Firewall Configuration Documentation

1. Overview

This document outlines the configuration and deployment of a pfSense virtual firewall within a virtual cybersecurity lab. The firewall is used to simulate a real-world enterprise-grade network security environment and manage traffic between the attacker (Kali) and target (Windows) machines.

2. Tools and Resources

- Oracle VM VirtualBox
- pfSense ISO Installer
- Kali Linux VM
- Windows 10 VM

3. pfSense VM Setup

A new virtual machine was created in VirtualBox with the following configuration:
- Name: pfSense
- Type: BSD
- Version: FreeBSD (64-bit)
- RAM: 1–2 GB
- Storage: 10 GB
- Processor: 1 core
- Network Adapters:
  - Adapter 1: Internal Network
  - Adapter 2: NAT

4. Installation Process

The pfSense ISO was mounted to the VM and the default installation steps were followed:
- Auto-partitioned the disk
- Used default kernel and settings
- Rebooted after installation
- Removed the ISO image after installation

5. Network Configuration

During initial boot, pfSense was configured to assign:
- WAN Interface: Adapter 2 (NAT)
- LAN Interface: Adapter 1

The LAN interface was assigned the IP address 192.168.1.1. Kali and Windows machines were configured with static IPs in the same subnet.

6. Kali and Windows Integration

Both Kali and Windows virtual machines were reconfigured to connect via Internal Network. Each machine was manually assigned a static IP and the pfSense LAN IP was set as the gateway. Connectivity was confirmed via ping and browser access to the pfSense web interface.

7. Firewall Rules Configuration

Rules were added in the pfSense Web UI under Firewall > Rules > LAN. The following actions were tested:

- Allowed HTTP and HTTPS traffic
- Blocked specific ports (e.g., FTP, SSH)
- Confirmed traffic restrictions using Kali's terminal and browser

This allowed for controlled access and helped simulate real-world traffic filtering scenarios.

8. Summary

The pfSense firewall was successfully deployed and integrated within the cybersecurity lab. It allowed for comprehensive testing of network isolation, rule creation, and firewall management—key components in securing an enterprise environment.