TASK 1: SCAN YOUR LOCAL NETWORK FOR OPEN PORTS

Executive Summary

This report presents the findings of a network scan conducted using Nmap to identify open ports and potential security risks within the local network range of 192.168.1.0/24. The scan revealed one IP address with multiple open ports, posing potential security risks.

Scan Details

- Target IP Range: 192.168.1.0/24

- Scan Type: TCP SYN scan (nmap -sS)

- Target IP Address: 192.168.1.1

- Open Ports: 21, 53, 80, 443

Open Ports and Services

Port Number | Service

21 - FTP (File Transfer Protocol)

53 - DNS (Domain Name System)

80 - HTTP (Hypertext Transfer Protocol)

443 - HTTPS (Hypertext Transfer Protocol Secure)

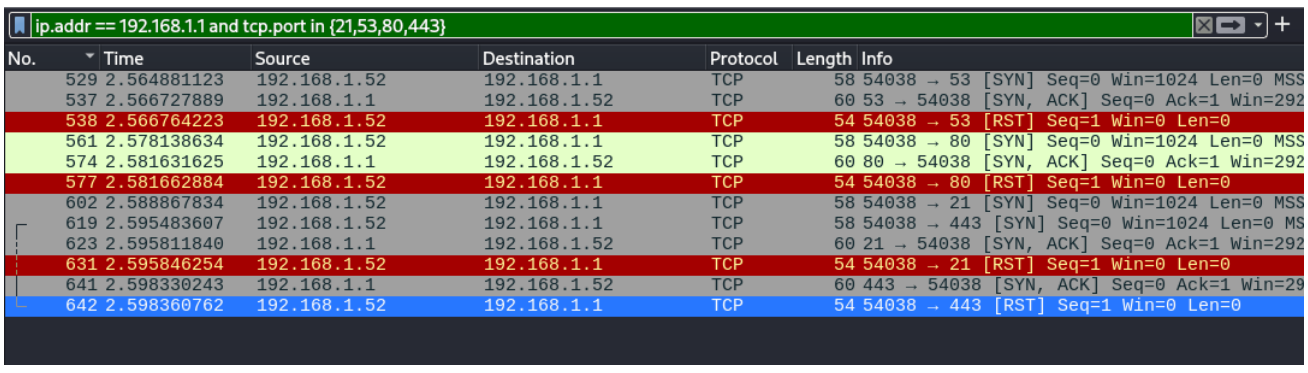
```
└─$ nmap -sS 192.168.1.0/24
Starting Nmap 7.95 ( https://nmap.org )
Nmap scan report for 192.168.1.1
Host is up (0.0039s latency).
Not shown: 992 closed tcp ports (reset)
PORT    STATE    SERVICE
21/tcp  open     ftp
22/tcp  filtered ssh
23/tcp  filtered telnet
53/tcp  open     domain
80/tcp  open     http
139/tcp filtered netbios-ssn
443/tcp open     https
445/tcp filtered microsoft-ds
```

Packet Capture Analysis

The packet capture was analyzed using Wireshark, revealing the following:

- TCP SYN packets: Sent to the target IP address to initiate connections.

- SYN-ACK packets: Received from the target IP address, indicating open ports.



Potential Security Risks

- Port 21 (FTP): Potential for unauthorized access, weak password vulnerabilities, and data breaches.

- Port 53 (DNS): Potential for DNS amplification attacks, cache poisoning, and DNS tunneling.

- Port 80 (HTTP): Potential for web application vulnerabilities (e.g., SQL injection, cross-site scripting).

- Port 443 (HTTPS): Potential for SSL/TLS vulnerabilities (e.g., Heartbleed, POODLE).

Recommendations

- Secure FTP: Implement SFTP or FTPS to encrypt file transfers.

- Secure DNS: Implement DNSSEC to prevent DNS spoofing and amplification attacks.

- Secure Web Applications: Ensure web applications are up-to-date and patched against known vulnerabilities.

- Regularly Update SSL/TLS: Regularly update SSL/TLS certificates and ensure they are properly configured.

STEPS PERFORMED:

1. Installed Nmap: Pre-installed Nmap in Kali Linux, which is a network scanning tool used to discover hosts and services on a computer network.
2. Identified Local IP Range: I identified your local IP range as 192.168.1.0/24, which is a common IP range for home networks.
3. Run Nmap Scan: I ran an Nmap scan using the command nmap -sS 192.168.1.0/24 to perform a TCP SYN scan on the local network. This type of scan is used to identify open ports on target hosts.
4. Noted IP Addresses and Open Ports: I noted the IP address 192.168.1.1 and the open ports 21, 53, 80, and 443. These ports are commonly associated with FTP, DNS, HTTP, and HTTPS services.
5. Analyzed Packet Capture: I analyzed the packet capture using Wireshark, which is a network protocol analyzer. This step helps to understand the network traffic and identify potential security issues.
6. Researched Common Services: I researched the common services running on the open ports, which helps to understand the potential security risks associated with each service.
7. Identified Potential Security Risks: I identified potential security risks associated with the open ports, such as unauthorized access, weak password vulnerabilities, and data breaches.