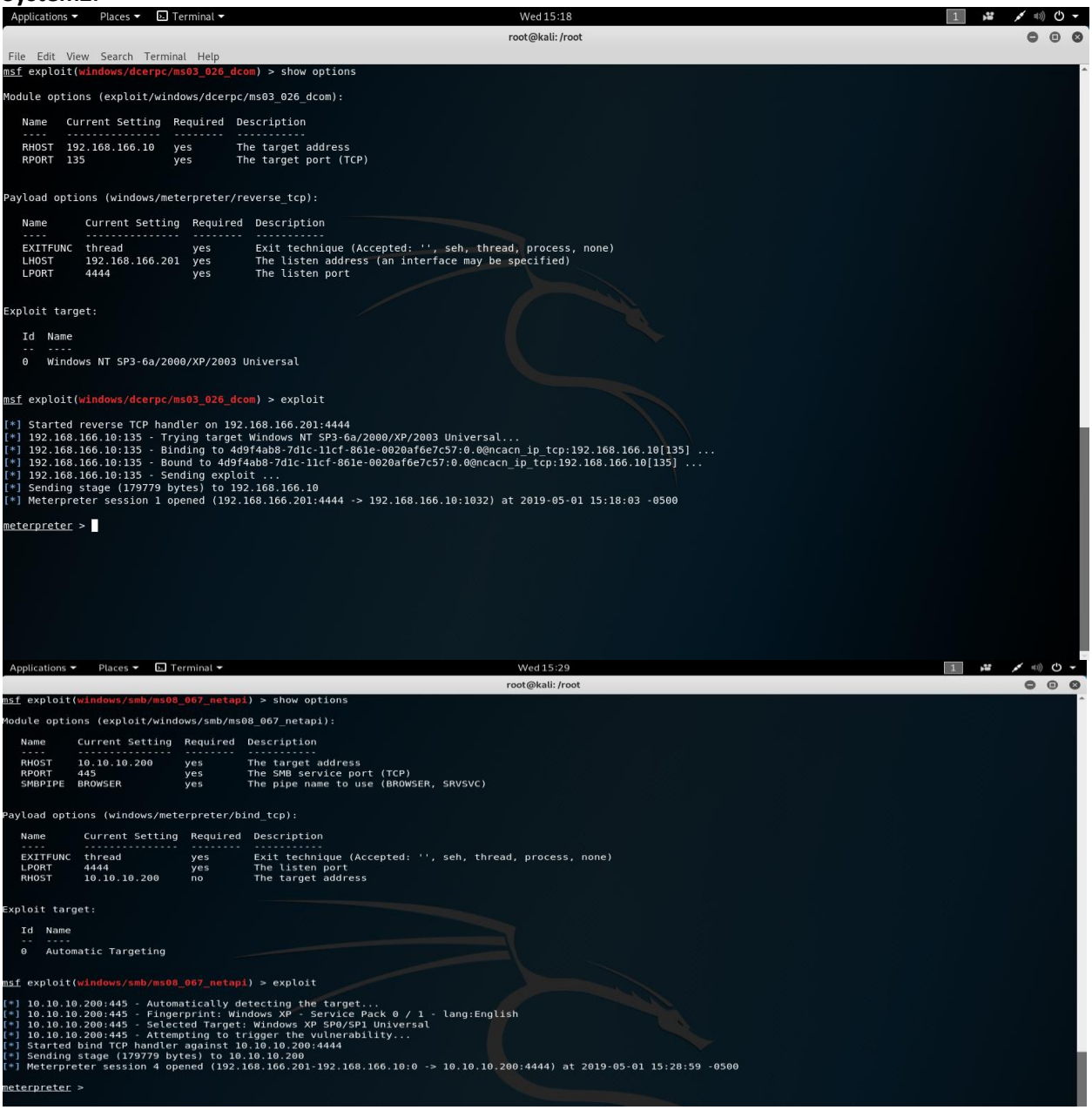
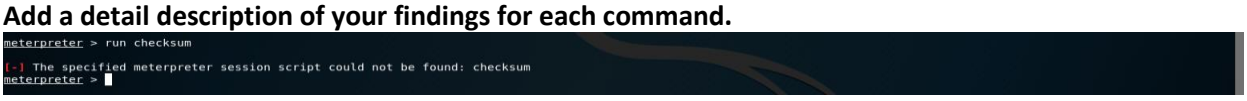
1. From Kali Linux, use any exploit to access to System1, and then enable a Meterpreter session on System2.



Kali linux accessing System1 through exploit windows/dcerpc/ms03_026_dcom. Once accessed, run arp_scanner to find related systems then add the route to connect to System2. Scan auxiliary ports to find out vulnerable ports, in this case 445. Then, exploit windows/smb/ms08_067_netapi because it utilizes port 445 to enable a meterpreter session on System2.

2. Once you open a Meterpreter session in System2 execute the following commands: a. run checksum b. run get_env c. run get_application_list
Add a detail description of your findings for each command.

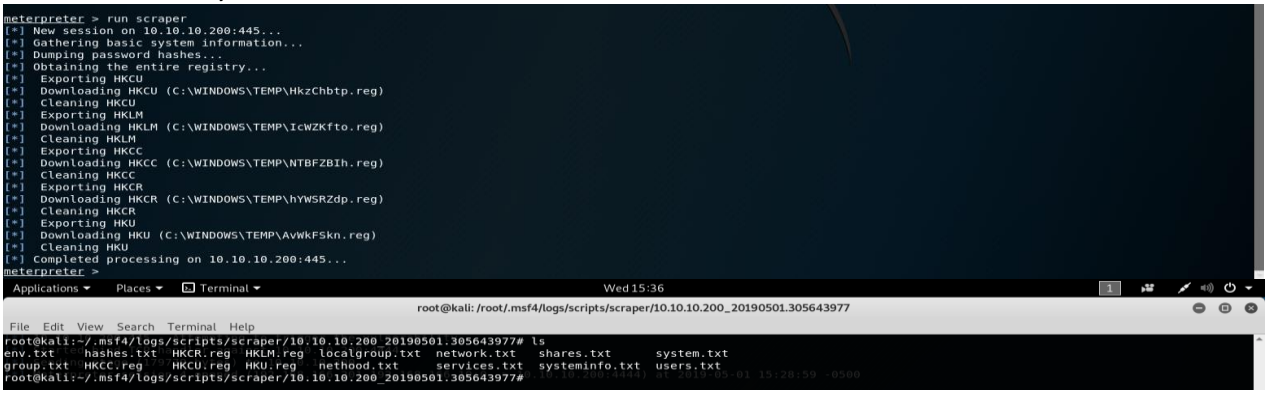


The script to execute checksum is not found so there were no findings for this command.

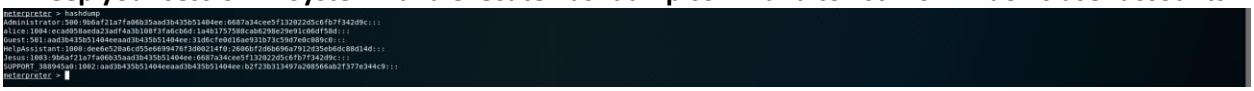
Lists of environment variable values of certain processes.

List of installed applications along with the version number. In this case, only version 3.1 of Windows Installer is installed.

3. Keep your session in System2 and execute run scraper command, Are you able to get some information? if so, what kind of information?



4. Keep your session in System2 and execute hashdump command to list MS Windows user accounts.



List of user accounts of System2, in this instance I have also created user ‘alice’ which is also listed with the default accounts.

5. In Linux, user ID (located in /etc/passwd) in the range of 0 to 99 should be statically allocated by the system, while UIDs from 100 to 499 should be reserved for dynamic allocation by system administrators and post install scripts. Is there a similar logic of UID ranges for Windows users?
Windows utilizes Security Identifiers, or SID, in pace of UID. SID follows similar log of UID ranges like Linux, such as administrator accounts ending in 500 or guest accounts ending in 501, and so on and so on.

6. Keep your session in System2, enable the windows shell and create a network_[YOUR_PAWPRINT].txt file with the content of the ipconfig /all command execution. Can you copy the file to the Kali system, add a line to the end of the file and copy it back to System2?.

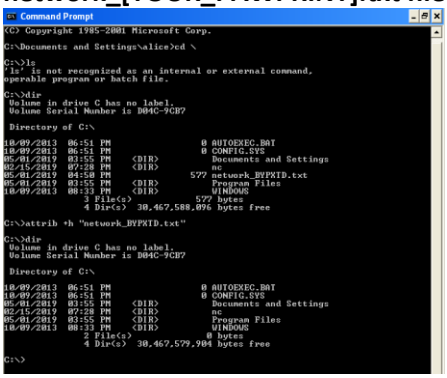
Creation of network_BYPXTD.txt with the contents of ipconfig /all command execution.

Downloading network_BYPXTD.txt onto the kali system. Then editing the file “vi network_BYPXTD.txt” and adding a new line to the end of the file.

Uploading network_BYPXTD.txt back to System2.

Contents of network_BYPXTD.txt displayed on System2.

7. Keep your session in System2 with windows shell enabled and hide the network_[YOUR_PAWPRINT].txt file located (Use only command line in Windows).



Open the command prompt of System2 and change the directory to where network_BYPXTD.txt is located. Then executing “attrib +h ‘network_BYPXTD.txt’” in order to hide the file from the command line.

Display of System2 directory from kali showing the file is hidden here as well.