PT 2. VirtualBox Networking Lab (Beginner + Small Advanced Extension)

Simple Network with pfSense & Routing via Metasploitable

Main Objectives:

To help you:

- Configure VirtualBox Internal Network mode.
- Use pfSense as a router for internet access.
- Set dynamic (auto) IPs on Ubuntu and Metasploitable.
- Access the Metasploitable web server from Ubuntu.
- Test connectivity using Ubuntu.

Extension Objective (Advanced Touch)

To introduce basic network routing by:

- Enabling Metasploitable's second adapter in a new network (172.28.0.0/16).
- Connecting it to Kali Linux (on the same new network).
- Configuring Metasploitable to route between networks.
- Testing cross-network pings:
    - Tiny Core → Ubuntu
    - Tiny Core → Pfsense

🔍 This teaches how a multi-homed VM can act as a router between isolated networks.

🖥️ ***Virtual Machines (VMs) List***

pfsense-router	pfSense	1	Main gateway (LAN:192.168.20.1)
metasploitable	Metasploitable 2	2	Web server + Router between networks
ubuntu-client	Ubuntu 22.04	1	Client to browse web server
tinycore-client	Tiny Core Linux	1	Connectivity tester (resides in network 2)

✅ All VMs are pre-installed.

🌐 ***WAN Connection***

WAN network:

Obtained by PFSense via NAT in its first adapter

🌐 ***Network Design (LAN)***

Network 1: LabNet (via Internal Network)

- Name: intnet-LabNet
- Subnet: 192.168.1.0/24
- Purpose: Main lab network with internet via pfSense
- Devices:
    - pfSense (192.168.1.1)
    - Metasploitable (DHCP IP) — Adapter 1
    - Ubuntu (DHCP IP)

Network 2: BackNet (Manual, Isolated)

- Name: intnet-BackNet
- Subnet: 172.28.0.0/16
- Purpose: Private network between Metasploitable and Tiny Core
- Devices:
    - Metasploitable (172.28.0.1/16) — Adapter 2
    - Tiny Core Linux (172.28.0.2/16)

🔁 Metasploitable is dual-homed — it connects both networks.

✅ **Part 1: Basic Lab Setup (LAN)**

Follow the same steps as before.

Step 1: Create Internal Network intnet-LabNet

- Go to File → Host Network Manager → Create
- IPv4: 192.168.1.1, Mask: 255.255.255.0
- The PfSense has Enable DHCP by default
- Name: intnet-LabNet

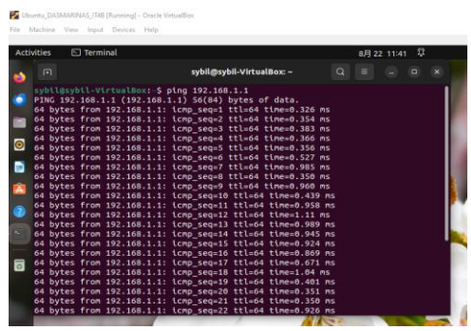
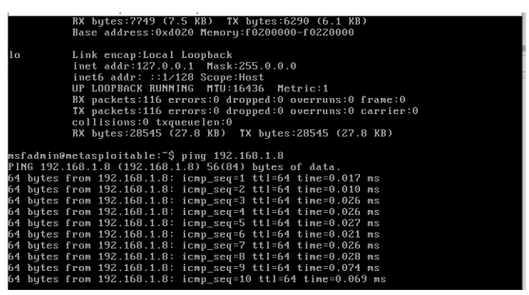
Step 2: Configure VMs (Adapter 1 only for now)

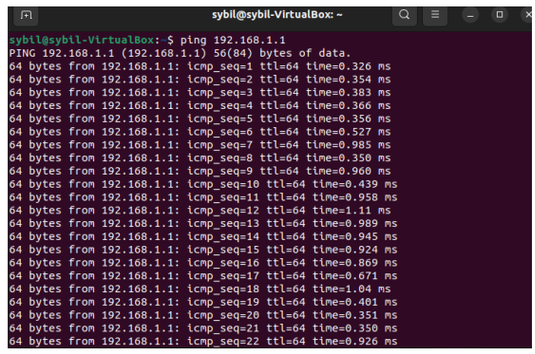
Virtual machine	Network Adapter	IP Address
pfsense-router	Internal:intnet-LabNet	192.168.1.1/24
metasploitable	Internal:intnet-LabNet	DHCP (automatic)
ubuntu-client	Internal:intnet-LabNet	DHCP (automatic)

Set IPs using ifconfig or ip addr commands inside each VM.

Step 3: Test Basic Connectivity

Run these tests:

		Success?
Ping from Ubuntu to pfSense	ping <pfsense address>	 YES
Ping from Ubuntu to Metasploitable	ping <meta address)	 YES
Access web server from Ubuntu	curl http://192.168.20.20 or use Firefox	

		Success?
		
Ubuntu internet access	ping google.com	YES

🎉 If all work — Part 1 is complete!

Part 2: Advanced Extension – Enable Routing via Metasploitable

Now, let's make Metasploitable a router between two networks.

Step 1: Create Second Internal Network

- Go to Host Network Manager → Create another
- Name: intnet-BackNet
- Network address: 172.28.0.0, Mask: 255.255.0.0 (/16)
- ❌ Disable DHCP

Step 2: Configure Adapters

🔹 Metasploitable (Adapter 2)

- Adapter 2:
  - Mode: Internal Network
  - Name: intnet-BackNet
  - IP: 172.28.0.1/16 (set inside VM)

💡 **Use ifconfig eth1 172.28.0.1 netmask 255.255.0.0 up**
(Use ifconfig to check interface name — often eth1)

🔹 TinyCore Linux

- Adapter 1:
  - Mode: Internal Network
  - Name: intnet-BackNet
  - IP: 172.28.0.2/16, Gateway: 172.28.0.1

Inside Tiny Core:

sudo ip addr add 172.28.0.2/16 dev eth0

sudo ip link set eth0 up

sudo ip route add default via 172.28.0.1

or you can set it via GUI!

Step 3: Enable IP Forwarding on Metasploitable

Metasploitable must forward packets between its two network interfaces.

Run this command inside Metasploitable:

Enable routing (IP forwarding)

echo 1 | sudo tee /proc/sys/net/ipv4/ip_forward

Optional: Make it permanent (add to /etc/sysctl.conf later)

✅ This turns Metasploitable into a simple router.

Step 4: Add Routes on Tiny Core (Already Done)

Kali already has:

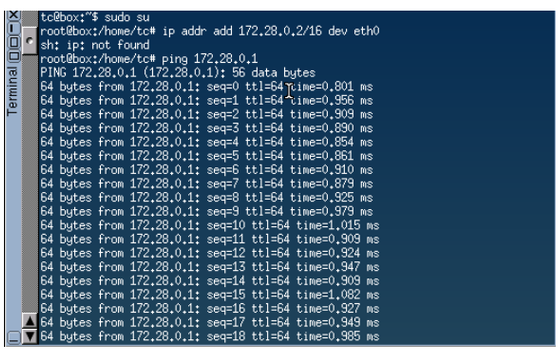
- IP: 172.28.0.2
- Gateway: 172.28.0.1 (Metasploitable)

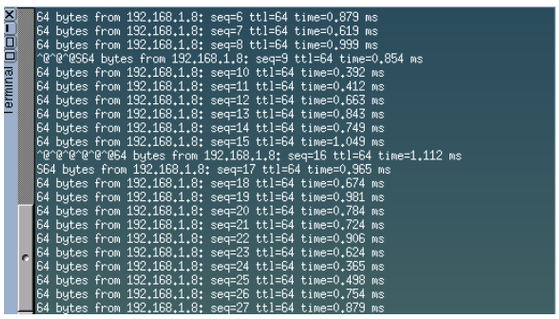
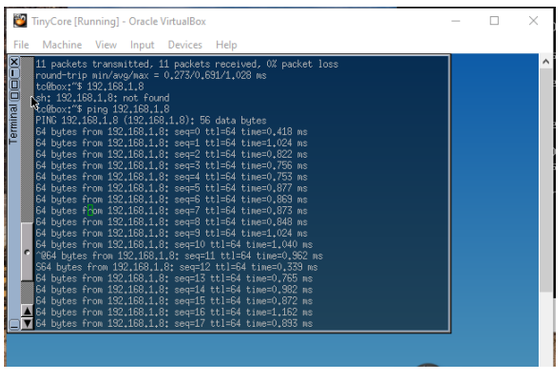
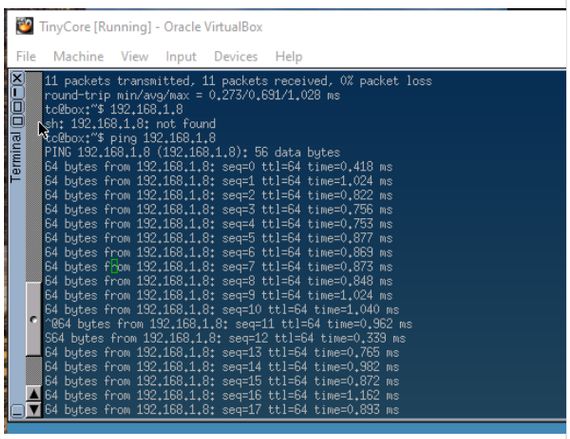
So it can reach the 192.168.20.0/24 network through Metasploitable.

Step 5: Test Cross-Network Connectivity

Now test if Tiny Core can reach machines in the first network.

From Tiny Core Linux terminal:

1. Can Tiny Core ping Metasploitable (172.28.0.1)?	ping 172.28.0.1	

2. Can Tiny Core ping Metasploitable (192.168.20.20)?	ping 192.168.20.20	
3. Can Tiny Core ping Ubuntu?	ping 192.168.20.10	
5. Can Tiny Core access web server?	curl http://192.168.20.20	

🎊 If all succeed — you've built a working router!

Questions (Beginner + Extension)

- Practical & Observation Questions

1. What happens if you don't enable IP forwarding on Metasploitable?
    - Try disabling it: echo 0 > /proc/sys/net/ipv4/ip_forward
    - Then test ping from Kali to Ubuntu. What happens?
        - ➢ Without IP forwarding, Metasploitable cannot pass traffic between networks. This means Tiny Core would only reach Metasploitable's own IP but not Ubuntu or pfSense. The communication stops there.
2. Why do we need a gateway on Tiny Core? What does it do?
    - ➢ The gateway tells Tiny Core where to send traffic that is outside of its own network. Without the gateway set to Metasploitable, it would only talk to

devices inside the 172.28.0.0/16 range and would never reach Ubuntu in 192.168.20.0/24.

3. Can Ubuntu ping Tiny Core (172.28.0.2) without adding a route?
    - Try it: ping 172.28.0.2 from Ubuntu
    - Why does it fail? (Hint: no return route)
        - ➢ No, because Ubuntu does not know about the 172.28.0.0/16 network. Even if Tiny Core sends replies, Ubuntu has no route for the return traffic.
4. How is Internal Network different from Host-Only?
    - ➢ An Internal Network isolates communication to only VMs that belong to it. Host-Only, however, also includes the host computer as part of the network.
5. Why did we use Internal Network instead of Bridged for intnet-BackNet?
    - ➢ Because the BackNet was meant to stay isolated from the outside world. If we used Bridged mode, it would connect to our real physical LAN, which is not safe and not part of the lab design.

🔹 Reasoning & Logic Questions

6. Why can Tiny Core reach Ubuntu, but Ubuntu cannot reach Kali?
    - Explain using routing tables and direction of traffic.
        - ➢ Tiny Core has a proper route to Ubuntu via Metasploitable. But Ubuntu has no knowledge of the 172.28.0.0/16 network. So the request might leave Ubuntu, but the reply never comes back.
7. What would happen if Metasploitable's eth1 (172.28.0.1) was turned off?
    - Could Kali still access the internet?
        - ➢ The BackNet would lose its connection to LabNet. Tiny Core would no longer access Ubuntu or the internet since its gateway would be gone.
8. If you added a second VM on intnet-BackNet, could it also reach Ubuntu?
    - What would its gateway need to be?
        - ➢ Yes, but only if its gateway is also set to Metasploitable (172.28.0.1). That way, it can route traffic across networks.
9. What security risk does enabling IP forwarding on Metasploitable create?
    - Could an attacker use this to move deeper into a network?
        - ➢ It opens the possibility of an attacker using Metasploitable as a pivot point to move from one isolated network into another. In real-life scenarios, this could let a hacker spread deeper inside a secure network.

📝 **Assessment Rubric**

Createdintnet-LabNetand set IPs correctly	10

pfSense, Ubuntu, Tiny Core, Metasploitable can ping each other	15
Ubuntu can accesshttp://192.168.20.20	10
Ubuntu has internet access	10
Createdintnet-BackNetand set Kali IP	10
Enabled IP forwarding on Metasploitable	10
Kali can ping Ubuntu and Tiny Core	15
Answered 5+ questions correctly	20
Total	100

🎉 **Final Words**

✅ You've done two things today:

1. Built a working virtual lab with internet and web access.
2. Turned Metasploitable 2.0 into a router so Tiny Core can ping other VMs!

Network Diagram: