
🛡️ Cybersecurity Home Lab with pfSense, Kali Linux, and Ubuntu

Simulate, analyze, and defend network attacks with a fully isolated VirtualBox lab environment.

📌 Table of Contents

🎯 Introduction

In this cybersecurity home lab, you will build a practical scenario to simulate a Denial-of-Service (DoS) attack and defend against it using **pfSense** as a firewall, **Kali Linux** as an attacker machine, **Ubuntu** as a victim, and **Wireshark** for packet capture.

This project is a fantastic, portfolio-ready showcase to demonstrate:

✅ Network segmentation
✅ Firewall rule configuration
✅ Attack detection
✅ Mitigation and verification

🎯 Lab Goals

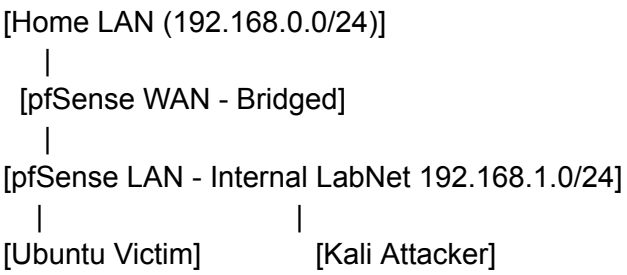
- Understand how network segmentation works
- Practice setting up and configuring pfSense
- Launch a simulated DoS attack
- Monitor traffic with Wireshark
- Block malicious traffic with pfSense
- Verify mitigation using firewall logs

🚀 Benefits

- Realistic, hands-on cybersecurity skills
- Safe and isolated environment
- Open-source and completely free tools
- Portfolio-friendly project
- Repeatable for further experiments

- Demonstrates critical blue-team skills

🗺️ Architecture Diagram



IP Plan

Device	Interface	IP Address	Role
pfSense WAN	vtnet0	192.168.0.x (DHCP)	Connected to home LAN
pfSense LAN	vtnet1	192.168.1.1/24	Gateway for LabNet
Kali Linux	eth0	192.168.0.200 (DHCP)	External attacker
Ubuntu	eth0	192.168.1.100 (DHCP)	Internal victim

⚙️ Requirements

Software:

- VirtualBox 7.x or higher
- pfSense CE 2.7.x ISO
- Kali Linux latest ISO
- Ubuntu 22.04 Desktop ISO
- Wireshark

Hardware:

- Host PC with at least 8GB RAM

- 40GB free disk
- Internet connection
- Admin rights on your host

⚙️ Setup Overview

pfSense

- 2 vCPU, 2GB RAM, 20GB disk
- Adapter 1: Bridged (WAN)
- Adapter 2: Internal Network (`LabNet`)
- LAN: 192.168.1.1/24 with DHCP (192.168.1.100–199)
- WAN: DHCP from your home network
- Add a WAN firewall rule for HTTPS GUI access
- Add a temporary rule to allow Kali access to Ubuntu

Kali Linux

- 2 vCPU, 2GB RAM, 15GB disk
- Adapter 1: Bridged
- Get a DHCP IP, e.g. 192.168.0.200

Add a static route:

sudo ip route add 192.168.1.0/24 via <pfSense-WAN-IP>

- (replace `<pfSense-WAN-IP>` with the actual address)

Ubuntu

- 2 vCPU, 2GB RAM, 15GB disk
- Adapter 1: Internal Network (`LabNet`)
- Receives DHCP from pfSense (e.g. 192.168.1.100)

Confirm Internet access with:

```
ping -c3 google.com
```

-

🛠️ Attack Simulation

On Ubuntu, install and start Wireshark:

```
sudo apt update
sudo apt install -y wireshark
sudo wireshark &
```

1. Capture on `eth0`.

On Kali, launch a flood:

```
sudo hping3 -1 --flood 192.168.1.100
```
or:
```
sudo hping3 --flood -S -p 80 192.168.1.100
```

2. Watch Wireshark for the spike in traffic.

🛡️ Defense & Mitigation

1. In pfSense GUI, create a block rule on WAN:
    - Action: Block
    - Source: Kali IP
    - Destination: Ubuntu IP

    - Enable logging
    - Description: Block Kali DoS
    - Apply and save
2. Check Wireshark — the traffic should stop.
3. Check pfSense logs:
   Status > System Logs > Firewall
   to confirm the block rule is working.

✅ Verifying Results

- Ubuntu still reachable for normal traffic
- Wireshark no longer sees flood packets
- pfSense logs show the blocked traffic
- Lab worked as intended!

🎓 Lessons Learned

- Virtual network segmentation is essential for defense
- pfSense is a powerful, free firewall
- Logging and verification are key
- Safe labs are crucial to practice blue-team skills
- This type of hands-on project builds portfolio credibility

📚 References

- pfSense Documentation (docs.netgate.com)
- Kali Linux Docs (kali.org/docs)
- Wireshark Documentation (wireshark.org/docs)
- VirtualBox Networking Manual (virtualbox.org/manual/ch06.html)
