**Cyber Security Internship - Task 1**

**Local Network Port Scanning with Nmap**

**Objective**

The objective of this task was to discover open ports on devices within my local network to understand network exposure and potential security risks.

**Tools Used**

- **\*\*Nmap\*\***: For port scanning.

- **\*\*Kali Linux\*\***: The operating system used to perform the scan.

**Steps Taken**

1. **\*\*Installed Nmap\*\***: Nmap was pre-installed on the Kali Linux VM.

2. **\*\*Found Local IP Range\*\***: Used the `ip a` command to find my local IP address and determine the network range. My IP was `192.168.1.15`, so the scan target was set to `192.168.1.0/24`.

3. **\*\*Performed TCP SYN Scan\*\***: Executed the following command:

```bash

nmap -sS 192.168.1.0/24

```

4. **\*\*Analyzed Results\*\***: Noted down the IP addresses and open ports found during the scan.

5. **\*\*Researched Services\*\***: Researched the common services associated with the open ports to identify their purpose and potential risks.

**Scan Results Summary**

| **IP Address** | **Open Ports** | **Service Names** | **Purpose & Potential Risks** |

|----------------|------------|---------------|---------------------------|

| `192.168.1.1` | 80, 443, 53 | http, https, domain | **\*\*Router Admin Interface.\*\*** Risk: Weak credentials could allow unauthorized access to network settings. |

| `192.168.1.105`| 22, 9090 | ssh, zeus-admin | **\*\*SSH Access & a Web Service.\*\*** Risk: SSH could be brute-forced. The `zeus-admin` port is unknown and should be investigated. |

| `192.168.1.120`| 445, 5357 | microsoft-ds, wsdapi | **\*\*Windows File Sharing & Web Services.\*\*** Risk: SMB (port 445) can be vulnerable to exploits like EternalBlue if not patched. |

**Identified Security Risks & Mitigation**

- **\*\*Risk 1:\*\*** Open administrative interfaces (port 80/443 on the router). **\*\*Mitigation:\*\*** Use strong, unique passwords and disable remote administration if not needed.

- **\*\*Risk 2:\*\*** Open SSH port (22) on a client device. **\*\*Mitigation:\*\*** Use key-based authentication instead of passwords, or change the SSH port to a non-default one.

- **\*\*Risk 3:\*\*** Unknown service on port 9090. **\*\*Mitigation:\*\*** Identify the application running on this port and ensure it is updated and properly configured. Close ports that are not necessary.

**Conclusion**

This task provided hands-on experience with network reconnaissance using Nmap. Understanding what ports are open is the first step in securing a network, as it reveals the potential attack surface. The key takeaway is the principle of **\*\*"Least Privilege"\*\*** for network services: only keep essential ports open.