# Home Network Lab Guide

This document provides a beginner-friendly guide to building a home cybersecurity and networking lab. It simulates an enterprise-like environment for practicing networking fundamentals, Blue Team defense, and Red Team penetration testing. The lab is designed with free and open-source tools, aligned with certifications such as CompTIA Network+, Security+, and OSCP.

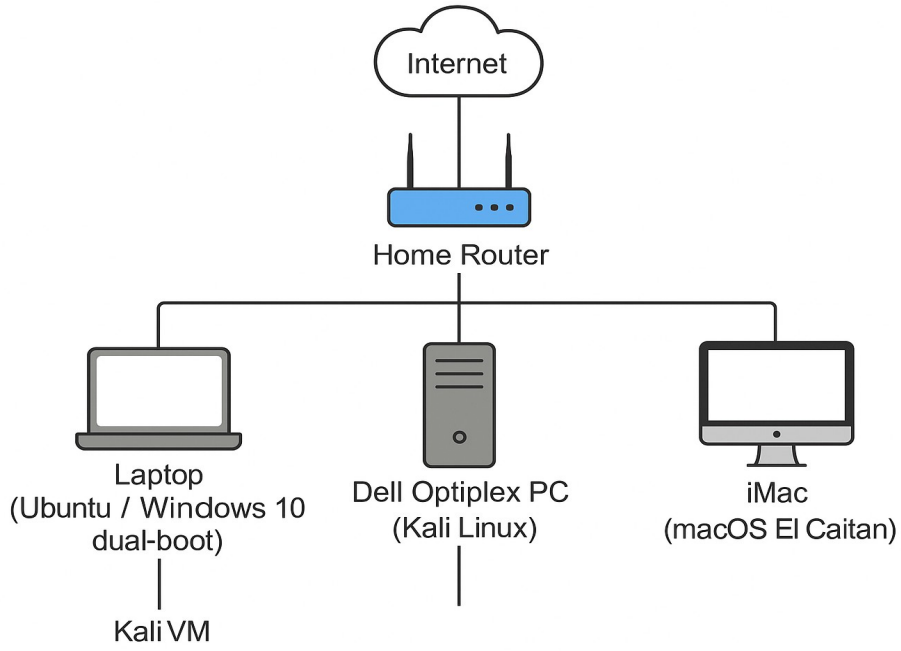
**Hardware & Devices Used:**
- Laptop: Dual-boot Ubuntu + Windows 10, running Kali Linux VM, Windows 10, Metasploitable 2, Ubuntu Server
- Dell Optiplex: Running Kali Linux natively
- iMac: Running macOS El Capitan (10.11)
- Home Wi-Fi router with internet connection

**Software & Tools Used:**
- Virtualization: VirtualBox, VMware Workstation Player (free)
- Networking simulation: GNS3, pfSense, Cisco Packet Tracer (optional)
- Security tools: Kali Linux, Wireshark, Nmap, Metasploit, Burp Suite Community
- Learning platforms: TryHackMe, HackTheBox
- Monitoring tools: ELK Stack, Suricata, Zeek

**Lab Setup Overview:**

**Physical Topology:**
- Laptop, Dell PC, and iMac connected to home router via LAN/Wi-Fi
- Router assigns IP addresses via DHCP
- Devices segmented logically for simulation

**Virtual Topology:**
- Ubuntu/Windows laptop hosts multiple VMs (Kali, pfSense, vulnerable OSes)
- Dell Optiplex acts as attacker or defender node
- iMac acts as a “corporate user” machine for simulation




**What You Will Learn:**
1. Networking fundamentals – IP addressing, routing, switching, NAT, VLANs, firewalls
2. Defensive skills – IDS/IPS setup, monitoring logs, configuring firewalls
3. Offensive skills – Scanning, enumeration, exploitation, privilege escalation, lateral movement
4. Enterprise simulation – Operating online/offline environments with realistic attack/defense workflows
5. Certification prep – Network+, Security+, OSCP

**Pros:**
- Uses mostly free/open-source tools
- Hands-on practice with real attack/defense scenarios
- Prepares for both Blue Team & Red Team paths
- Expandable later with Raspberry Pi, switches, cloud

**Cons:**
- Limited by existing hardware (older iMac, Dell)
- Router may not support advanced enterprise features (consider pfSense)
- Requires time to configure & maintain

**Future Expansion Ideas:**
- Add Raspberry Pi for IoT/edge device testing
- Integrate a managed switch for VLAN practice
- Use cloud platforms (AWS free tier, Azure student credits)
- Add SIEM tools like Splunk or Wazuh for SOC simulation

**30-Day Roadmap:**

**Week 1:** Set up physical devices, install VMs, configure IPs, learn basic Linux & Windows commands
**Week 2:** Configure pfSense firewall & VLANs in GNS3, practice Wireshark and Nmap scanning
**Week 3:** Set up ELK or Wazuh for monitoring, simulate attacks with Kali (Metasploit, Hydra, SQLmap)
**Week 4:** Perform mini penetration tests across the lab, document findings like a professional pentest report