

2-

```
(kali㉿kali)-[~]
$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=114 time=127 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=114 time=32.0 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=114 time=35.6 ms
^C
--- 8.8.8.8 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2002ms
rtt min/avg/max/mdev = 31.973/64.999/127.390/44.141 ms
```

Ping command sends ICMP packets to a destination to check the connectivity, if responses are received then there is a connection, if not there's not.

The ip address of 8.8.8.8 is the google DNS server, it is used to translate domain names to ip addresses to connect to servers.

The objective of running this command is to check if my machine is connected to the internet.

2.1-

```
(kali㉿kali)-[~]
$ traceroute 8.8.8.8
traceroute to 8.8.8.8 (8.8.8.8), 30 hops max, 60 byte packets
1 192.168.1.254 (192.168.1.254) 4.580 ms 4.524 ms 7.562 ms
2 105.99.128.1 (105.99.128.1) 9.630 ms 9.608 ms 9.585 ms
3 10.104.216.61 (10.104.216.61) 19.713 ms 10.104.216.49 (10.104.216.49) 19.675 ms 10.104.216.61 (10.104.216.61) 19.662 ms
4 * * 172.28.50.14 (172.28.50.14) 19.573 ms
5 142.250.163.34 (142.250.163.34) 41.489 ms 10.16.116.16 (10.16.116.16) 22.487 ms 10.50.150.16 (10.50.150.16) 22.455 ms
6 * 142.250.163.34 (142.250.163.34) 36.292 ms 172.28.50.2 (172.28.50.2) 35.800 ms
7 142.250.163.34 (142.250.163.34) 33.197 ms 142.250.174.126 (142.250.174.126) 35.737 ms 38.338 ms
8 209.85.247.245 (209.85.247.245) 33.097 ms 142.250.163.34 (142.250.163.34) 35.622 ms 192.178.105.171 (192.178.105.171) 33.055 ms
9 dns.google (8.8.8.8) 46.548 ms 52.485 ms 209.85.247.245 (209.85.247.245) 32.935 ms
```

This shows all the hops (routers) that a packet passes through in order to arrive at the destination address (google dns server).

it takes 9 hops.

Each line represents:

- header: destination address, maximum hops count, packet size
- line 1: my home IP router
- line 2: ISP gateway
- line 3-4: isp routers
- line 5-8: internetwork shift
- line 9: destination address

3-

Appropriate command to find the ip address in windows is (ipconfig) and in linux (ifconfig)

linux:

```
(kali㉿kali)-[~]
$ ifconfig
docker0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
      inet 172.17.0.1 netmask 255.255.0.0 broadcast 172.17.255.255
        ether 02:42:7e:dd:ac:34 txqueuelen 0 (Ethernet)
          RX packets 0 bytes 0 (0.0 B)
          RX errors 0 dropped 0 overruns 0 frame 0
          TX packets 0 bytes 0 (0.0 B)
          TX errors 0 dropped 8 overruns 0 carrier 0 collisions 0

eth0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
      ether 00:24:81:4d:fa:86 txqueuelen 1000 (Ethernet)
        RX packets 0 bytes 0 (0.0 B)
        RX errors 0 dropped 0 overruns 0 frame 0
        TX packets 0 bytes 0 (0.0 B)
        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
        device interrupt 17

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 13 bytes 720 (720.0 B)
          RX errors 0 dropped 0 overruns 0 frame 0
          TX packets 13 bytes 720 (720.0 B)
          TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

wlan0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
      inet 192.168.1.50 netmask 255.255.255.0 broadcast 192.168.1.255
      inet6 fe80::2d20:4745:9430:fb49 prefixlen 64 scopeid 0x20<link>
        ether 00:21:6b:ba:47:1e txqueuelen 1000 (Ethernet)
          RX packets 125286 bytes 168372654 (160.5 MiB)
          RX errors 0 dropped 207 overruns 0 frame 0
          TX packets 93959 bytes 10669043 (10.1 MiB)
          TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

ip = 192.168.1.50

windows:

ip = 192.168.1.75

pinging a machine to another:

in linux: ping 192.168.1.75

this doesn't work

in windows: ping 192.168.1.50

this doesn't work

The host can't initiate communication to the VM because NAT mode hides the VM behind the host's IP. They are in two different networks. one in the LAN and the other behind the VirtualBox NAT.

4-

NAT	BRIDGED ADAPTER
The vm is fully isolated from the network and gets an ip from the NAT of the hypervisor. External devices cannot directly reach the VM.	VM gets IP from the host's physical network and appears like a normal host on the network.

The VM is able to ping the host machine and vice versa in BRIDGED mode.

Observations:

- in NAT mode:

The host and VM are on **different logical networks**. The host is in the main network (e.g., `192.168.1.x`), while the VM is on a separate private VirtualBox NAT network (typically `10.0.2.x`).

From the VM's perspective, the host's real IP is not directly routable. The VM's default gateway (e.g., `10.0.2.1`) is the VirtualBox virtual router.

- in BRIDGED mode

Both the host and the VM are on the **same physical/logical network** (e.g., `192.168.1.x`). They receive IP addresses from the same DHCP pool.

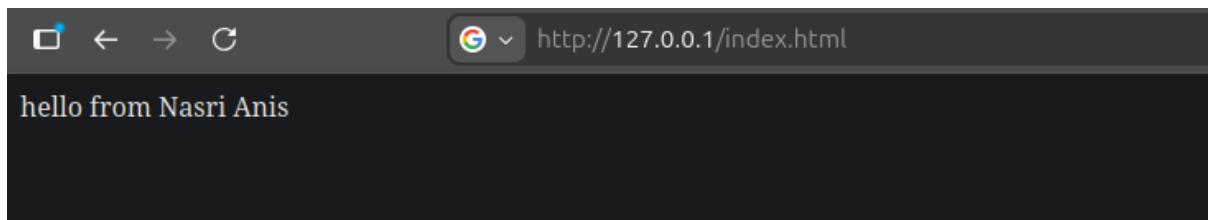
They appear as two hosts on a network

6-

IP address used to access the local web server is the loopback `127.0.0.1`

7-

in windows:



8-

No its not possible

To be able to access it from any device in my network i need to configure XAMPP for network access, configure the firewall to let in traffic through port 80 after open the port 80 for http and set up virtual box in BRIDGED mode.

What should be done:

Step 1: Edit XAMPP configuration

1. Open XAMPP Control Panel
2. Click **Config → Apache (httpd.conf)**
3. Find **Listen 80** and change to **Listen 0.0.0.0:80**

Step 2: Add Firewall Rule

1. Open Windows Defender Firewall
2. "Allow an app through firewall"
3. Find "httpd.exe" (Apache) or add new rule for port 80
4. Allow both Private and Public networks

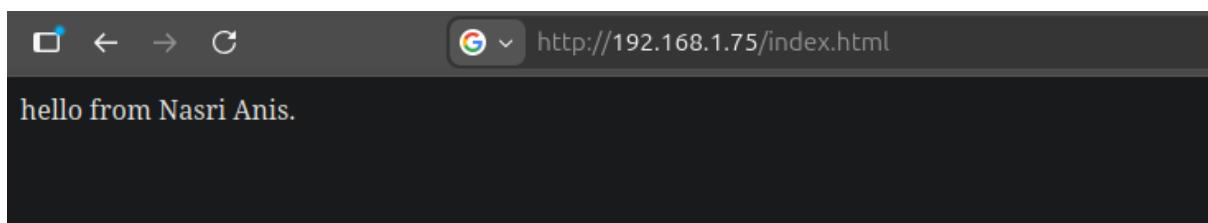
step 3:configuring virtual box with BRIDGED

step 4: connect

go to the web browser in kali and type '<http://192.168.1.75/index.html>'

it works:

in linux:



9-

After performing an nmap -sV scan on windows:

```
Host is up (0.0083s latency).
Not shown: 995 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp     ProFTPD
22/tcp    open  ssh     OpenSSH 10.2p1 Debian 3 (protocol 2.0)
80/tcp    open  http    Apache httpd 2.4.58 ((Unix) OpenSSL/1.1.1w PHP/8.0.30 mod_perl/2.0.12 Perl/v5.34.1)
443/tcp   open  ssl/http Apache httpd 2.4.58 ((Unix) OpenSSL/1.1.1w PHP/8.0.30 mod_perl/2.0.12 Perl/v5.34.1)
3306/tcp  open  mysql   MariaDB (unauthorized)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.09 seconds
```

i found port 80 (http) and 3386 (mysql MariaDB), also port 21 (proFTPD), 22, 443

the version of the web server is Apache httpd 2.4.58 (Unix) OpenSSL/1.1.1w PHP/8.0.30 mod_perl/2.0.12 Perl/v5.34.1)

the database server is mysql MariaDB but its version is unauthorized