Tables of Content

Tables of Figures

Introduction

In this lab, we will create an isolated network between two virtual machines (VMs) Kali Linux and Windows 7 using Oracle VirtualBox. The goal is to configure the network adapters of both VMs to communicate with each other in an isolated environment, without any external network interference. This setup is useful for penetration testing, network security experiments, and learning how to configure static IP addresses and network settings in different operating systems.

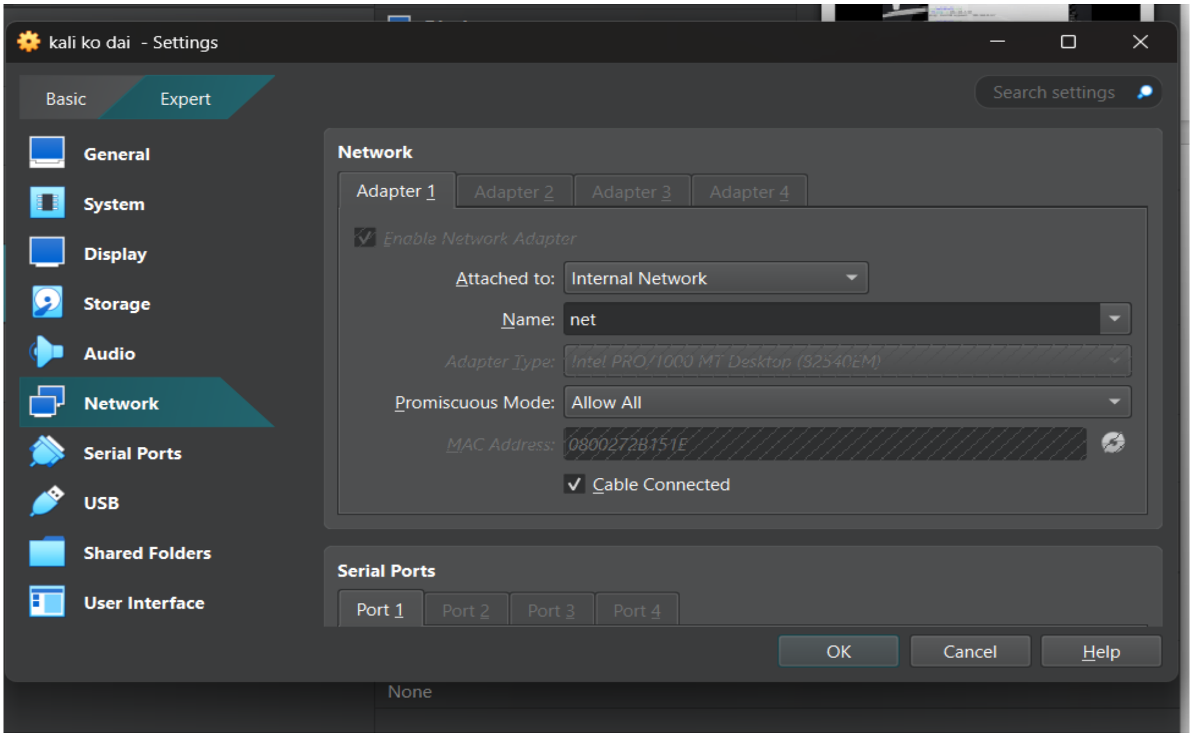
Objective

The primary objective of this lab is to:

1. **Configure an isolated internal network between Kali Linux and Windows 10 VMs using VirtualBox.**
2. **Assign static IP addresses to both VMs to ensure proper communication.**
3. **Test the connectivity between the two VMs using the ping command.**
4. **Understand the basics of network configuration in both Linux and Windows environments.**

Part 1: Configure the VM Network Adapter Setting

- Change the Default Network Adapter for the Kali Linux VM
- Open the settings for the Kali Linux VM.
- Navigate to the “Network” section.
- Change the network adapter from NAT to Internal Network.



kali ko dai - Settings

Network

Adapter 1

☑ Enable Network Adapter

Attached to: Internal Network

Name: net

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

Promiscuous Mode: Allow All

MAC Address: 0800272B151E

☑ Cable Connected

Serial Ports

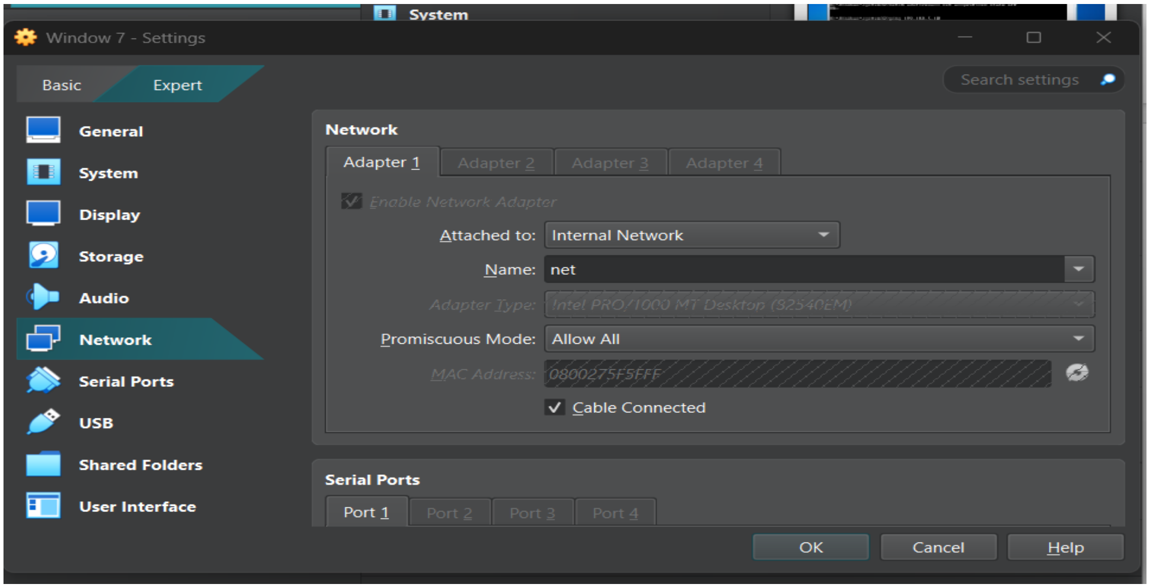
Port 1

None

Figure 1 VirtualBox Default NAT adapter setting for Kali Linux VM.

Part 2: Configure the Network Adapter for Window 10 VM

- Change the Default Network Adapter for the Window 10 VM
- Open the settings for the Window 10 VM.
- Navigate to the “Network” section.
- Change the network adapter from NAT to Internal Network.



☑ Enable Network Adapter

Attached to: Internal Network

Name: net

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

Promiscuous Mode: Allow All

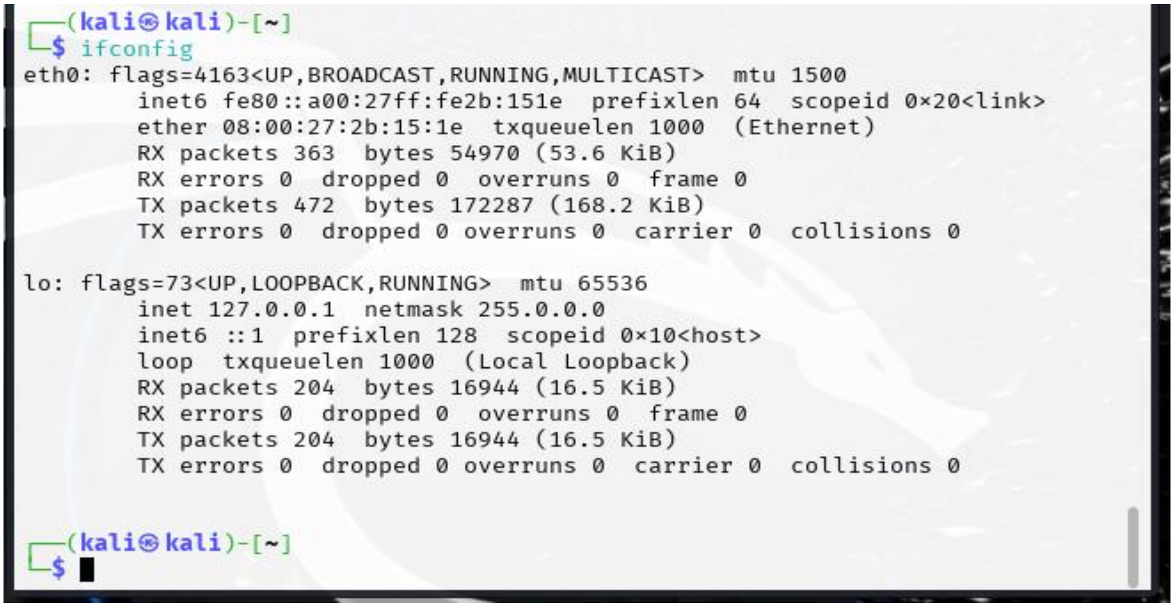
MAC Address: 0800275F5FFF

☑ Cable Connected

Figure 2 VirtualBox Default NAT adapter setting for Window VM.

Part 3: Initial IP Check

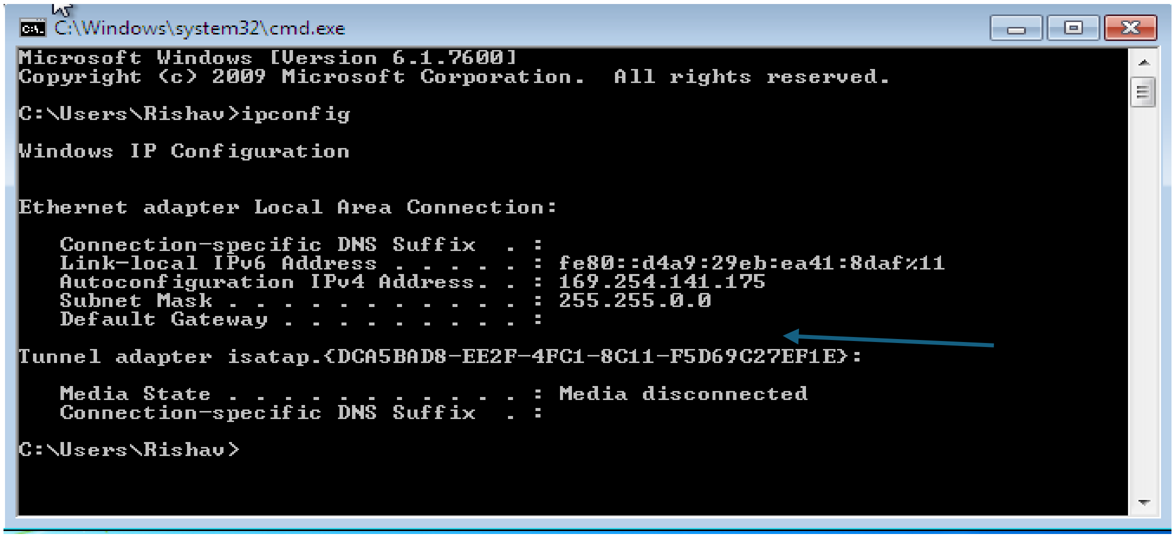
- Click the Terminal icon in Kali Linux.
- Type the ifconfig command in the terminal and click Enter to check the IP address for the Kali Linux machine.



```
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet6 fe80::a00:27ff:fe2b:151e  prefixlen 64  scopeid 0×20<link>
        ether 08:00:27:2b:15:1e  txqueuelen 1000  (Ethernet)
        RX packets 363  bytes 54970 (53.6 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 472  bytes 172287 (168.2 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0×10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 204  bytes 16944 (16.5 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 204  bytes 16944 (16.5 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0


┌──(kali㉿kali)-[~]
└─$ █
```

Figure 3 ifconfig command results for kali Linux machine

Part 4: Type the ipconfig command in the Windows command prompt and click Enter.



```
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\Rishav>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::d4a9:29eb:ea41:8daf%11
   Autoconfiguration IPv4 Address. . : 169.254.141.175
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
   Default Gateway . . . . . . . . . :

Tunnel adapter isatap.{DCA5BAD8-EE2F-4FC1-8C11-F5D69C27EF1E}:

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

C:\Users\Rishav>
```

Figure 4 Red arrows point to the ipconfig command and the IPv4 address.

Part 5: Configuring Kali Linux Network

- Edit the Wired Connection Settings

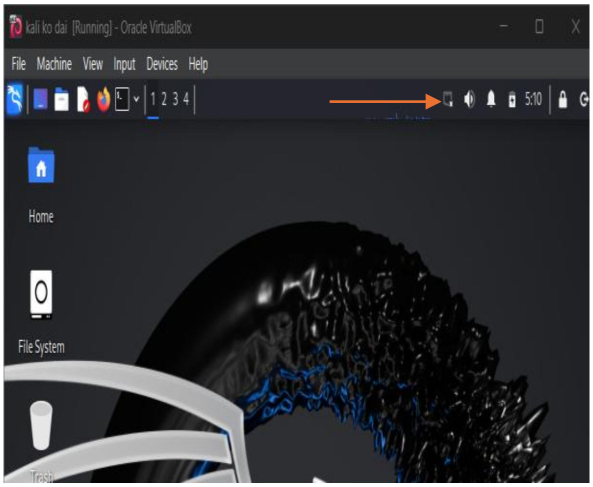


Figure 5 Right-click on the network icon

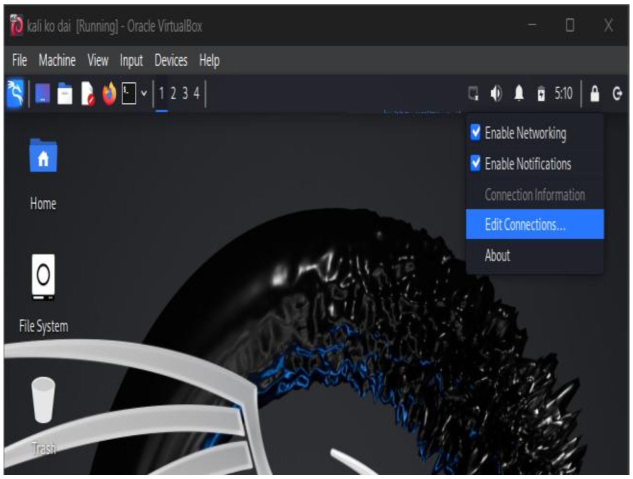


Figure 6 select “Edit Connections.”

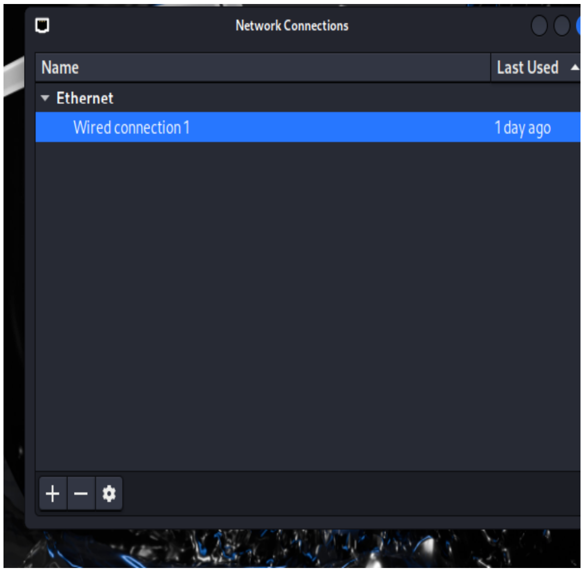
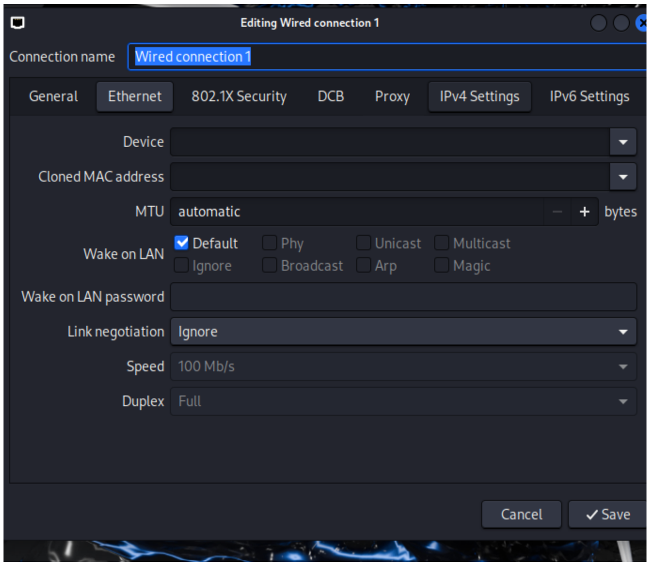


Figure 7 select “Wired Connection 1”


Editing Wired connection 1

Connection name: Wired connection 1

Device

Cloned MAC address

MTU: automatic bytes

Wake on LAN: ☑ Default ☐ Phy ☐ Unicast ☐ Multicast ☐ Ignore ☐ Broadcast ☐ Arp ☐ Magic

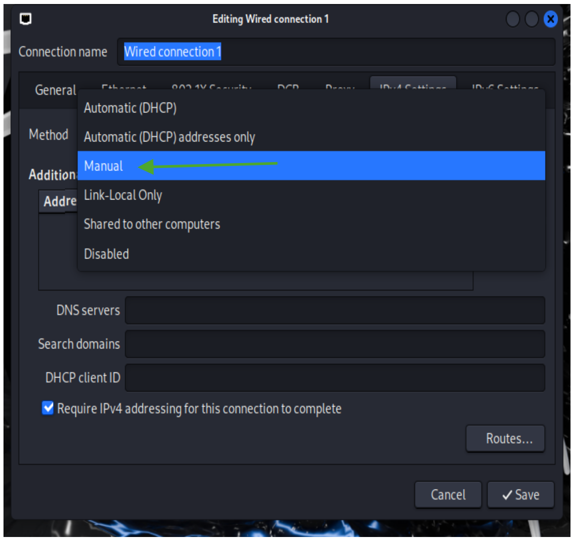
Wake on LAN password

Link negotiation: Ignore

Speed: 100 Mb/s

Duplex: Full

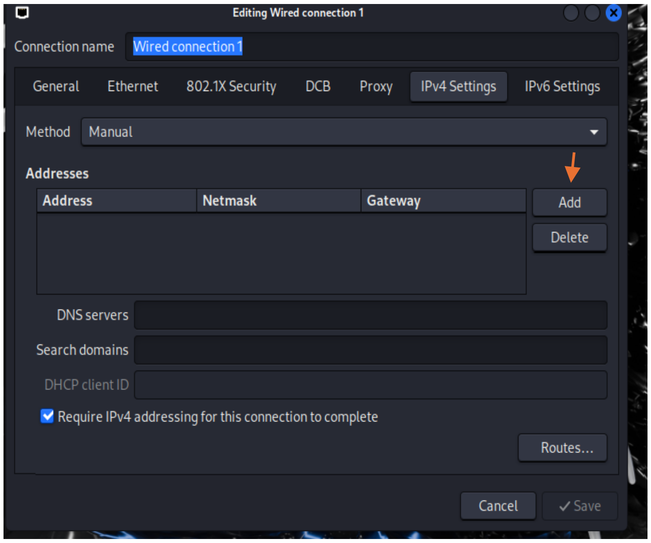
Figure 8 open this interface


Editing Wired connection 1

Connection name: Wired connection 1

☑ Require IPv4 addressing for this connection to complete

Figure 9 change IP Address Configuration to Manual


Editing Wired connection 1

Connection name: Wired connection 1

Method: Manual

Addresses

Address	Netmask	Gateway

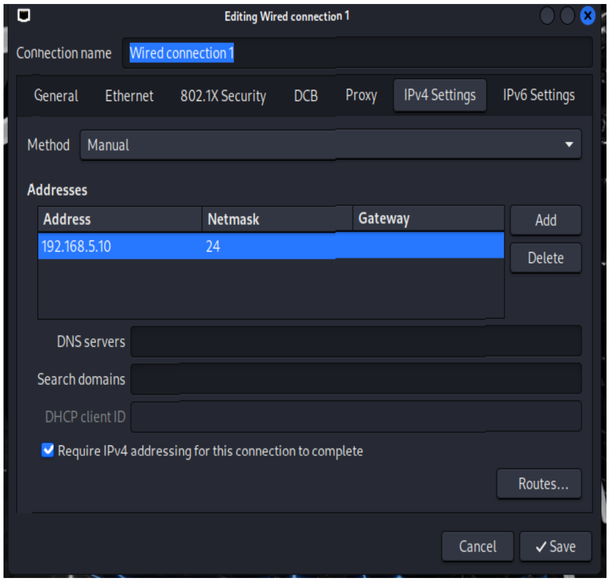
DNS servers

Search domains

DHCP client ID

☑ Require IPv4 addressing for this connection to complete

Figure 10 click on add



Editing Wired connection 1

Connection name: Wired connection 1

Method: Manual

Addresses

Address	Netmask	Gateway
192.168.5.10	24	

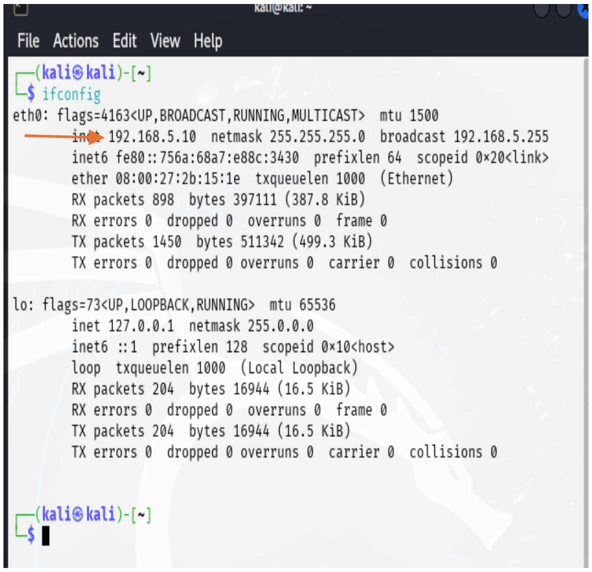
DNS servers

Search domains

DHCP client ID

☑ Require IPv4 addressing for this connection to complete

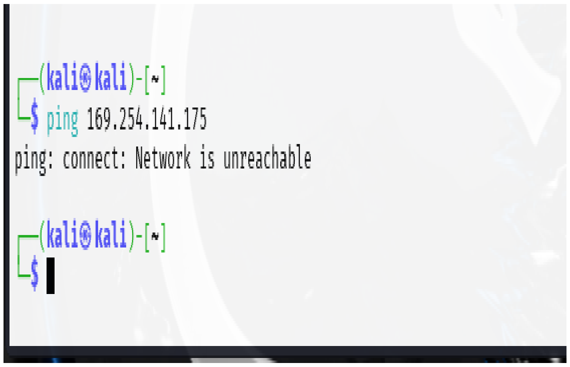
Figure 11 Insert IPv4



```
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.5.10  netmask 255.255.255.0  broadcast 192.168.5.255
        inet6 fe80::756a:68a7:e88c:3430  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:2b:15:1e  txqueuelen 1000  (Ethernet)
        RX packets 898  bytes 397111 (387.8 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1450  bytes 511342 (499.3 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 204  bytes 16944 (16.5 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 204  bytes 16944 (16.5 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0


┌──(kali㉿kali)-[~]
└─$ 
```

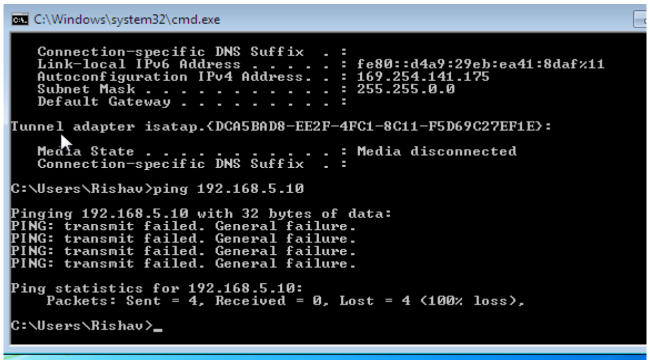
Figure 12 Verifying the IP Address on kali

Part 6: Pinging the Machines



```
┌──(kali㉿kali)-[~]
└─$ ping 169.254.141.175
ping: connect: Network is unreachable

┌──(kali㉿kali)-[~]
└─$ 
```

Figure 13 can't ping 169.254.141.175 on kali



```
   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::d4a9:29eb:ea41:8daf%11
   Autoconfiguration IPv4 Address. . : 169.254.141.175
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
   Default Gateway . . . . . . . . . :

Tunnel adapter isatap.{DCA5BAD8-EE2F-4FC1-8C11-F5D69C27EF1E}:

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

C:\Users\Rishav>ping 192.168.5.10

Pinging 192.168.5.10 with 32 bytes of data:
PING: transmit failed. General failure.
PING: transmit failed. General failure.
PING: transmit failed. General failure.
PING: transmit failed. General failure.

Ping statistics for 192.168.5.10:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\Rishav>_
```

Figure 14 can't ping 192.168.5.10 on window

Part 7: Configuring Windows 10 Network

- ### Access Network Settings

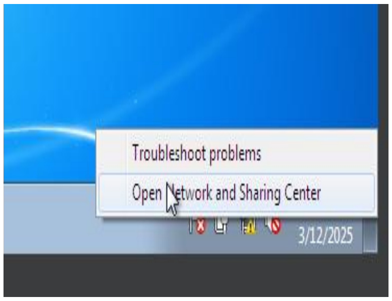


Figure 15 Navigate to "open Network & sharing center"

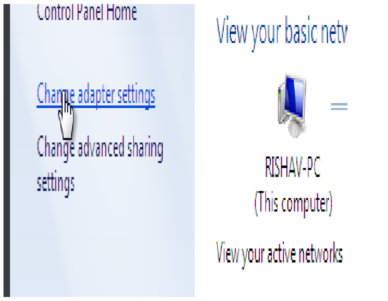


Figure 16 Click on "Change adapter setting"

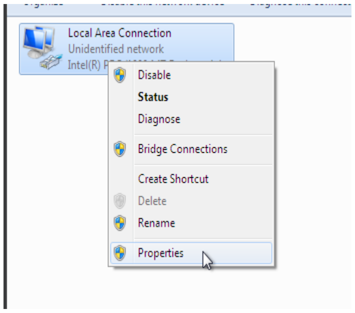
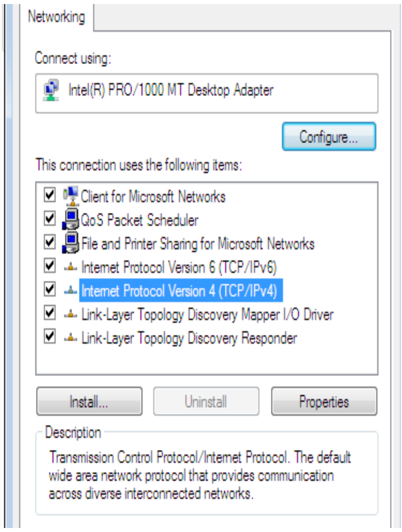


Figure 17 Right-click on it and select "Properties"

- ### Configure IPv4 Settings



Connect using:

Intel(R) PRO/1000 MT Desktop Adapter

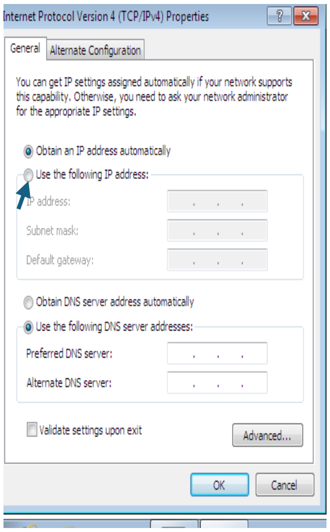
This connection uses the following items:

- ☑ Client for Microsoft Networks
- ☑ QoS Packet Scheduler
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ Internet Protocol Version 6 (TCP/IPv6)
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- ☑ Link-Layer Topology Discovery Mapper I/O Driver
- ☑ Link-Layer Topology Discovery Responder

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

Figure 18 select "Internet Protocol Version 4 (TCP/IPv4)"



You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

- ● Obtain an IP address automatically
- ○ Use the following IP address:

IP address:

Subnet mask:

Default gateway:

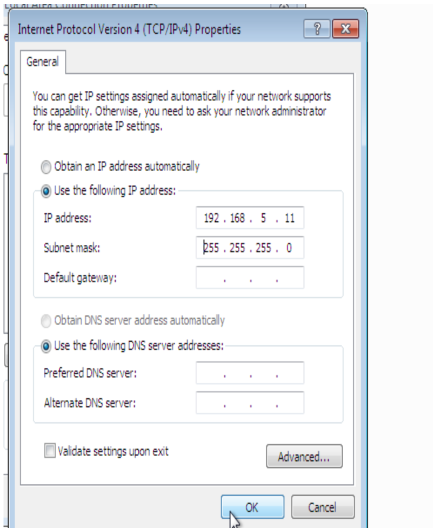
- ○ Obtain DNS server address automatically
- ● Use the following DNS server addresses:

Preferred DNS server:

Alternate DNS server:

□ Validate settings upon exit

Figure 19 Click on Marked option



You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

- ○ Obtain an IP address automatically
- ● Use the following IP address:

IP address: 192 . 168 . 5 . 11

Subnet mask: 255 . 255 . 255 . 0

Default gateway:

- ○ Obtain DNS server address automatically
- ● Use the following DNS server addresses:

Preferred DNS server:

Alternate DNS server:

□ Validate settings upon exit

Figure 20 Assign a Static IP Address

- **Enable Network Discovery and File Sharing**
- **Navigate to the "Network and Sharing Center"**

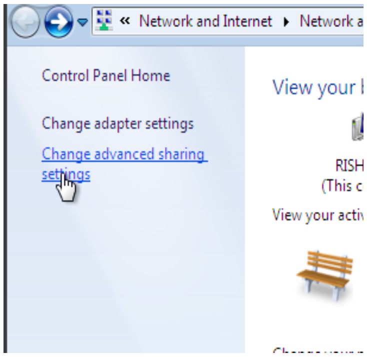
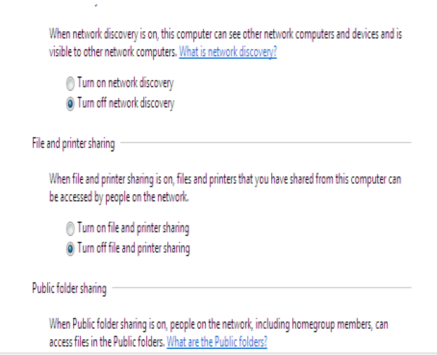


Figure 21click "Change advanced sharing settings."


When network discovery is on, this computer can see other network computers and devices and is visible to other network computers. What is network discovery?

- ○ Turn on network discovery
- ● Turn off network discovery

File and printer sharing

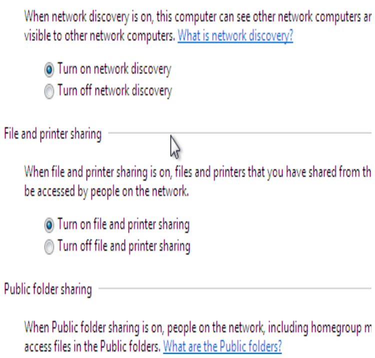
When file and printer sharing is on, files and printers that you have shared from this computer can be accessed by people on the network.

- ○ Turn on file and printer sharing
- ● Turn off file and printer sharing

Public folder sharing

When Public folder sharing is on, people on the network, including homegroup members, can access files in the Public folders. What are the Public folders?

Figure 22 select "Turn on network discovery" and "Turn on file and printer sharing"


When network discovery is on, this computer can see other network computers ar visible to other network computers. What is network discovery?

- ● Turn on network discovery
- ○ Turn off network discovery

File and printer sharing

When file and printer sharing is on, files and printers that you have shared from th be accessed by people on the network.

- ● Turn on file and printer sharing
- ○ Turn off file and printer sharing

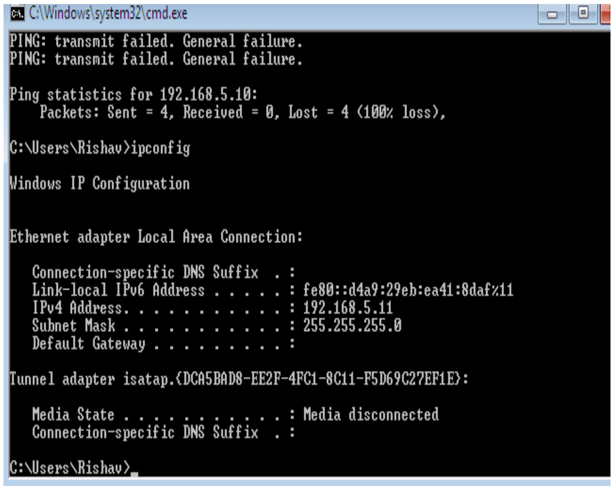
Public folder sharing

When Public folder sharing is on, people on the network, including homegroup m access files in the Public folders. What are the Public folders?

Figure 23 click on save

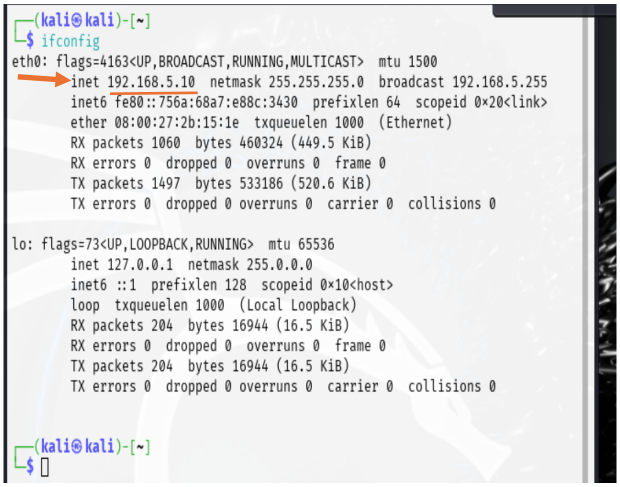
Part 8: Confirm the IP Address

- Use the "ipconfig" command in the Windows command prompt and on kali "ifconfig" to verify that the Windows 7 VM and kali has the assigned static IP address.



```
PING: transmit failed. General failure.
PING: transmit failed. General failure.

Ping statistics for 192.168.5.10:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\Rishav>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::d4a9:29eb:ea41:8daf%11
   IPv4 Address. . . . . . . . . . . : 192.168.5.11
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Tunnel adapter isatap.{DCA5BAD8-EE2F-4FC1-8C11-F5D69C27EF1E}:

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

C:\Users\Rishav>_
```

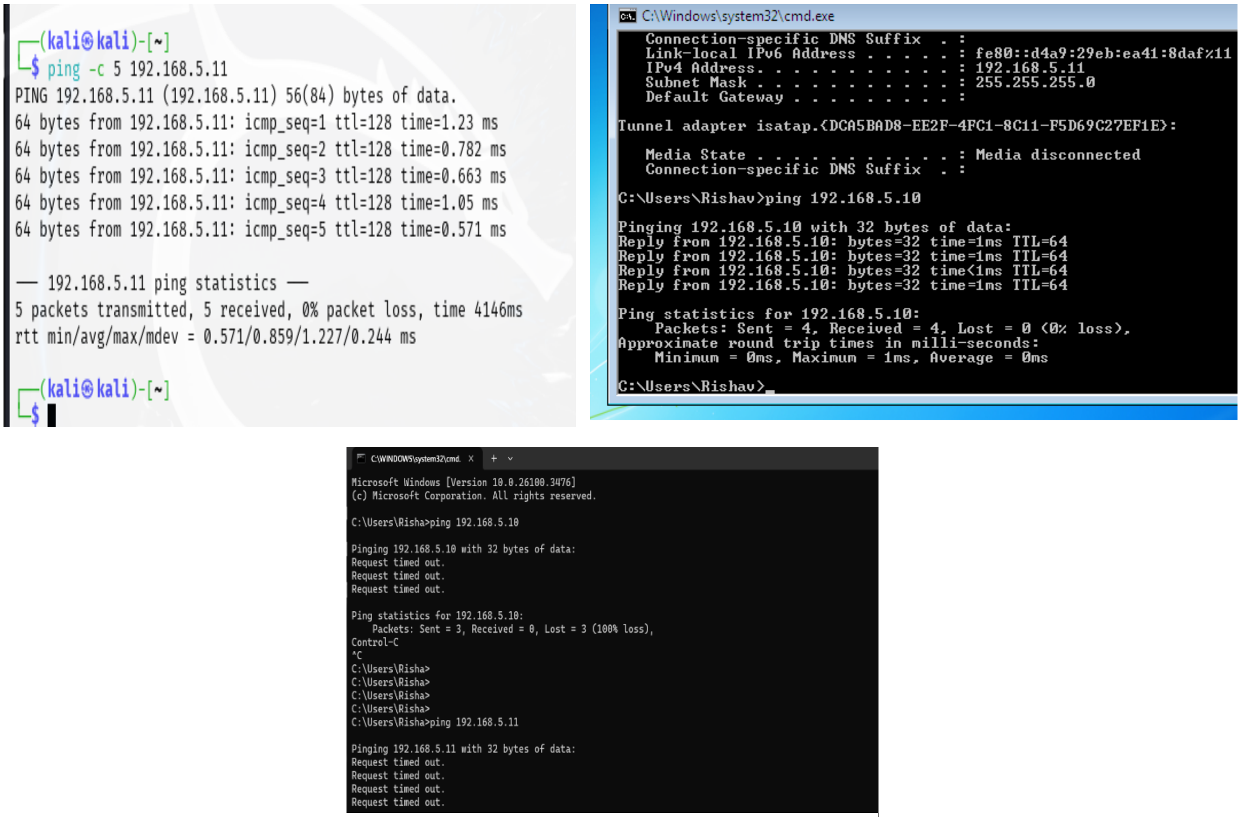
Figure 24 Windows command prompt displaying IP address 192.168.5.11



```
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.5.10  netmask 255.255.255.0  broadcast 192.168.5.255
        inet6 fe80::756a:68a7:e88c:3430  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:2b:15:1e  txqueuelen 1000  (Ethernet)
        RX packets 1060  bytes 460324 (449.5 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1497  bytes 533186 (520.6 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 204  bytes 16944 (16.5 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 204  bytes 16944 (16.5 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0


┌──(kali㉿kali)-[~]
└─$ ▯
```

Figure 25 displays Ip address 192.168.5.10

Part 9: The Final Ping



```
┌──(kali㉿kali)-[~]
└─$ ping -c 5 192.168.5.11
PING 192.168.5.11 (192.168.5.11) 56(84) bytes of data.
64 bytes from 192.168.5.11: icmp_seq=1 ttl=128 time=1.23 ms
64 bytes from 192.168.5.11: icmp_seq=2 ttl=128 time=0.782 ms
64 bytes from 192.168.5.11: icmp_seq=3 ttl=128 time=0.663 ms
64 bytes from 192.168.5.11: icmp_seq=4 ttl=128 time=1.05 ms
64 bytes from 192.168.5.11: icmp_seq=5 ttl=128 time=0.571 ms

— 192.168.5.11 ping statistics —
5 packets transmitted, 5 received, 0% packet loss, time 4146ms
rtt min/avg/max/mdev = 0.571/0.859/1.227/0.244 ms

┌──(kali㉿kali)-[~]
└─$ █
```

```
   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::d4a9:29eb:ea41:8daf%11
   IPv4 Address. . . . . . . . . . . : 192.168.5.11
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Tunnel adapter isatap.{DCA5BAD8-EE2F-4FC1-8C11-F5D69C27EF1E}:

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

C:\Users\Rishav>ping 192.168.5.10

Pinging 192.168.5.10 with 32 bytes of data:
Reply from 192.168.5.10: bytes=32 time=1ms TTL=64
Reply from 192.168.5.10: bytes=32 time=1ms TTL=64
Reply from 192.168.5.10: bytes=32 time<1ms TTL=64
Reply from 192.168.5.10: bytes=32 time=1ms TTL=64

Ping statistics for 192.168.5.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Users\Rishav>_
```

```
Microsoft Windows [Version 10.0.26100.3476]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Risha>ping 192.168.5.10

Pinging 192.168.5.10 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.5.10:
    Packets: Sent = 3, Received = 0, Lost = 3 (100% loss),
Control-C
^C
C:\Users\Risha>
C:\Users\Risha>
C:\Users\Risha>
C:\Users\Risha>
C:\Users\Risha>ping 192.168.5.11

Pinging 192.168.5.11 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
```

Figure 26 Top Left: Kali Linux. Top Right: Windows 10. Bottom: Host machine.

In this lab, the Kali Linux and Windows 7 VMs are configured to use an **Internal Network** in VirtualBox. This type of network is isolated, meaning it only allows communication between the VMs that are part of the same internal network. The **host machine is** not part of this internal network, which is why it cannot ping or communicate with the VMs.

To communicate host machine with the VMs, we can change the network adapter settings in VirtualBox to use **Bridged Networking** or **Host-Only Networking**. However, this would no longer be an isolated network, and the VMs would be accessible from the host machine.

Conclusion

In this lab, we successfully created an isolated network between Kali Linux and Windows 10 VMs using VirtualBox. By configuring the network adapters to use an internal network and assigning static IP addresses, we ensured that the two VMs could communicate with each other without external interference. This setup is ideal for practicing network configuration, penetration testing, and understanding how different operating systems handle network settings.

The final step of pinging both machines confirmed that the network was properly configured, and both VMs could communicate seamlessly. This lab provides a solid foundation for more advanced networking experiments and security testing in a controlled environment.