OLD DOMINION UNIVERSITY

CYSE 301 CYBERSECURITY TECHNIQUES AND OPERATIONS

Assignment #4 Ethical Hacking

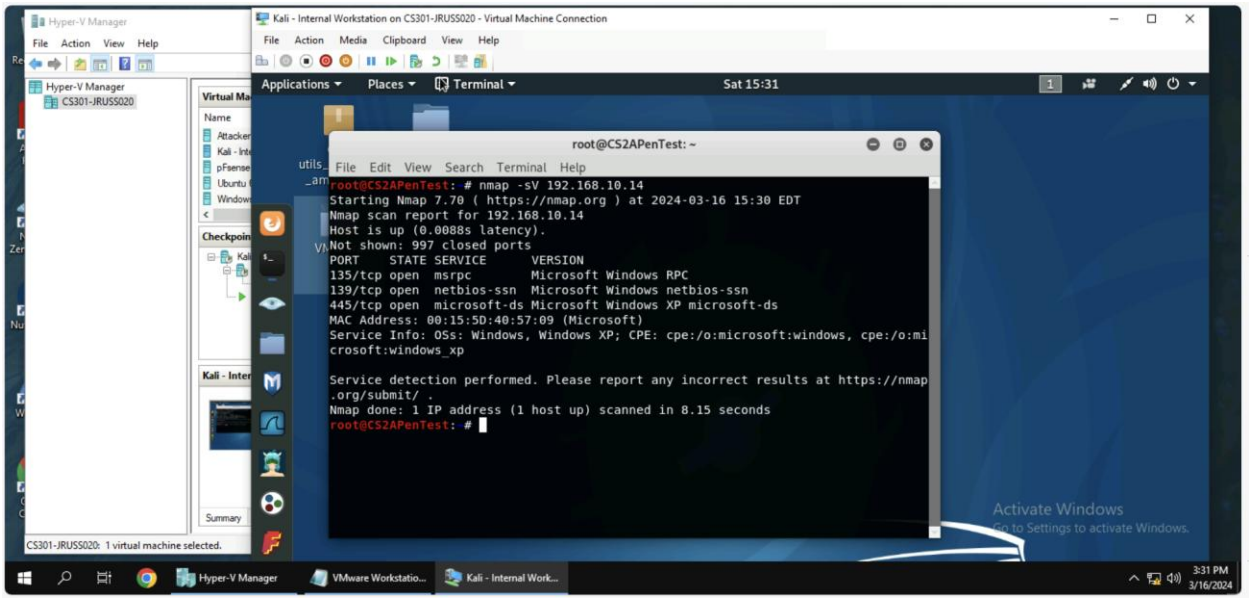
Joshua Russell

Task A.

Exploit SMB on Windows XP with Metasploit (20 pt, 2pt each)

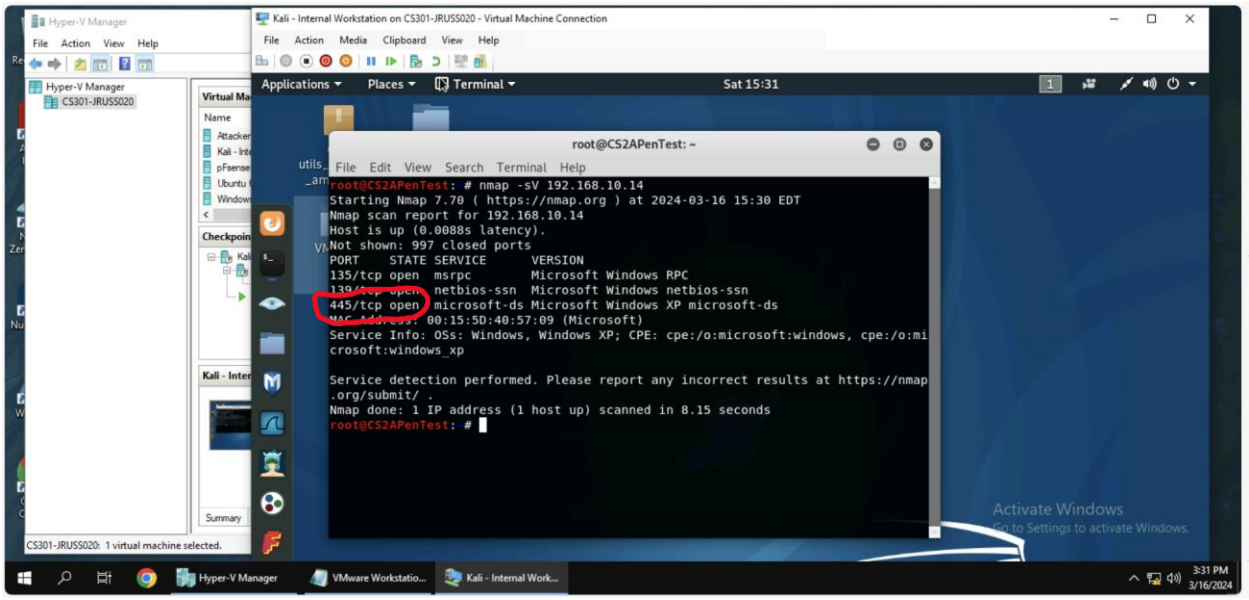
In this task, you need to complete the following steps to exploit SMB vulnerability on Windows XP.

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



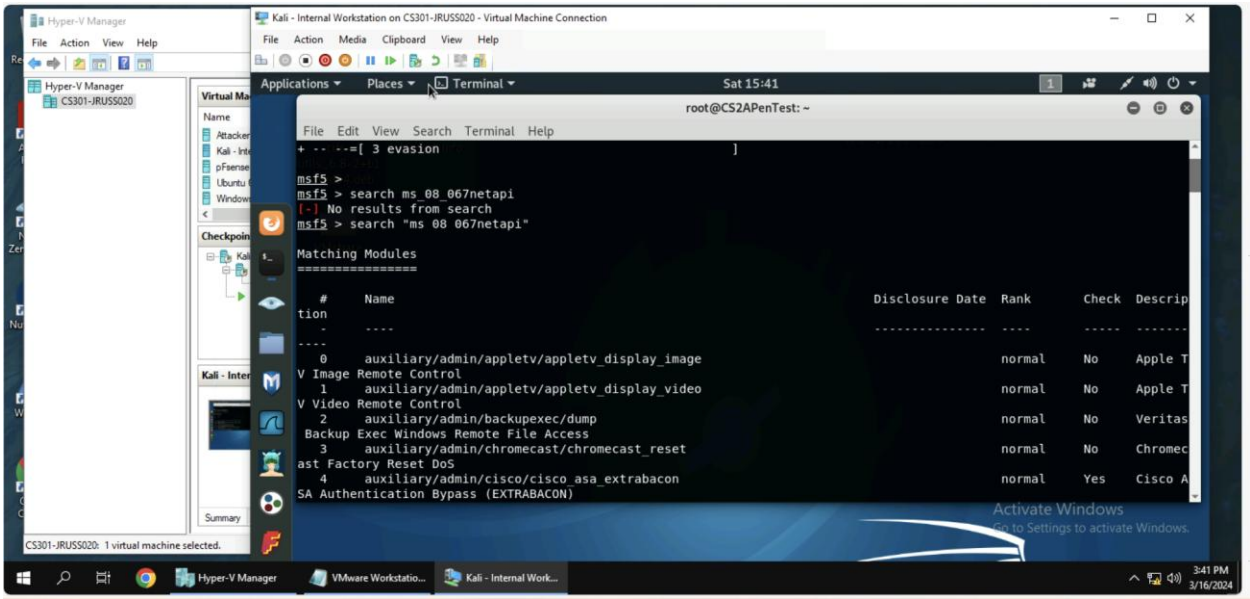
(The above screen shot shows a nmap scan of the Windows XP Server 192.168.10.14 to find open ports and services. The option -sV was used to detect version information).

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



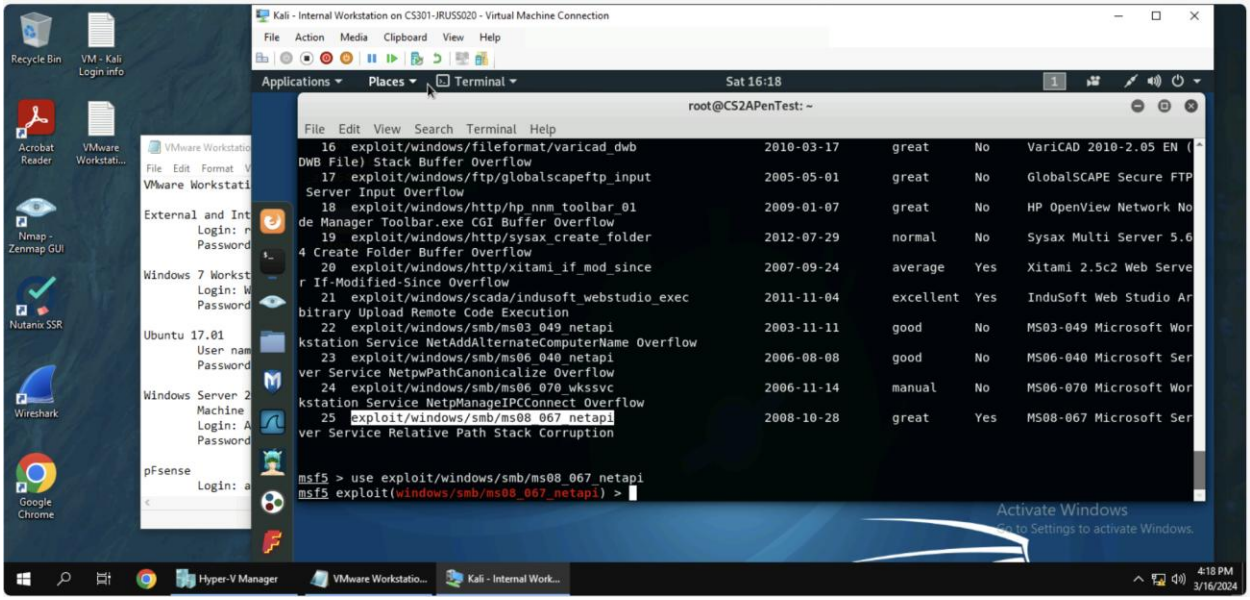
(In the above screenshot, port 445 the SMB port is open)

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

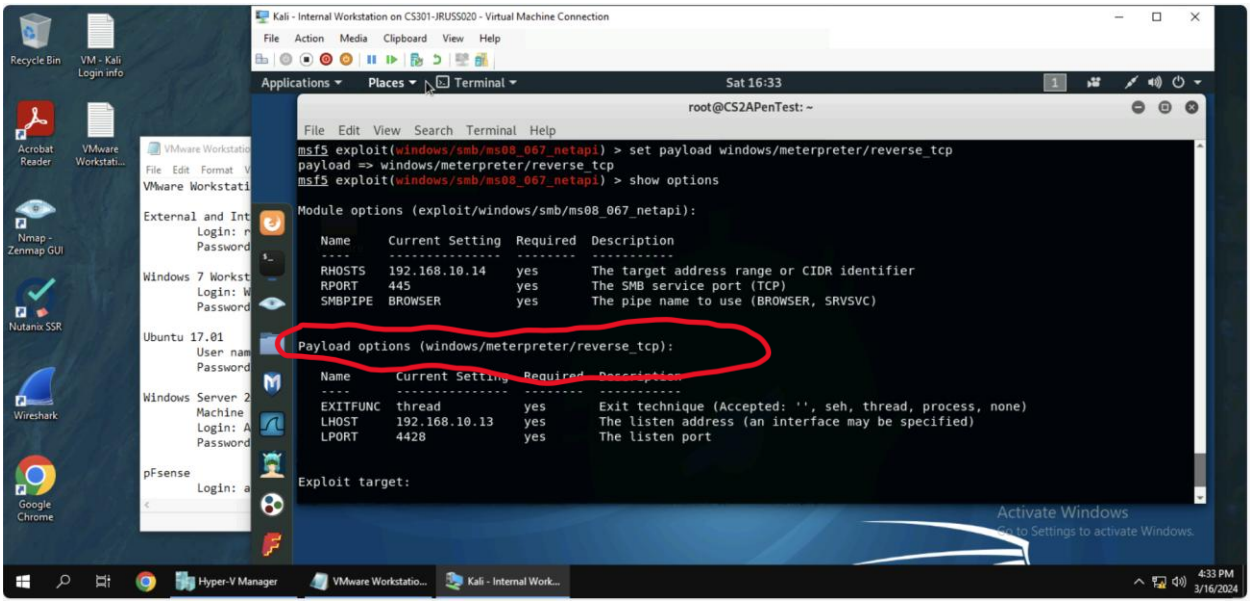


(In the above screenshot, a search for ms 08 067 netapi was performed)

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

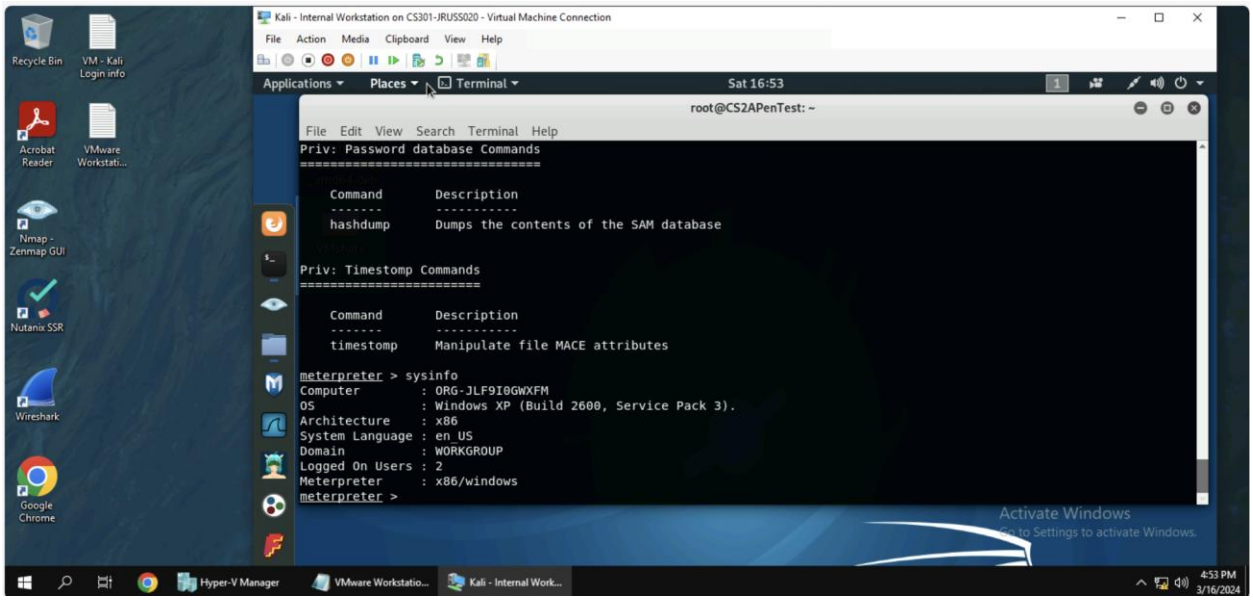


(In the above screenshot, the ms08 067 netapi exploit is used)



(In the above screenshot the meterpreter is set to a reverse tcp as payload)

5. Use XXXX (follow the lab instruction) as the listening port number. Configure the rest of the parameters. Display your configurations and exploit the target.


Kali - Internal Workstation on CS301-JRUSS020 - Virtual Machine Connection
File Action Media Clipboard View Help
Applications Places Terminal Sat 16:53
root@CS2APenTest: ~
File Edit View Search Terminal Help
Priv: Password database Commands
Command Description
hashdump Dumps the contents of the SAM database
Priv: Timestomp Commands
Command Description
timestomp Manipulate file MACE attributes
meterpreter > sysinfo
Computer : ORG-JLF9I0GWXFM
OS : Windows XP (Build 2600, Service Pack 3).
Architecture : x86
System Language : en_US
Domain : WORKGROUP
Logged On Users : 2
Meterpreter : x86/windows
meterpreter >
Activate Windows
Go to Settings to activate Windows.
Recycle Bin
VM - Kali Login info
Acrobat Reader
VMware Workstati...
Nmap - Zenmap GUI
Nutanix SSR
Wireshark
Google Chrome
Hyper-V Manager
VMware Workstatio...
Kali - Internal Work...
4:53 PM
3/16/2024