LAB 3

DHCP – NAT – IPTABLES

# Lab Objective

Set up a virtual lab in VMware Workstation with 3 virtual machines:  
  
- Client: Host-Only network only (DHCP client)  
- Kali Linux: Two NICs (Host-Only and NAT), acts as DHCP server, NAT gateway, and firewall  
- Web Server: Host-Only network only

Configure the Kali Linux machine to:  
- Provide DHCP service on Host-Only network  
- Provide Internet access (via NAT interface) for Client and Web Server  
- Apply iptables rules for basic firewall security

A diagram of a firewall

AI-generated content may be incorrect.

Example IP addresses tables.

| **Machine** | **Network Interface** | **IP Address** | **Role** |
| --- | --- | --- | --- |
| Client | Host-Only | DHCP | DHCP Client |
| Kali Linux | Host-Only | 192.168.100.1 | DHCP Server |
| Kali Linux | NAT | DHCP (e.g., 10.0.2.15) | NAT Gateway |
| Web Server | Host-Only | 192.168.100.20 | DHCP Client |

# PART 1. VMware Network Setup

# 1. Create Host-Only Network

1. Open VMware Workstation > Edit > Virtual Network Editor  
2. Click Add Network... and choose VMnet2 (or any available)  
3. Set it to Host-Only  
4. Uncheck Use local DHCP service → we will manually assign DHCP via Kali

# 2. Configure VM Network Interfaces

Kali Linux:  
- NIC 1 (Host-Only): Connected to VMnet2  
- NIC 2 (NAT): Connected to NAT  
  
Client and Web Server:  
- NIC (Host-Only): Connected to VMnet2

# PART 2. Step-by-Step Configuration

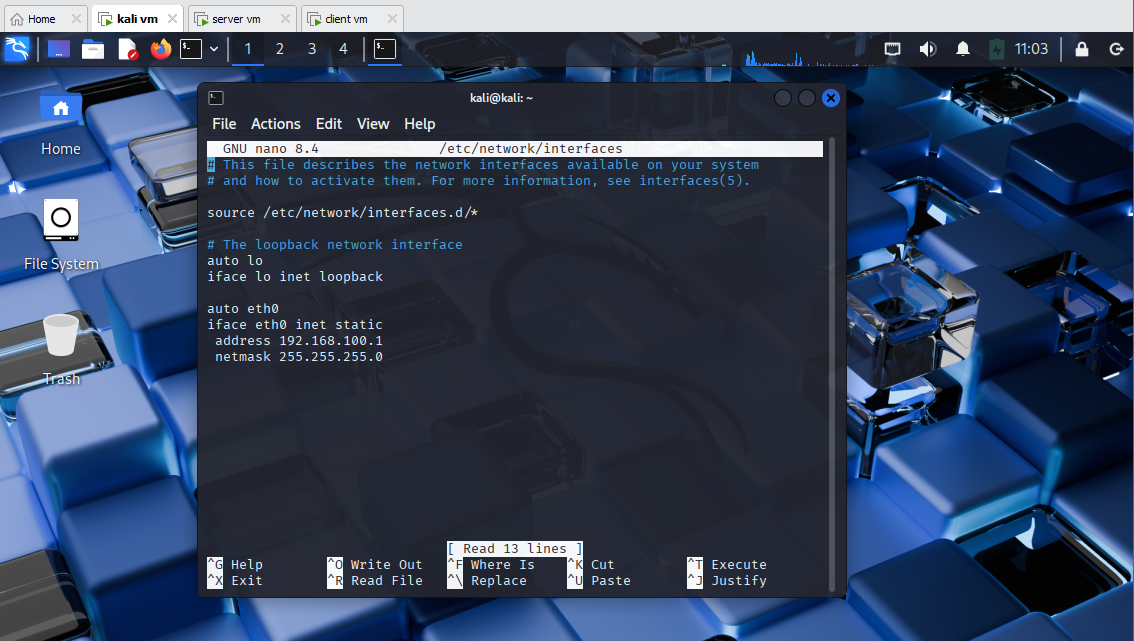
# 2.1 On Kali Linux (Gateway)

# 1. Identify Interfaces

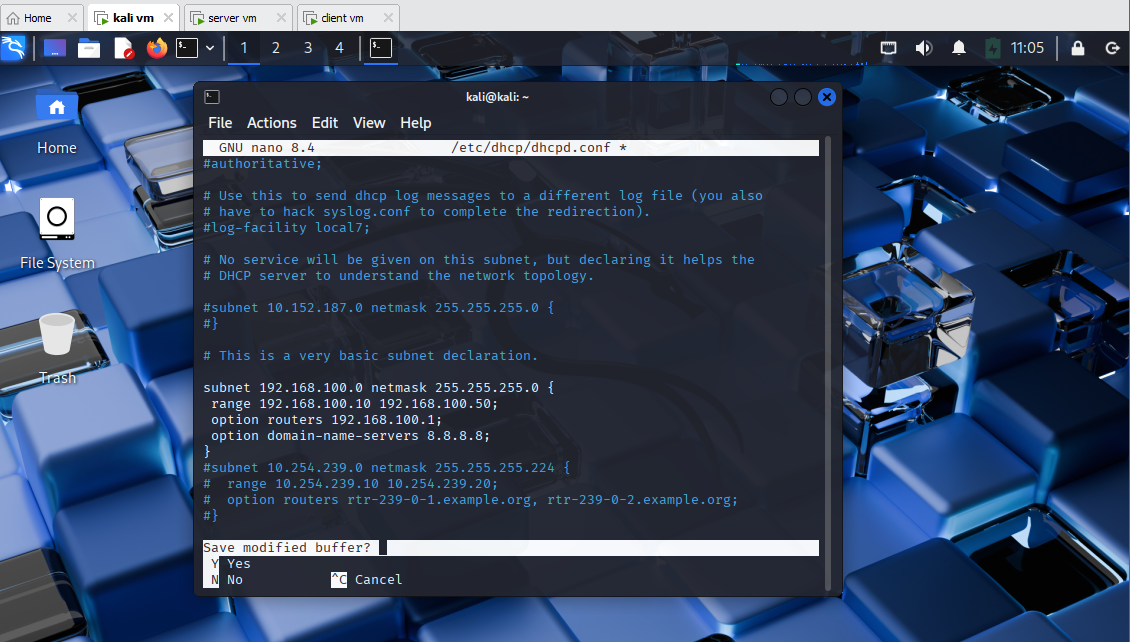
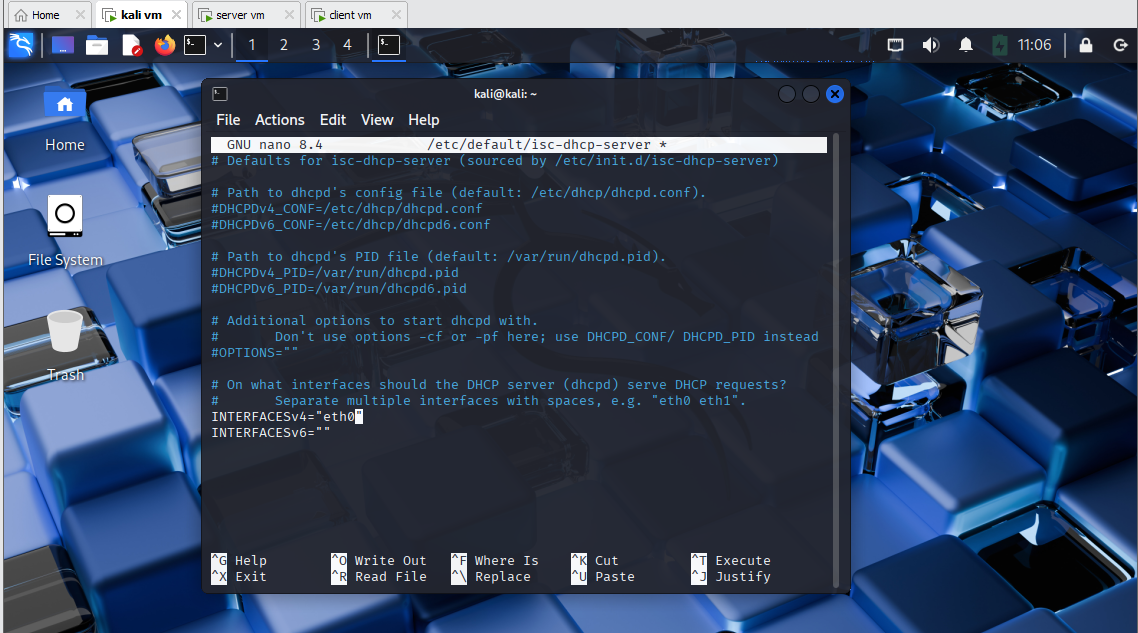
Run:  
  
ip a  
  
Assume:  
- eth0 → Host-Only  
- eth1 → NAT

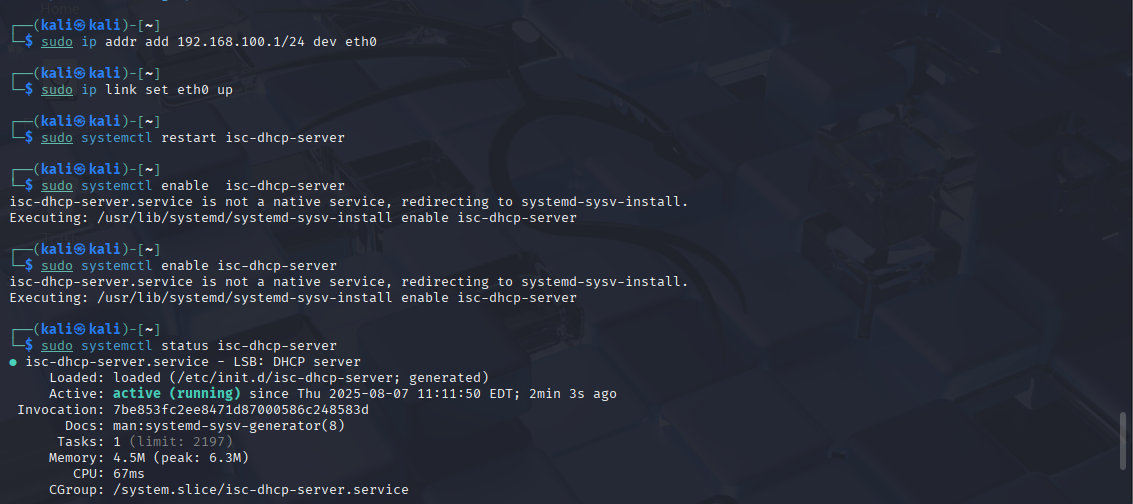
# 2. Set Static IP on Host-Only Interface

Edit interfaces file:  
  
sudo nano /etc/network/interfaces  
  
Add:  
auto eth0  
iface eth0 inet static  
 address 192.168.100.1  
 netmask 255.255.255.0  
  
Restart networking:  
  
sudo systemctl restart networking



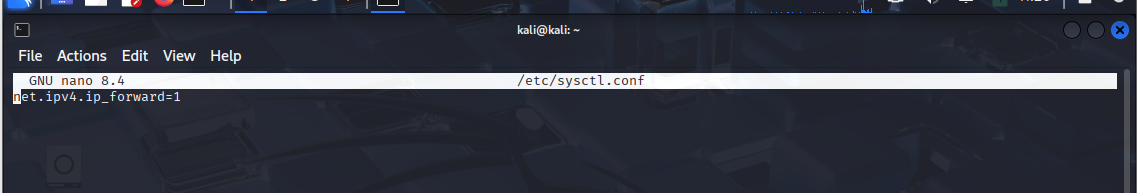
# 3. Install and Configure DHCP Server

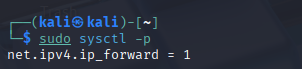
sudo apt update && sudo apt install isc-dhcp-server  
  
Edit config:  
  
sudo nano /etc/dhcp/dhcpd.conf  
  
Add:  
subnet 192.168.100.0 netmask 255.255.255.0 {  
 range 192.168.100.10 192.168.100.50;  
 option routers 192.168.100.1;  
 option domain-name-servers 8.8.8.8;  
}  
  
Set interface for DHCP:  
  
sudo nano /etc/default/isc-dhcp-server  
  
Set:  
INTERFACESv4="eth0"  
  
Restart service:  
sudo systemctl restart isc-dhcp-server  
  
Check status:  
sudo systemctl status isc-dhcp-server



Must assign ip address 192.168.100.1 to interface eth0 before restarting isc-dhcp-server, it is because of if interface eth0 had no ip address, the restart wont work

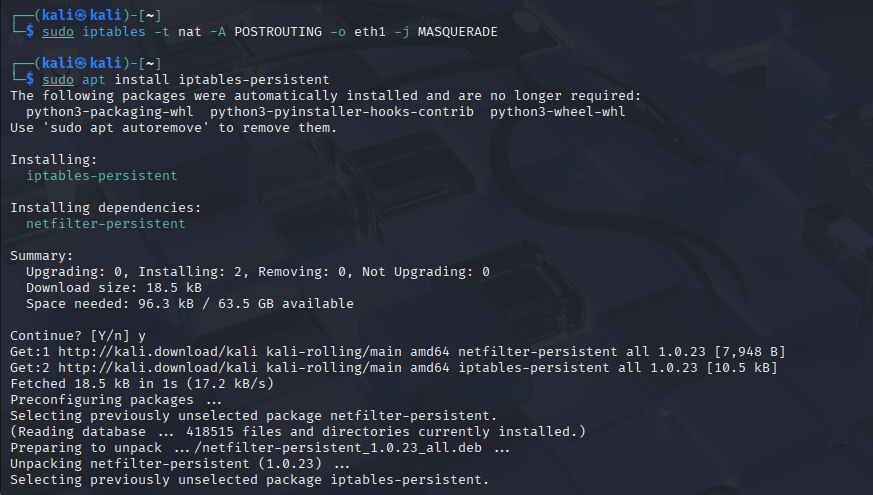
# 4. Enable IP Forwarding

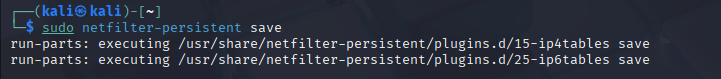
Edit file:  
  
sudo nano /etc/sysctl.conf  
  
Uncomment:  
net.ipv4.ip\_forward=1  
  
Apply:  
sudo sysctl -p



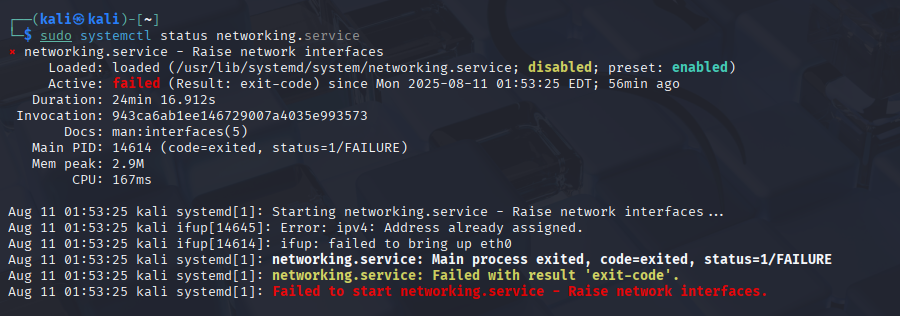
# 5. Set Up NAT with iptables

sudo iptables -t nat -A POSTROUTING -o eth1 -j MASQUERADE  
  
Make NAT rule persistent:  
  
sudo apt install iptables-persistent

  
sudo netfilter-persistent save



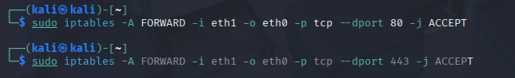
After assigning static address for the gateway, when restarting the networking service, an error should be raised since networking.service and isc-dhcp-server conflicts. So I disabled the networking.service file.



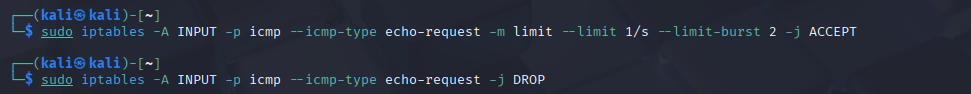
# 6. Basic Firewall Rules

Create Firewall rule and demontrate the result:

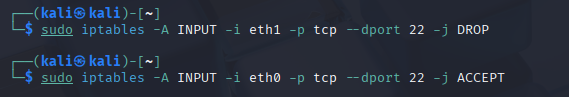
* Only allow the web access from NAT to Host-only

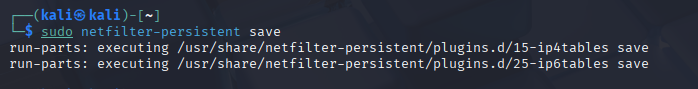


* Prevent the ICMP flood

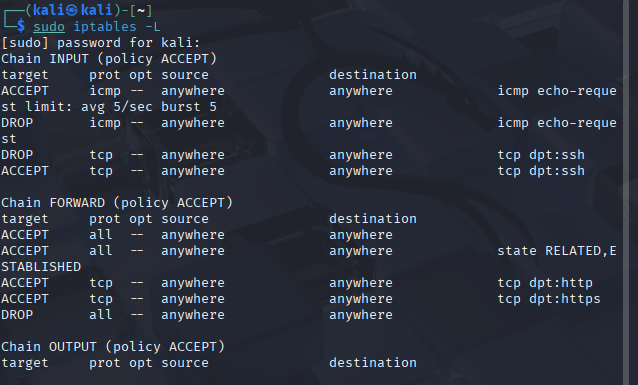


* Prevent the SSH access from the NAT interface



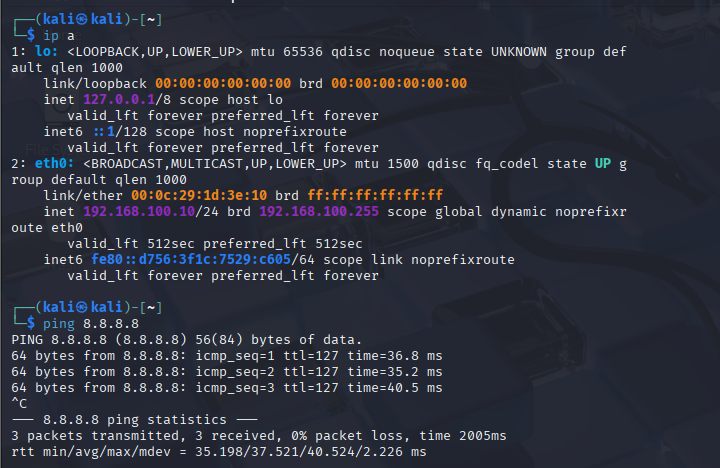
Save the rules: 

Configured rules:



# 2.2 Client Configuration

- Network: Host-Only (VMnet2)  
- DHCP should auto-assign from Kali  
- Check IP: ip a  
- Test Internet: ping 8.8.8.8

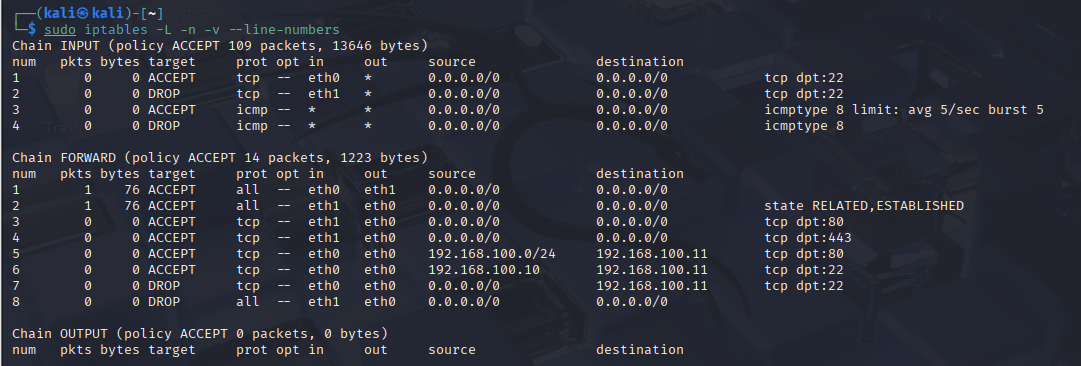


# 2.3 Web Server Configuration

- Same as Client (Host-Only network)  
- Check IP and Internet access  
- Create filewall rule and demontrate the result:

* Allow HTTP traffic (port 80) from the Host-Only network
* Allow SSH access (port 22) only from the client.

-This is how the iptables rules should look like after configuring the rules above:



# PART 3. Advanced part

Setup Iptables so that the client connect to NAT network can access the Web Server (Using port forwarding)

Configure as below:



The first command is to delete the drop all rule, so that the next 2 commands would not conflict with it, after configuring the new rules, add the drop rule back to reject every other connections.