Task 9: Network Vulnerability Scanning

Objective

To perform network vulnerability scanning on a local network using **Nmap**, identify open ports, detect running services, identify the operating system, analyze possible risks, and document the findings.

Tool Used

- **Nmap**

Target Details

- **Target IP Address:** `10.197.12.102`
- **Device Ownership:** Self-owned(used for learning purpose)
- **Network Type:** Local Wi-Fi Network
- **OS** : Android 9 rooted device

Scan Local Network

The target IP is scanned to check whether the host is up or not in a specific host id.

```
$ nmap -sn 10.197.12.0/24
```

The Kali NetHunter device (`10.197.12.102`) was found active on the network.

Identify Open Ports

```
$ nmap 10.197.12.102
```

- 996 TCP ports were closed
- Some ports were found open

Identify Operating System

```
$ nmap -O 10.197.12.102
```

OS Detection Result

- **Operating System:** Android 9 – 10
- **Kernel:** Linux 4.9 – 4.14
- **Device Type:** Mobile Phone (Kali NetHunter)

Analyze Vulnerabilities

```
$ nmap --script vuln 10.197.12.102
```

Vulnerability Scan Result

- No CSRF vulnerabilities detected
- No DOM-based XSS detected
- No Stored XSS detected
- Some scripts failed due to access restrictions

No critical vulnerabilities were found.

Save Scan Results

```
$ nmap -sV -O --script vuln 10.197.12.102 -oN network_scan.txt
```

~ Scan results were successfully saved in `network_scan.txt`.

Risk Analysis :

Finding	Risk Level
Open web services	Medium
Non-standard open ports	Medium
No critical vulnerabilities	Low

Overall Risk Level: Medium

Mitigation Suggestions

- Disable unused services
- Restrict access to web interfaces
- Apply firewall rules
- Keep Kali NetHunter and Android OS updated
- Use strong authentication methods

Conclusion

The network scan of the **Kali NetHunter device** identified several open ports and services. Although no critical vulnerabilities were detected, exposed services may increase the attack surface. Proper security measures are recommended to improve device security.

***NOTE* :**

This scan was conducted on a **self-owned Kali NetHunter Android device** of mine, on a local network for educational purposes as part of a cybersecurity internship. No exploitation was performed.