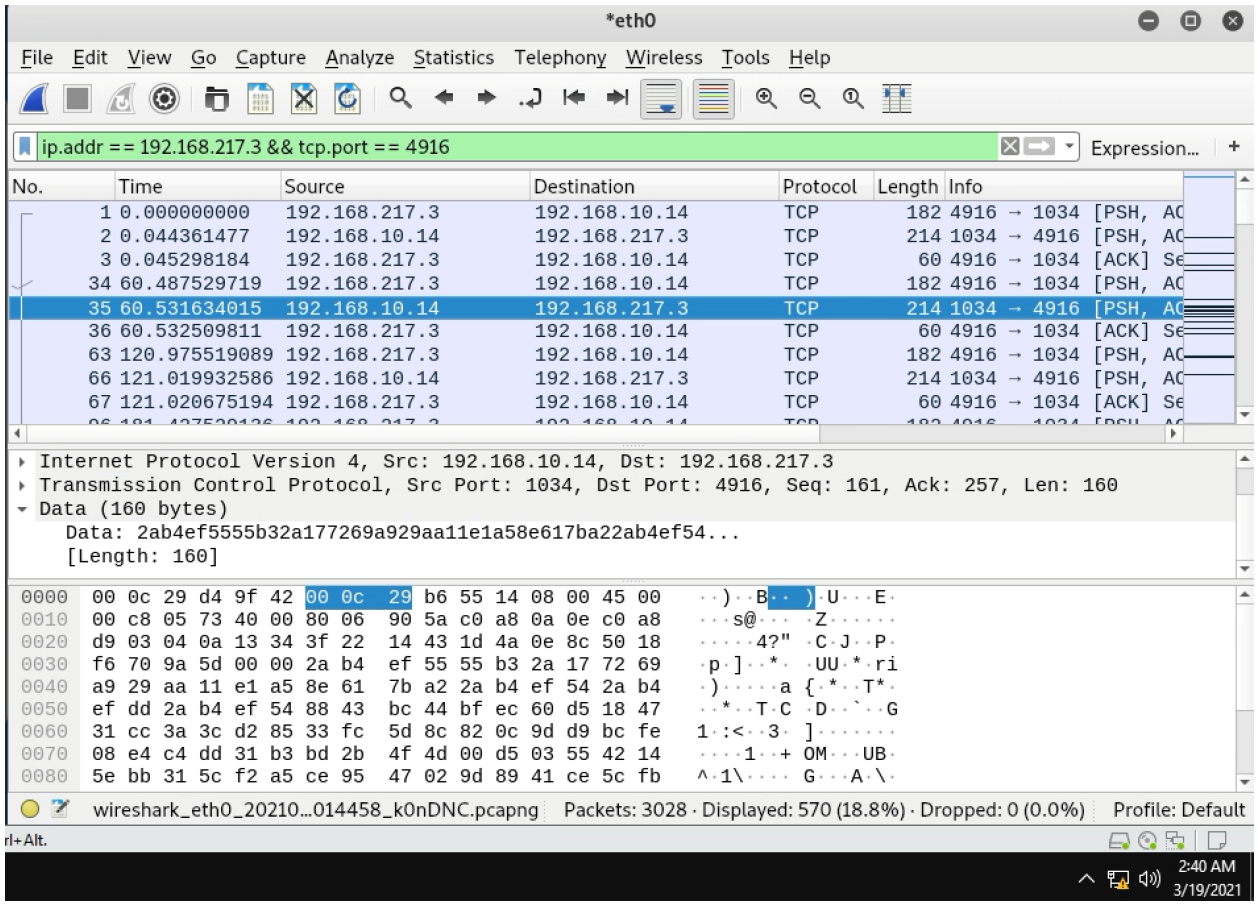

root@CS2APenTest: ~
File Edit View Search Terminal Help
[-] Error running command upload: Errno::ENOENT No such file or directory @ rb_file_s_stat - IMadeIT-jdigg007.txt
meterpreter > upload "IMadeIT-jdigg007.txt"
[-] Error running command upload: Errno::ENOENT No such file or directory @ rb_file_s_stat - IMadeIT-jdigg007.txt
meterpreter > upload "IMadeIT-jdigg007.txt"
[-] Error running command upload: Errno::ENOENT No such file or directory @ rb_file_s_stat - IMadeIT-jdigg007.txt
meterpreter > upload IMadeIT-jdigg007.txt
[-] Error running command upload: Errno::ENOENT No such file or directory @ rb_file_s_stat - IMadeIT-jdigg007.txt
meterpreter > dir
No entries exist in C:\Documents and Settings\user\Desktop
meterpreter > upload IMadeIT-jdigg007.txt
[-] Error running command upload: Errno::ENOENT No such file or directory @ rb_file_s_stat - IMadeIT-jdigg007.txt
meterpreter > upload "IMadeIT-jdigg007.txt"
[-] Error running command upload: Errno::ENOENT No such file or directory @ rb_file_s_stat - IMadeIT-jdigg007.txt
meterpreter > upload /root/Documents/IMadeIT-jdigg007.txt
meterpreter > upload "/root/Documents/IMadeIT-jdigg007.txt" C:\\"Documents and Settings\user\desktop"
meterpreter > echo "does this work" > IMadeIT-jdigg007.txt
[-] Unknown command: echo.
meterpreter > upload "/root/Documents/IMadeIT-jdigg007.txt" C:\"Documents and Settings\user\desktop"
[-] Parse error: Unmatched double quote: "upload \"/root/Documents/IMadeIT-jdigg007.txt\" C:\\\"Documents and Settings\\user\\desktop\""
meterpreter > upload "/root/Documents/IMadeIT-jdigg007.txt" C:\\"Documents and Settings\user\desktop"
[*] uploading : /root/Documents/IMadeIT-jdigg007.txt -> C:\Documents and Settings\user\desktop
[*] uploaded : /root/Documents/IMadeIT-jdigg007.txt -> C:\Documents and Settings\user\desktop\IMadeIT-jdigg007.txt
meterpreter >
2:28 AM
3/19/2021



Above is the screenshot of the file uploaded on the desktop of the target machine.

TASK D

Assume Internal Kali (the network admin) does not aware of this live attack. How to locate this session by checking the firewall logs and filter the related traffic in the Wireshark (running on Internal Kali)?



Above is the screenshot of the filtered traffic showing the session that we used.