## Detailed Guide for Setting Up a Cybersecurity Lab

**Step 1: Install a Virtualization Platform**

1. **Download and Install VirtualBox**:
   * [VirtualBox](https://www.virtualbox.org/) is free and supports most operating systems.
   * Alternatively, download VMware Workstation Player (VMware) for free.
2. **Enable Virtualization**:
   * Access your computer's BIOS/UEFI settings.
   * Enable **Intel VT-x** or **AMD-V** to support virtualization.
3. **Create a Base Virtual Machine**:
   * Set up a new VM and allocate:
     + **RAM**: 2 GB minimum (4 GB or more for resource-intensive VMs like Kali Linux).
     + **Storage**: 20 GB or more.
   * Attach an ISO file of your desired operating system (Windows/Linux) to install it.

**Step 2: Set Up Virtual Machines**

Let’s configure a basic lab with three types of systems: Attacker, Target, and Server.

**1. Attacker Machine**

* **Kali Linux**:
  + Download the ISO file from Kali Linux.
  + Create a VM, attach the ISO, and follow the installation steps.
  + Tools included:
    - Nmap, Wireshark, Metasploit, Burp Suite, etc.

**2. Target Machine**

* **Metasploitable**:
  + Download from SourceForge.
  + Import the VM file into VirtualBox/VMware.
  + Purpose: Practice exploiting common vulnerabilities.
* **OWASP Juice Shop**:
  + Download and install using Docker or Node.js:

bash

*Copy code*

docker pull bkimminich/juice-shop

docker run -d -p 3000:3000 bkimminich/juice-shop

* + Access the app in your browser via http://localhost:3000.

**3. Server Machine**

* Install **Ubuntu Server**:
  + Download the ISO file from [Ubuntu](https://ubuntu.com/download/server).
  + Configure roles such as web server (Apache, Nginx) or database server (MySQL).
* Install **Windows Server**:
  + Download a free trial from [Microsoft](https://www.microsoft.com/en-us/evalcenter/evaluate-windows-server).
  + Practice Active Directory setup and configuration.

**Step 3: Configure Networking**

* Open the **Network Settings** for each VM in VirtualBox/VMware:
  + Use **Host-Only Networking** to isolate lab traffic.
  + Alternatively, select **NAT** to enable internet access for software updates.

**Example:**

* Assign IP addresses manually to each VM:
  + Attacker (Kali Linux): 192.168.56.101
  + Target (Metasploitable): 192.168.56.102
  + Server: 192.168.56.103

**Step 4: Install Tools**

**On Kali Linux:**

* **Wireshark**:

bash

*Copy code*

sudo apt update && sudo apt install wireshark -y

* **Metasploit**: Pre-installed on Kali. Launch with:

bash

*Copy code*

msfconsole

**On Target/Server Machines:**

* Install vulnerable web applications like DVWA:

bash

*Copy code*

sudo apt update && sudo apt install apache2 php mysql-server -y

wget https://github.com/digininja/DVWA/archive/master.zip

*unzip master.zip*

mv DVWA-master /var/www/html/dvwa

**Step 5: Practice Scenarios**

1. **Network Reconnaissance**:
   * Use Nmap on the Kali VM to scan the Metasploitable VM:

bash

*Copy code*

nmap -sV 192.168.56.102

1. **Exploit Vulnerabilities**:
   * Launch Metasploit on Kali to exploit Metasploitable:

bash

*Copy code*

msfconsole

use exploit/multi/http/tomcat\_mgr\_deploy

set RHOST 192.168.56.102

run

1. **Traffic Analysis**:
   * Start Wireshark on Kali.
   * Capture traffic between VMs and analyze packets.
2. **Web Application Testing**:
   * Use Burp Suite to intercept and modify HTTP requests to Juice Shop or DVWA.

**Step 6: Document Findings**

* Maintain a **lab notebook** to record:
  + Configurations (network settings, IPs, etc.).
  + Tools used and outputs (e.g., screenshots of successful exploits).
  + Lessons learned or areas for improvement.