Port Scanning Report

## Task Title: Scan Your Local Network for Open Ports

## Objective: To discover open ports on devices in the local network and understand network exposure using nmap.

## 1.Tool Used

* Nmap : For Scanning the local network using TCP SYN scan.
* Wireshark : For packet analysis.

## 2.Network Details

* IP Range Scanned : 192.168.111.0/24
* Command used : nmap -sS 192.168.111.0/24
* Scan type : TCP SYN scan

## 3.Scan results

|  |  |  |
| --- | --- | --- |
| PORT | STATE | SERVICES |
| 21/tcp | open | ttp |
| 22/tcp | open | ssh |
| 23/tcp | open | telnet |
| 25/tcp | open | smtp |
| 80/tcp | open | http |
| 513/tcp | open | login |
| 514/tcp | open | shell |
| 3306/tcp | open | mysql |
| 53/tcp | open | domain |
| 111/tcp | open | rpcbind |

## 4.Analysis

* Common services found : HTTP(port 80) , SSH(port22), TELNET(port 23) , etc.
* Devices with open port could be server, router, or IOT devices.
* Possible vulnerabilities if port are unnecessarily open or unprotected

## 5.Security Risk Identification

* Open SSH port 22 might allow brute-force attacks
* HTTP on port 80 could expose unencrypted data.
* Unused services increase the attack surface.

## 6.Recommendations

* Close unused ports on devices.
* Use firewall to filter inbound/outbound connections.
* Enable encryption.
* Regularly scan network to detect exposure.

## 7.Optional Wireshark Insights

* Captured SYN packets and their responses.
* Verified handshake behavior.
* Detect anomalies or repeated SYN packets.

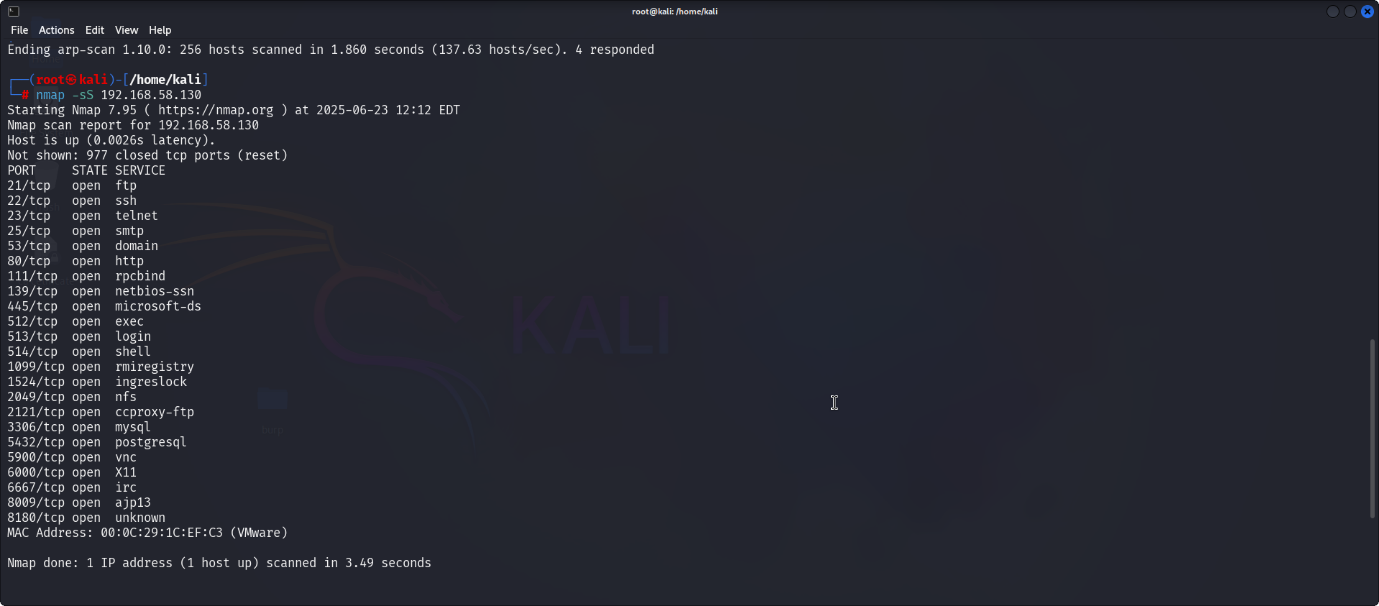
### 8.Scan Output File

* File format : result.txt
* Location : /home/ajmal/result.txt

## 9.Conclusion

The scan provide a clear view of which ports are open in the local network and what services are running . regular port scanning helps identifying exposed services and strengthen overall network security.

### 1.Scan result



## 2.Wireshark interface

