Nmap TCP SYN Scan Report

Name: **Gettiboyina Venu**

Target Network : 192.168.114.1

Date of Activity: September 22, 2025

Tool Used: Nmap (Network Mapper)

1. Objective

The purpose of this activity was to understand the fundamentals of network reconnaissance

through hands-on scanning using Nmap, a leading open-source tool in cybersecurity. The activity aimed to demonstrate how open ports, protocols, and services on a networked system can be discovered, analyzed, and documented for defensive or learning purposes. This task was conducted solely for educational purposes to simulate how security analysts and ethical hackers gather information about remote hosts in real-world scenarios — legally and responsibly.

2. About Nmap

Nmap (Network Mapper) is a versatile open-source tool widely used for:

- Network discovery

- Security auditing

- Host and service detection

- Operating system fingerprinting

- Vulnerability assessment (via NSE scripts)

It supports advanced scanning techniques for both TCP and UDP protocols and can be used to gather deep insights into the target systems' exposure.

3. Methodology

Multiple types of Nmap scans were conducted to explore different network behaviors and responses. Each scan targeted the IP 192.168.114.1, simulating a reconnaissance task.

4. Nmap Commands Used & Purpose

Command it's Purpose

1. **nmap -Pn 192.168.114.1 :** Full TCP port scan (all 1–65535 ports) to identify every open port.
2. **nmap -sS 192.168.114.1 :** Performs a stealthy TCP SYN (half-open) to discover which TCP ports are open , closed, or filtered.
3. **nmap -sV 192.168.114.1 :** Service version detection for identifying software versions on each port.

5. Skills Gained

- Understanding of TCP vs UDP scanning techniques
- Experience with different Nmap options and flags
- Learned how to responsibly perform reconnaissance
- Interpreted scan outputs to identify system-level exposure

6.Common Ports & Quick Rish Guide (for reference)

- **3306(MySQL) :** should be internal – only.
- **6881(BitTorrent) :** peer- to- peer file sharing (TCP / UDP).

7. Understanding Port States in Nmap

Nmap categorizes ports into various states based on their response:

- **Open**: An application is actively accepting connections.

- **Closed**: No application is listening on the port, but the port is reachable.

- **Filtered**: Packet filtering prevents Nmap from determining the state.

- **Unfiltered**: Nmap can reach the port, but can't determine its state.

- **Open|Filtered**: Nmap cannot determine whether the port is open or filtered.

- **Closed|Filtered**: Nmap cannot determine whether the port is closed or filtered.

Understanding these responses is crucial for interpreting scanning results accurately and

deciding the next steps.

8. Reflections and Future Plan

This project deepened my understanding of real-world scanning techniques and security postures. I realized how simple misconfigurations and open services can potentially expose an organization to threats. Practicing in an ethical and controlled manner allowed me to safely learn how attackers think.

Nmap is a gateway to more advanced security skills, and this exercise was just the beginning of that journey.