Old Dominion University

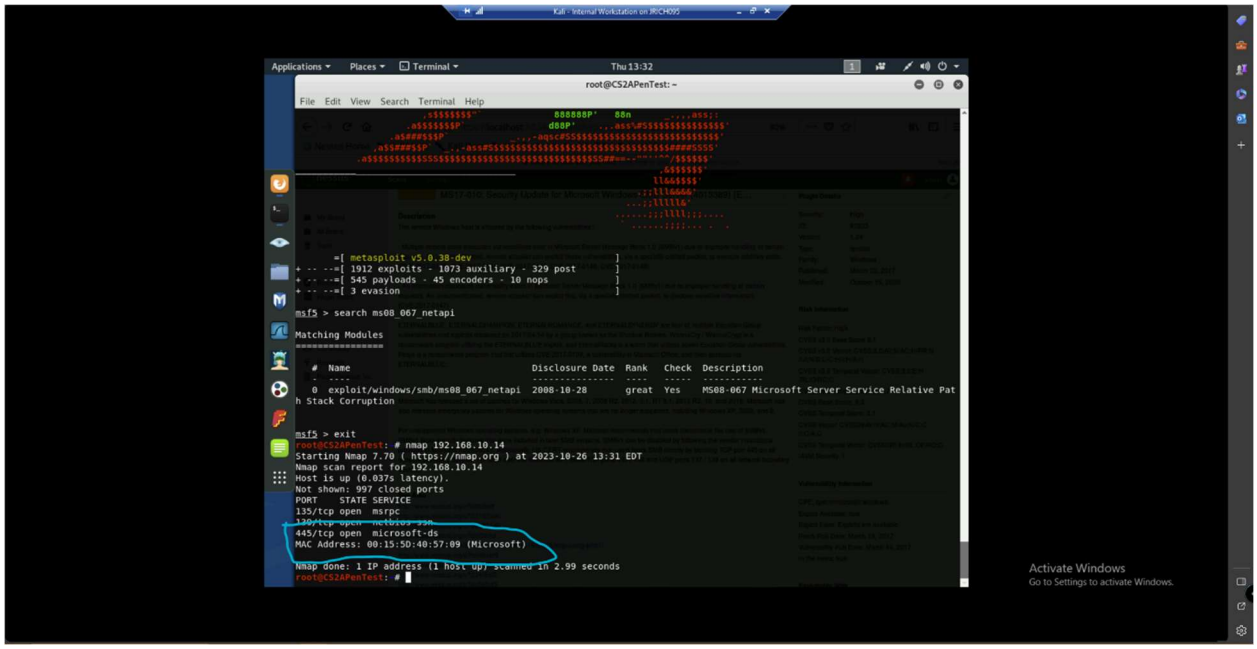
CYSE 301 Cybersecurity Techniques and Operations

Assignment #4 Ethical Hacking

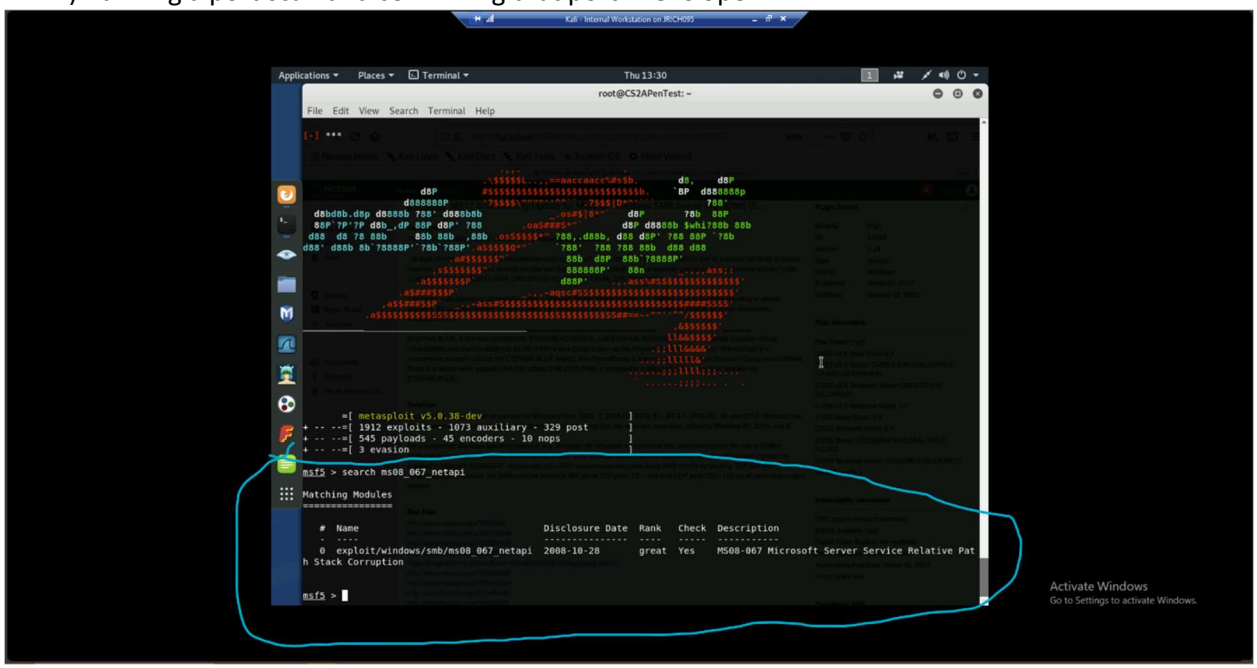
Jadyn Richardson

01221594

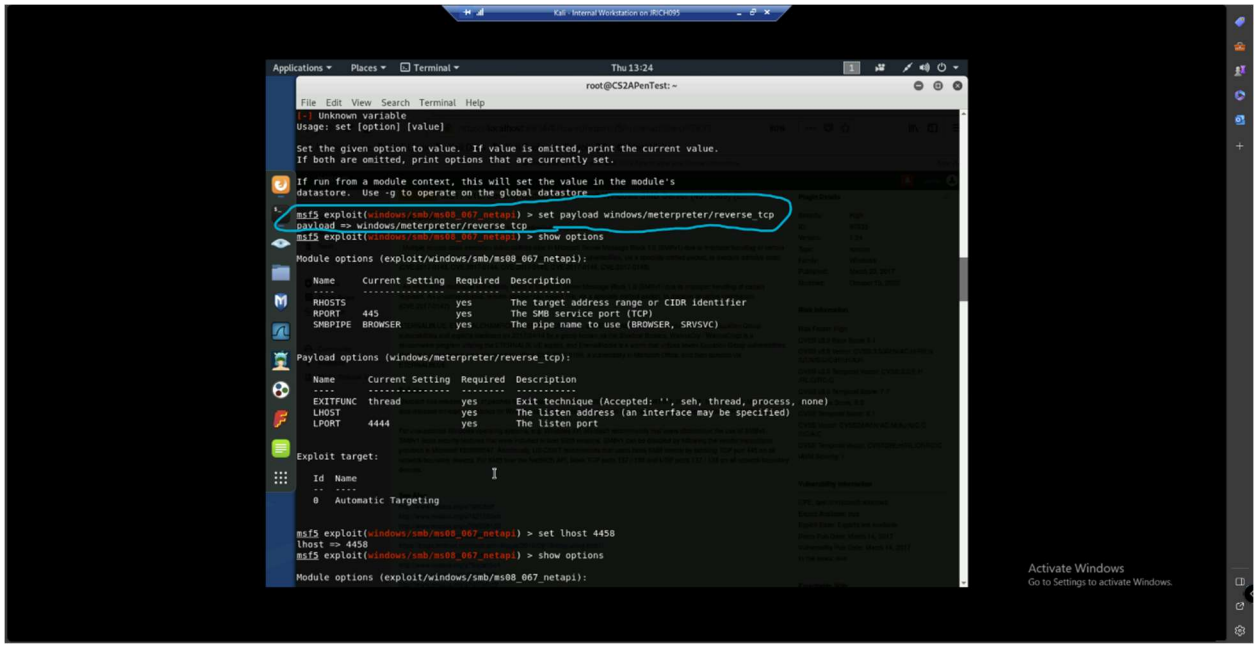
Task A.



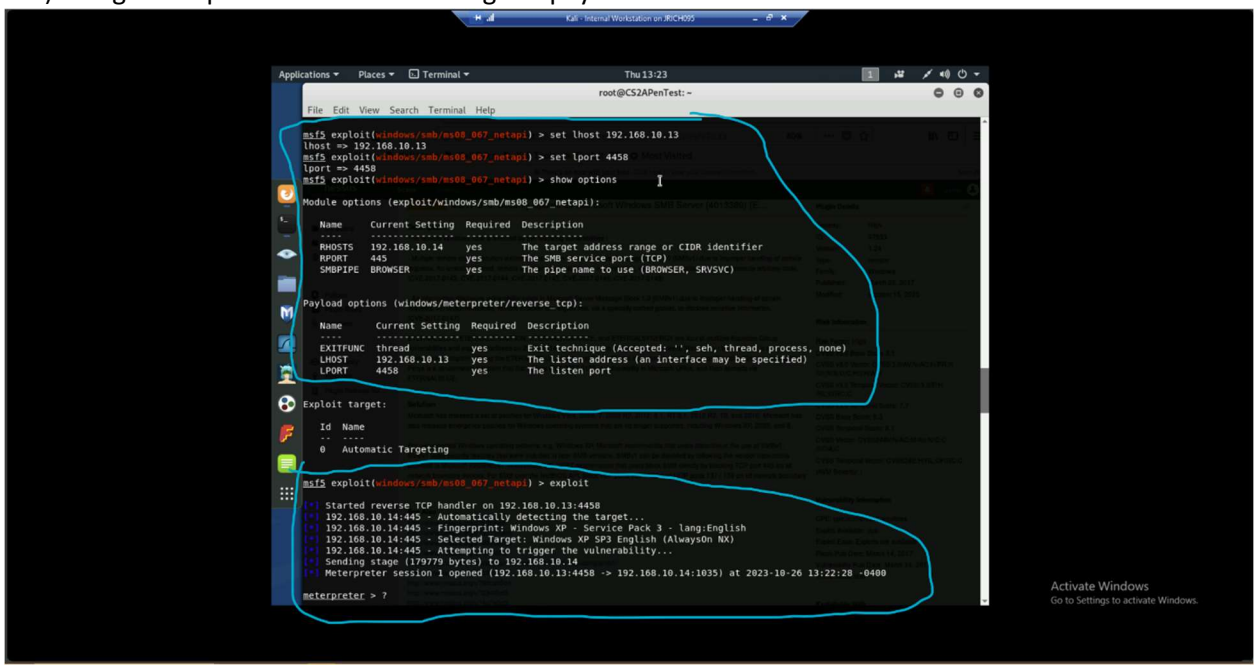
A.1-2) Running a port scan and confirming that port 445 is open.



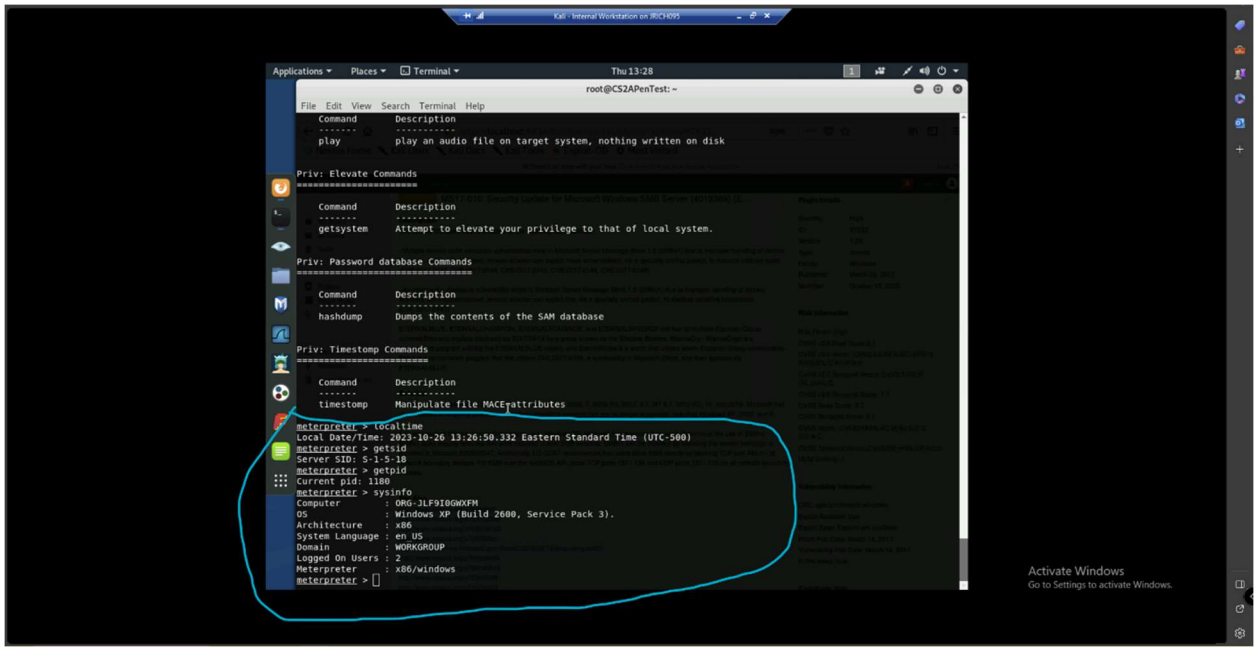
A.3) Launching Metasploit Framework and searching for the module ms09_067_netapi



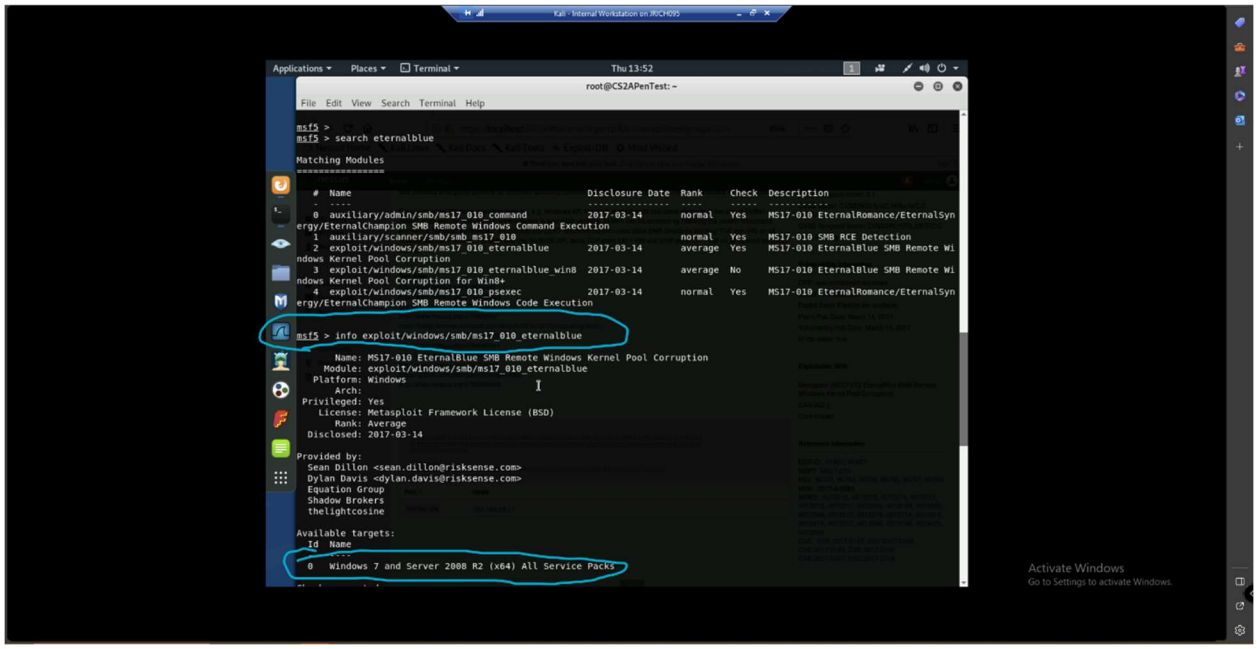
A.4) Using the exploit module and setting the payload.



A.5) setting 4458 as the listening port number, and setting the local host as 192.168.10.13, as well as exploiting the target successfully.

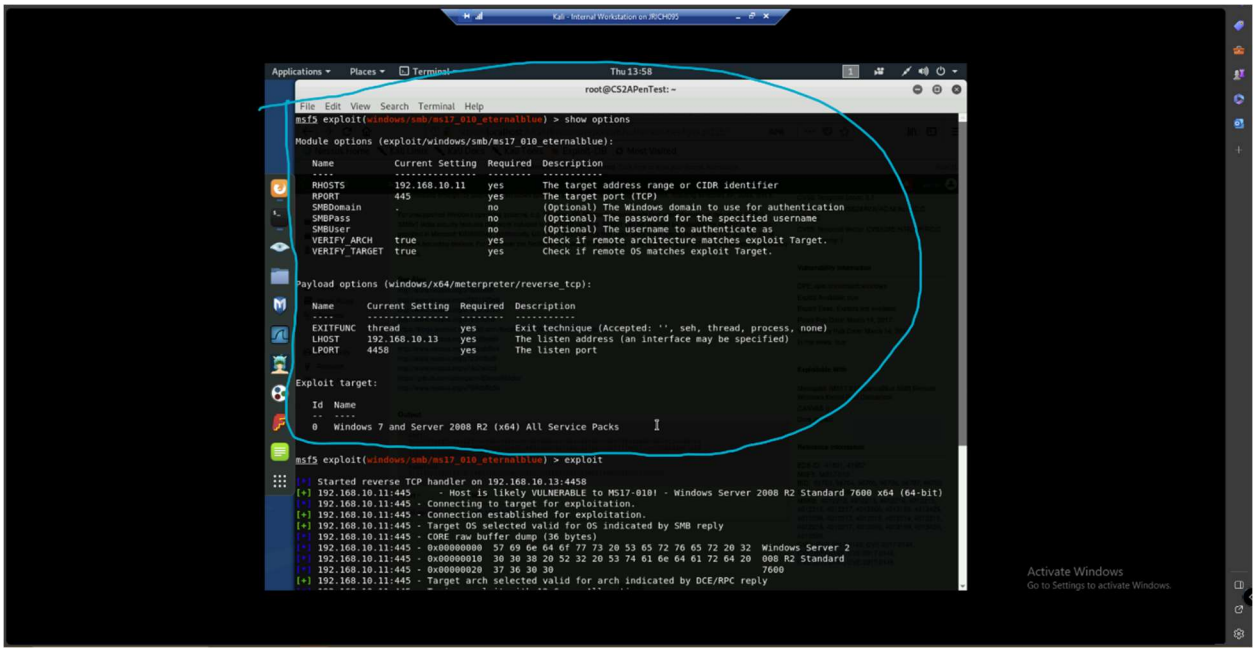


Task A.7-10) obtaining the local date and time, SID, PID, and system information of the target.

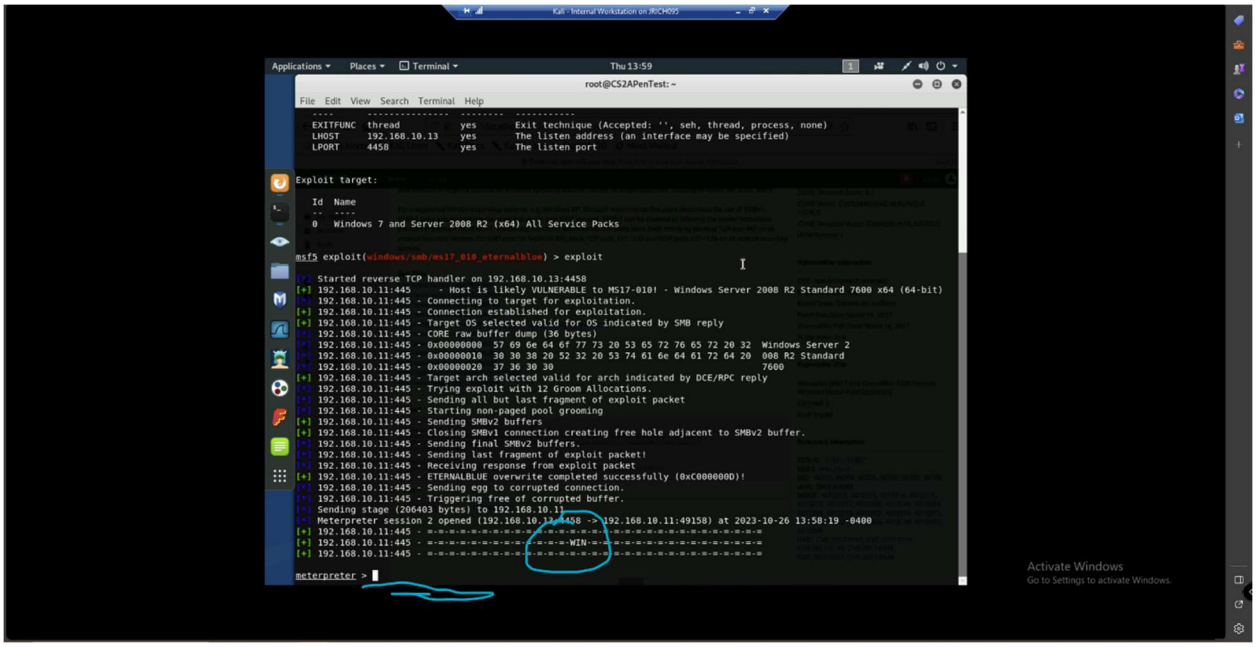


Task B.1) searching for the eternal blue exploit and its available targets.

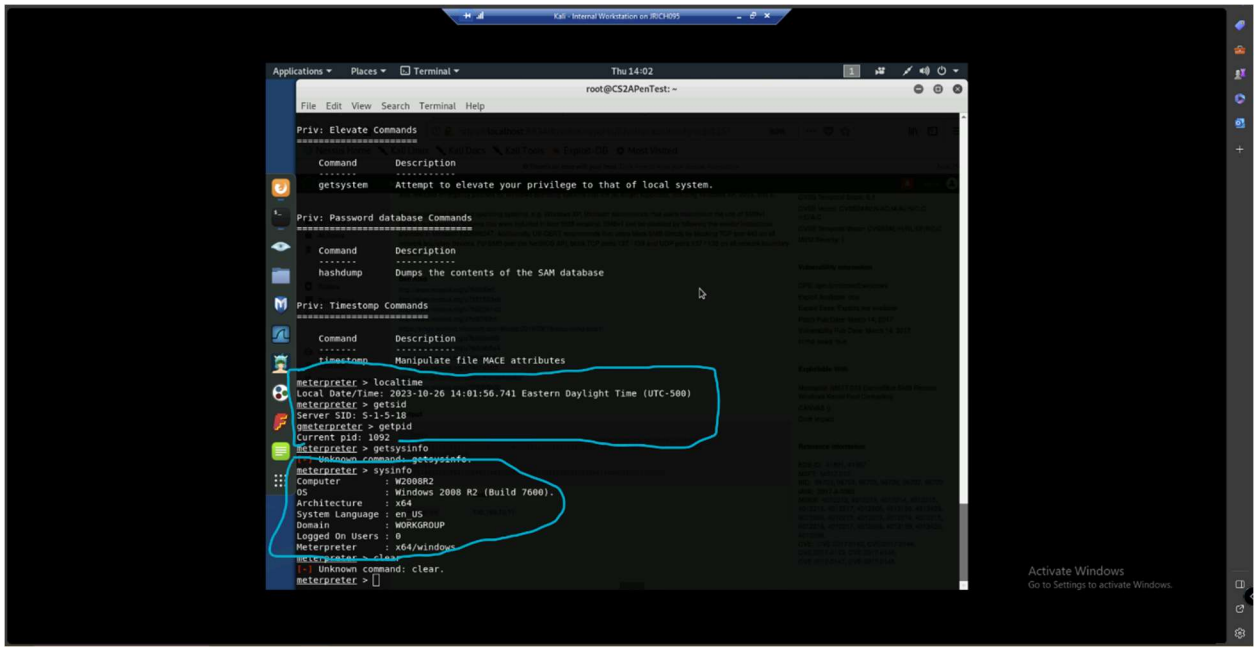
Task B



task B.1) Displaying the configuration of the exploit and payload.

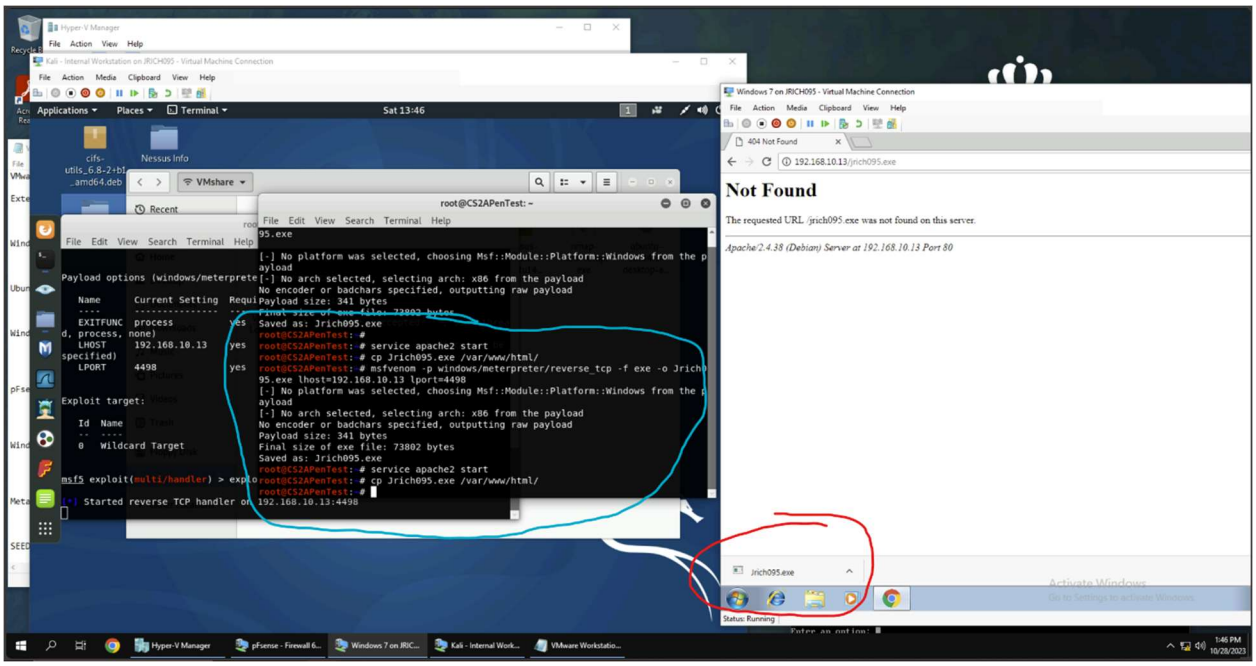


Task B.2) Showing that the exploit was successful.

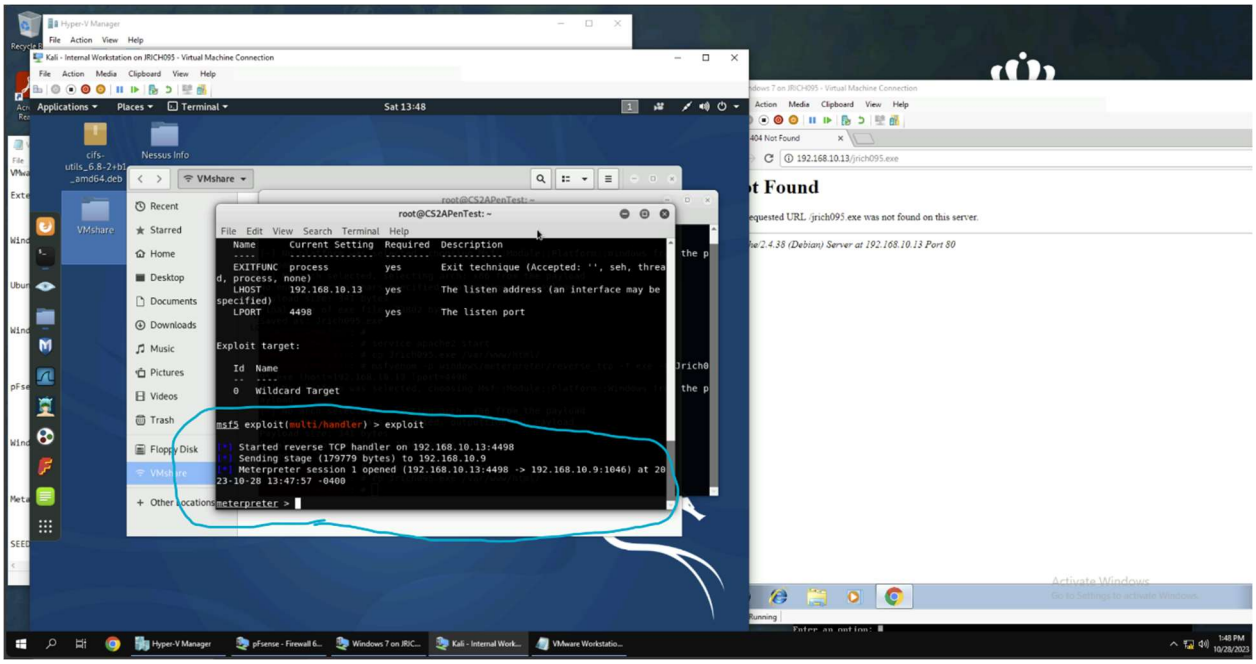


Task B.3-6) Showing the date and time, SID, PID, and system information of the target.

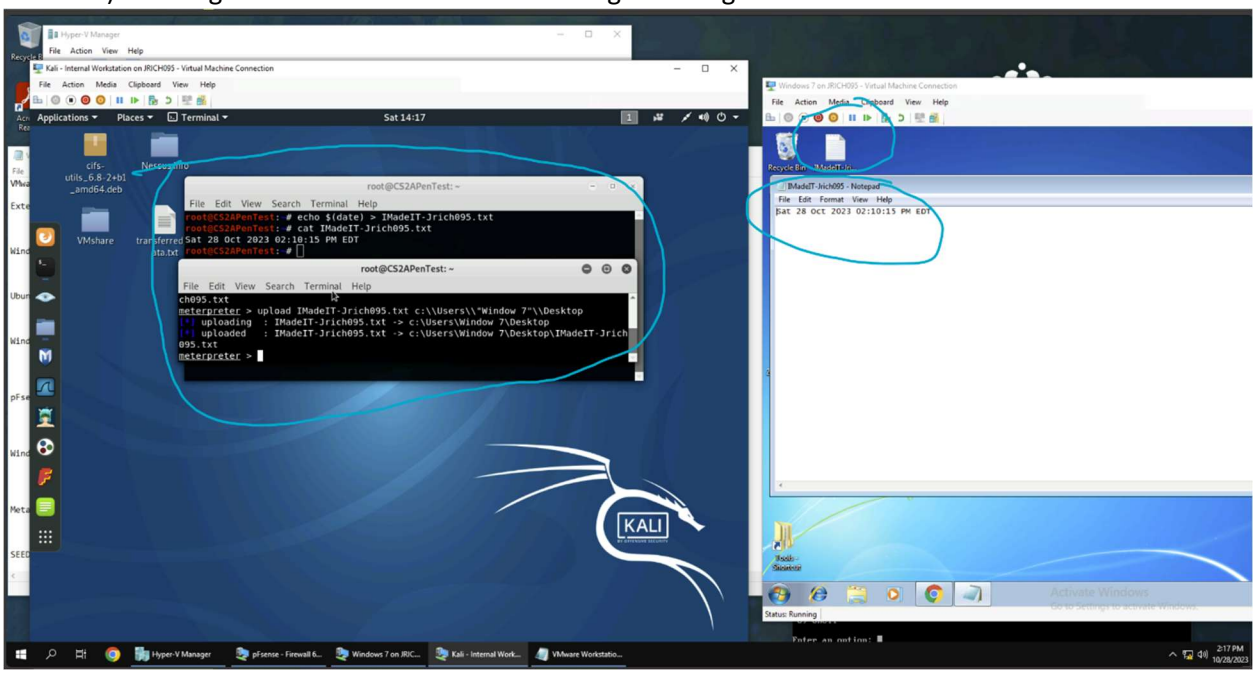
Task C



Task C.) Showing the creation and configuration of the payload, and the downloading of the payload on windows 7.



Task C 1.) Showing the successful connection through running the code on windows seven.



Task C2.) Showing the creation of the text file, uploading, and accessing the text file on the windows 7 machine.