CyberSecurity Internship with Elevate labs, assignment 1

1. Install nmap from official site (done)
2. Find your local IP range (e.g., 192.168.1.0/24). (
   1. Run “ipconfig” on command line
   2. It will return different ip addresses and subnet mask like
      1. Ethernet adapter Ethernet 3:
      2. Wireless LAN adapter Local Area Connection\* 1:
      3. Wireless LAN adapter Wi-Fi
      4. Unknown adapter ProtonVPN:
   3. All these are the windows IP connection of the device
3. Run: “*nmap -sS 192.168.1.0/24”* to perform TCP SYN scan
   1. TCP SYN scan is a method to check which TCP ports are open without completing a full TCP handshake.
   2. In a normal TCP handshake three messages are sent: *SYN, SYN-ACK, ACK.* To check this only first two messages are sent and third one is ignored.
   3. If the response is SYN-ACK, then the port is open otherwise, RST is sent which means port is closed.
   4. Hence also called half-open scan.
4. Note down IP addresses and open ports found
   1. For *192.168.1.2*

PORT STATE SERVICE

53/tcp open domain

80/tcp open http

139/tcp open netbios-ssn

443/tcp open https

445/tcp open microsoft-ds

* 1. For *192.168.1.4*

PORT STATE SERVICE

9000/tcp open cslistener

* 1. There were many ports with no-response or blocked ports by the firewall
  2. They were in ignored state

1. Research common services running on those ports
   1. Domain : it is DNS service which converts domain name to IP addresses
   2. HTTP : hosts unencrypted websites or applications
   3. NetBios: for legacy windows or printer sharing
   4. HTTPS : secure web traffic
   5. Microsoft-DS : server message block, it is modern replacement of NetBios and is used in windows sharing
   6. Cslistener : it is custom socket listener. Used by apps like node.js
2. Identify potential security risks from open ports.
   1. **Unauthorized Access**

Services like SSH (port 22), RDP (port 3389), or FTP (port 21) can be **brute-forced** if weak credentials are used.

Attackers may gain shell access or control of your system.

* 1. **Vulnerability Exploits**

Open ports may lead to **exploitable services** (e.g., outdated Apache server on port 80).

Exploits like:

Buffer overflows

Remote code execution (RCE)

SQL injection through open web ports

* 1. **Reconnaissance**

Open ports reveal **what services you're running**, their versions, and possible OS fingerprints.

This gives attackers a **blueprint of your system**, helping them plan further attacks.

* 1. **Data Leakage**

Open ports on services like **Databases (MySQL: 3306, MongoDB: 27017)** can expose sensitive data if not properly authenticated.

Some misconfigured ports allow unauthenticated access.

* 1. **Denial of Service (DoS/DDoS)**

Open services can be targeted with **flooding attacks** or malformed packets to exhaust system resources.

Common targets: DNS (53), HTTP (80/443), and SIP (5060).

* 1. **Backdoors or Malware Communication**

Malware often opens ports to receive commands from **Command and Control (C2) servers**.

Open outbound ports can allow **data exfiltration**.

1. Save scan results as a text or HTML file.
   1. Done through *“nmap -sS 192.168.1.0/24 -oN scan\_results.txt”*  command