Task 1: Scan Your Local Network for Open Ports

Internship day-1 Task 1

1. Install Nmap from the official website.** - **Explanation**: A candidate should demonstrate familiarity with securely obtaining and installing tools. Nmap, a network scanning tool, is available at `nmap.org`. –

   Steps:

1.1. Visit `https://nmap.org/download.html`.

1.2 . Select the appropriate installer for your OS (e.g., Windows `.exe`, Linux `.rpm` or source, macOS `.dmg`).

1.3 Verify the download's integrity using checksums (e.g., SHA256) provided on the site to ensure it's not tampered.

1.4 Install Nmap following the installer prompts (e.g., `sudo apt install nmap` for Debian-based Linux or run the Windows installer).

1.5 Confirm installation by running `nmap --version` in a terminal or command prompt.

---

2. Find your local IP range (e.g., 192.168.146.0/24).** - **Explanation**: Identifying the local IP range requires understanding network configurations and basic command-line skills. –

   Steps:

   2.1 On Windows, open Command Prompt and run `ipconfig`. Look for the IPv4 address (e.g., 192.168.146.100) and subnet mask (e.g., 255.255.255.0, which indicates a /24 range).

   2.2 On Linux/macOS, open a terminal and run `ifconfig` or `ip addr`. Identify the network interface (e.g., `eth0` or `wlan0`) and note the IP and subnet mask.

   2.3. The range is derived from the IP and subnet mask. For example, an IP of 192.168.146.100 with a 255.255.255.0 mask means the range is 192.168.146.0/24 (256 addresses from 192.168.146.0 to 192.168.146.255).

---

3. Run: nmap -sS 192.168.146.0/24 to perform TCP SYN scan.**

- **Explanation**: The `-sS` flag performs a TCP SYN scan, a stealthy scan that sends SYN packets to detect open ports without completing a full TCP handshake. –

Steps:

   3.1. Open a terminal or command prompt with administrative/root privileges (required for SYN scans).

3.2. Run the command: `nmap -sS 192.168.146.0/24`.

3.3. Wait for the scan to complete, which identifies active hosts and their open TCP ports within the specified range.

---

3. Note down IP addresses and open ports found.** - **Explanation**: Documenting results is a key skill for reporting vulnerabilities in cybersecurity roles. – **Steps**:

4.1. Review Nmap's output, which lists active IP addresses (e.g., 192.168.146.10,

192.168.146.20) and their open ports (e.g., 22, 80, 443).

4.2. Record details manually or use Nmap's output option

4.3. Example output might show: - 192.168.146.10: Ports 22 (SSH), 80 (HTTP) - 192.168.146.20: Port 445 (SMB)

---

5. Optionally analyze packet capture with Wireshark.** - **Explanation**: Wireshark is used to capture and analyze network traffic, providing deeper insight into scan results or services. –

Steps:

5.1. Install Wireshark from `https://www.wireshark.org` (verify checksums for security).

5.2. Open Wireshark, select the active network interface (e.g., `eth0` or Wi-Fi), and start capturing.

5.3. Re-run the Nmap scan or interact with a specific IP/port (e.g., access 192.168.1.10:80 via a browser) to generate traffic.

5.4. Filter packets in Wireshark (e.g., `tcp.port == 80` for HTTP) to analyze communication patterns, headers, or anomalies.

---

6. Research common services running on those ports.** -

Steps:

6.1. Use a port reference (e.g., IANA list or Nmap's service detection) to identify services.

Common examples: - Port 22: SSH (remote access). - Port 80: HTTP (web server). - Port 445: SMB (file sharing, Windows).

6.2. Run `nmap -sV 192.168.146.0/24` for service version detection to get specifics (e.g., Apache 2.4.41 on port 80).

---

7. Identify potential security risks from open ports.** - **Explanation**: Open ports can expose vulnerabilities if services are misconfigured or outdated. –

Steps:

7.1. Analyze each open port and service: - Port 22 (SSH): Risk of brute-force attacks if weak credentials or outdated SSH versions are used. - Port 80 (HTTP): Vulnerable to web-based attacks (e.g., SQL injection) if the server lacks security patches. - Port 445 (SMB): High risk due to exploits like EternalBlue if unpatched (e.g., WannaCry ransomware).

7.2. Check for unnecessary open ports (e.g., SMB on a device that doesn't need file sharing).

7.3. Recommend mitigation: Update software, use strong credentials, or close unused ports via firewall rules.

---

8. Save scan results as a text or HTML file.**

Saving results ensures documentation for reporting or audits. –

Steps:

8.1. Modify the Nmap command to save output: - Text file: `nmap -sS 192.168.146.0/24 -oN /home/kali/Downloads/scan_results.txt` - HTML file: `nmap -sS 192.168.146.0/24 -oX /home/kali/Downloads/scan_results.xml && xsltproc scan_results.xml -o scan_results.html`

8.2. Verify the file contains IPs, ports, and service details.