OLD DOMINION UNIVERSITY

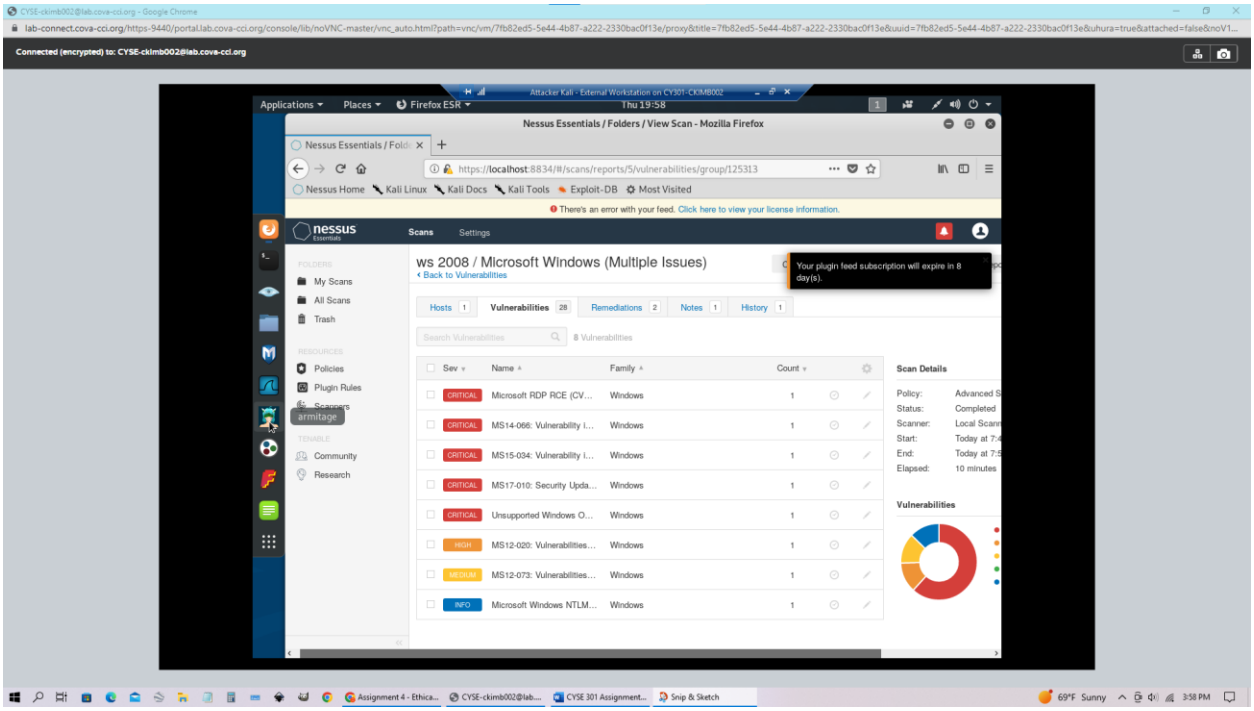
CYSE 301 CYBERSECURITY TECHNIQUES AND OPERATIONS

ASSIGNMENT #4 ETHICAL HACKING (WINDOWS SERVER 2008)

Clarence V. Kimbrell Jr.

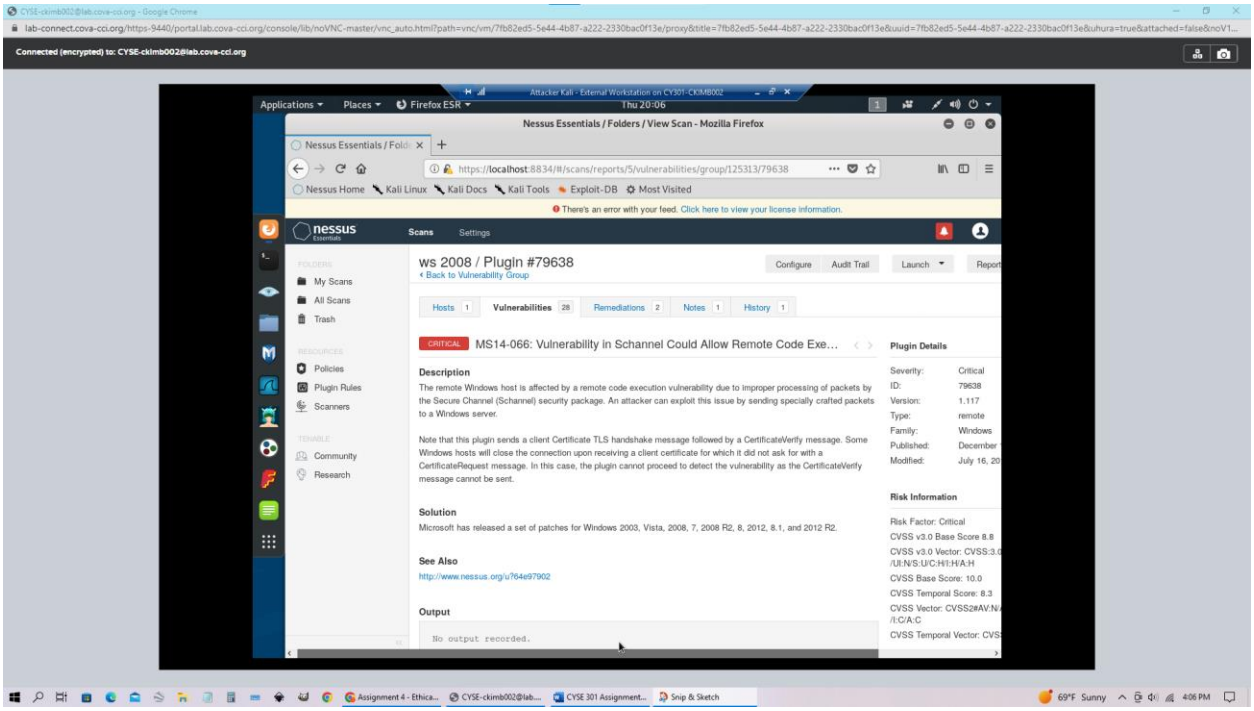
UIN 01207106

Task A Part 1



This is Nessus with the five critical security issues in the target Window Server 2008. This was completed by using the advanced scan tool on the Nessus website. Once complete there were 1 host, 28 vulnerabilities, 2 remediations, 1 note, and 1 history.

Task A Part 2

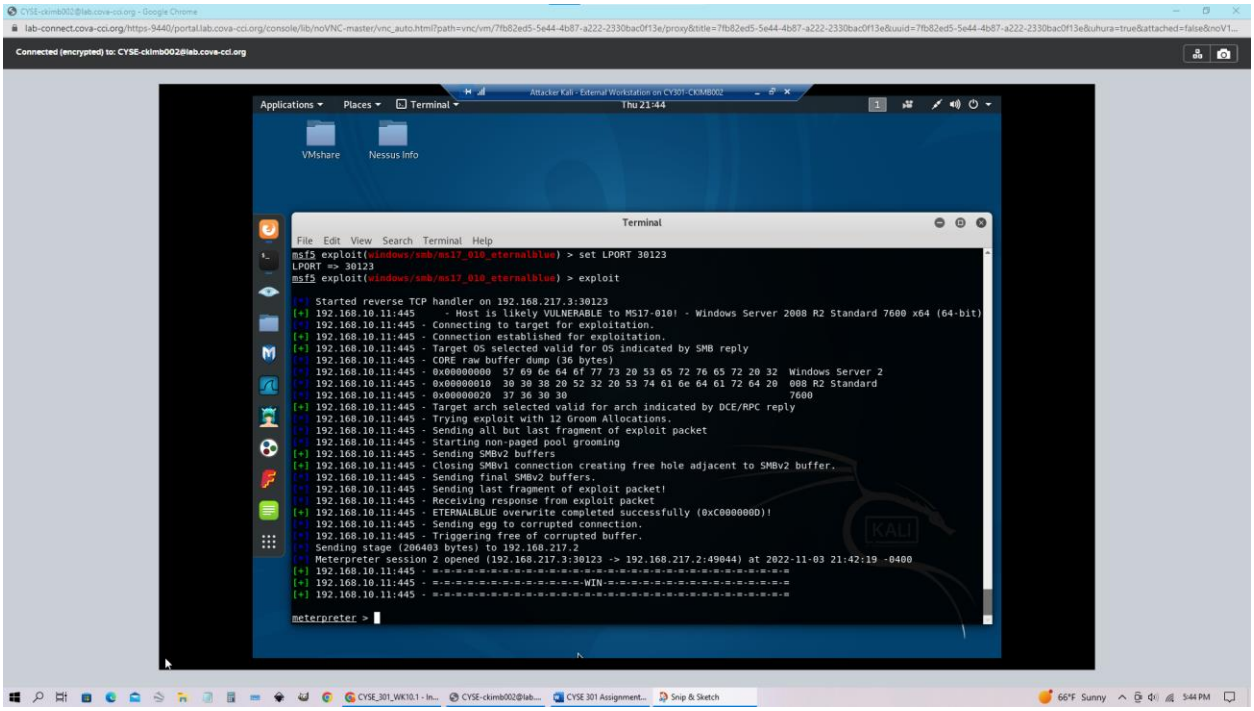


Out of the five critical vulnerabilities I choose MS14-066. This vulnerability did not have an associated database but still could be potentially damaging.

Task A Part 3

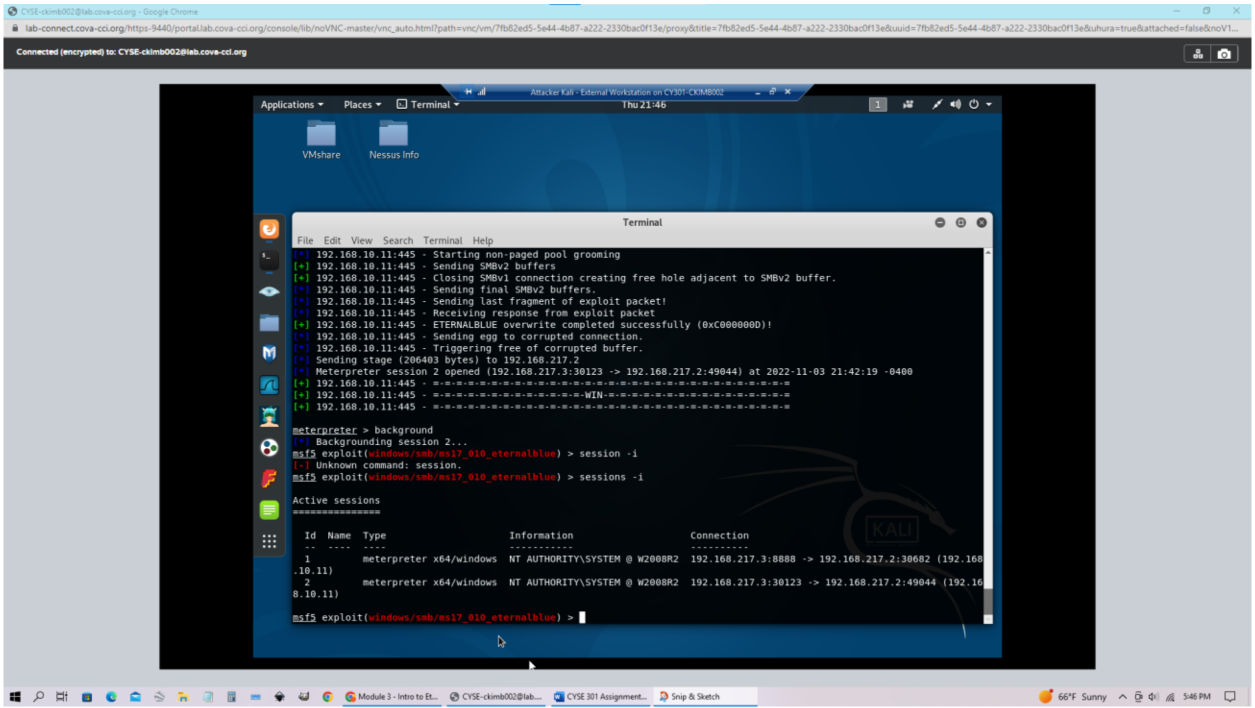
This is a security issue due to the improper processing of packets in the Schannel security package. In the description, it states that this can be exploited by sending specially crafted packets to a Windows server.

Task B Part 1



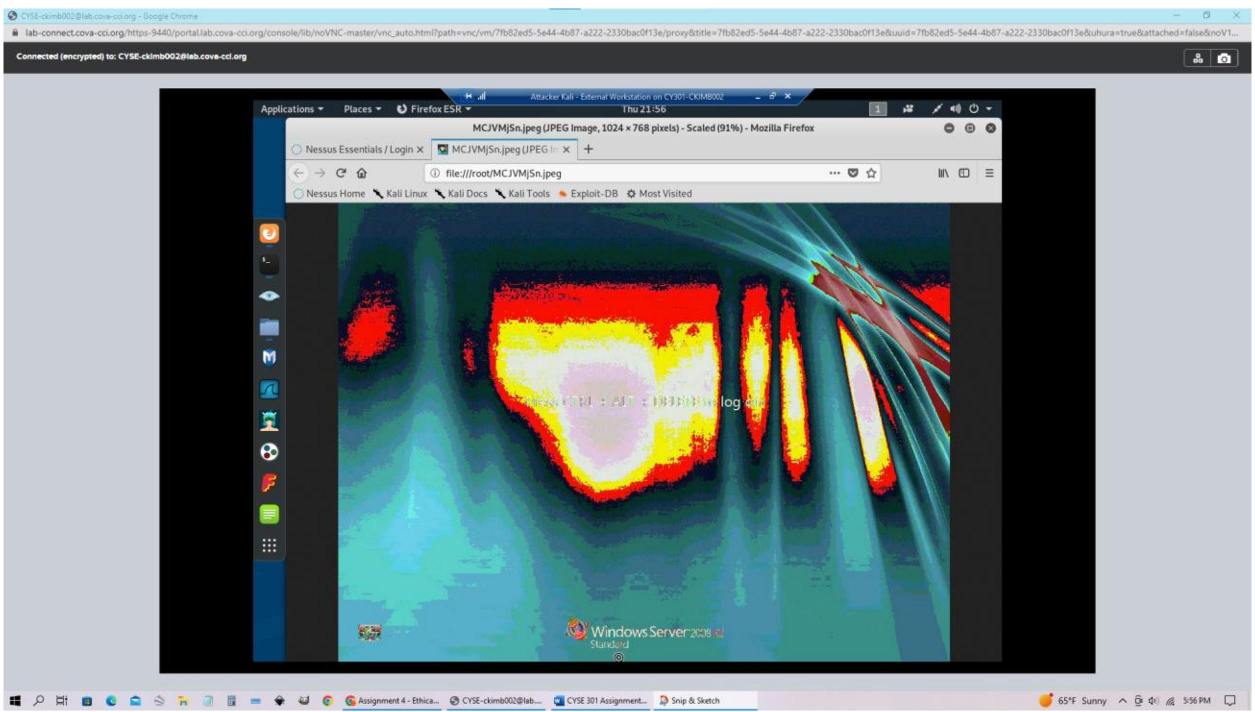
This is a reverse_tcp exploit and payload that was launched using eternal blue with the use of a listening port (LPORT) 30123.

Task B Part 2



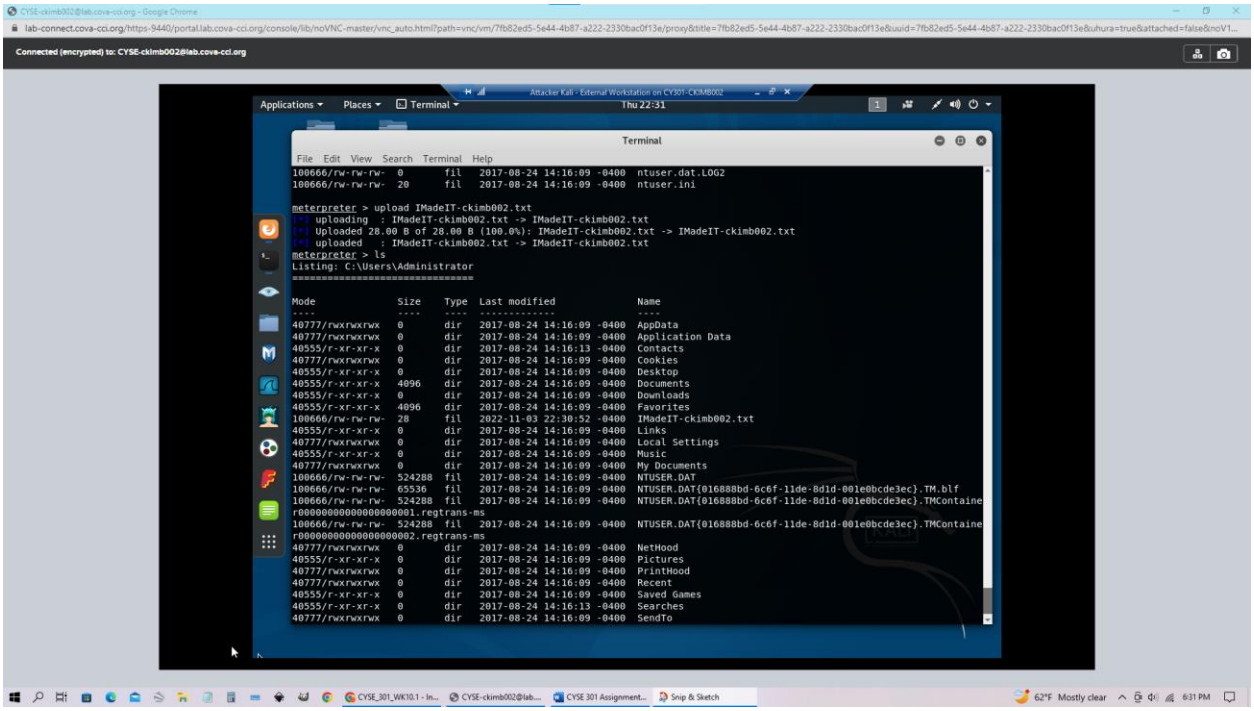
This is backgrounded the meterpreter sessions and displaying them with the command “sessions -i”.

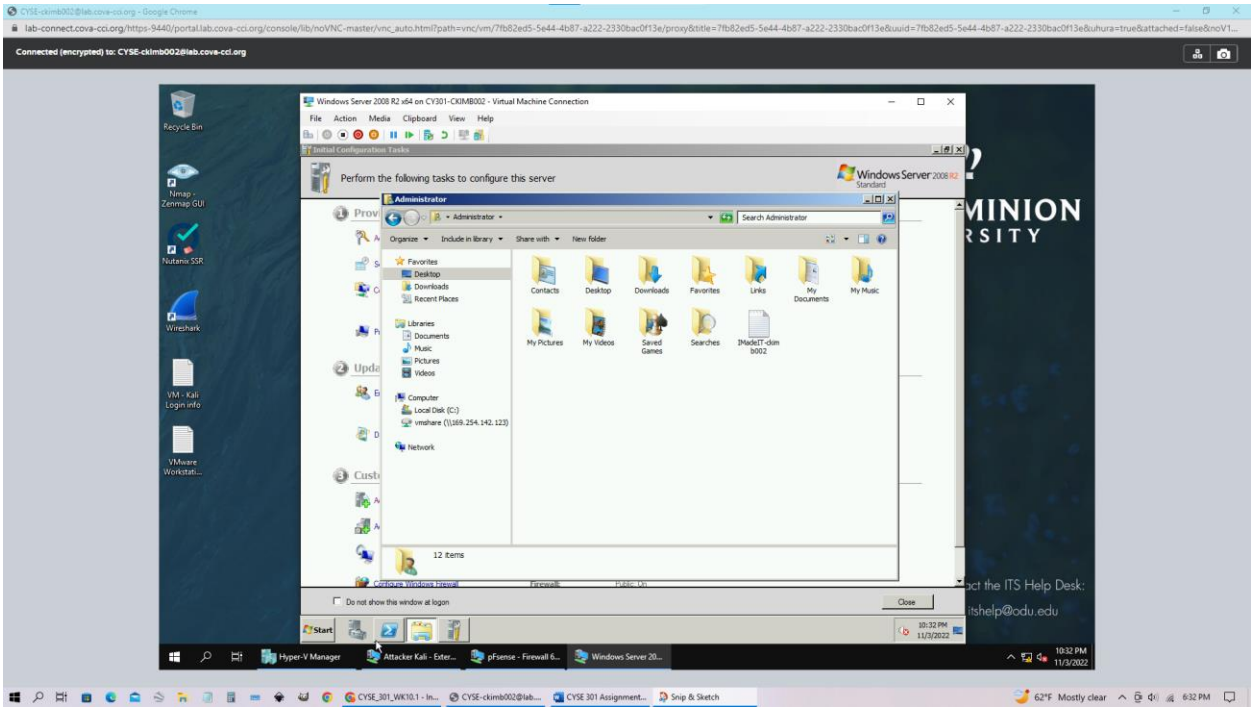
Task C Part 1



This is a screenshot of the target machine login screen. It is a little distorted but still visible and can be updated in real-time if the command was run again.

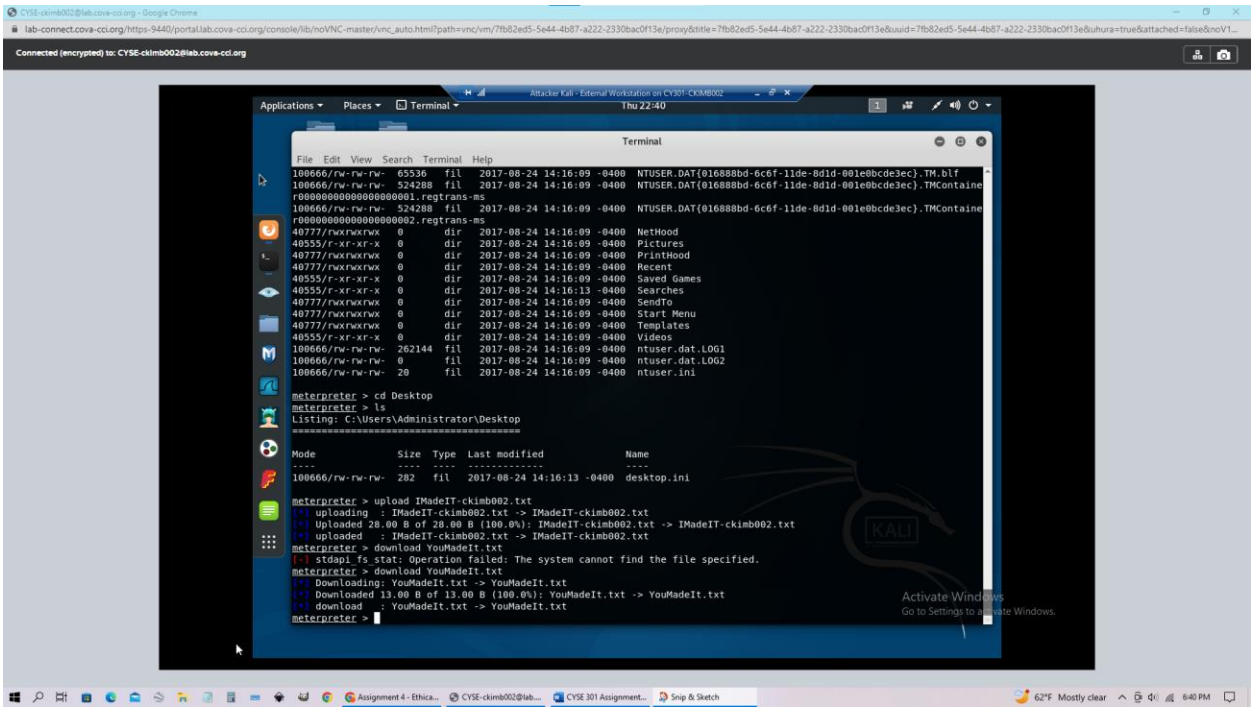
Task C Part 2





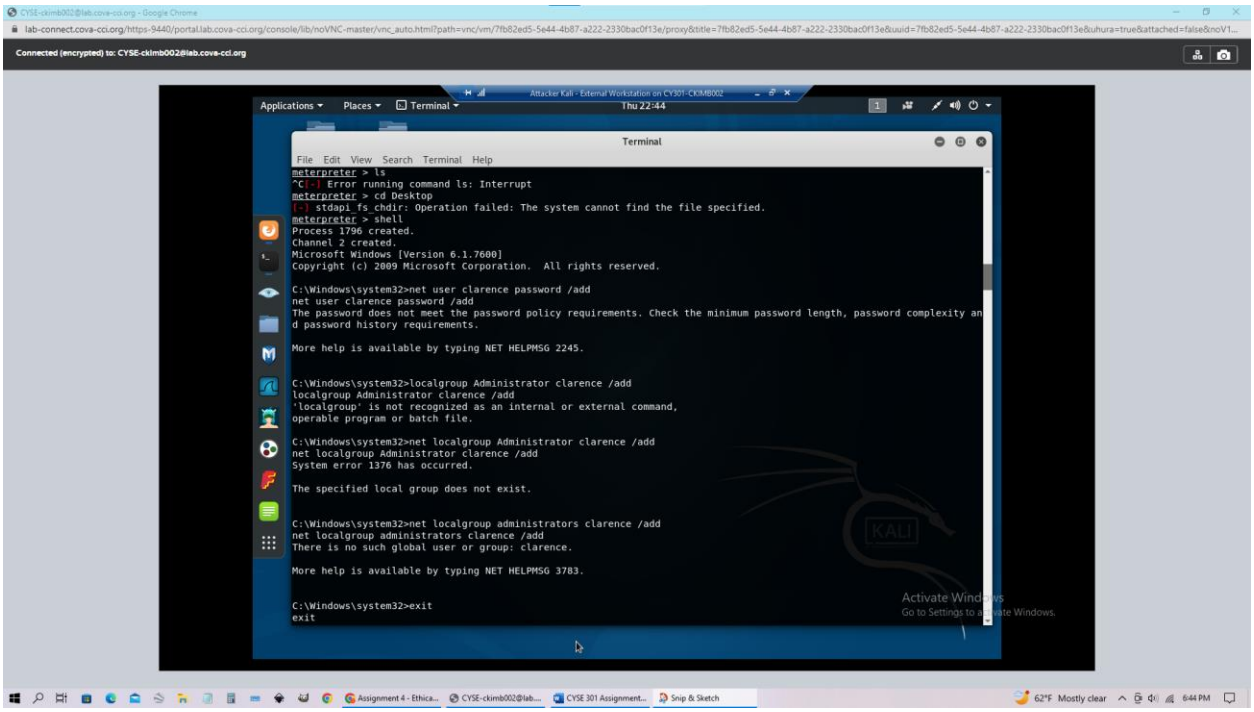
This is a file created by the kali machine and then sent using meterpreter. Then displayed on the target machine.

Task C Part 3



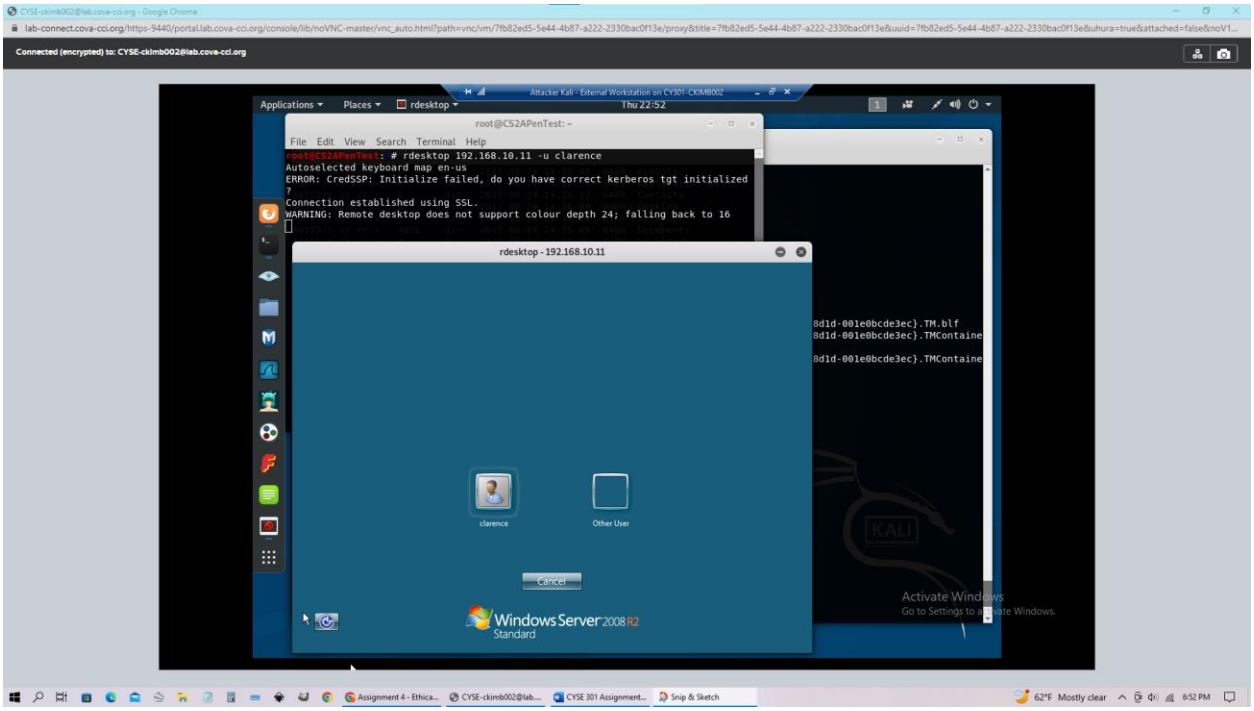
The above image is me downloading a file from the target machine, by using the download command in meterpreter.

Task C Part 4



In the shell prompt, I was able to create a new user and make that user an admin. By doing this I was able to have access to things without ever being on the target computer directly.

Task C Part 5



Using the rdesktop I can see the live target machine and use it as if I was there.