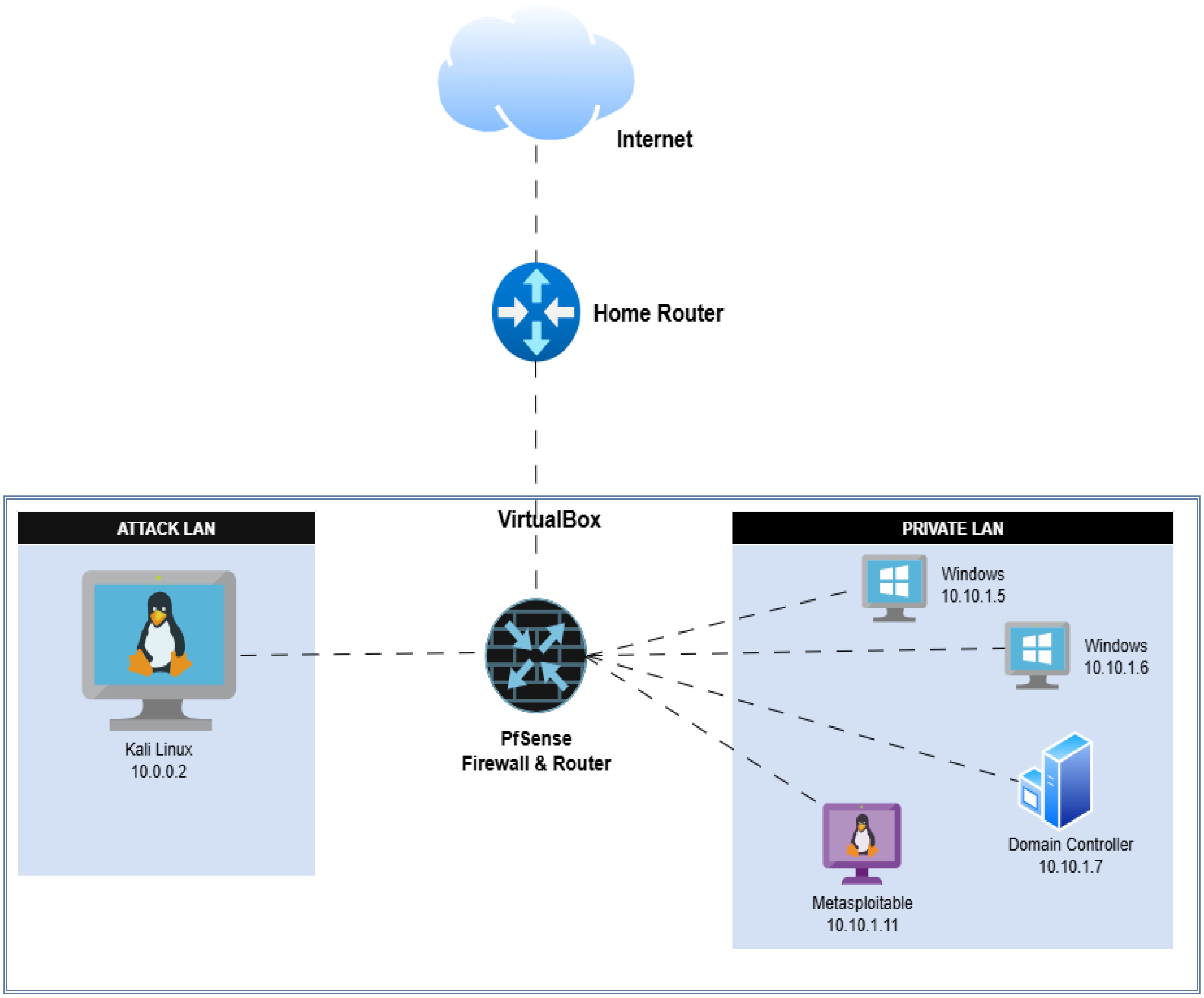
# Setting Up Home Lab Environment

If you are looking to set up a home lab environment and do not know how to start or what tools to configure, this document will guide you to set up a home lab.

Why? → To get hands-on experience on cybersecurity tools, techniques, and scenarios, and simulate real world cyber issues in an isolated and controlled environment. To avoid several risks of the real-world system while learning hands-on.

The network diagram below shows what my virtual environment will look like.

## Network Topology



**Note: The IP addresses  maybe different when setting up your lab but it is important to be mindful on the subnet**

### Overview

This is a **virtualized network topology** running inside **VirtualBox**. It is segmented into two main networks:

1. **Attack LAN**
2. **Private LAN**

The virtual environment is isolated from your physical network by using **PfSense**, which acts as a **firewall and router** between the subnets.

---

### Internet & Home Router

- Your **home router** connects to the **internet**.
- It provides external access and might also offer DHCP to your host machine running VirtualBox.

---

### VirtualBox

This is where all the virtual machines (VMs) live:

- All components (PfSense, Kali, Windows, etc.) are virtual machines inside **VirtualBox**.
- VirtualBox simulates network interfaces and subnets for testing without affecting your real home network.

---

### PfSense Firewall & Router

- **PfSense** is the heart of your virtual network. It:
  - Routes traffic between the **Attack LAN (10.0.0.0/24)** and **Private LAN (10.10.1.0/24)**.
  - Acts as a firewall, potentially controlling what traffic is allowed.
- It connects to both LANs and the home router, via a bridged adapter.

---

### Attack LAN (10.0.0.2/24)

- This is your **offensive security network**.

- Contains a **Kali Linux** machine (10.0.0.2) a powerful tool for penetration testing and ethical hacking.
- The Kali Box targets systems in Private LAN to test vulnerabilities.

---

### Private LAN (10.10.1.0/24)

This is your **target/test environment** where you simulate a production network:

- **Windows Machines (10.10.1.5 & 10.10.1.6)**: Could be workstations or servers.
- **Domain Controller (10.10.1.7)**: Provides Active Directory services, DNS, DHCP — simulates a real enterprise environment.
- **Metasploitable (10.10.1.11)**: A purposely vulnerable machine used for testing exploits safely.

---

### Use Cases

This setup is perfect for:

- Practicing **penetration testing** and **red teaming**
- Learning **network segmentation and firewall configuration**
- Testing exploits, payloads, and **Active Directory attacks**
- Studying **defensive strategies**, like IDS/IPS or hardening