VMware Virtual Network

Lab Setup & Configuration Report

Cybersecurity Home Lab Environment

Prepared by: Mahi

Platform: VMware Workstation Pro

Lab Type: Penetration Testing / Network Segmentation

1. Lab Overview & Objective

This report documents the complete setup process of a segmented virtual network lab using VMware Workstation. The goal of this lab is to simulate a realistic corporate network environment where a Kali Linux attacker machine is placed in an external network, and the internal network consists of a Domain Controller, Application Server, and Employee System. A pivoting machine (Metasploitable 2 / Web Server) sits between both networks, acting as a bridge.

This type of setup is commonly used in penetration testing labs to practice techniques such as network pivoting, lateral movement, and post-exploitation — all in a completely isolated and safe virtual environment.

2. Network Architecture Design

2.1 Topology Diagram Summary

The overall network is divided into two segments as shown in the architecture diagram (Image 11):

- External Network (vLan1) — 192.168.50.0/24: Contains the Kali Linux attacker machine.
- Internal Network (vLan2) — 10.10.10.0/24: Contains the Domain Controller, App Server, and Employee System.
- Web Server (Metasploitable 2): Acts as the pivot point with one interface in each network.

2.2 IP Address Assignment Table

Machine	Network	IP Address	Role
Kali Linux	vLan1 (External)	192.168.50.2	Attacker Machine
Metasploitable 2	vLan1 (External)	192.168.50.3	Web Server / Pivot (eth0)
Metasploitable 2	vLan2 (Internal)	10.10.10.5	Web Server / Pivot (eth1)
Domain Controller	vLan2 (Internal)	10.10.10.2	Windows AD DC
App Server	vLan2 (Internal)	10.10.10.3	Windows Server
Employee System	vLan2 (Internal)	10.10.10.4	Windows 10 Client

3. Step-by-Step Setup Process

Step 1: Creating Virtual Networks in VMware (Virtual Network Editor)

Reference: Image 1 — VMware Virtual Network Editor

The first step was to open the VMware Virtual Network Editor and create two custom virtual networks to segment the lab traffic. The following networks were configured:

Network Name	Type	Subnet Address	Purpose
vLan1	Custom	192.168.50.0	External Network (Attacker Side)
vLan2	Custom	10.10.10.0	Internal Network (Target Side)

Important: Both networks were set to Custom type with DHCP disabled, meaning all IP addresses were assigned manually (statically). This provides full control over the IP configuration of each machine.

Step 2: Configuring the Kali Linux VM Network Adapter

Reference: Image 2 — Kali Linux VM Settings

Kali Linux is the attacker machine and should only have access to the external network. The network adapter was configured as follows:

- Network Adapter: Custom (vLan1)
- Virtual Network: vLan1
- IP Range: 192.168.50.0/24

This ensures Kali Linux can only reach other machines on the vLan1 (External) network — specifically the Web Server's external interface.

Step 3: Configuring the Metasploitable 2 VM (Web Server / Pivot Machine)

Reference: Image 3 — Metasploitable 2 VM Settings

Metasploitable 2 is the most critical machine in this lab because it acts as the bridge between both networks. It was given TWO network adapters:

- Network Adapter 1 (eth0): Connected to vLan1 (External) — 192.168.50.0/24
- Network Adapter 2 (eth1): Connected to vLan2 (Internal) — 10.10.10.0/24

This dual-NIC setup is what makes Metasploitable 2 the pivot machine. Once an attacker compromises this machine, they can use it to reach the internal network which is otherwise inaccessible from Kali Linux directly.

Step 4: Configuring the Windows Machine (Employee System) Network Adapter

Reference: Image 4 — Windows VM Settings

The Windows machine (Employee System) is part of the internal network only. Its network adapter was configured as:

- Network Adapter: Custom (vLan2)
- Virtual Network: vLan2
- IP Range: 10.10.10.0/24

This machine has no direct connection to the external network or Kali Linux, simulating a real internal corporate user system.

Step 5: Setting Static IP on Kali Linux

Reference: Image 5 & Image 6 — Kali Linux IP Configuration

On the Kali Linux machine, the network interface file was edited using the nano text editor to assign a static IP address:

Parameter	Value
Interface	eth0
Address	192.168.50.2
Netmask	255.255.255.0
Gateway	192.168.50.1

File edited: /etc/network/interfaces

After editing, the ifconfig command confirmed the IP was assigned correctly to eth0 as 192.168.50.2 with the correct netmask and no external connectivity beyond vLan1.

Step 6: Setting Static IPs on Metasploitable 2 (Both Interfaces)

Reference: Image 7 & Image 8 — Metasploitable 2 IP Configuration

Metasploitable 2 required two interfaces configured. The /etc/network/interfaces file was edited with the following entries:

Interface	Section	IP Address	Gateway
eth0	#External	192.168.50.3	192.168.50.1
eth1	#Internal	10.10.10.5	10.10.10.1

After saving the file, the networking service was restarted using: /etc/init.d/networking restart

The ifconfig command confirmed both interfaces were active: eth0 at 192.168.50.3 and eth1 at 10.10.10.5, with correct broadcast and subnet mask values on both.

Step 7: Setting Static IP on the Windows Machine (Employee System)

Reference: Image 9 & Image 10 — Windows IP Configuration

The Windows machine's IP was configured through the TCP/IPv4 Properties dialog (Network Settings):

Parameter	Value
IP Address	10.10.10.4
Subnet Mask	255.255.255.0
Default Gateway	10.10.10.1
Preferred DNS Server	10.10.10.2

Note: The DNS Server was set to 10.10.10.2 which points to the Domain Controller. This is because in a real Active Directory environment, the Domain Controller also serves as the DNS server for internal name resolution.

The ipconfig command on the Windows machine confirmed the correct IP assignment of 10.10.10.4 with the expected gateway and subnet mask.

4. Network Connectivity Logic

After completing all configuration steps, the connectivity flow in this lab works as follows:

From	To	Reachable?
Kali Linux (192.168.50.2)	Web Server eth0 (192.168.50.3)	**YES - Same vLan1**
Kali Linux (192.168.50.2)	Internal Network (10.10.10.x)	**NO - Direct access blocked**
Web Server (10.10.10.5)	Internal Network (10.10.10.x)	**YES - Same vLan2**
Employee System	Web Server eth0 (External)	**NO - Different VLAN**
Kali via pivot	Internal Network	**YES - After compromising Web Server**

5. Key Concepts Practiced

- Network Segmentation: Isolating attacker and target machines into different VLANs using VMware custom virtual networks.
- Dual-NIC Configuration: Setting up a pivot machine (Metasploitable 2) with two network interfaces to bridge two isolated networks.
- Static IP Assignment: Manually configuring IP addresses on Linux (via /etc/network/interfaces) and Windows (via TCP/IPv4 Properties) without DHCP.
- Network Pivoting Concept: Understanding how an attacker can reach internal systems only after compromising a machine that has access to both networks.

- DNS Configuration: Pointing Windows client DNS to the Domain Controller at 10.10.10.2 for proper Active Directory integration.
- VMware Virtual Network Editor: Creating and managing custom isolated network segments in VMware Workstation.

6. Conclusion

The lab setup was completed successfully with all three machines (Kali Linux, Metasploitable 2, and Windows Employee System) configured with proper static IPs and connected to the correct virtual network segments. The network architecture mirrors a real-world scenario where an external attacker (Kali) can reach a vulnerable internet-facing server (Metasploitable 2 / Web Server), but cannot directly access internal assets. The only path to the internal network is through pivoting via the compromised Web Server.

This lab serves as an excellent foundation for practicing penetration testing techniques including enumeration, exploitation, post-exploitation, and lateral movement in a completely safe and isolated environment.