# **Comprehensive Home Lab Setup Documentation**

## **1. Overview**

This home lab is designed for in-depth cybersecurity practice, simulating real-world network environments. It provides a safe, isolated space to improve your skills in penetration testing, vulnerability assessment, network security monitoring, and incident response.

## **2. VMware Setup (Expanded)**

VMware serves as the foundation of your virtual lab environment.

Detailed Setup:

1. Install VMware Workstation/Player on your host computer.
2. Create a new virtual network in VMware: a. Go to Edit > Virtual Network Editor b. Add a new custom VMnet (e.g., VMnet2) c. Set it to "Host-only" for isolation d. Configure the subnet IP.
3. For each VM, allocate resources based on your preferences:
   * Kali Linux: 4GB RAM, 2 CPU cores, 40GB storage
   * Windows XP/7: 2GB RAM, 1 CPU core, 20GB storage
   * Windows 10: 2GB RAM, 2 CPU cores, 20GB storage
   * Metasploitable 2: 1GB RAM, 1 CPU core, 8GB storage
   * Ubuntu: 2GB RAM, 2 CPU cores, 20GB storage
   * Parrot OS: 4GB RAM, 2 CPU cores, 40GB storage

Tip: Adjust these based on your host machine's capabilities.

## **3. Virtual Machines (Expanded)**

### **3.1 Kali Linux**

Purpose: Your main attack platform.

Detailed Setup:

1. Download the latest Kali Linux ISO from the official website.
2. In VMware, create a new VM, selecting "Debian 64-bit" as the guest OS.
3. During installation, choose the "Metapackages" option for a full tool set.
4. Install common tools: Metasploit, Nmap, Wireshark, Burp Suite.
5. Post-installation: a. Update: sudo apt update && sudo apt upgrade -y b. Install additional tools: sudo apt install
6. Advanced Usage:

* Network scanning: nmap -sV 192.168.1.0/24
* Vulnerability exploitation: Use Metasploit to attack other VMs.

### **3.2 Windows XP**

Purpose: An outdated, vulnerable system to practise on.

Detailed Setup:

1. Obtain a Windows XP ISO (ensure you have proper licensing).
2. Create a VM, choosing "Windows XP (32-bit)" as the guest OS.
3. Post-installation: a. Disable Windows Firewall: Control Panel > Windows Firewall > Off b. Disable automatic updates c. Install outdated software (e.g., old versions of Adobe Reader, Java)

Usage:

* Target for exploiting old vulnerabilities.
* Practice privilege escalation techniques.

**3.3 Windows 10 and Windows 7**

Purpose: Represent modern and slightly older Windows environments.

Detailed Setup for Windows 10:

1. Download Windows 10 ISO from Microsoft.
2. Create VM, selecting "Windows 10 (64-bit)" as guest OS.
3. Post-installation: a. Install common software (browsers, Office suite, PDF readers) b. Create multiple user accounts with varying privileges

Windows 7 Setup:

1. Similar to Windows 10, but choose "Windows 7 (64-bit)" as guest OS.
2. Deliberately leave some known vulnerabilities unpatched.

Usage:

* Practice post-exploitation techniques.
* Test Windows-specific malware in a safe environment.
* On Windows 7, install vulnerable services (e.g., outdated Apache, MySQL) for exploitation practice.

### 

### **3.4 Metasploitable 2**

Purpose: Intentionally vulnerable Linux for easy exploitation practice.

Detailed Setup:

1. Download Metasploitable 2 VM image.
2. In VMware, choose "Open a Virtual Machine" and select the downloaded .vmdk file.
3. Configure network adapter to your isolated VMnet.

Usage:

* Practice exploiting each vulnerable service systematically.
* Ideal for beginners to practise basic exploitation.
* Example: Try to gain root access using known vulnerabilities.

### **3.5 Ubuntu**

Purpose: A general-purpose Linux environment.

Detailed Setup:

1. Download Ubuntu Server ISO.
2. Create a new VM, choosing "Ubuntu 64-bit" as guest OS.
3. Post-installation: a. Update: sudo apt update && sudo apt upgrade -y b. Install LAMP stack: sudo apt install apache2 mysql-server php libapache2-mod-php php-mysql c. Install vulnerable web apps: DVWA.

Usage:

* Host vulnerable web applications for testing.
* Practise Linux system administration and hardening.

### **3.6 Parrot OS**

Purpose: Alternative to Kali for penetration testing.

Detailed Setup:

1. Download Parrot Security ISO.
2. Create a new VM, choosing "Debian 64-bit" as guest OS.
3. Post-installation: a. Update: sudo parrot-upgrade b. Explore unique Parrot tools not found in Kali

Usage:

* Use AnonSurf for anonymous browsing practice.
* Similar to Kali, use for penetration testing and ethical hacking.
* Try tools that might not be available in Kali.

## **4. Snort Setup**

Snort is your Intrusion Detection System (IDS).

Detailed Setup:

1. On Ubuntu VM: sudo apt install snort
2. Configure Snort to monitor your virtual network: a. Edit /etc/snort/snort.conf b. Set the HOME\_NET variable to your VMnet subnet c. Customise rules in /etc/snort/rules/local.rules

Advanced Usage:

* Create custom Snort rules to detect specific attacks you're simulating.
* Monitor network traffic: snort -dev -l ./log
* Create custom rules to detect specific attacks you're practising.

## **5. Extended Lab Scenarios**

### **Scenario 1: Full Penetration Test**

1. Use Kali to perform reconnaissance on all lab VMs.
2. Identify and exploit vulnerabilities in Windows and Linux targets.
3. Establish persistence on compromised systems.
4. Go through the network to access segmented systems.
5. Extract sample data from compromised machines.
6. Document findings in a professional penetration test report.

### **Scenario 2: Advanced Web Application Security**

1. Set up multiple vulnerable web apps on Ubuntu (DVWA).
2. Perform a full web application assessment: a. Use Burp Suite for manual testing. b. Employ automated scanners like OWASP ZAP. c. Exploit SQL Injection, XSS, CSRF, and file inclusion vulnerabilities.
3. Attempt to achieve remote code execution through web app vulnerabilities.
4. Practice and re-testing.

### **Scenario 3: Wireless Network Attacks**

1. Add a virtual wireless adapter to a VM.
2. Set up a virtual wireless access point.
3. Practice WiFi hacking techniques: a. WEP/WPA/WPA2 cracking on wireless networks

### **Scenario 4: Incident Response Simulation**

1. Simulate a security incident (e.g. data breach).
2. Practice incident response steps: a. Identification b. Containment c. Eradication d. Recovery e. Lessons Learned
3. Use digital forensics tools to investigate the incident.
4. Create a detailed incident response report.

## **6. Advanced Lab Expansion Ideas**

1. Network Segmentation: Use pfSense as a virtual firewall/router to create multiple network segments.
2. IoT Security: Add virtual IoT devices (can be simulated with lightweight VMs) to practise IoT security concepts.
3. Cloud Security: Integrate cloud services (AWS/Azure free tier) into your lab for cloud security practice.
4. Threat Intelligence: Set up a threat intelligence platform (e.g., MISP) to practice working with threat data.
5. Deception Technology: Implement honeypots (e.g., T-pot) to study attacker behaviour.

## **7. Continuous Learning**

1. Regularly update your lab components to practice with the latest technologies and vulnerabilities.
2. Participate in online CTFs (Capture The Flag) competitions using your lab.
3. Simulate real-world scenarios based on recent cybersecurity incidents reported in the news.
4. Document your learning process, creating your own knowledge base or blog.

Remember,The key to mastery is consistent practice, curiosity, and continuously challenging yourself with new scenarios and technologies. Always adhere to ethical guidelines and legal requirements when practising cybersecurity techniques.