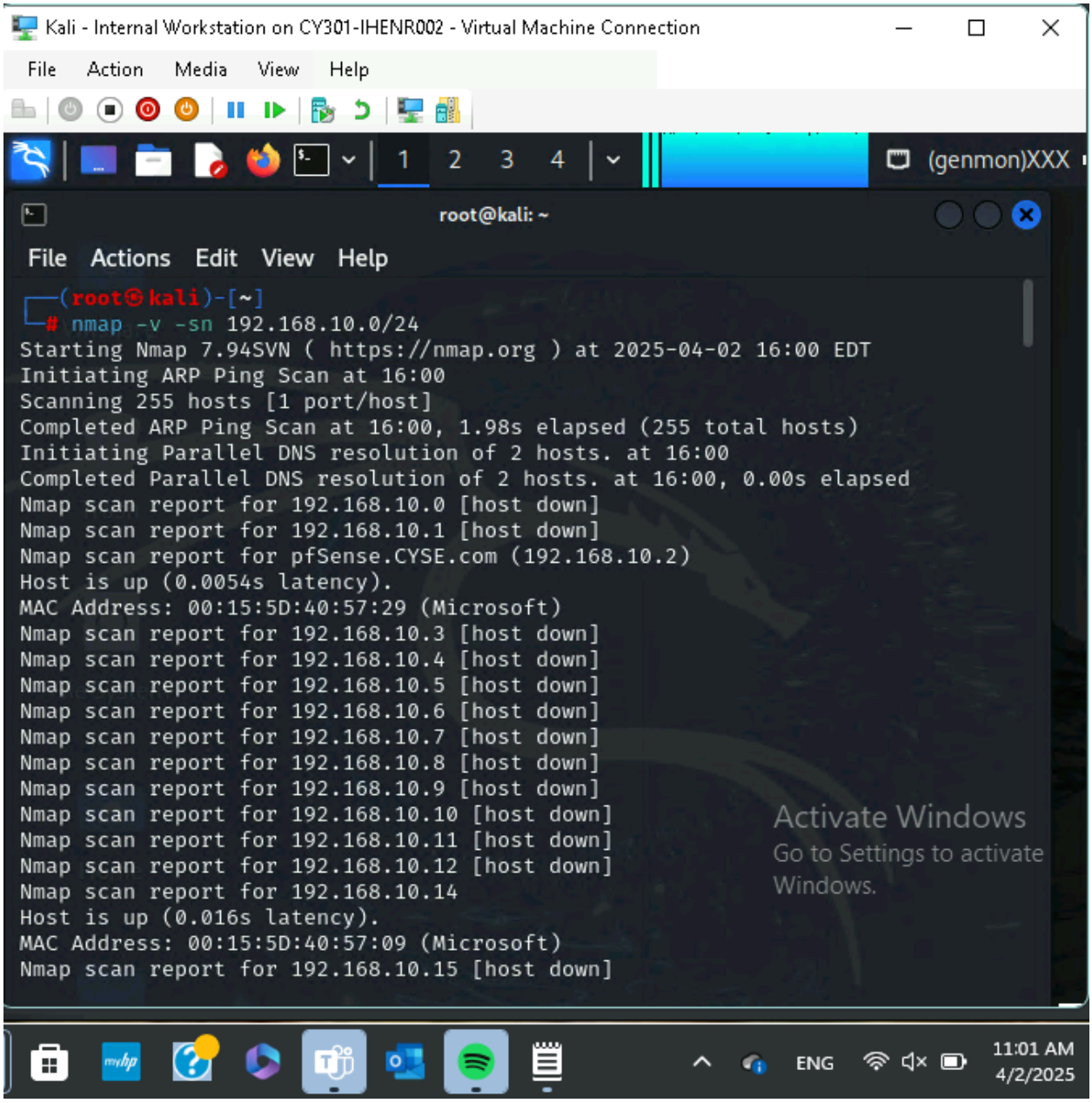
**India Henry**
**CYSE 301 - 32781**
**Shideh Yavary Mehr**
**4 April 2025**
**CYSE: Cybersecurity Techniques and Operations**
**Assignment: Lab 4 - Ethical Hacking**

*Power on the following VMs for this assignment:*
***Internal Kali (Attacker)***
*pfSense VM (power on only)*
*Windows XP, Windows 2022, or Windows 7 (depending on the subtasks)*

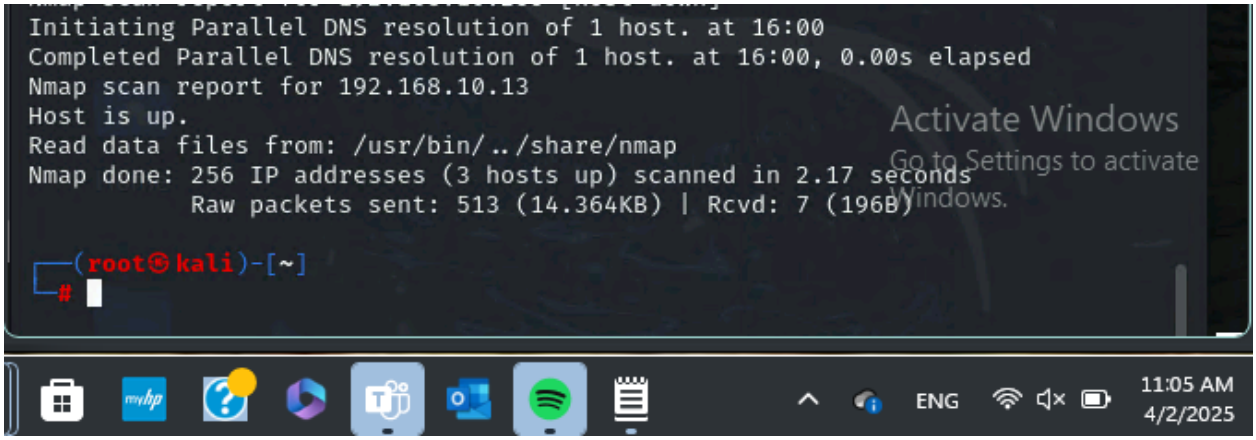
**Task A: Exploit SMB on Windows XP with Metasploit**

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



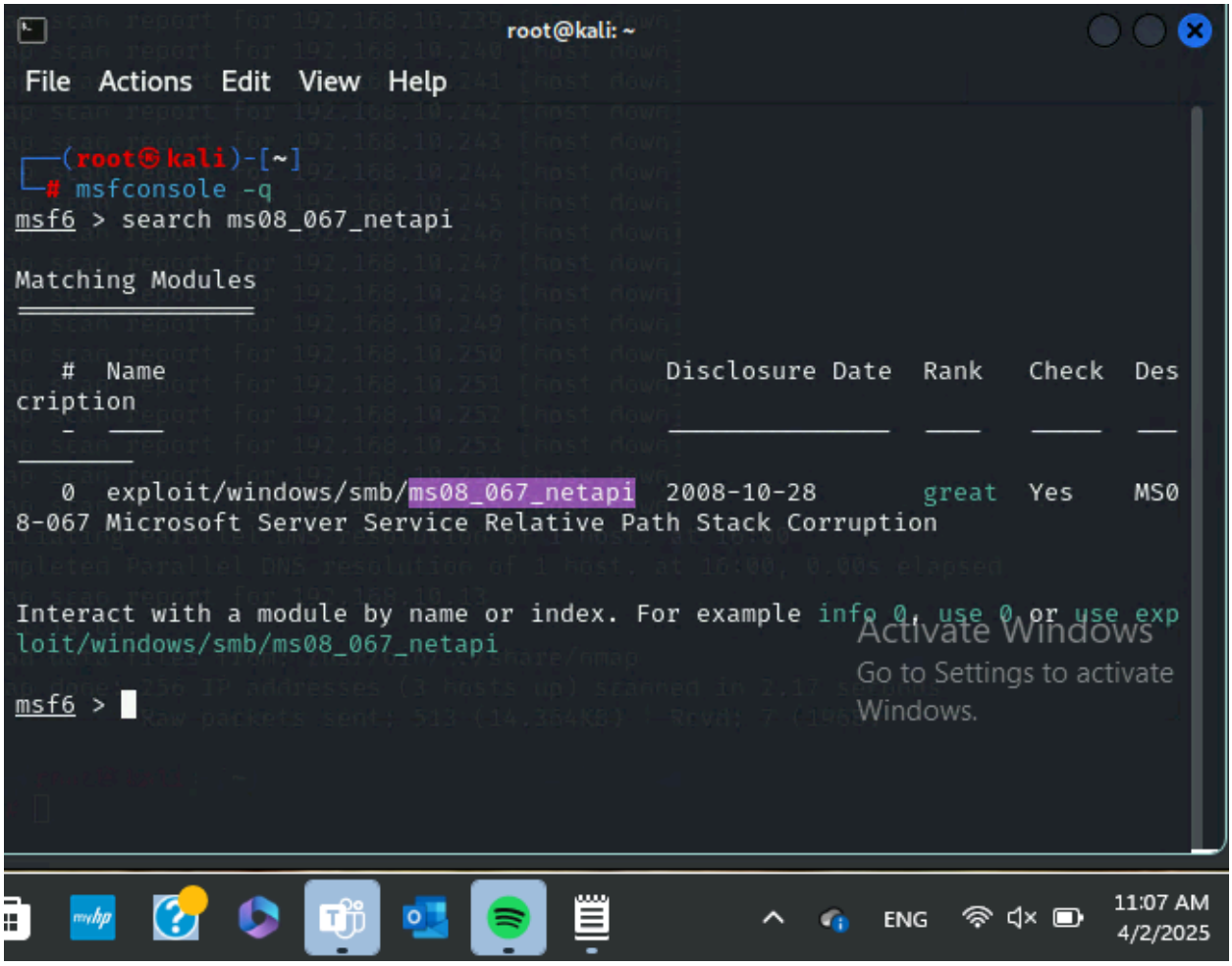

I ran an nmap scan to see if there were any open ports.

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



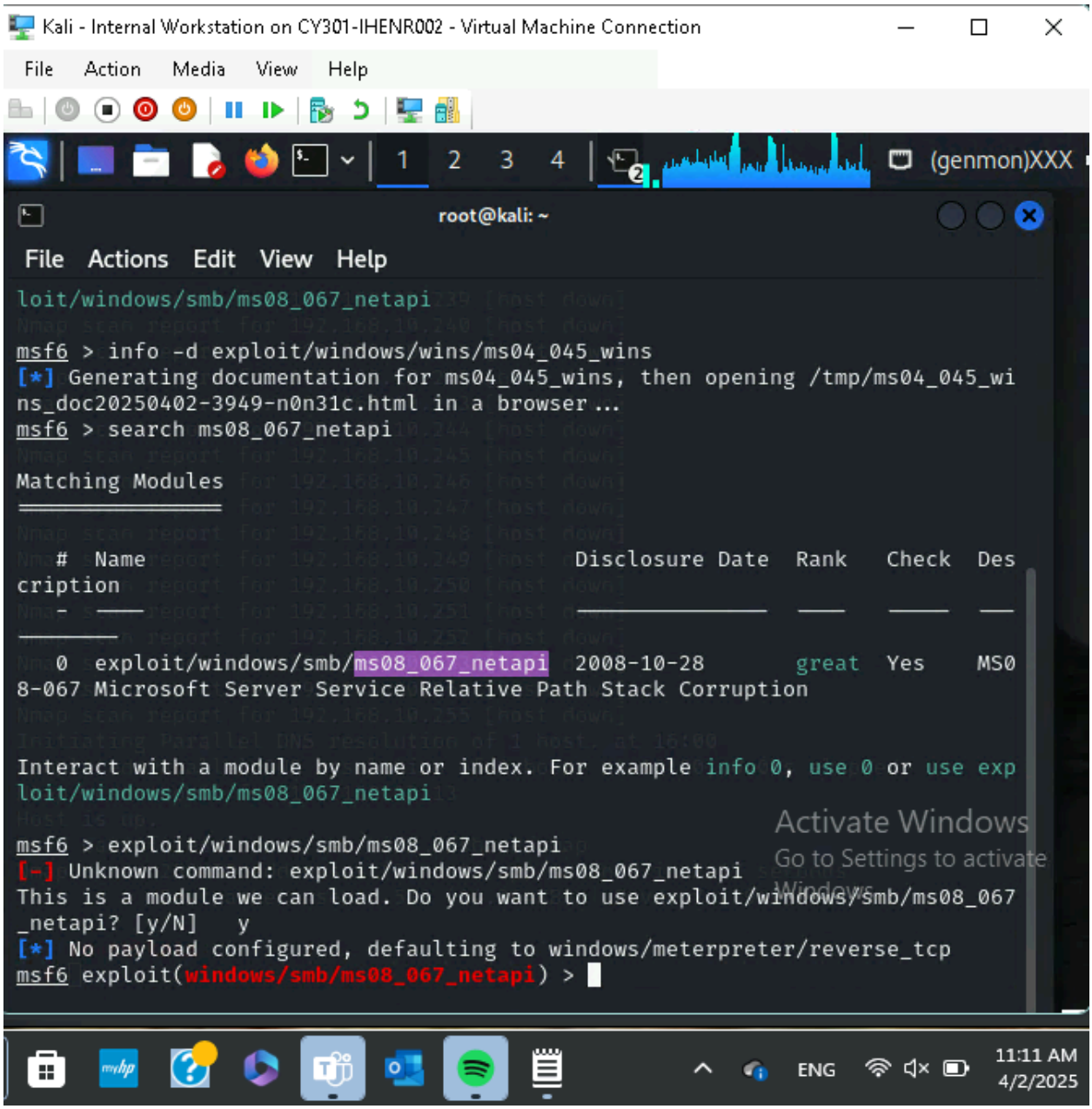

Confirming the port is open at the end of the nmap scan

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



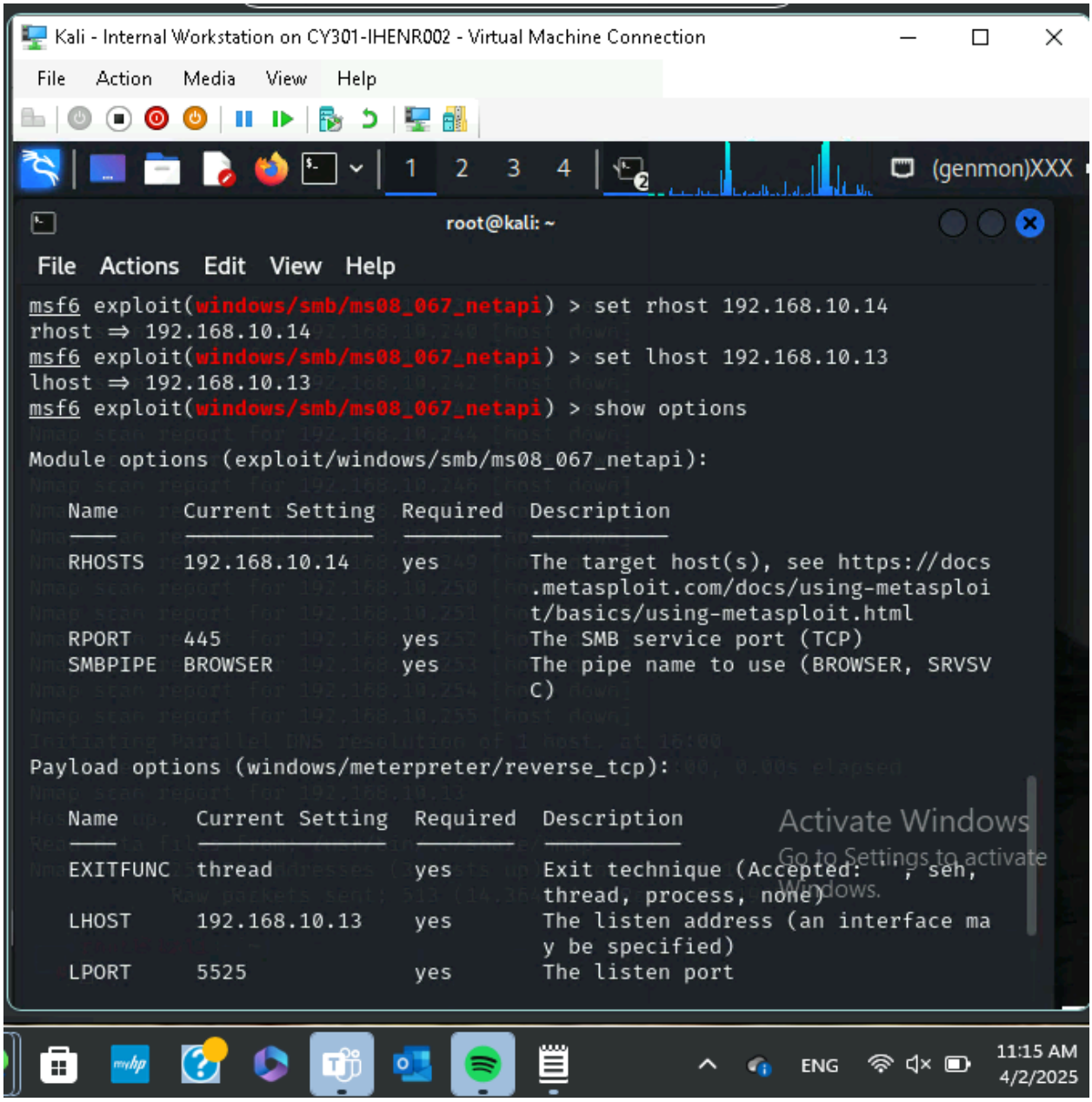

Launching metasploit; searching the netapi exploit command

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




Using the exploit searched in the last step; configuring the payload

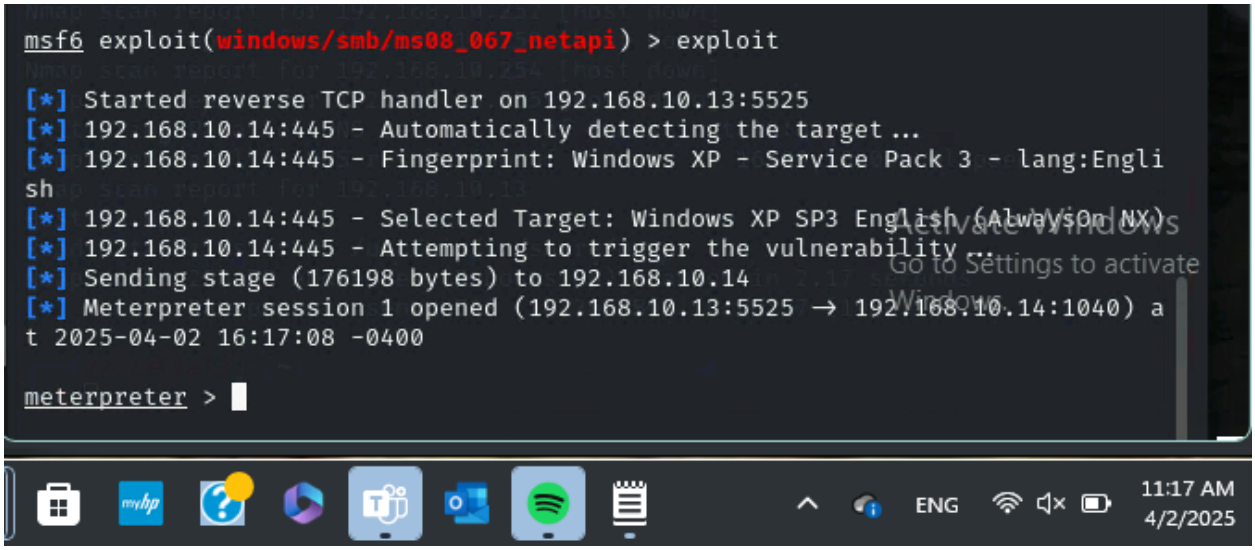
5. **Use 5525 as the listening port number. Configure the rest of the parameters. Display your configurations and exploit the target**




Setting rhost to Windows XP; Setting lhost to Internal Kali; Setting port to 5525; Showing options to display configurations before performing the exploit

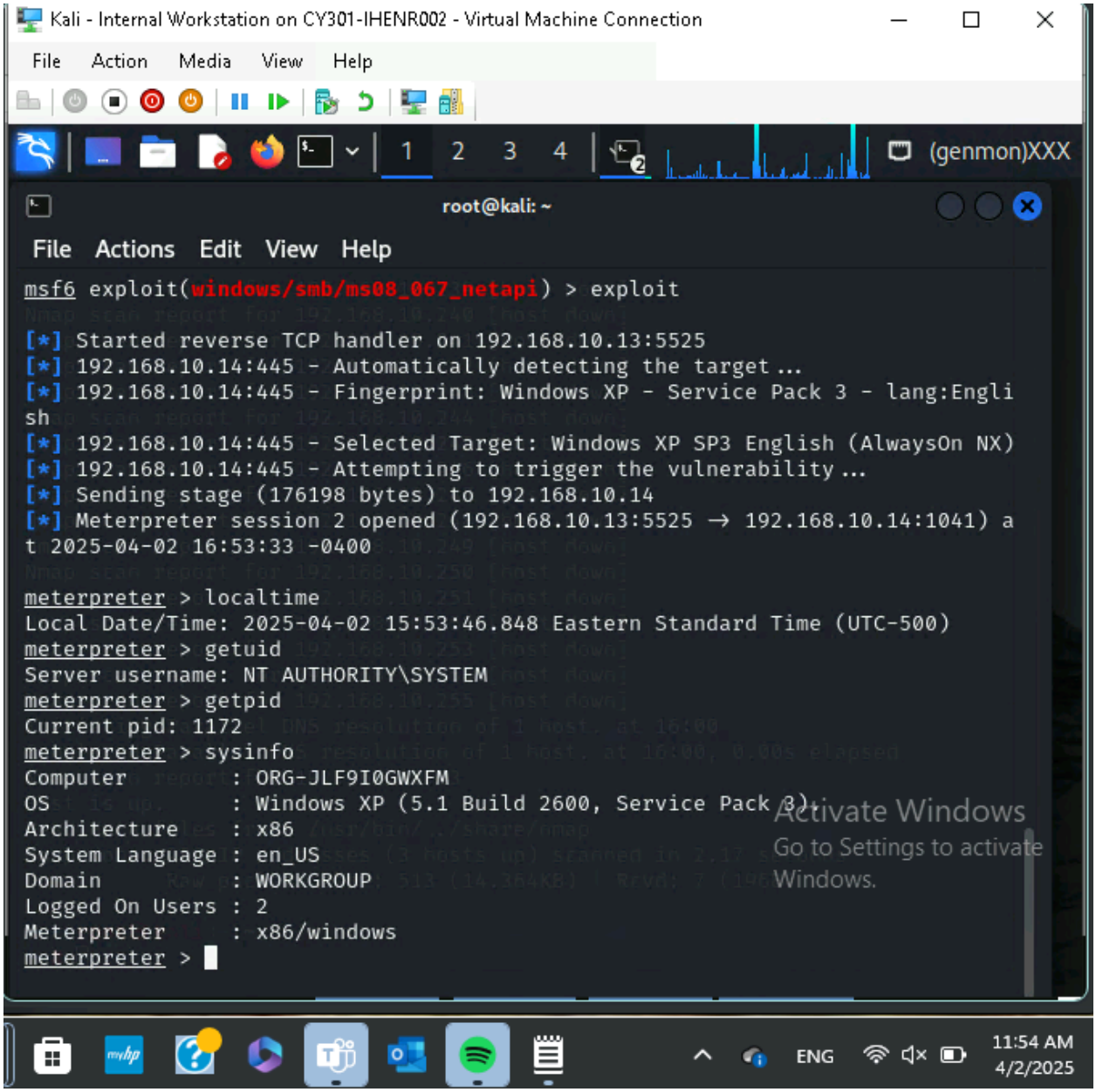
**Post Exploitation**

6. **Execute the screenshot command to take a screenshot of the target machine if the exploit is successful**




Running exploit

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




7. Using the localtime command to get local date and time
8. Using the getuid command to get the SID of the user
9. Using the getpid command to get the current process identifier
10. Using the sysinfo command to get system information about the target