**Lab Report: Use a Port Scanner to Detect Open Ports**

**Objectives**

* Use **Nmap**, a port scanner and network mapping tool, to detect open ports .

**Background / Scenario**

Nmap is an open-source utility for network discovery and security auditing. It is used to scan hosts and services, identify potential vulnerabilities, and manage security. In this lab, Nmap was used inside the **CSE-LABVM** environment to detect open ports and analyze their security implications .

**Required Resources**

* PC with the **CSE-LABVM** installed in VirtualBox .

**Lab Steps**

**Step 1: Open a terminal window in the CSE-LABVM**

* Launch the VM.
* Open the **Terminal**.

**Step 2: Run Nmap (Basic TCP Scan)**

nmap localhost

* Scans first **1024 TCP ports** .
* Open ports found: **22 (SSH), 23 (Telnet), 631 (IPP)**.

**Step 3: Run a UDP Scan**

Sudo nmap -sU localhost

* Detected UDP services: **123/udp (NTP), 631/udp (IPP), 5353/udp (mDNS/zeroconf)** .

**Step 4: Service and Version Detection**

nmap -sV localhost

* Identifies software versions, e.g., **OpenSSH 8.2p1**, **Linux telnetd**, **IPP (CUPS)** .

**Step 5: Aggressive Scan with Script Detection**

nmap -A localhost

* Captures additional details such as **SSH keys** .

**Lab Questions and Answers**

1. **What TCP ports are open?**  
   → Ports **22 (SSH), 23 (Telnet), 631 (IPP)**
2. **Describe the purpose of the TCP services associated with each port.**
   * **Port 22 (SSH):** Secure remote administration using encrypted communication.
   * **Port 23 (Telnet):** Remote CLI communication but unencrypted (insecure).
   * **Port 631 (IPP):** Printing services using the Internet Printing Protocol.
3. **What UDP ports are open?**  
   → Ports **123 (NTP), 631 (IPP), 5353 (mDNS/zeroconf)**
4. **Describe the purpose of the UDP services associated with each port.**
   * **Port 123 (NTP):** Synchronizes system time.
   * **Port 631 (IPP):** Handles network printing.
   * **Port 5353 (mDNS):** Resolves hostnames in local networks without DNS.
5. **Research the vulnerabilities associated with each of these open ports.**
   * **Port 22 (SSH):** Target for brute-force and credential theft attacks.
   * **Port 23 (Telnet):** Insecure, vulnerable to sniffing and MitM attacks.
   * **Port 631 (IPP):** Vulnerable to DoS, remote code execution.
   * **Port 123 (NTP):** Can be exploited for DDoS amplification.
   * **Port 5353 (mDNS):** Can be abused for information disclosure and DoS if exposed to the internet

**Learning Outcomes**

* Gained hands-on experience with **Nmap** scanning techniques.
* Learned how to identify **open TCP and UDP ports**.
* Understood the **purpose of services** running on common ports.
* Researched **real-world vulnerabilities** linked to exposed services.
* Practiced analyzing **security implications** of scan results.

**Summary**

In this lab, Nmap was used to perform basic TCP scans, UDP scans, version detection, and aggressive scans on the **CSE-LABVM** system. Several ports and services were identified, including SSH, Telnet, IPP, NTP, and mDNS. The exercise demonstrated how attackers could use this information to identify vulnerabilities and plan potential exploits. This highlights the importance of **regular port scanning, vulnerability assessment, and system hardening** in cybersecurity.





