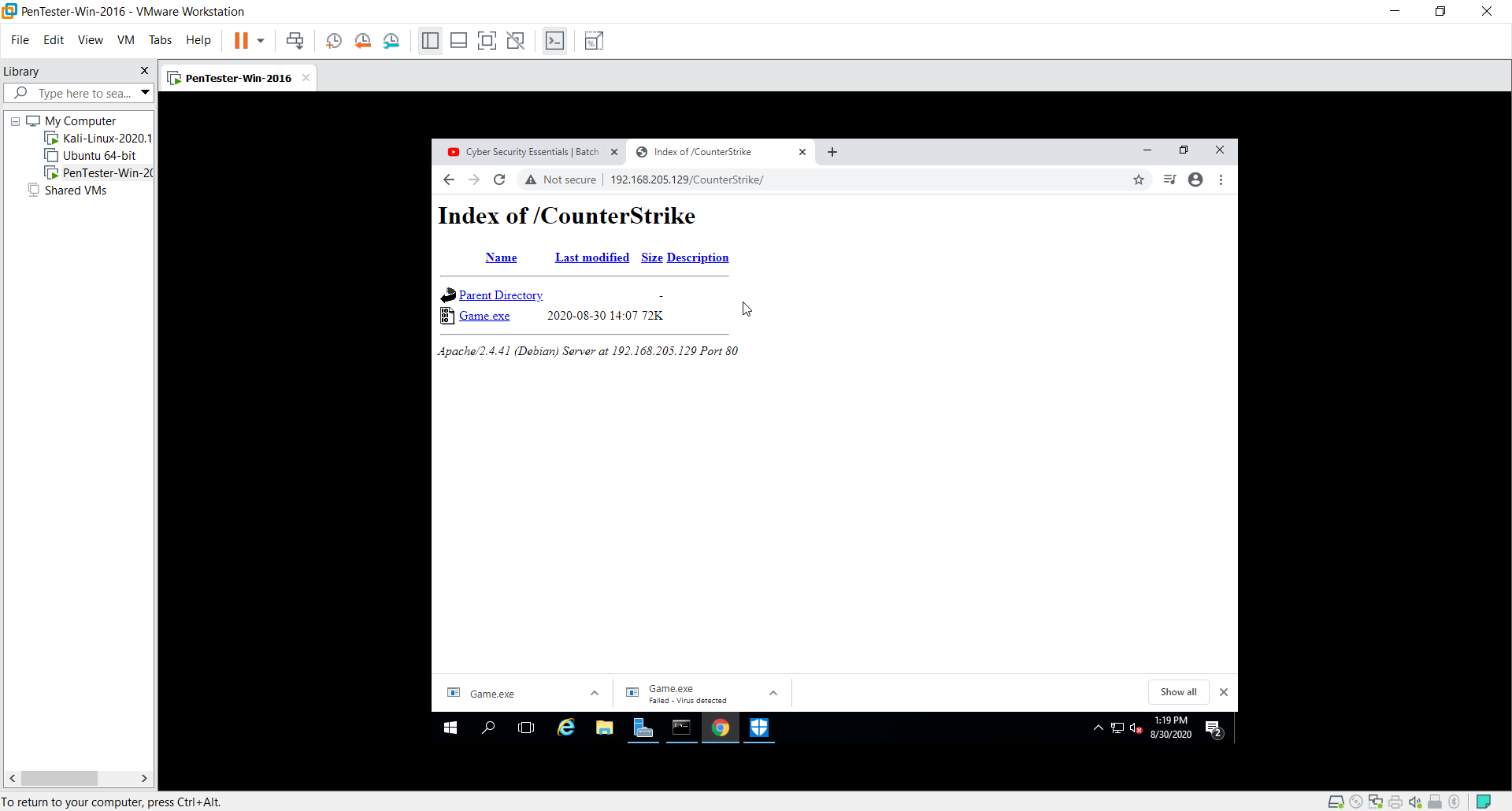
ASSIGNMENT 2 (DAY-6)

Question 1:

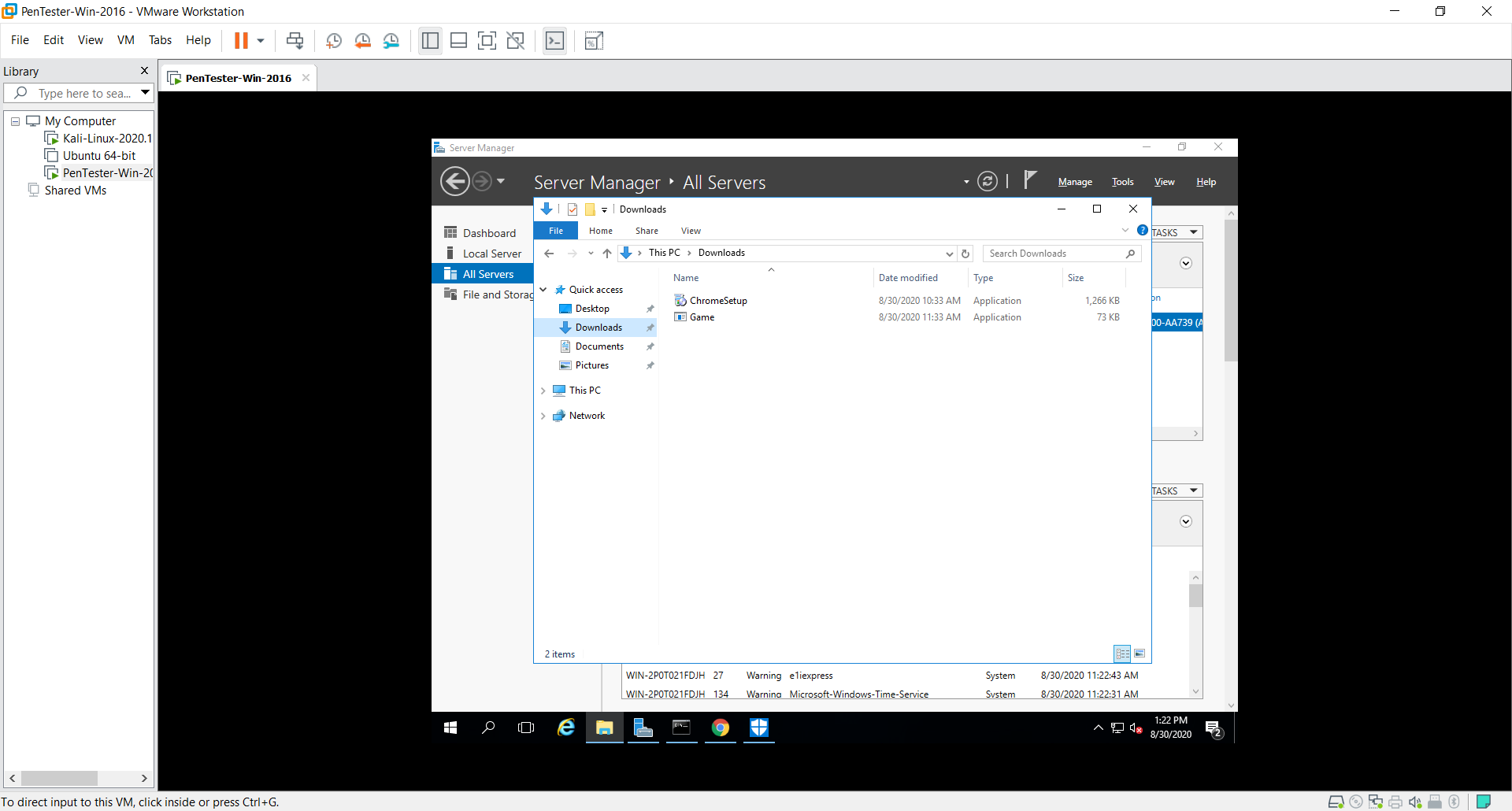
* Create payload for windows.
* Transfer the payload to the victim's machine.
* Exploit the victim's machine.

Answer:

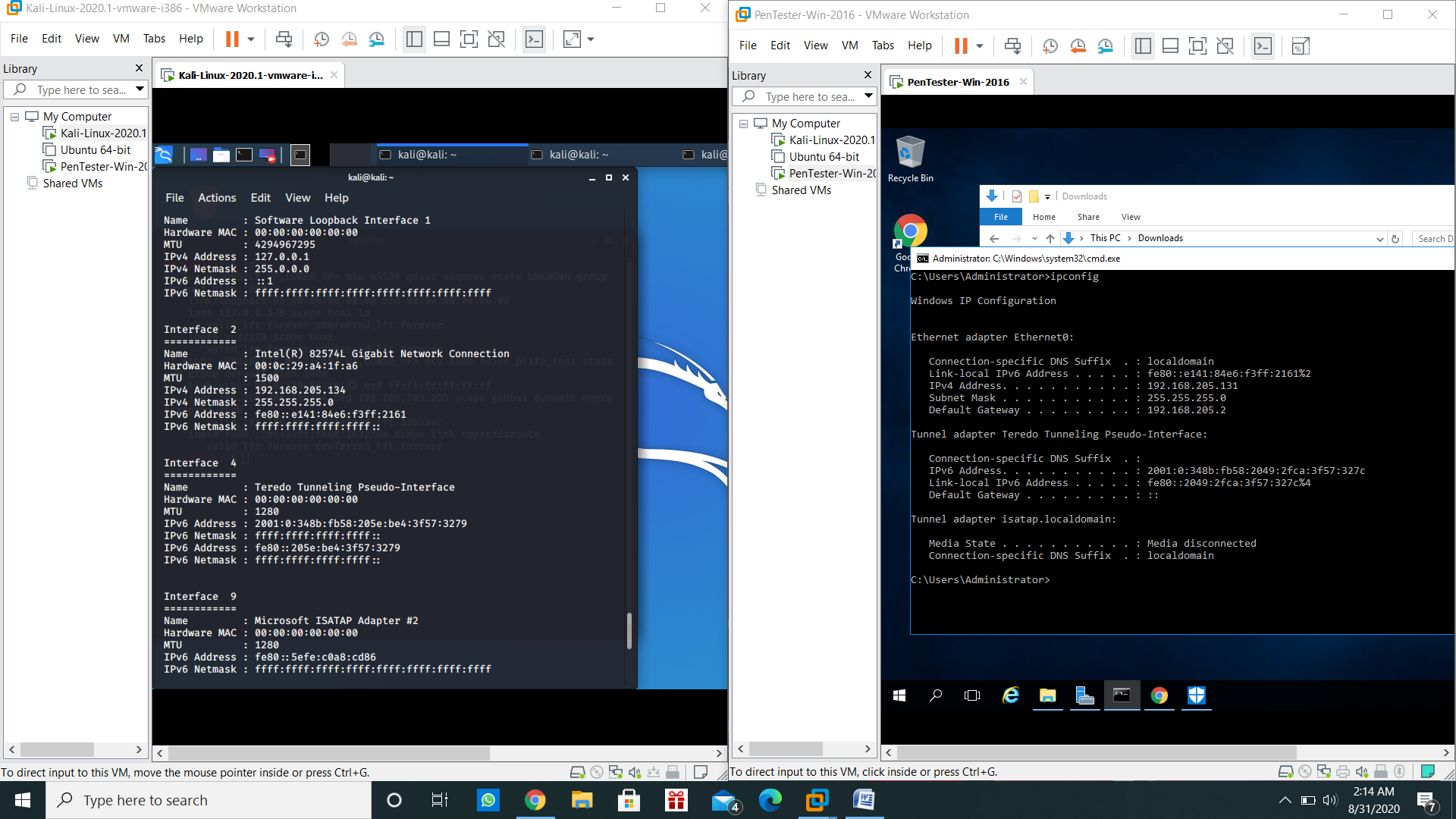
I used the Kali Linux machine to create a payload. First of all I created a web server using apache2 (system enable apache2). After that I hosted venom (an exploit) on the web server with the name as game.exe. Then I downloaded the venom with the victim machine and waited with the meterpreter session using msfconsole. Then I executed the exploit in the victim machine and as soon as I executed it I got into the msf5. There were number of commands which could be executed from the attacker machine to the victim machine. I used sysinfo, ipconfig, upload, download, and screenshot. The exploit was able to fetch the details accurately. Also I used powershell command to take control of the victim’s machine and run a command (get-child -recurse | get-content) to make the victim’s machine busy. Hence I successfully created a payload, transferred it to the victim’s machine and exploited it.



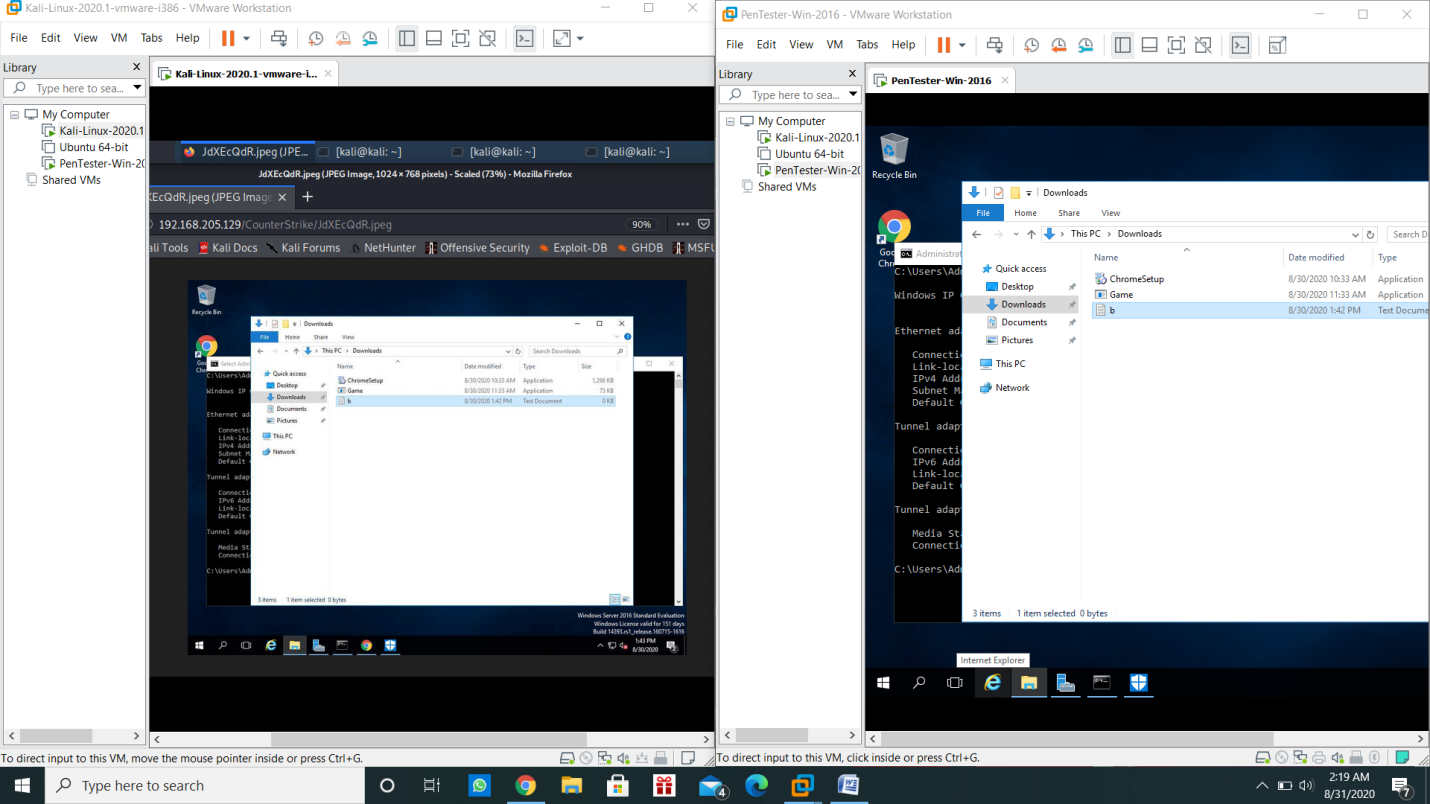
Game.exe (venom)



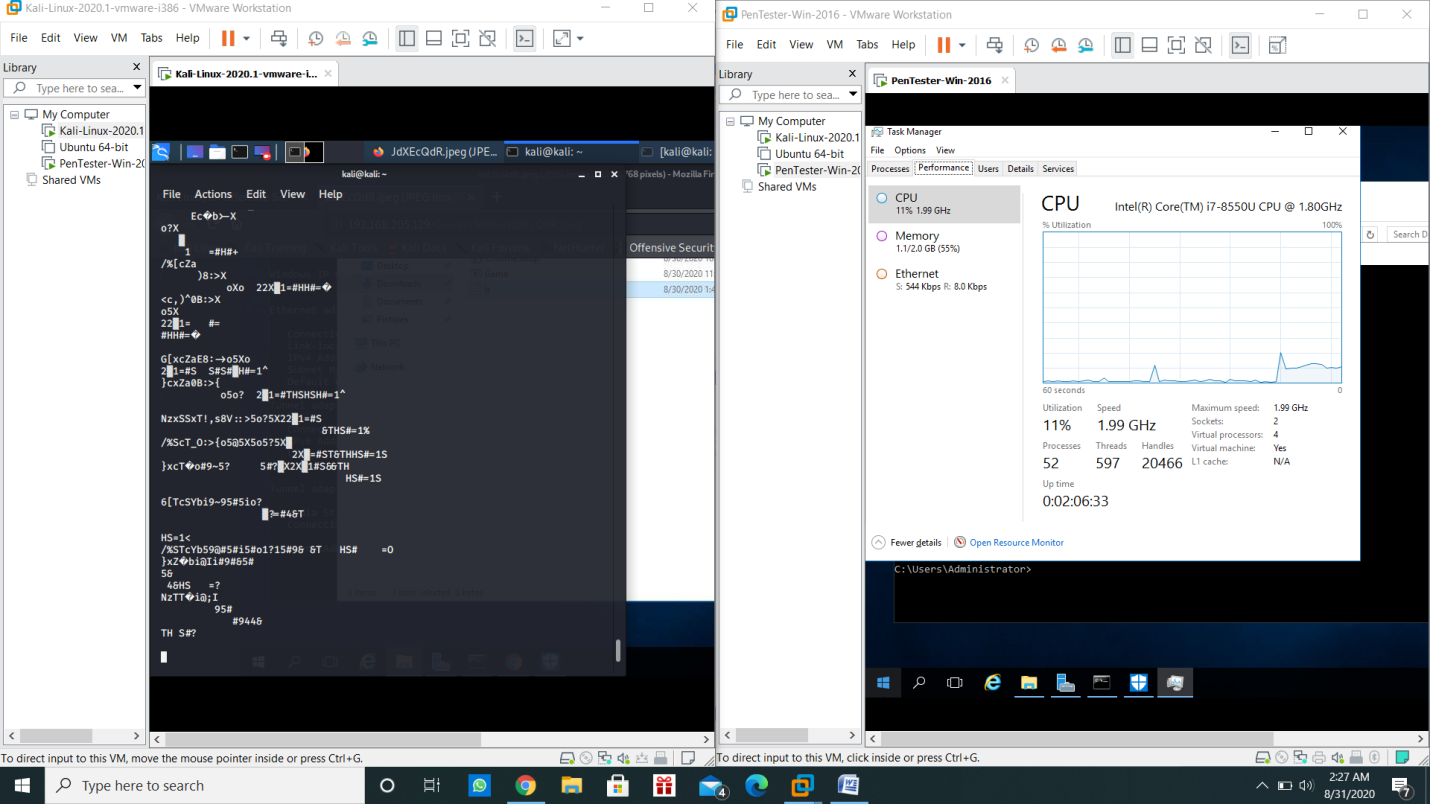
Victim downloaded the exploit.



Attacker used ipconfig to get the victim’s data.



Attacker used screenshot to take screenshot of the victim’s machine.



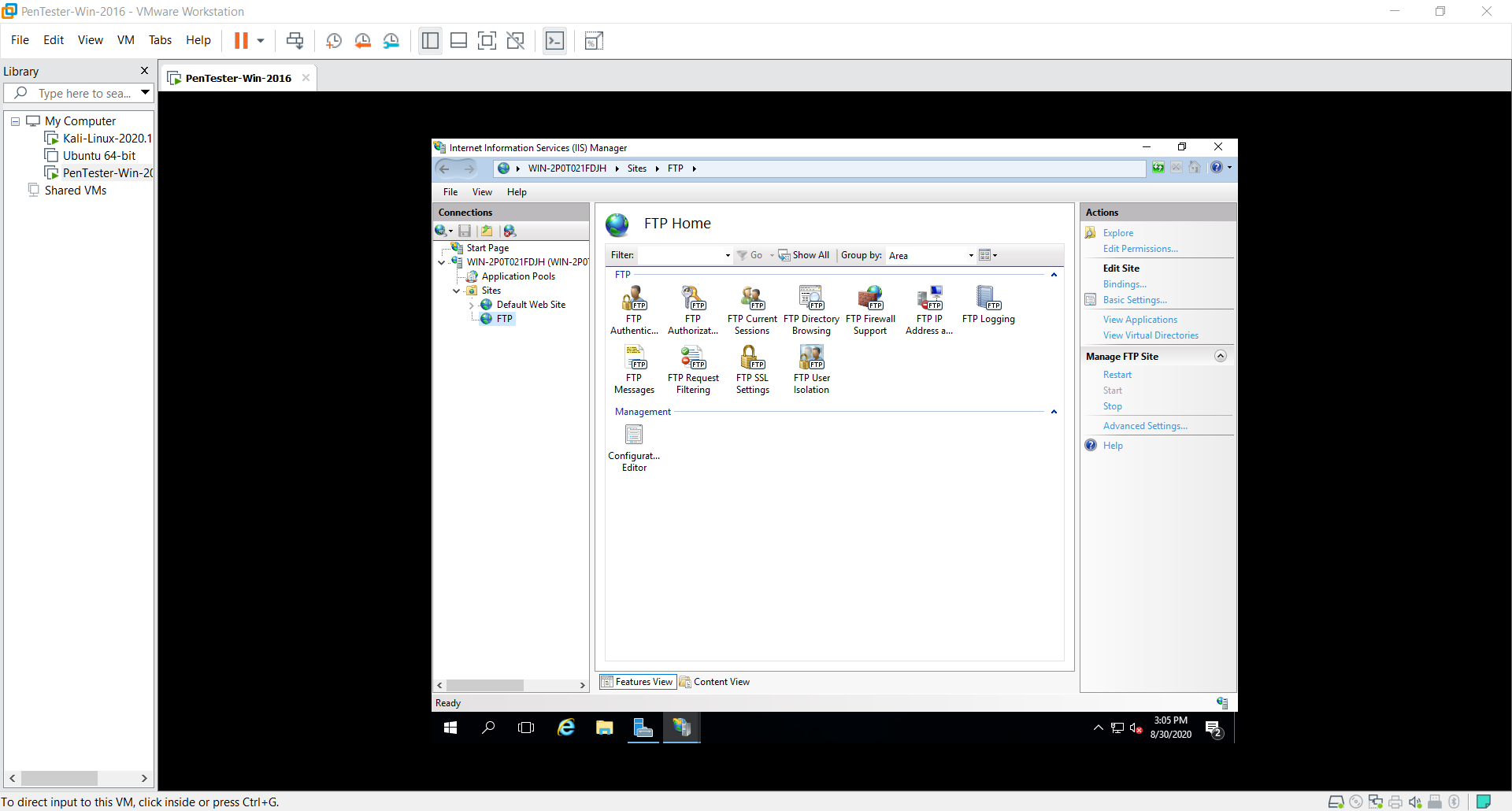
Attacker used payload to make the victim’s machine busy.

Question 2:

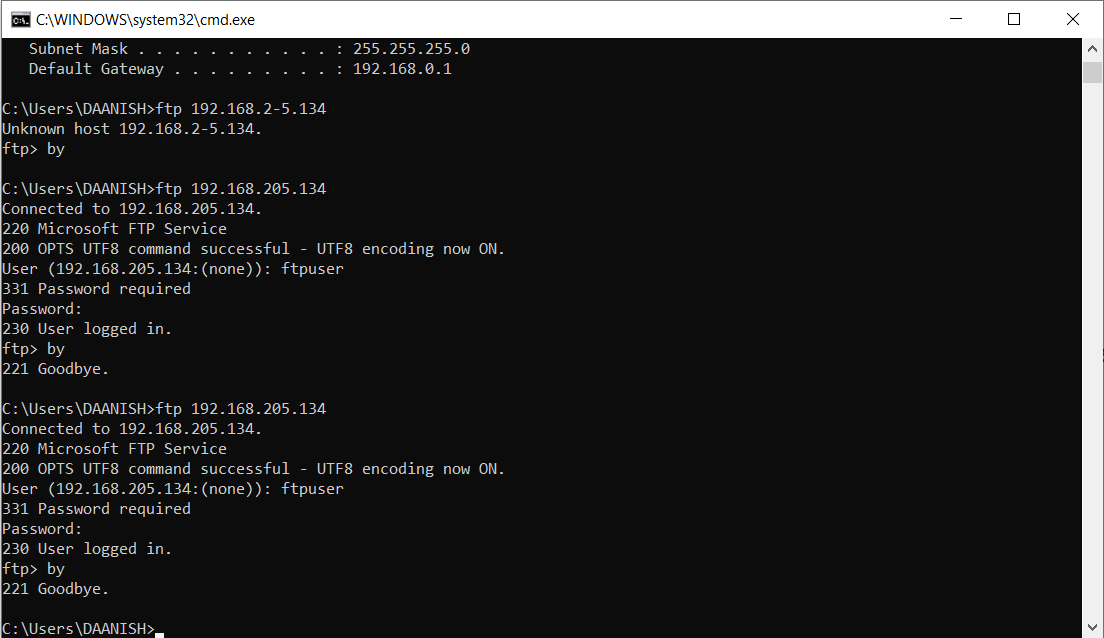
* Create an FTP server
* Access FTP server from windows command prompt
* Do a mitm and username and password of FTP transaction using wireshark and dsniff.

Answer:

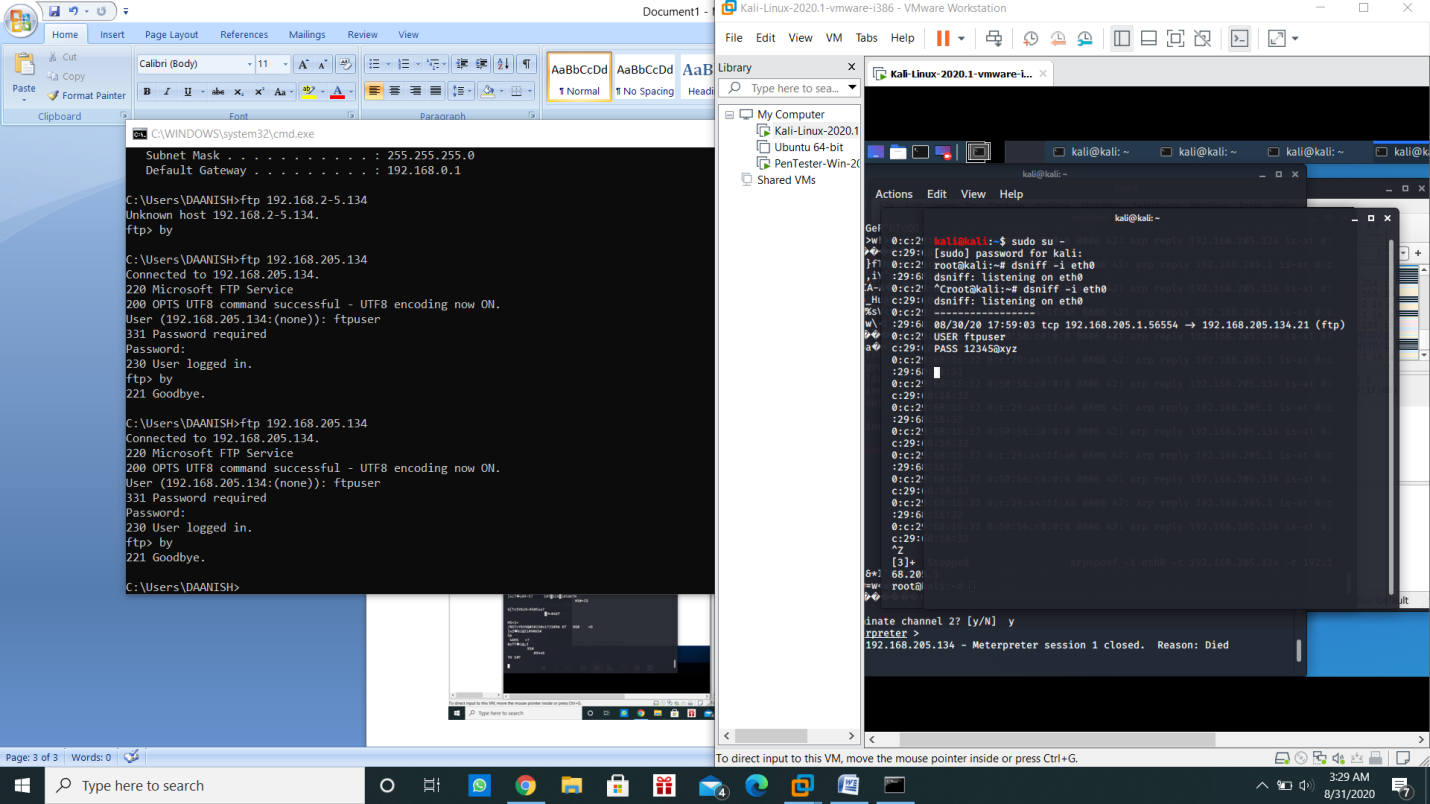
First of all I created a FTP server. To do that we have to go into server manager and select a FTP server, give the site name and add the folder of the FTP and install it. Then I created a user by the name of ftpuser which can connect to the FTP server as a client. Then in the kali linux machine I installed dsniff that catches the packets. It is executed with the help of commands such as arpspoof –i eth0 –t [IP of server] –r [IP of client]. It is known as mitm attack. Then we find out all the IP’s using nmap in kali linux. Now we start capturing packets using dsniff –i eth0 and also we can get detail sniffing by using wireshark. Then I accessed the FTP server from windows using command prompt. I logged in successfully but the username and password was captured by both dsniff and wireshark. Hence I created a FTP server, accessed it and did a mitm attack to get username and password of FTP transaction using wireshark and dsniff.



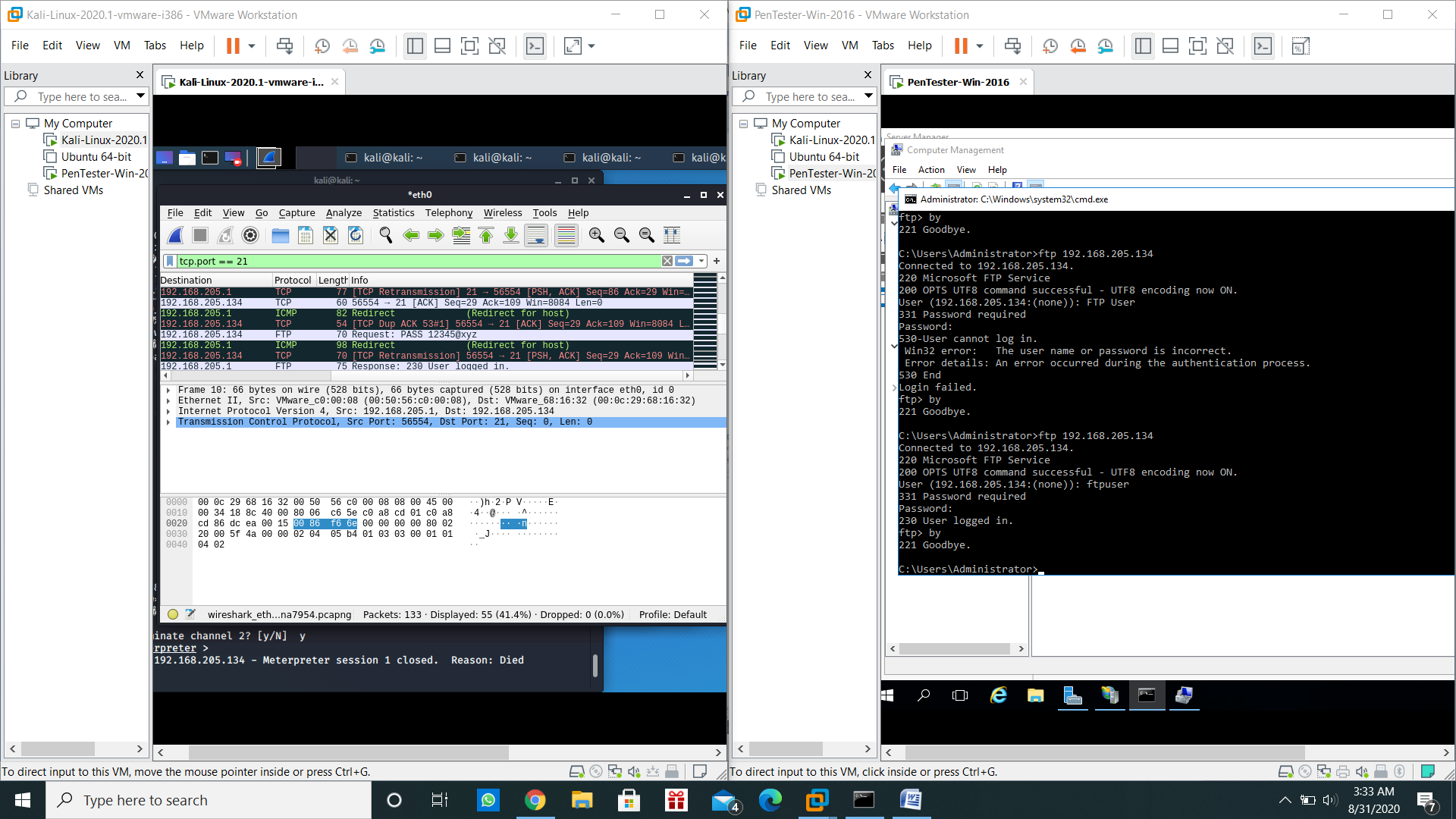
Creation of FTP server.



Accessing FTP using command prompt.



Dsniff caught the username and password during FTP transaction.



Wireshark also caught the username and the password.

BY

DAANISH KATHI

[dkgamer213@gmail.com](mailto:dkgamer213@gmail.com)