**Nmap Network Scan Report**

**Tool Used:** Nmap  
**Platform:** Windows 10 (Command Prompt)

**1. Objective**

To perform a basic Nmap TCP SYN scan on the local network and analyze open ports, services, and potential security vulnerabilities.

**2. Steps Followed**

**Step 1: Installed Nmap**

* Downloaded from the official site: [https://nmap.org](https://nmap.org/)
* Installed on Windows 10 successfully.

**Step 2: Found Local IP Range**

* Ran ipconfig in Command Prompt.
* IPv4 Address found: 192.168.29.7
* Subnet Mask: 255.255.255.0 → Network range: 192.168.29.0/24

**Step 3: Ran TCP SYN Scan**

Command used:

nmap -sS 192.168.29.0/24

**Step 4: Noted Down Hosts and Open Ports**

**Host: 192.168.29.1**

* Open Ports: 53, 80, 443, 1900, 7443, 8080, 8443

**Host: 192.168.29.20**

* No open ports

**Host: 192.168.29.118**

* Open Ports: 2869, 9080

**Host: 192.168.29.168**

* Open Ports: 135, 139, 445

**Host: 192.168.29.7 (Self)**

* Open Ports: 135, 139, 445, 7070, 16992

**Step 5: Optional Wireshark Analysis**

* Skipped in this task. (Wireshark not used.)

**Step 6: Researched Common Services**

* Port 80/8080: HTTP (Unsecured web services)
* Port 443/8443: HTTPS (Secured web services)
* Port 135/139/445: Windows file sharing / RPC
* Port 1900: UPnP (device discovery)
* Port 16992: Intel AMT (remote admin)

**Step 7: Identified Security Risks**

* Ports 135/139/445 are vulnerable to malware like EternalBlue.
* Port 16992 (Intel AMT) is a serious vulnerability if not disabled.
* Port 1900 (UPnP) may expose router to DDoS amplification attacks.
* HTTP services on 80/8080 could be misconfigured and publicly exposed.

**Step 8: Saved Scan Result**

Faced errors while saving to Desktop due to path issues. Resolved by:

* Creating folder C:\nmap\_results
* Saving output using:

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

**3. Difficulties Faced**

* **Command not saving output**: Initial attempts to save the scan output using %USERPROFILE%\Desktop failed with "path not specified" error.
* **Scan returned no hosts up**: First scan result showed "0 hosts up" due to using wrong network range or lack of devices connected at that time.
* **Confusion about how to start and structure the task**: Needed help with converting the raw output into useful security analysis.
* **Command Prompt-only approach**: All actions were performed in Windows CMD with no GUI tools, which limited visualization.

**4. Conclusions & Learnings**

* Successfully performed a network scan using Nmap.
* Learned to identify open ports and understand what services typically run on them.
* Learned how to interpret Nmap output and extract security risks.
* Understood common vulnerabilities (e.g., SMB, UPnP, Intel AMT).
* Faced real-world troubleshooting: command errors, saving files, path permissions.

**5. Recommendations**

* Disable unnecessary services such as UPnP, SMB, or Intel AMT if not in use.
* Keep all firmware and OS up to date to patch known port vulnerabilities.
* Use firewalls to block unused ports.
* Consider using tools like Wireshark or Nessus for deeper analysis.

6. **References**

* <https://nmap.org/download.html#windows>
* <https://www.freecodecamp.org/news/what-is-nmap-and-how-to-use-it-a-tutorial-for-the-greatest-scanning-tool-of-all-time/>
* <https://en.wikipedia.org/wiki/Nmap>
* <https://nmap.org/book/intro.html>
* <https://www.geeksforgeeks.org/what-is-nmap-a-comprehensive-guide-for-network-mapping/>
* <https://www.upguard.com/blog/smb-port#toc-2>