**README.md for Task 2 – Nmap Network Scan**

# Task 2: Nmap Network Scanning and Security Risk Analysis

## Objective

To perform a TCP SYN scan using \*\*Nmap\*\* on a local Wi-Fi network, identify active hosts, enumerate open ports, research services, and assess potential security risks.

##Tools & Environment

- \*\*Operating System:\*\* Windows 10

- \*\*Tool Used:\*\* Nmap 7.97

- \*\*Interface:\*\* Windows Command Prompt (CMD)

##Steps Followed

1. \*\*Installed Nmap\*\* from [https://nmap.org](https://nmap.org).

2. \*\*Identified IP range\*\* using `ipconfig`:

- Local IP: `192.168.29.7`

- Subnet Mask: `255.255.255.0`

- Scan Range: `192.168.29.0/24`

3. \*\*Ran TCP SYN Scan\*\*:

```bash

nmap -sS 192.168.29.0/24

1. **Analyzed scan results**:
   * 5 devices found active.
   * Ports like 53, 80, 135, 445, 8080, 16992 were open.
2. **Attempted to save results**:  
   Faced an error while saving:
3. Failed to open normal output file: The system cannot find the path specified.

Resolved by creating the folder manually and using:

nmap -sS 192.168.29.0/24 -oN "C:\nmap\_results\nmap\_scan.txt"

**Key Devices & Open Ports**

| **IP Address** | **Open Ports** | **Services** |
| --- | --- | --- |
| 192.168.29.1 | 53, 80, 443, 7443 | DNS, HTTP, HTTPS, Oracle HTTPS |
| 192.168.29.118 | 2869, 9080 | ICSLAP, GLRPC |
| 192.168.29.168 | 135, 139, 445 | RPC, NetBIOS, SMB |
| 192.168.29.7 | 135, 139, 445, 7070 | RPC, SMB, RealServer, AMT |

**Security Risks Identified**

* **Port 445/139** – SMB vulnerability; exploited by ransomware (e.g., WannaCry).
* **Port 135** – RPC used for remote commands; can be abused for enumeration.
* **Port 16992** – Intel AMT remote access; risky if not secured.
* **Port 1900** – UPnP; often abused in DDoS attacks.
* **Port 80/8080** – HTTP traffic without encryption; vulnerable to sniffing or injection.

**Challenges Faced**

* ❌ "Path not specified" error while saving scan output.
* ❌ Initial scan showed 0 hosts up (due to timing or device states).
* 🧠 Full execution done via command-line without GUI tools.
* Required guidance to interpret scan output and services.

**Learning Outcomes**

* Gained hands-on experience with real-world network scanning tools.
* Understood IP ranges and subnet structures.
* Learned how to recognize security-sensitive ports and their associated services.
* Gained troubleshooting skills with file saving and terminal errors.