**Nmap Lab**

**1. Prerequisites**

* **Kali Linux**: A penetration testing distribution with Nmap pre-installed.
* **Metasploitable 2**: A deliberately vulnerable virtual machine for testing.
* **Virtualization Software**: VMware Workstation, VirtualBox, or any other hypervisor.
* **Network Configuration**: Ensure both machines are on the same network (e.g., NAT or Host-Only).

**2. Download and Install Required Software**

1. **Download Kali Linux**:
   * Get the latest Kali Linux ISO from the official website: <https://www.kali.org/>.
   * Install it on a virtual machine using VMware or VirtualBox.
2. **Download Metasploitable 2**:
   * Download Metasploitable 2 from SourceForge: <https://sourceforge.net/projects/metasploitable/>.
   * Extract the files and import the VM into your virtualization software.

**3. Configure the Virtual Machines**

1. **Set Up Kali Linux**:
   * Start the Kali Linux VM.
   * Log in with the default credentials (kali/kali).
   * Update the system:

sudo apt update && sudo apt upgrade -y

1. **Set Up Metasploitable 2**:
   * Start the Metasploitable 2 VM.
   * Log in with the default credentials (msfadmin/msfadmin).
   * Note the IP address of the Metasploitable machine by running:

ifconfig

1. **Network Configuration**:
   * Ensure both VMs are on the same network (e.g., NAT or Host-Only in VirtualBox/VMware).
   * Test connectivity between the two machines by pinging from Kali to Metasploitable:

ping <Metasploitable\_IP>

**4. Introduction to Nmap**

* **What is Nmap?**
  + Nmap is a network scanning tool used to discover hosts and services on a network.
  + It can also identify open ports, operating systems, and running services.
* **Basic Nmap Commands**:
  + Scan a single IP:

nmap <Metasploitable\_IP>

* + Scan for open ports:

nmap -p- <Metasploitable\_IP>

* + Detect the operating system:

nmap -O <Metasploitable\_IP>

* + Aggressive scan (includes OS detection, version detection, script scanning, and traceroute):

nmap -A <Metasploitable\_IP>

**5. Lab Exercise: Scanning Metasploitable 2**

1. **Open a Terminal in Kali Linux**.
2. **Run a Basic Nmap Scan**:
   * Scan the Metasploitable machine to identify open ports:

nmap <Metasploitable\_IP>

* + Observe the results. You should see several open ports (e.g., 21, 22, 80).

1. **Run a Service Version Detection Scan**:
   * Identify the versions of services running on open ports:

nmap -sV <Metasploitable\_IP>

1. **Run an Aggressive Scan**:
   * Perform a comprehensive scan to gather detailed information:

nmap -A <Metasploitable\_IP>

1. **Run a Script Scan**:
   * Use Nmap scripts to detect vulnerabilities:

nmap --script vuln <Metasploitable\_IP>

**6. Analyze the Results**

* Discuss the findings with students:
  + Which ports are open?
  + What services are running?