🔧 Project Goal

✅ Set up Kali Linux (Attacker) and Ubuntu (Target)
✅ Connect both using **Bridged Network**
✅ Use tools like nmap, ping, and Wireshark for network practice

---

🧱 Prerequisites

- Install **VirtualBox**: Download Here
- Download ISO files:
    - Kali Linux ISO
    - Ubuntu Desktop ISO
- Create two Virtual Machines:
    - **Kali Linux VM**
    - **Ubuntu Linux VM**

🛠️ Step-by-Step Setup (Both VMs)

✅ 1. Set Bridged Network

For **both Kali and Ubuntu**:

1. Open VirtualBox
2. Click on the VM → Settings
3. Go to Network tab
4. **Attached to** → Select Bridged Adapter
5. Under **Name**, choose your active internet adapter (e.g., Wi-Fi or Ethernet)
6. Check **Cable Connected**
7. Click OK

✅ 2. Boot Both VMs

- Start both the **Kali** and **Ubuntu** VMs
- Log in to the desktop

✅ 3. Check IP Addresses

Run this command on **both VMs**:

bash

CopyEdit

```
ip a
```

Look for something like:

yaml

CopyEdit

```
eth0 or enp0s3: 192.168.x.x
```

Make sure:

- **Each VM has a different IP**
- Both are in the **same subnet** (e.g., 192.168.1.100 and 192.168.1.101)

✅ 4. Ping Test (Are they connected?)

From **Kali**, run:

bash

CopyEdit

```
ping <Ubuntu_IP>
```

From **Ubuntu**, run:

bash

CopyEdit

```
ping <Kali_IP>
```

✅ If they both respond, your network is working!

❌ If not, check that both VMs are set to **Bridged Adapter**, and firewall isn't blocking ICMP.

✅ 5. Basic Attacker Tools from Kali

Now you can try simple tools:

🔍 Nmap (Network Scanner)

Scan open ports on Ubuntu:

bash

CopyEdit

```
nmap <Ubuntu_IP>
```

🧪 Netcat (Port listener test)

On Ubuntu:

bash

CopyEdit

```
nc -lvp 1234
```

From Kali:

bash

CopyEdit

```
nc <Ubuntu_IP> 1234
```

Type messages → You'll see a live terminal chat (proof of connection).

🕵️ Wireshark (Packet Capture)

In Kali:

bash

CopyEdit

```
sudo wireshark
```

- Select network interface (e.g., eth0)

- Start capture
- Try ping or nmap again
- Watch live traffic between Kali and Ubuntu

✅ 6. Enable SSH on Ubuntu (Optional)

On Ubuntu:

bash

CopyEdit

```
sudo apt update
sudo apt install openssh-server
sudo systemctl start ssh
```

Check status:

bash

CopyEdit

```
sudo systemctl status ssh
```

Then from Kali:

bash

CopyEdit

```
ssh <Ubuntu_username>@<Ubuntu_IP>
```

🧠 Final Result

You now have:

- A **Kali VM** ready to attack/test tools
- An **Ubuntu VM** acting as a server or target
- Both are on the **same real network** using Bridged Adapter
- You can scan, ping, and test firewall/SSH/etc.