Nmap Scan Report Summary

Target IP Address: 192.168.xx.xx

Scan Tool: Nmap

Observation: The following TCP ports were founds to be open.

This is the list of port that Nmap found to be open on my local network or home network that my device is connected to.

Port 135/tcp – Service: msrpc

- Service Name: Microsoft RPC (Remote Procedure Call)
- Purpose: Used by Microsoft systems for DCOM services and various administrative functions.
- Security Note: This port is commonly targeted for exploitation, particularly in older Windows systems (e.g., MS03-026 Blaster Worm). It should be firewalled or disabled if not required.

Port 139/tcp – Service: netbios-ssn

- Service Name: NetBIOS Session Service
- Purpose: Used for file and printer sharing on Windows networks.
- Security Note: This port can reveal sensitive file shares and machine information. It is often exploited in SMB-related attacks. Disable if not in use.

Port 445/tcp – Service: microsoft-ds

- Service Name: Microsoft Directory Services (SMB over TCP)
- Purpose: Used for Active Directory, file sharing, and printer services in modern Windows networks.
- Security Note: Frequently targeted (e.g., EternalBlue exploit used in WannaCry). Best practice is to restrict access and patch systems.

Port 7070/tcp – Service: realserver

- Service Name: RealNetworks RealServer
- Purpose: Used by RealMedia streaming services to deliver audio and video content.
- Security Note: If not used for media streaming, this port should be closed. Older versions of RealServer have had vulnerabilities.

Port 8090/tcp – Service: opsmessaging

- Service Name: Ops Messaging or custom web services
- Purpose: Often used by Java or custom applications (e.g., admin interfaces, development services).

- Security Note: This is a non-standard port and may be used by internal tools or APIs. Check what application is bound to this port and secure it appropriately.