

OLD DOMINION UNIVERSITY

CYSE 301 CYBERSECURITY TECHNIQUES AND OPERATIONS

Assignment #4 Ethical Hacking (Windows Server
2008)

Patrick Hurley

01170834

Task A: Select your exploits

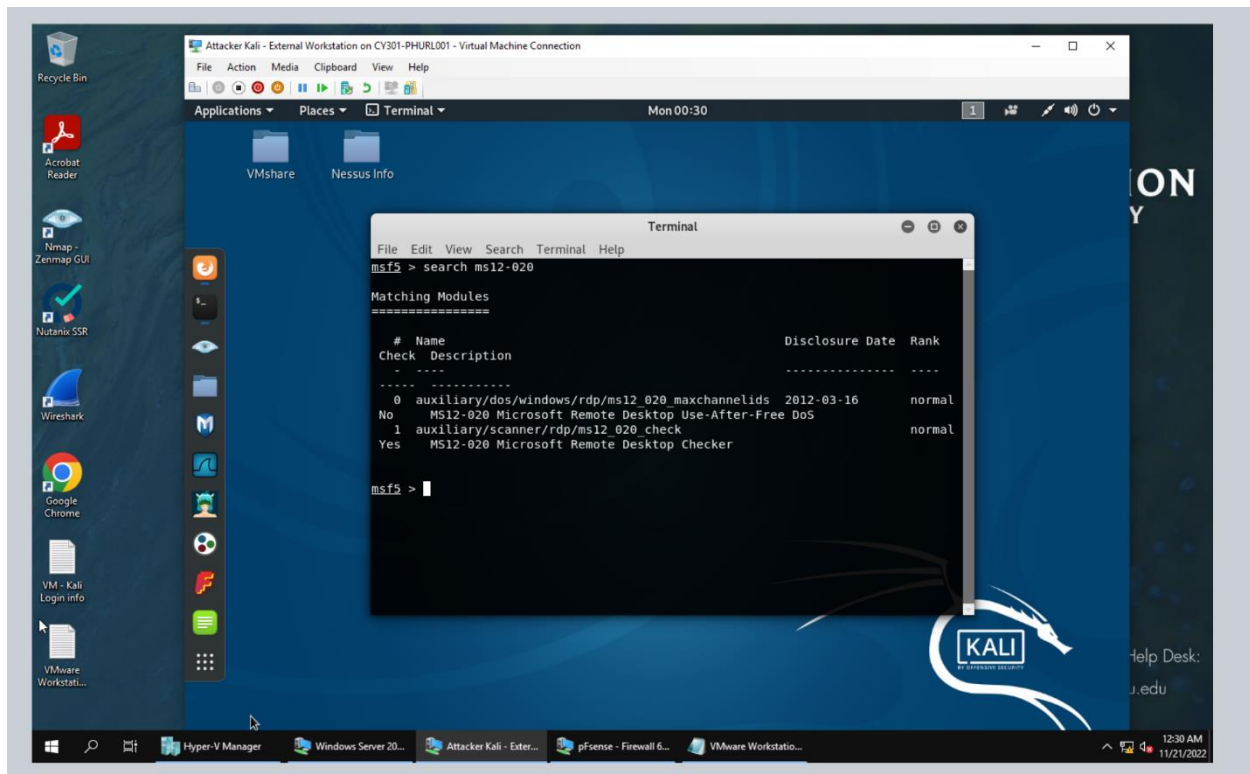
The screenshot shows the Nessus Essentials interface for a scan on host 192.168.10.11. The interface includes a sidebar with navigation options like 'My Scans', 'All Scans', and 'Trash'. The main content area displays the scan details for 'phurl001', including the host IP, scan status (Completed), and a donut chart showing the distribution of vulnerabilities by severity. The donut chart is mostly blue (Info) and green (Low), with a small portion of yellow (Medium) and red (High).

Severity	Count
Critical	0
High	0
Medium	1
Low	1
Info	16

The screenshot shows a detailed view of vulnerabilities for Microsoft Windows. The interface displays a table of vulnerabilities with columns for severity, name, family, and count. The vulnerabilities listed include several critical issues related to RDP and Windows OS, as well as high and medium severity updates.

Sev	Name	Family	Count
CRITICAL	Microsoft RDP RCE (CVE...	Windows	1
CRITICAL	MS14-066: Vulnerability I...	Windows	1
CRITICAL	Unsupported Windows OS...	Windows	1
HIGH	MS12-020: Vulnerabilities...	Windows	1
HIGH	MS17-010: Security Updat...	Windows	1
MEDIUM	MS12-073: Vulnerabilities...	Windows	1
INFO	Microsoft Windows NTLM...	Windows	1
INFO	WMI Not Available	Windows	1

Step1) I used Nessus to scan the windows 2008 server for vulnerabilities. I had done 3 scans in total, two advanced scans and one basic scan. They all kept giving me the same results, and I could only get 3 critical security vulnerabilities to show up in all of them. Three critical vulnerabilities, three high Vulnerabilities and eleven medium vulnerabilities.

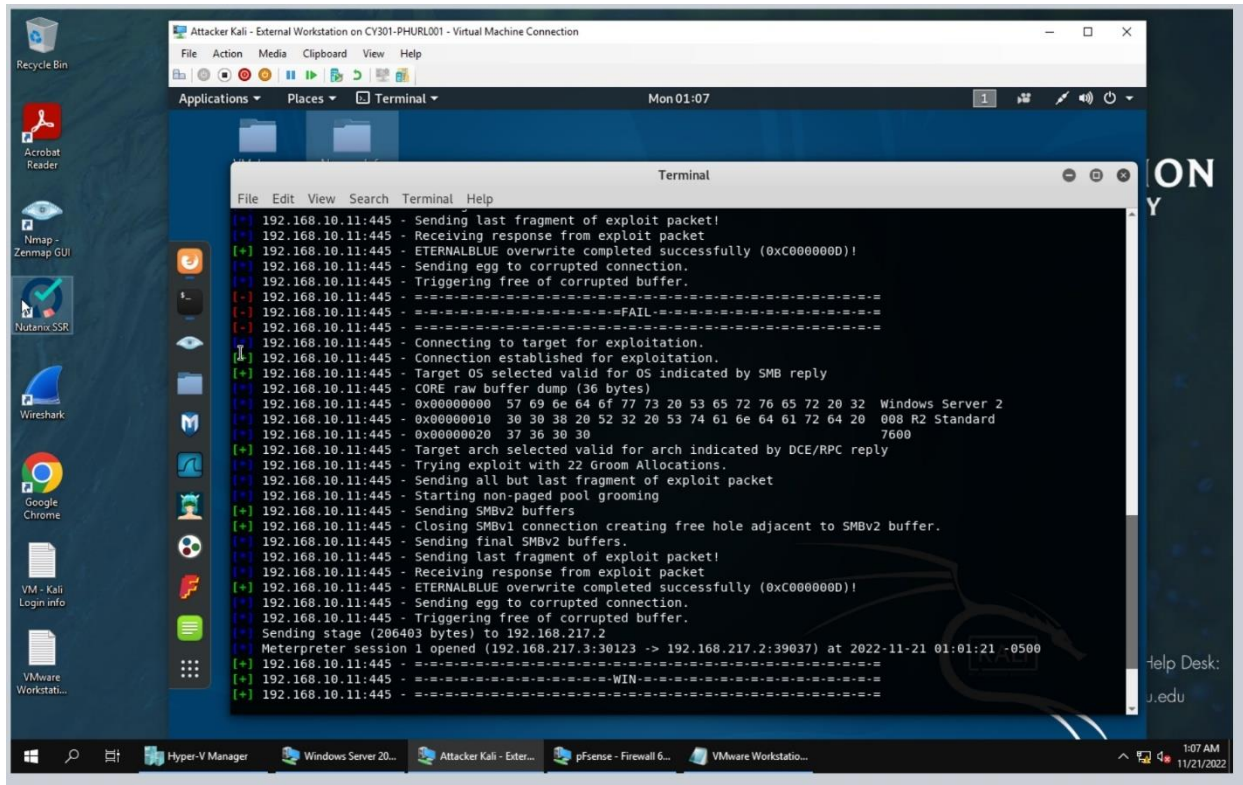


Step 2) In the screenshot above I used one of the high vulnerabilities named MS12-020, and did a search of it in the Metasploit console.

Step 3) The MS12-020 vulnerability shows up when there is a vulnerability in the code that implements the remote desktop protocol. Because of this vulnerability a remote attacker could use their computer to send code to the system and make it run that code.

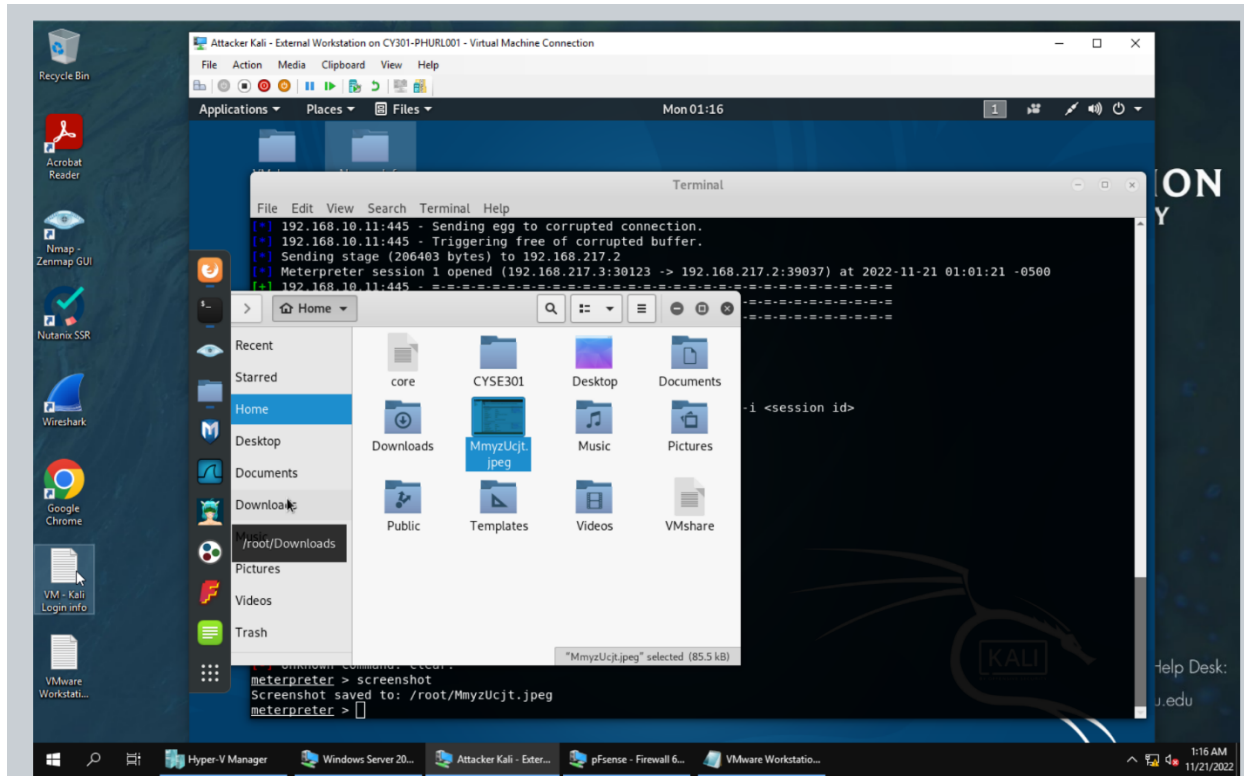
Pre-Step 1) I used the search command and searched for ms17-010, and then found the eternal blue exploit. I then used the “use” command to use the eternal blue. I then set a payload in the second screenshot and used reverse_tcp as the exploit.

Step 1) I used the port that was given to us in the assignment instructions and set a listening port to 30123. After I then set listening host which is kali Linux. Lastly, I then set the windows 2008 sever as the receiving host.

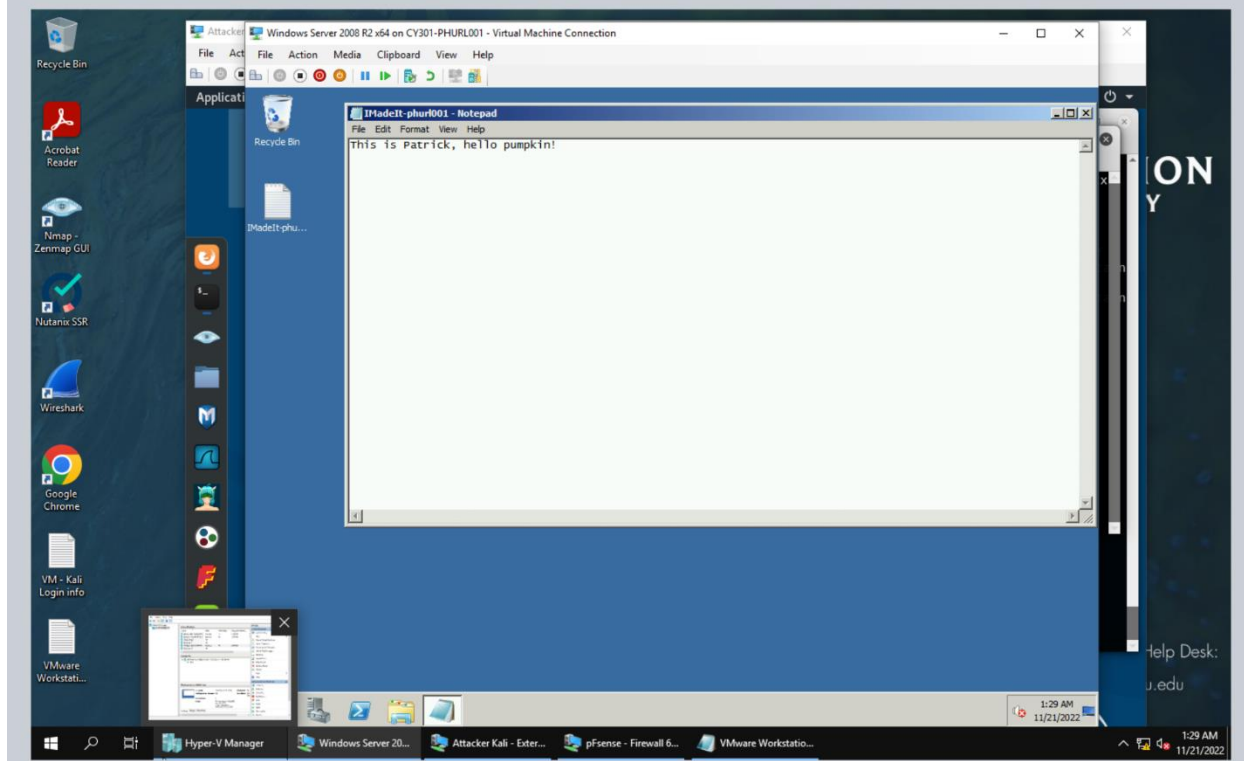
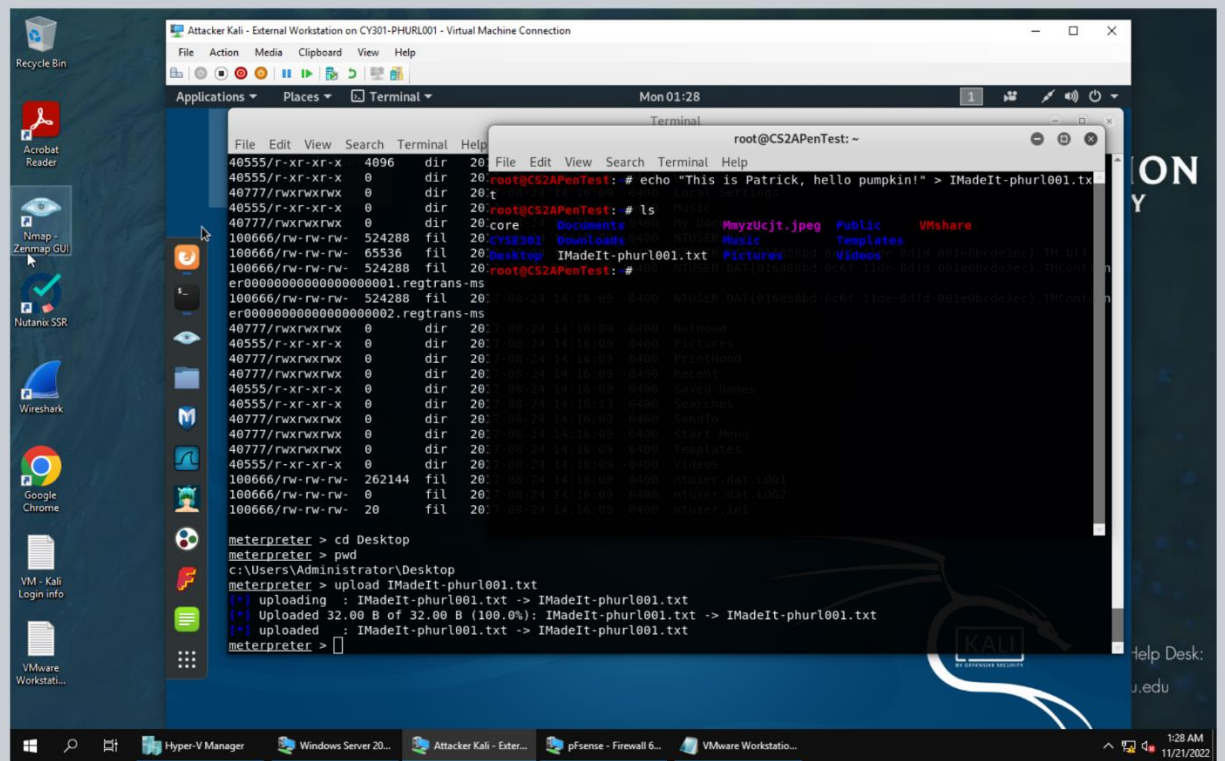


Step 2) I then used the exploit command to gain access to the windows server machine.

Task C: Basic Information Harvesting

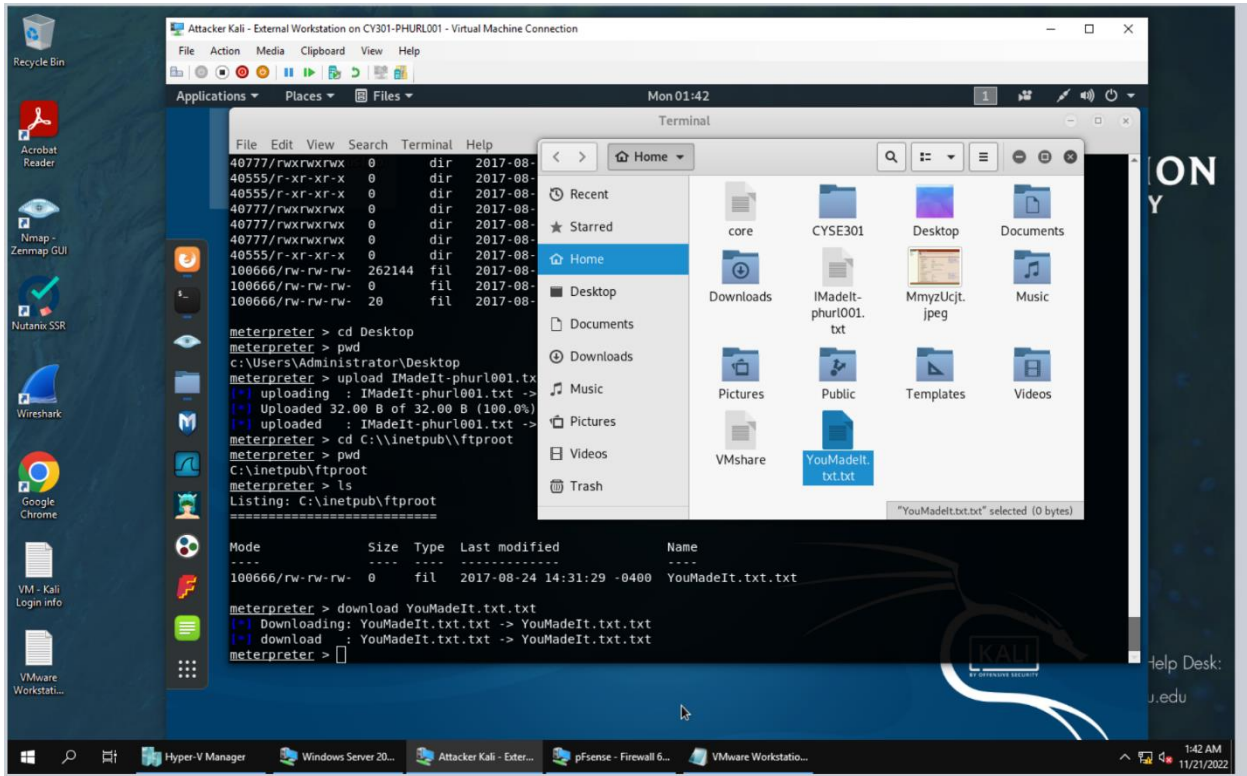


Step 1) after I got access to the windows 2008 server I used the screen shot command to take a screen shot of the windows desktop and save it in my root directory.

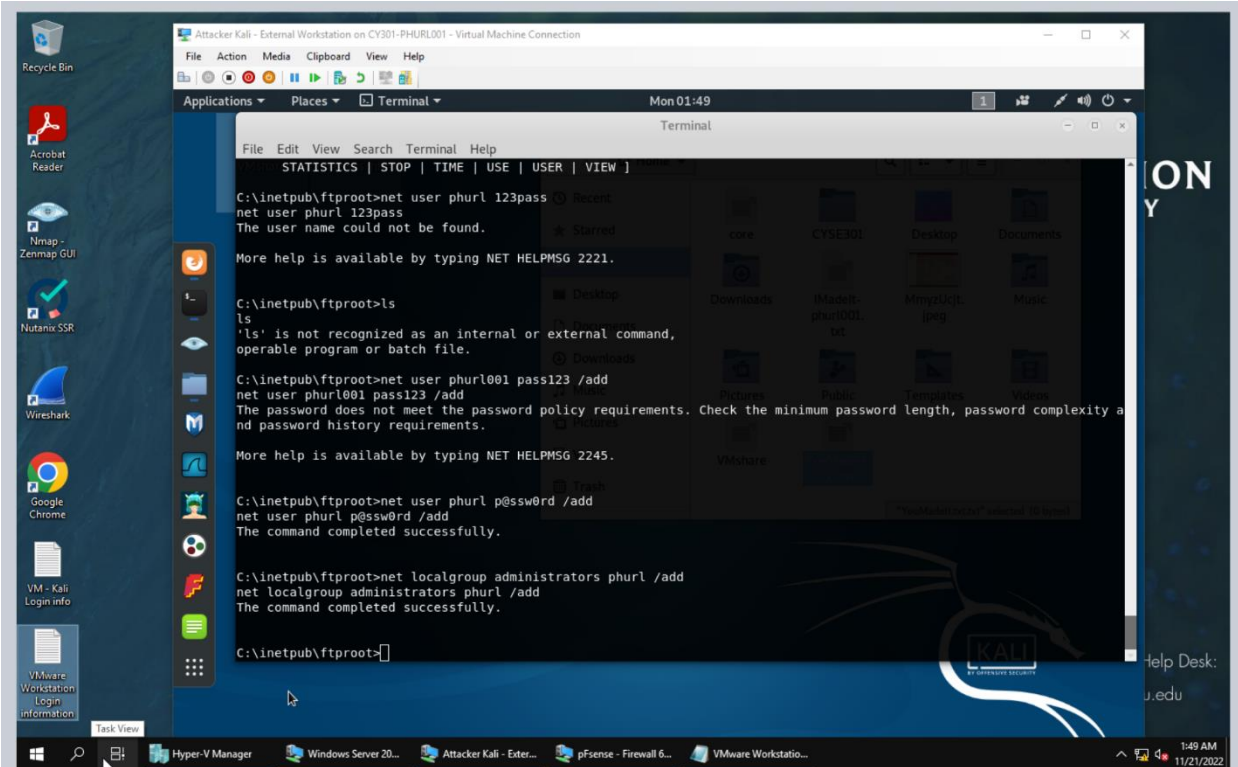


Step 2) In this step I did a couple things. First, in the first screenshot it shows that I had created a .txt file with the words "This is Patrick, hello pumpkin!" Second, I had to browse through the many directories in the kali terminal that has access to the windows server. After I found the right directory that allowed me

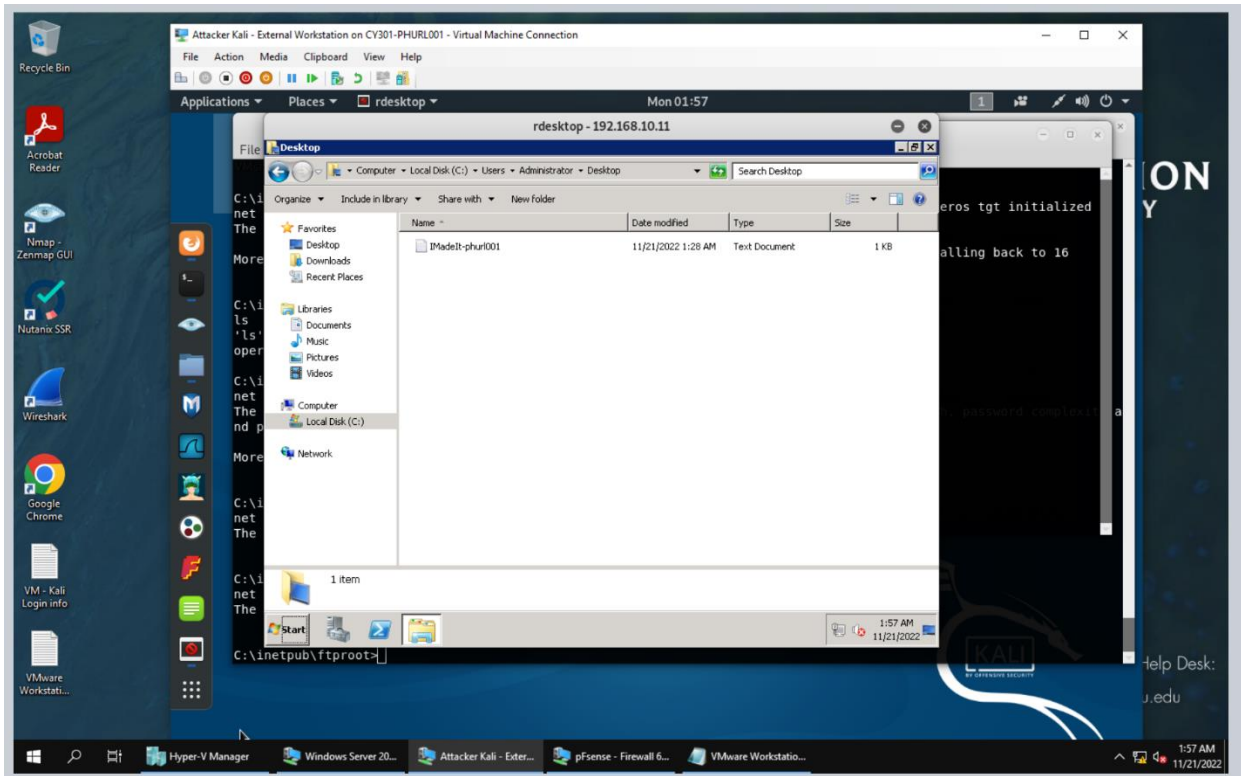
access to the desktop, I then uploaded the .txt file. In the second screen shot you can see that the windows server has the txt file on the desktop and it contains the right phrases.



Step 3) In this step I wanted to take a file from the windows server named YouMadeIt.txt. First used the cd command to go to the correct directory and then used the download command to get the file.



Step 4) I then created a user using my MIDAS id using the net user command and made that user an administrator with the net localgroup command.



Step 5) In this final step, I used another terminal and made a remote desk of the windows server. I was able to log in with the user I had created and was able to access every users' files. As seen in the screen shot you can see that I am in the administrator's desktop, which is where the IMadeIt-phurl001.txt should be in.