VIRTUAL CYBERSECURITY LAB SETUP

1. Introduction

Ethical hacking requires a safe and isolated environment to practice and test vulnerabilities without risking real systems. A virtual lab provides this isolation, allowing users to sharpen their skills and learn from mistakes without causing harm.

2. Essential Components

To set up a virtual cybersecurity lab, I made use of three main components:

- Virtualization Software (VirtualBox): This software allows a single physical computer (host) to run multiple virtual machines (VMs). Each VM acts as a separate computer with its own operating system. In this project I used two virtual machines with Kali Linux and windows 7 as the operating systems.
- Attacking Machine (VM): This VM is used to perform penetration testing and vulnerability assessments. Kali Linux OS is used as it come pre-installed with a wide array of cybersecurity tools
- Target Machine (VM): This VM is the system that will be attacked and analyzed. I made use of windows 7 OS for this project.

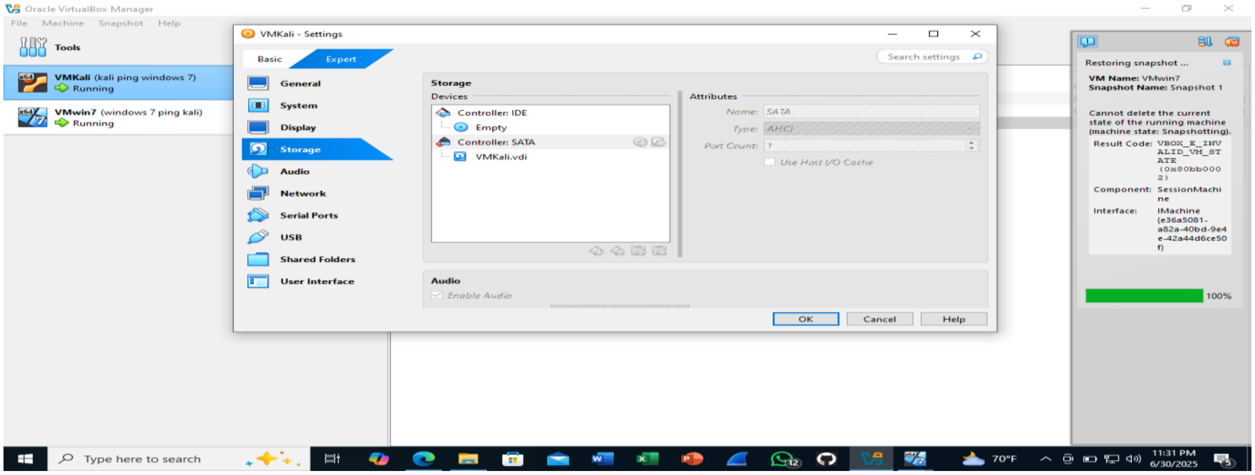
3. Installation Process

Install VirtualBox

I downloaded and install VirtualBox from its official website. I ensured I also download and install the VirtualBox Extension Pack.

Install Attacking Machine (Kali Linux)

I downloaded the VirtualBox image for Kali Linux OS iso file. uploaded the downloaded iso file into logical optical anchor of the storage section in the virtual machine.



VMKali (kali ping windows 7)
Running

VMwin7 (windows 7 ping kali)
Running

Storage

Devices

- Controller: IDE
  - Empty
- Controller: SATA
  - VMKali.vdi

Attributes

Name: SATA

Type: AHCI

Port Count: 1

□ Use Host I/O Cache

Audio

☑ Enable Audio

Restoring snapshot ...

VM Name: VMwin7
Snapshot Name: Snapshot 1

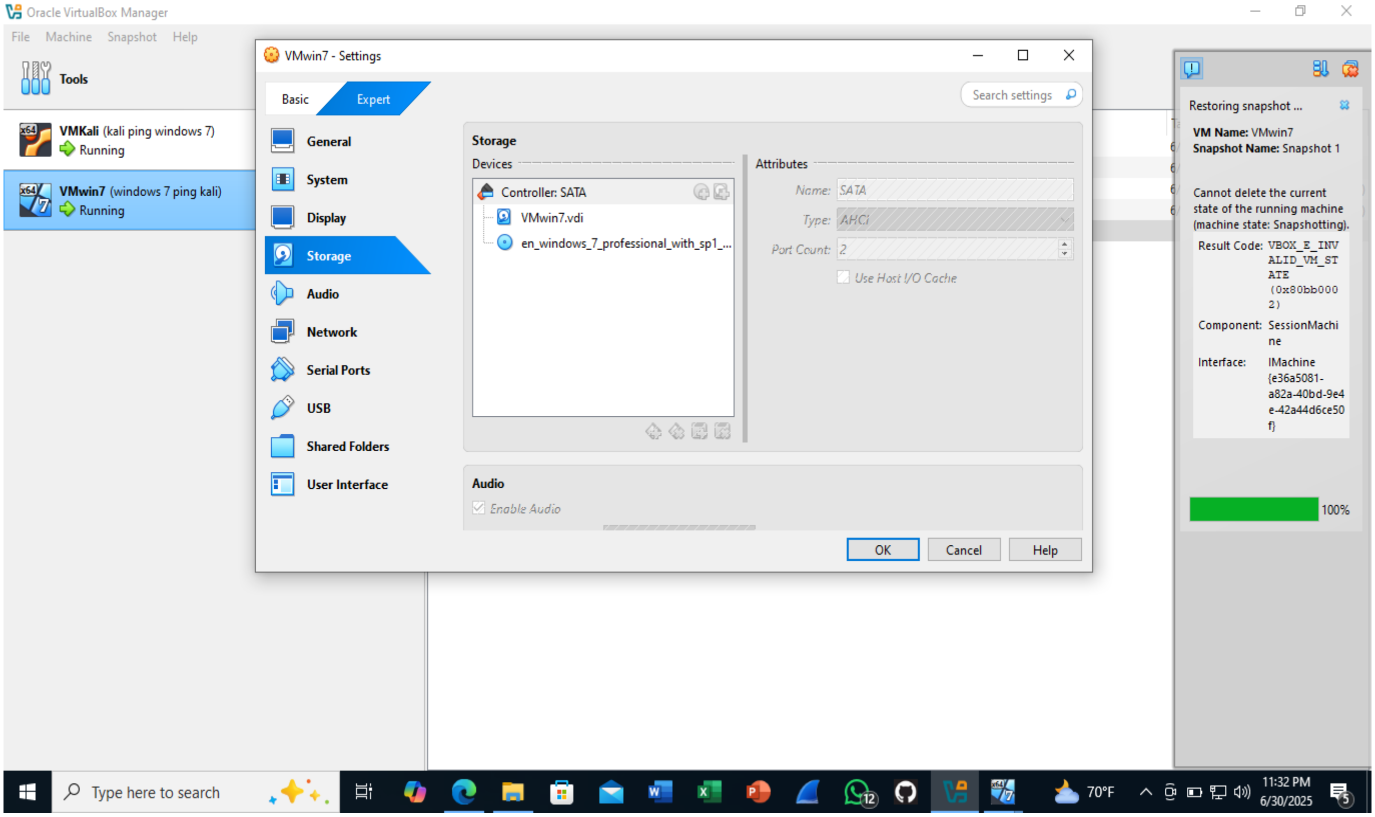
Cannot delete the current state of the running machine (machine state: Snapshotting).

Result Code:	VBOX_E_INVALID_VM_STATE (0x80bb0002)
Component:	SessionMachine
Interface:	IMachine {e36a5081-a82a-40bd-9e4e-42a44d6ce50f}

100%

Install Target Machine (Windows 7 OS)

I downloaded windows 7 OS iso file as a vulnerable VM attached the iso file to the logical optical CD of the storage section of the virtual machine.



Storage

Devices

- Controller: SATA
  - VMwin7.vdi
  - en_windows_7_professional_with_sp1_...

Attributes

Name: SATA

Type: AHCI

Port Count: 2

☐ Use Host I/O Cache

Audio

☑ Enable Audio

Restoring snapshot ...

VM Name: VMwin7
Snapshot Name: Snapshot 1

Cannot delete the current state of the running machine (machine state: Snapshotting).

Result Code: VBOX_E_INVALID_VM_STATE (0x80bb0002)

Component: SessionMachine

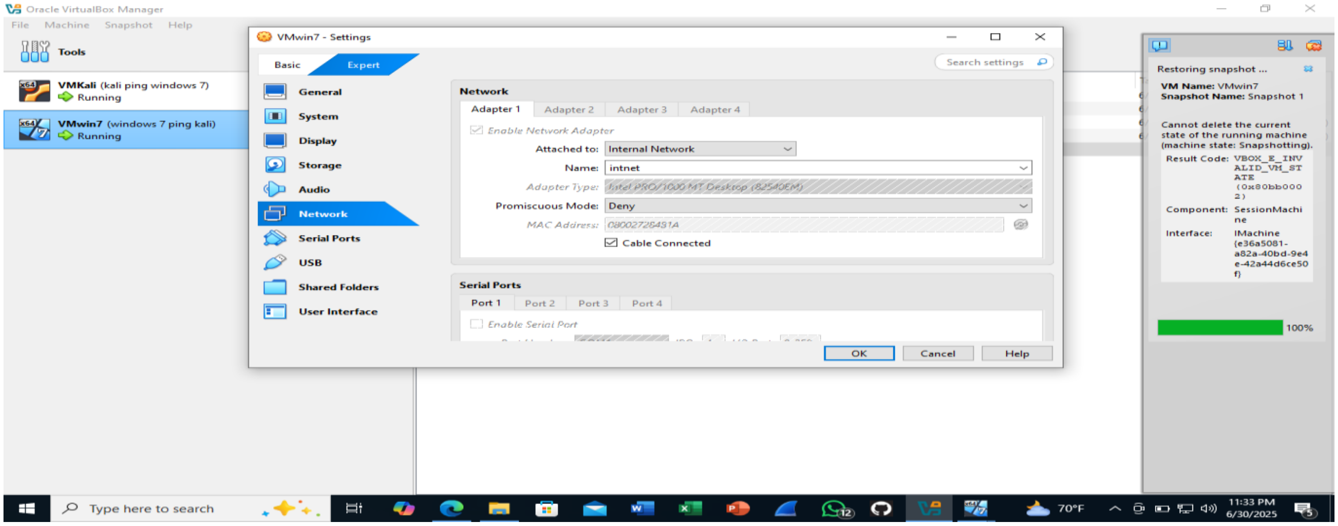
Interface: IMachine {e36a5081-a82a-40bd-9e4e-42a44d6ce50f}

100%

4. Network Configuration (Internal Network)

To isolate my lab from the public internet and allow VMs to communicate with each other, internal Network was used. This setup ensures that my hacking activities remain within the virtual lab and do not affect my host machine or external networks. Similar to Host-Only, but VMs can only communicate with other VMs on the same internal network, not with the host machine. This offers even greater isolation.

Windows 7 network settings



VMwin7 - Settings

Network

Adapter 1 | Adapter 2 | Adapter 3 | Adapter 4

☑ Enable Network Adapter

Attached to: Internal Network

Name: intnet

Adapter Type: Intel PRO/1000 MT Desktop (82540EM)

Promiscuous Mode: Deny

MAC Address: 08002726431A

☑ Cable Connected

Serial Ports

Port 1 | Port 2 | Port 3 | Port 4

□ Enable Serial Port

Restoring snapshot ...

VM Name: VMwin7
Snapshot Name: Snapshot 1

Cannot delete the current state of the running machine (machine state: Snapshotting).

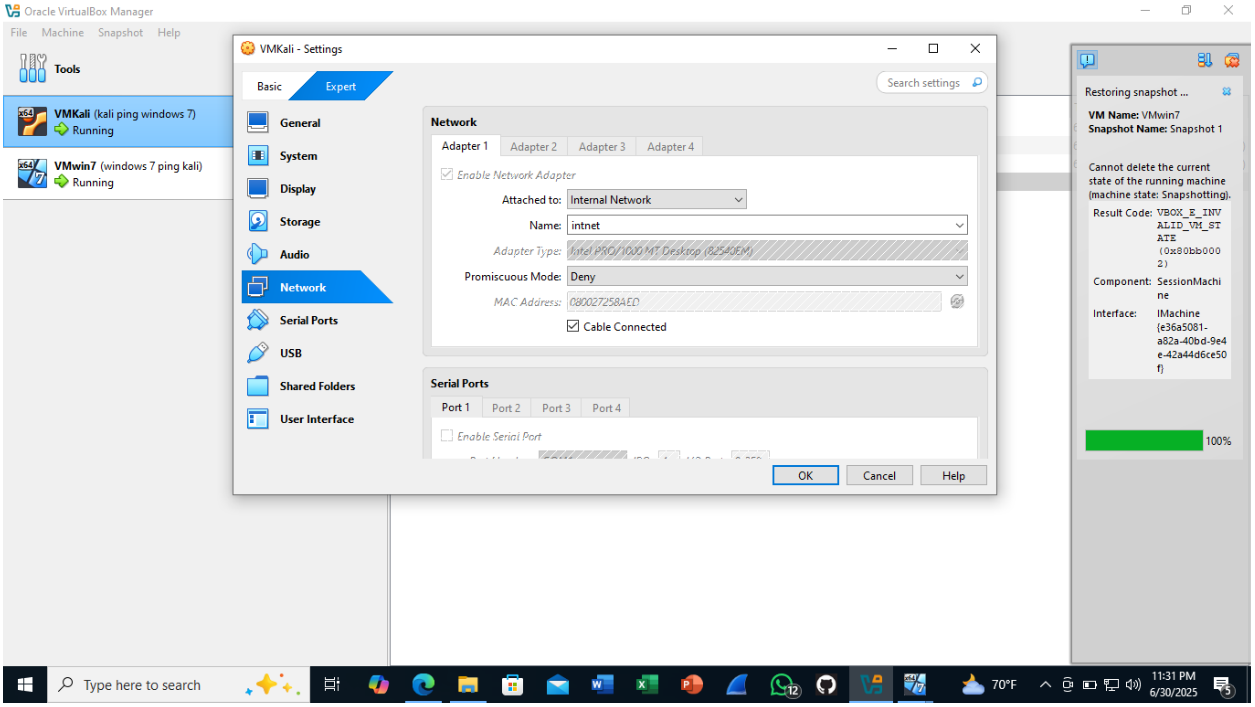
Result Code: VBOX_E_INVALID_VM_STATE (0x80bb0002)

Component: SessionMachine

Interface: IMachine {e36a5081-a82a-40bd-9e4e-42a44d6ce50f}

100%

Kali Linux network setting



VMKali - Settings

Network

Adapter 1 | Adapter 2 | Adapter 3 | Adapter 4

☑ Enable Network Adapter

Attached to: Internal Network

Name: intnet

Adapter Type: Intel PRO/1000 MT Desktop (82540EM)

Promiscuous Mode: Deny

MAC Address: 080027258AED

☑ Cable Connected

Serial Ports

Port 1 | Port 2 | Port 3 | Port 4

□ Enable Serial Port

Restoring snapshot ...

VM Name: VMwin7
Snapshot Name: Snapshot 1

Cannot delete the current state of the running machine (machine state: Snapshotting).

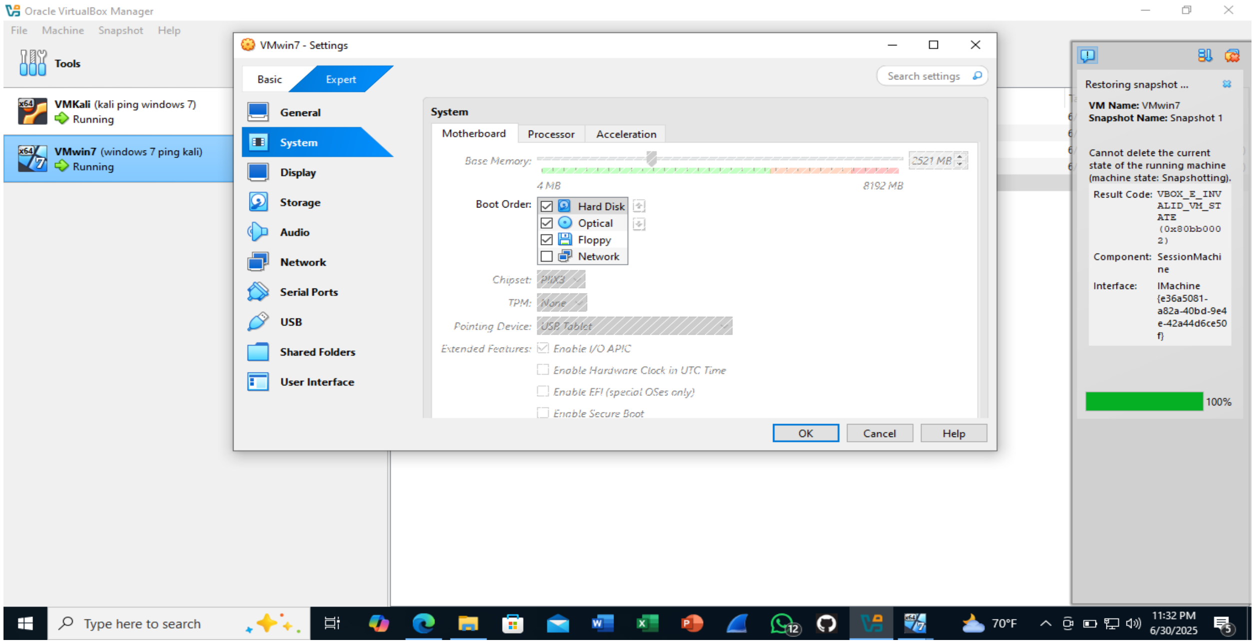
Result Code: VBOX_E_INVALID_VM_STATE (0x80bb0002)

Component: SessionMachine

Interface: IMachine {e36a5081-a82a-40bd-9e4e-42a44d6ce50f}

100%

Boot order settings



System

Base Memory: 2521 MB (4 MB – 8192 MB)

Boot Order:
- ☑ Hard Disk
- ☑ Optical
- ☑ Floppy
- □ Network

Chipset: PIIX3

TPM: None

Pointing Device: USB Tablet

Extended Features: ☑ Enable I/O APIC
□ Enable Hardware Clock in UTC Time
□ Enable EFI (special OSes only)
□ Enable Secure Boot

Restoring snapshot ...

VM Name: VMwin7
Snapshot Name: Snapshot 1

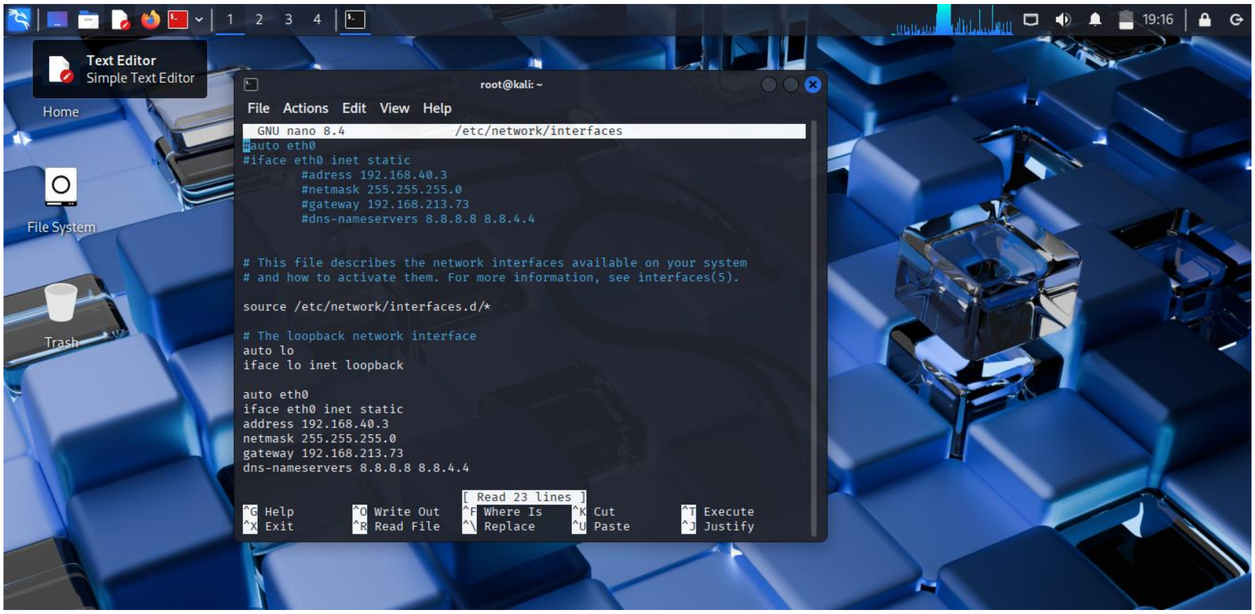
Cannot delete the current state of the running machine (machine state: Snapshotting).

Result Code: VBOX_E_INVALID_VM_STATE (0x80bb0002)
Component: SessionMachine
Interface: IMachine {e36a5081-a82a-40bd-9e4e-42a44d6ce50f}

100%

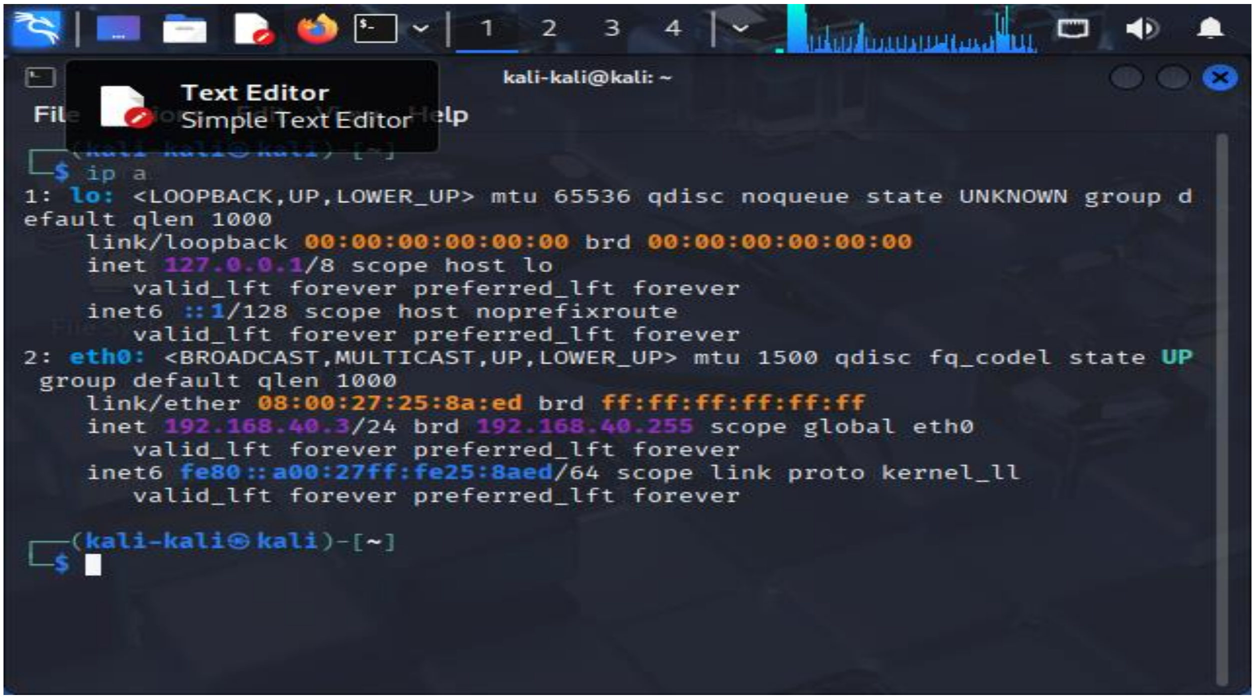
5. Verifying connectivity via ping test

Configuring Kali Linux static ip address



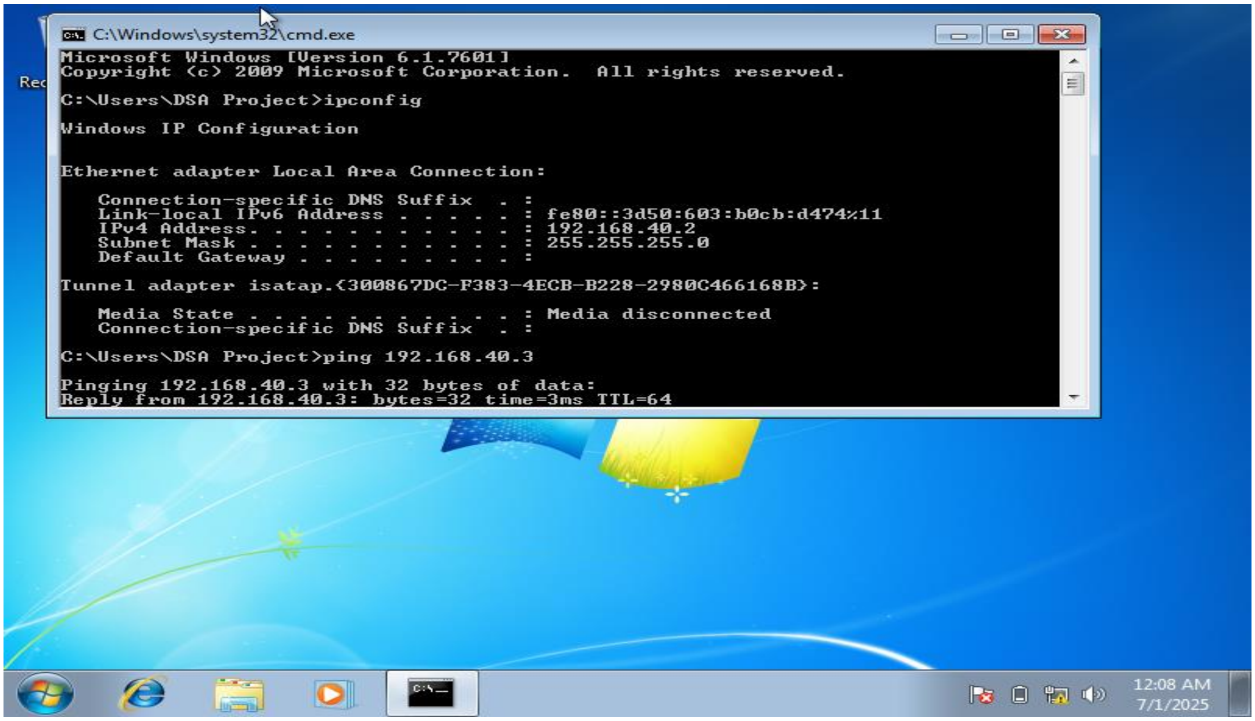
```
  GNU nano 8.4                 /etc/network/interfaces
#auto eth0
#iface eth0 inet static
        #adress 192.168.40.3
        #netmask 255.255.255.0
        #gateway 192.168.213.73
        #dns-nameservers 8.8.8.8 8.8.4.4


# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

auto eth0
iface eth0 inet static
address 192.168.40.3
netmask 255.255.255.0
gateway 192.168.213.73
dns-nameservers 8.8.8.8 8.8.4.4

                              [ Read 23 lines ]
^G Help         ^O Write Out    ^F Where Is     ^K Cut          ^T Execute
^X Exit         ^R Read File    ^\ Replace      ^U Paste        ^J Justify
```

Confirming Kali Linux static ip address



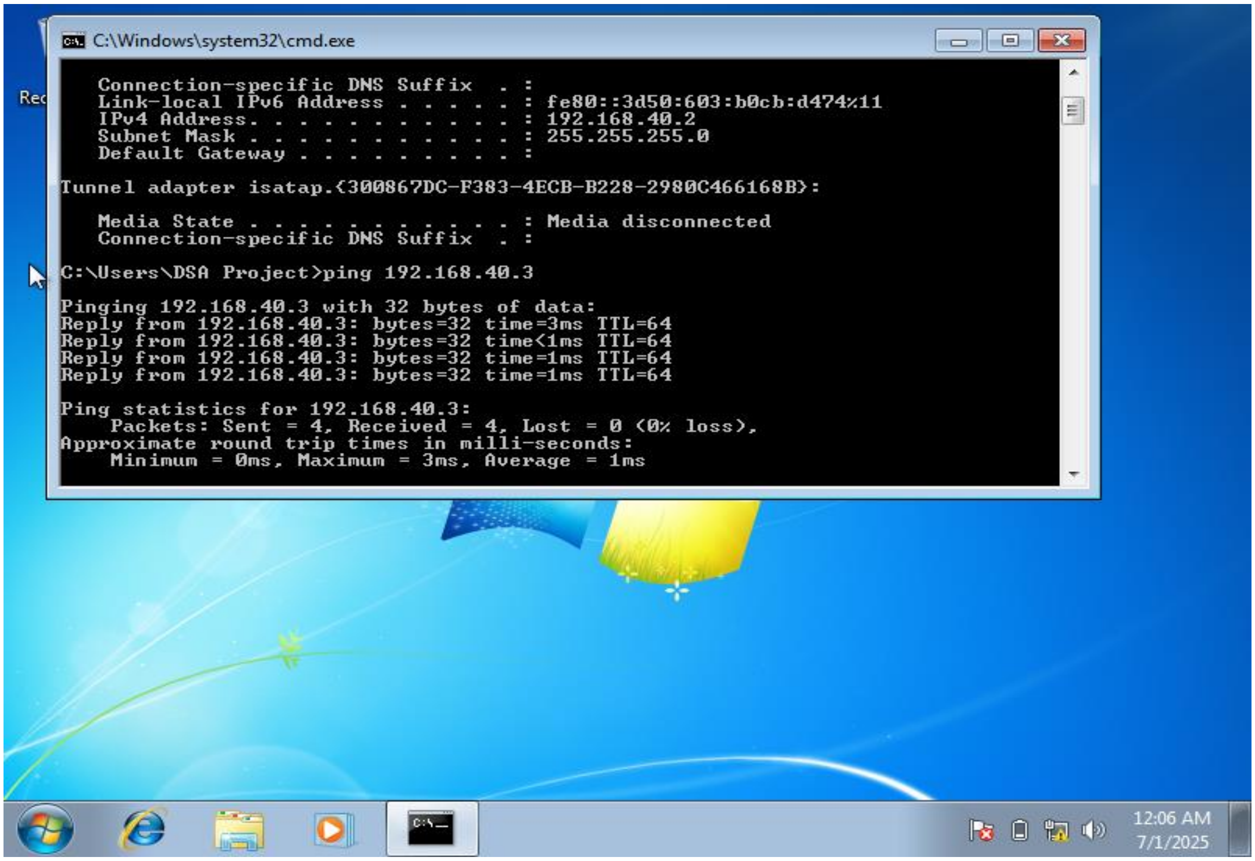
```
┌──(kali-kali㉿kali)-[~]
└─$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group d
efault qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP
 group default qlen 1000
    link/ether 08:00:27:25:8a:ed brd ff:ff:ff:ff:ff:ff
    inet 192.168.40.3/24 brd 192.168.40.255 scope global eth0
       valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe25:8aed/64 scope link proto kernel_ll
       valid_lft forever preferred_lft forever

┌──(kali-kali㉿kali)-[~]
└─$ 
```

Windows 7 static ip address



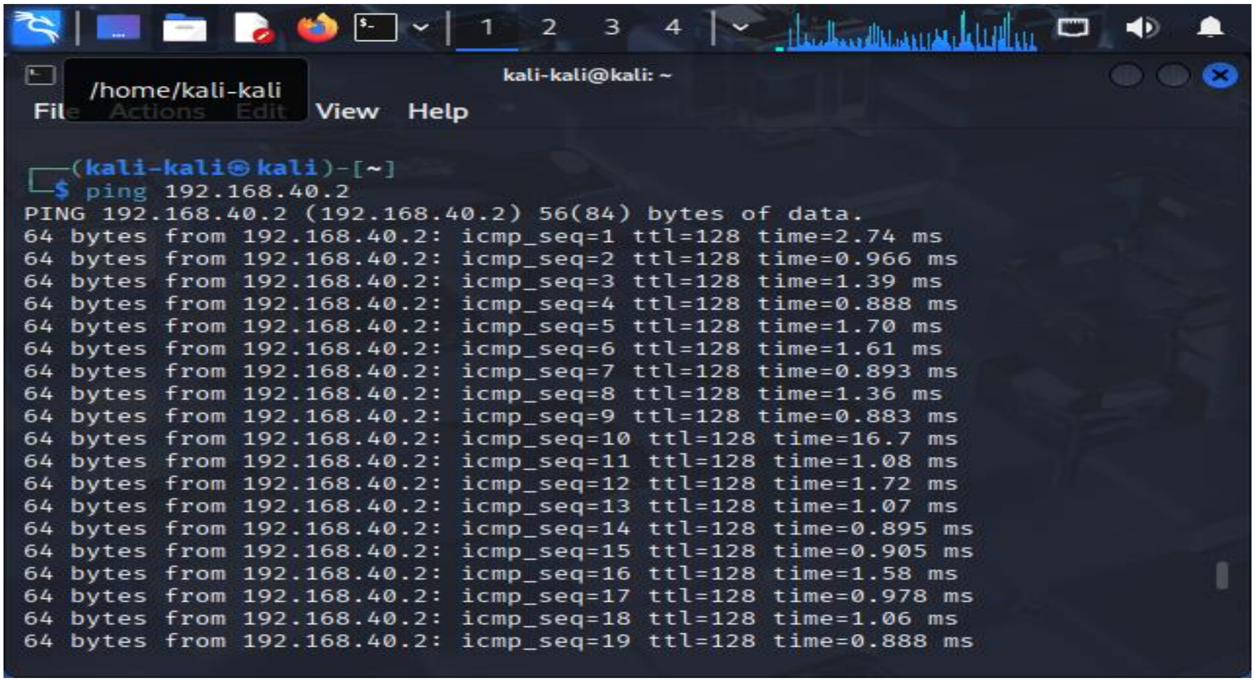
```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\DSA Project>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::3d50:603:b0cb:d474%11
   IPv4 Address. . . . . . . . . . . : 192.168.40.2
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Tunnel adapter isatap.{300867DC-F383-4ECB-B228-2980C466168B}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

C:\Users\DSA Project>ping 192.168.40.3

Pinging 192.168.40.3 with 32 bytes of data:
Reply from 192.168.40.3: bytes=32 time=3ms TTL=64
```

Pinging Kali Linux from Windows 7



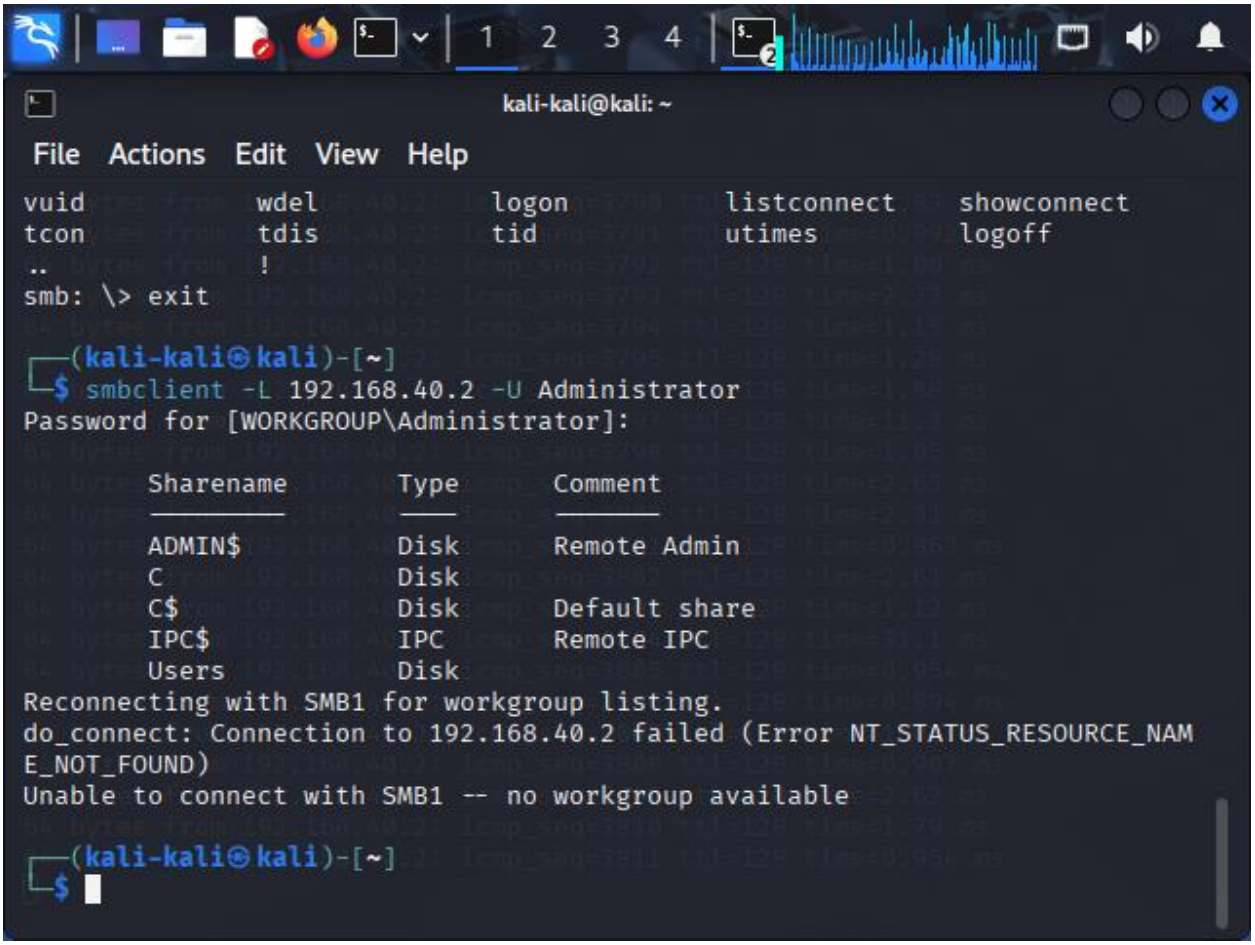
```
   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::3d50:603:b0cb:d474%11
   IPv4 Address. . . . . . . . . . . : 192.168.40.2
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Tunnel adapter isatap.{300867DC-F383-4ECB-B228-2980C466168B}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

C:\Users\DSA Project>ping 192.168.40.3

Pinging 192.168.40.3 with 32 bytes of data:
Reply from 192.168.40.3: bytes=32 time=3ms TTL=64
Reply from 192.168.40.3: bytes=32 time<1ms TTL=64
Reply from 192.168.40.3: bytes=32 time=1ms TTL=64
Reply from 192.168.40.3: bytes=32 time=1ms TTL=64

Ping statistics for 192.168.40.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 3ms, Average = 1ms
```

Pinging windows 7 from Kali Linux



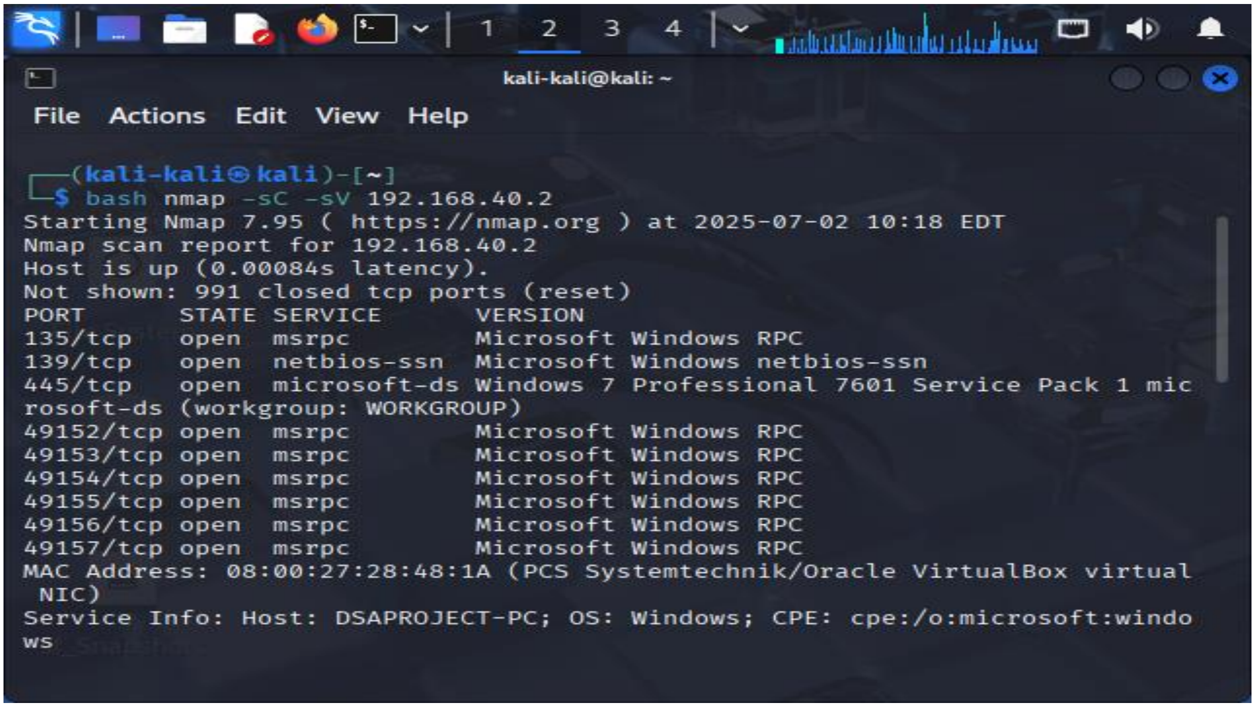
```
┌──(kali-kali㉿kali)-[~]
└─$ ping 192.168.40.2
PING 192.168.40.2 (192.168.40.2) 56(84) bytes of data.
64 bytes from 192.168.40.2: icmp_seq=1 ttl=128 time=2.74 ms
64 bytes from 192.168.40.2: icmp_seq=2 ttl=128 time=0.966 ms
64 bytes from 192.168.40.2: icmp_seq=3 ttl=128 time=1.39 ms
64 bytes from 192.168.40.2: icmp_seq=4 ttl=128 time=0.888 ms
64 bytes from 192.168.40.2: icmp_seq=5 ttl=128 time=1.70 ms
64 bytes from 192.168.40.2: icmp_seq=6 ttl=128 time=1.61 ms
64 bytes from 192.168.40.2: icmp_seq=7 ttl=128 time=0.893 ms
64 bytes from 192.168.40.2: icmp_seq=8 ttl=128 time=1.36 ms
64 bytes from 192.168.40.2: icmp_seq=9 ttl=128 time=0.883 ms
64 bytes from 192.168.40.2: icmp_seq=10 ttl=128 time=16.7 ms
64 bytes from 192.168.40.2: icmp_seq=11 ttl=128 time=1.08 ms
64 bytes from 192.168.40.2: icmp_seq=12 ttl=128 time=1.72 ms
64 bytes from 192.168.40.2: icmp_seq=13 ttl=128 time=1.07 ms
64 bytes from 192.168.40.2: icmp_seq=14 ttl=128 time=0.895 ms
64 bytes from 192.168.40.2: icmp_seq=15 ttl=128 time=0.905 ms
64 bytes from 192.168.40.2: icmp_seq=16 ttl=128 time=1.58 ms
64 bytes from 192.168.40.2: icmp_seq=17 ttl=128 time=0.978 ms
64 bytes from 192.168.40.2: icmp_seq=18 ttl=128 time=1.06 ms
64 bytes from 192.168.40.2: icmp_seq=19 ttl=128 time=0.888 ms
```

Shared resources on windows 7 access from Kali Linux



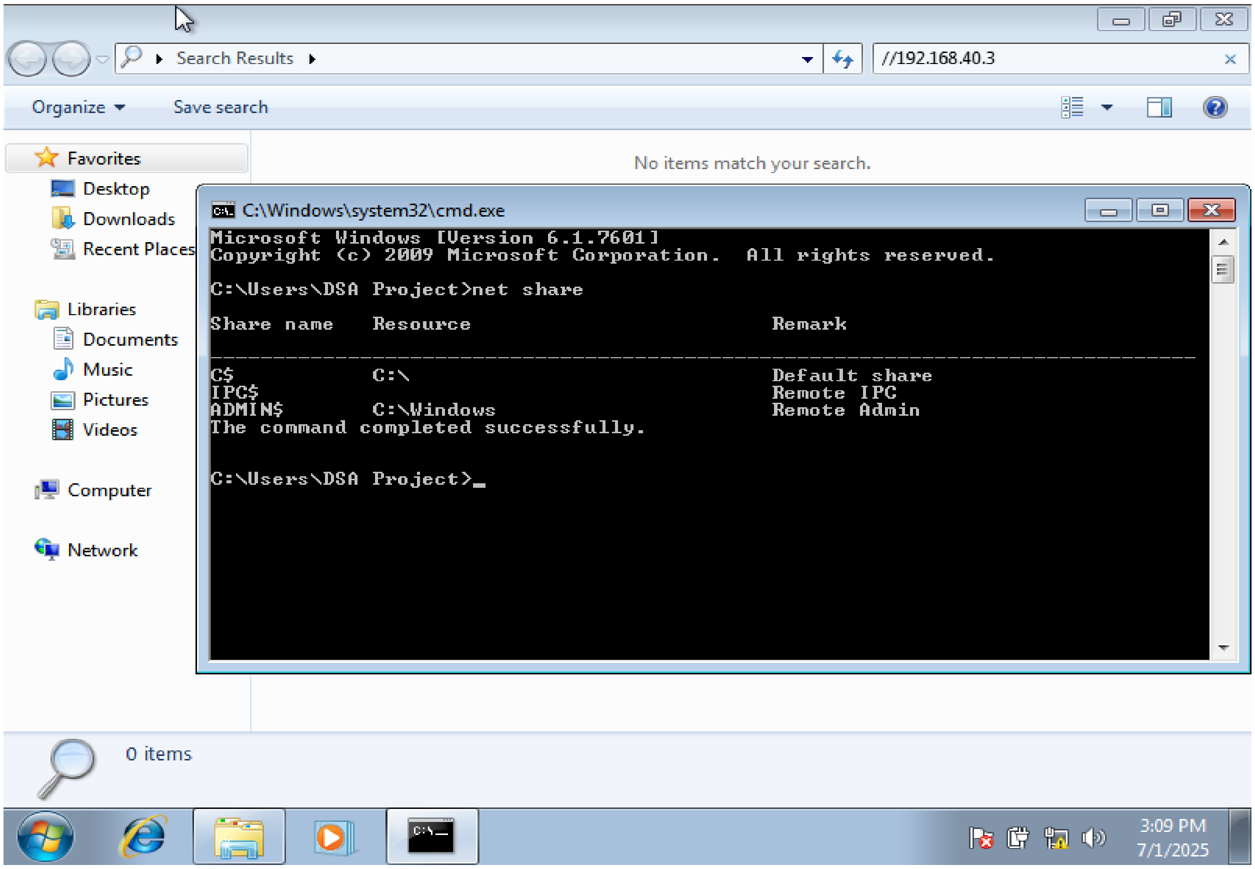
```
vuid           wdel           logon          listconnect    showconnect
tcon           tdis           tid            utimes         logoff
..             !
smb: \> exit

┌──(kali-kali㉿kali)-[~]
└─$ smbclient -L 192.168.40.2 -U Administrator
Password for [WORKGROUP\Administrator]:

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Remote Admin
        C               Disk
        C$              Disk      Default share
        IPC$            IPC       Remote IPC
        Users           Disk
Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 192.168.40.2 failed (Error NT_STATUS_RESOURCE_NAM
E_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available

┌──(kali-kali㉿kali)-[~]
└─$ 
```

Services shared on windows 7 accessed from Kali Linux



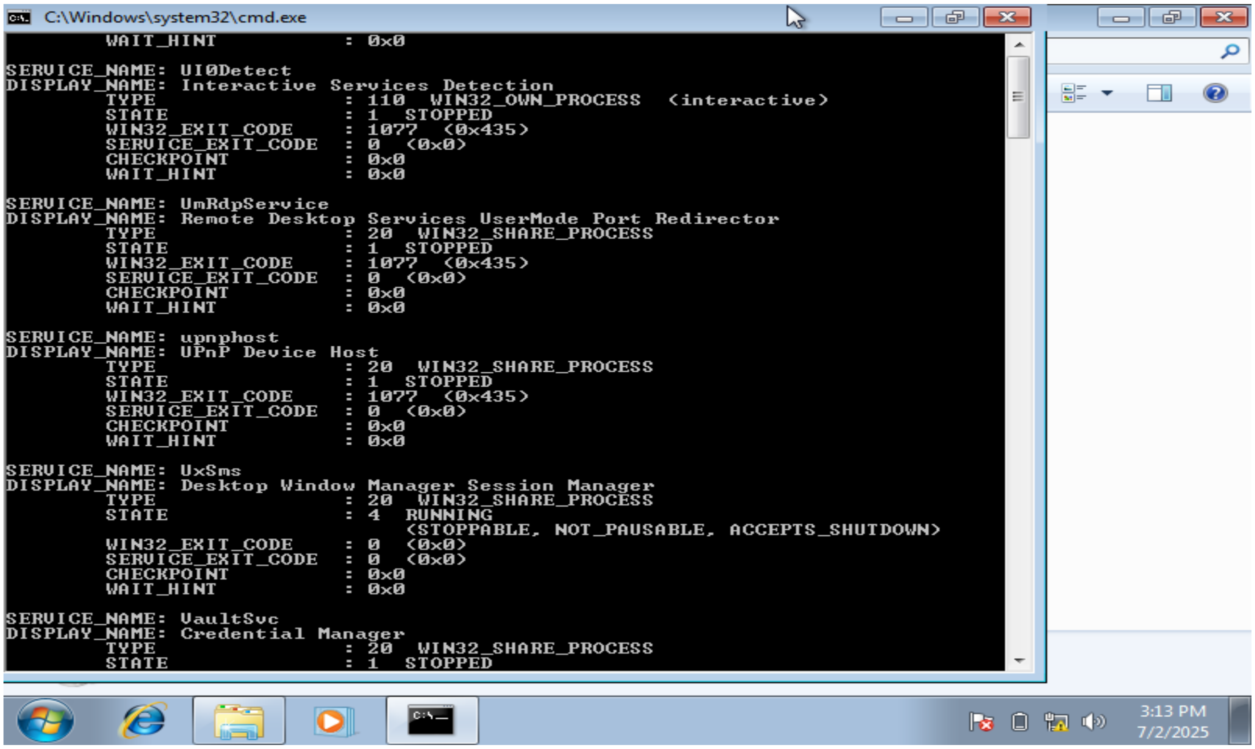
```
┌──(kali-kali㉿kali)-[~]
└─$ bash nmap -sC -sV 192.168.40.2
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-02 10:18 EDT
Nmap scan report for 192.168.40.2
Host is up (0.00084s latency).
Not shown: 991 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Windows 7 Professional 7601 Service Pack 1 mic
rosoft-ds (workgroup: WORKGROUP)
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49156/tcp open  msrpc        Microsoft Windows RPC
49157/tcp open  msrpc        Microsoft Windows RPC
MAC Address: 08:00:27:28:48:1A (PCS Systemtechnik/Oracle VirtualBox virtual
 NIC)
Service Info: Host: DSAPROJECT-PC; OS: Windows; CPE: cpe:/o:microsoft:windo
ws
```

folders shared on Kali Linux accessed from windows 7



```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\DSA Project>net share

Share name   Resource                        Remark

-------------------------------------------------------------------------------
C$           C:\                             Default share
IPC$                                         Remote IPC
ADMIN$       C:\Windows                      Remote Admin
The command completed successfully.


C:\Users\DSA Project>_
```

Services enumeration on Kali-Linux



```
        WAIT_HINT          : 0x0

SERVICE_NAME: UI0Detect
DISPLAY_NAME: Interactive Services Detection
        TYPE               : 110  WIN32_OWN_PROCESS  (interactive)
        STATE              : 1  STOPPED
        WIN32_EXIT_CODE    : 1077  (0x435)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x0

SERVICE_NAME: UmRdpService
DISPLAY_NAME: Remote Desktop Services UserMode Port Redirector
        TYPE               : 20  WIN32_SHARE_PROCESS
        STATE              : 1  STOPPED
        WIN32_EXIT_CODE    : 1077  (0x435)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x0

SERVICE_NAME: upnphost
DISPLAY_NAME: UPnP Device Host
        TYPE               : 20  WIN32_SHARE_PROCESS
        STATE              : 1  STOPPED
        WIN32_EXIT_CODE    : 1077  (0x435)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x0

SERVICE_NAME: UxSms
DISPLAY_NAME: Desktop Window Manager Session Manager
        TYPE               : 20  WIN32_SHARE_PROCESS
        STATE              : 4  RUNNING
                                (STOPPABLE, NOT_PAUSABLE, ACCEPTS_SHUTDOWN)
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x0

SERVICE_NAME: VaultSvc
DISPLAY_NAME: Credential Manager
        TYPE               : 20  WIN32_SHARE_PROCESS
        STATE              : 1  STOPPED
```