**Task 1: Scan Your Local Network for Open Ports.**

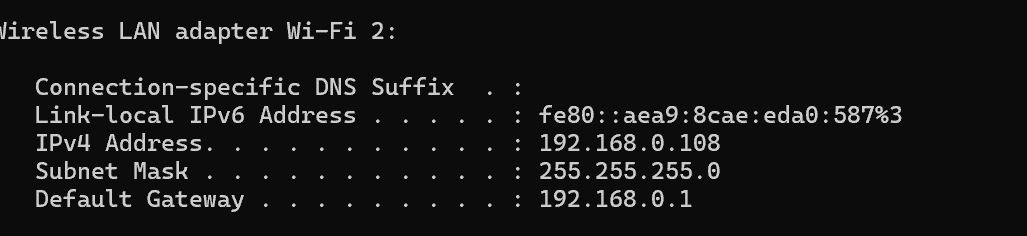
**Objective: Learn to discover open ports on devices in your local network to understand**

**network exposure.**

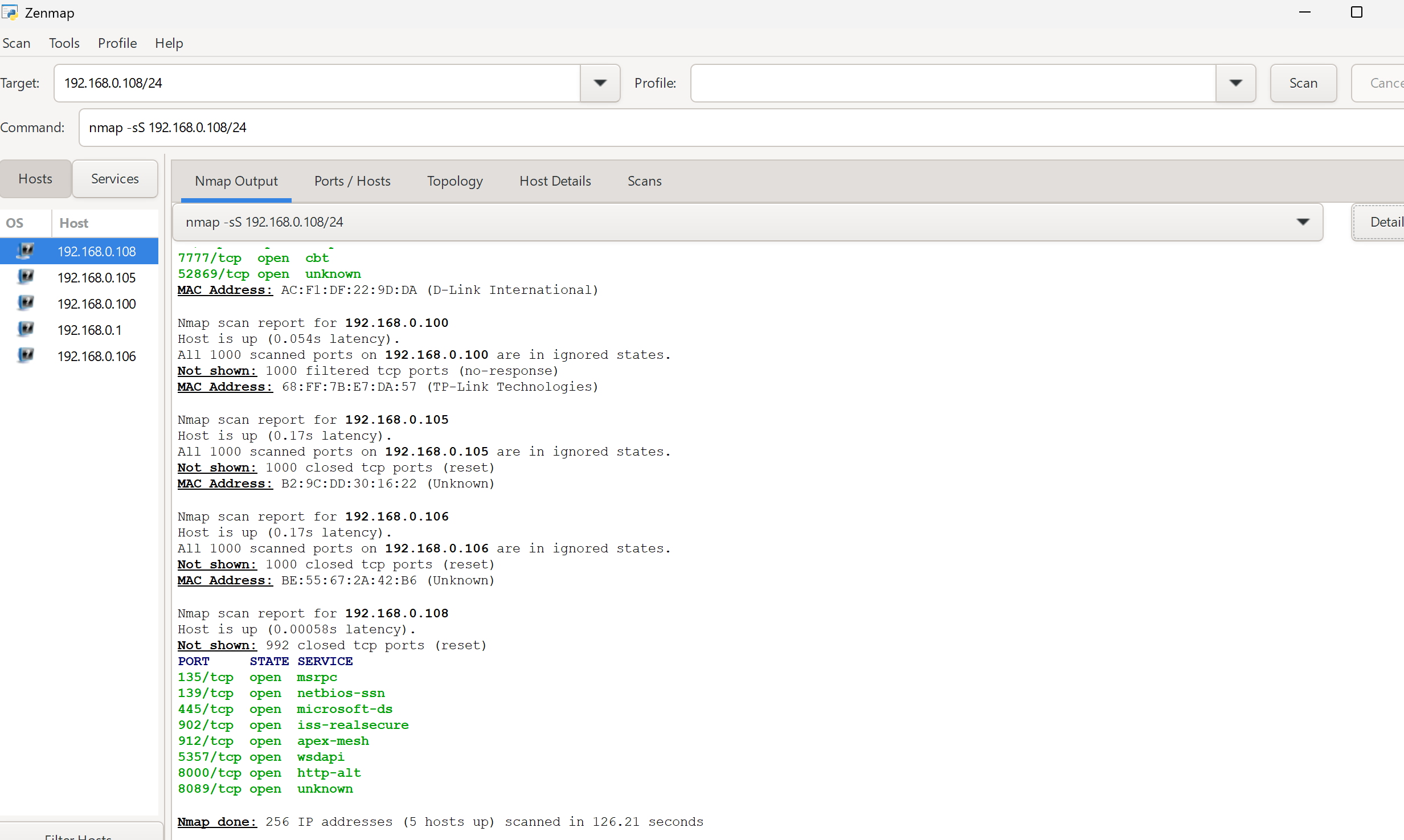
**Tools: Nmap (free), Wireshark (optional).**

**1.installed Nmap**

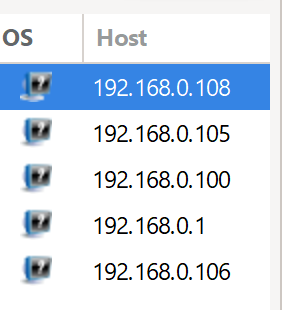
**2. got the local ip , subnet mask, default gateway using cmd : ipconfig**

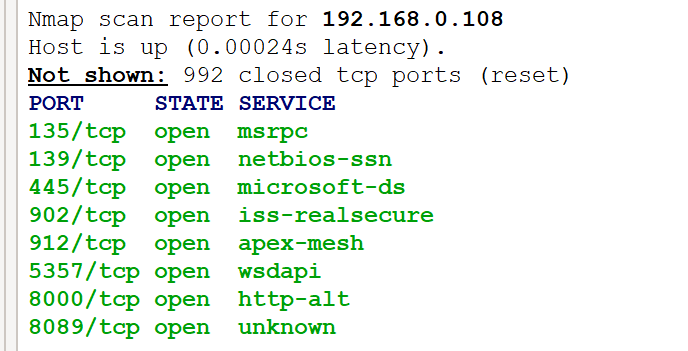


3.Now : nmap -sS 192.168.1.0/24 to perform TCP SYN scan



4. Got the scan result as: there are 4 devices connected on my local network with following ip address as mentioned in screenshot.



5. Also found the following ports are open on my host with ip 192.168.0.108 .

Port 135 is primarily used for Remote Procedure Call (RPC) services in Windows environments, facilitating communication between different applications and systems. Specifically, it acts as an [RPC endpoint mapper](https://www.google.com/search?sca_esv=b0c8a5b5dae9aa98&sxsrf=AE3TifMbYhe-dAbNpjdF45YR0LmTGegXyg%3A1754322101841&q=RPC+endpoint+mapper&sa=X&ved=2ahUKEwjOss6Nv_GOAxUS1zgGHcAcMxcQxccNegQIJhAB&mstk=AUtExfDPMkBj8sTPQOI5l2-JGA5q5VO9B-bVZA7YvcGuzM6T_uSR_XFqpqUymIGNaF9vKuqSBAHJFrmxzfKRCTuOwT1AMRRuZtPcvClYS502QVimJerf2-HuQkVmY7tYZTEdRypfSIiwfDU_lzWPnGxWfLSUWvFh6f89u5laN0X1MwLS9BcHi_iEDHC9JGzuTeL-PWEPt3ia3QJgP6BQ0dNR-fbOaL12cz5vNyvq7LFYAK--dhy4Ep1MnIM0DAtT4iIBu6-Q-AQcP10dKasyW2UgVC1s&csui=3), helping clients locate and connect to available RPC services on a server. This functionality is crucial for various Windows operations, including [Active Directory](https://www.google.com/search?sca_esv=b0c8a5b5dae9aa98&sxsrf=AE3TifMbYhe-dAbNpjdF45YR0LmTGegXyg%3A1754322101841&q=Active+Directory&sa=X&ved=2ahUKEwjOss6Nv_GOAxUS1zgGHcAcMxcQxccNegQINhAB&mstk=AUtExfDPMkBj8sTPQOI5l2-JGA5q5VO9B-bVZA7YvcGuzM6T_uSR_XFqpqUymIGNaF9vKuqSBAHJFrmxzfKRCTuOwT1AMRRuZtPcvClYS502QVimJerf2-HuQkVmY7tYZTEdRypfSIiwfDU_lzWPnGxWfLSUWvFh6f89u5laN0X1MwLS9BcHi_iEDHC9JGzuTeL-PWEPt3ia3QJgP6BQ0dNR-fbOaL12cz5vNyvq7LFYAK--dhy4Ep1MnIM0DAtT4iIBu6-Q-AQcP10dKasyW2UgVC1s&csui=3) replication and remote management.

Port 139 is primarily used for the NetBIOS Session Service, which enables communication for file and printer sharing in Windows networks using the [Server Message Block](https://www.google.com/search?sca_esv=b0c8a5b5dae9aa98&sxsrf=AE3TifNnwdaZl2aJMO59DOCTcHqRg9y7Kg%3A1754322148098&q=Server+Message+Block&sa=X&ved=2ahUKEwj55NWjv_GOAxUNwjgGHViBBlgQxccNegQIKxAC&mstk=AUtExfACRkmN58St56a1f7NUHxps7qb71BgXS2qu0NRcD1u8MR7bpgRnzM0Mlrk56cG7xTtZ0WWNkIM5Mi_p0JWzQydmNB7-6Pu8Ah6zL1en44N4u8nBSU4b_m43kM_NBSaaYEuLXPYbIMViQkrdS53cDCzVJ2OtDO_IHYLXIKrHxWmzkv5uRA8zIp26Blp80oJpeCFQSdIhJavx1h-mtXRJJWGwlsAcAVEera5ilEOPjjcBhMUk9FDMmUtVXtcH2Q-aSTAw6k6wni-ElUbqnAlhqf3RmWMt421hyqGVNAR3gKB_Kw&csui=3) (SMB) protocol over [NetBIOS](https://www.google.com/search?sca_esv=b0c8a5b5dae9aa98&sxsrf=AE3TifNnwdaZl2aJMO59DOCTcHqRg9y7Kg%3A1754322148098&q=NetBIOS&sa=X&ved=2ahUKEwj55NWjv_GOAxUNwjgGHViBBlgQxccNegQIKxAD&mstk=AUtExfACRkmN58St56a1f7NUHxps7qb71BgXS2qu0NRcD1u8MR7bpgRnzM0Mlrk56cG7xTtZ0WWNkIM5Mi_p0JWzQydmNB7-6Pu8Ah6zL1en44N4u8nBSU4b_m43kM_NBSaaYEuLXPYbIMViQkrdS53cDCzVJ2OtDO_IHYLXIKrHxWmzkv5uRA8zIp26Blp80oJpeCFQSdIhJavx1h-mtXRJJWGwlsAcAVEera5ilEOPjjcBhMUk9FDMmUtVXtcH2Q-aSTAw6k6wni-ElUbqnAlhqf3RmWMt421hyqGVNAR3gKB_Kw&csui=3). It facilitates the sharing of resources like files and printers between computers on a local area network (LAN).

Port 445 is primarily used for Server Message Block (SMB) traffic, particularly in Windows environments for file and printer sharing. It allows for direct communication over TCP/IP, unlike the older [NetBIOS](https://www.google.com/search?sca_esv=b0c8a5b5dae9aa98&sxsrf=AE3TifNWUd6GZ2n9cbJP7WLGnCCFvK9H2g%3A1754322185605&q=NetBIOS&sa=X&ved=2ahUKEwj1g8e1v_GOAxVZ_6ACHXzxCscQxccNegQIIxAB&mstk=AUtExfAvFscC8gn9GCtv1D9J9_kZNnYG3d2KlIuQiHhxwhg4E6NTVHZIPB85lf_3Di1AQ3016h7JPO4j_hExnp4FDb0eSDP-W13ki-bS-knIiBqCwH5eXW5Xg1vfUbU5RMRKNvMp1CqqDSYzB_jyFOohZVj7a_IDGf7KDhi_DyH9OEGKYLGuNRU7hHNKOktp93AcAgSnCAlBS7q9Prf1KTFDAFxZ11xaSCpxbSKE8a-dn60Af99pO4HFefIhlMVheFd0UyUUqDrFce5-m2rjUx7NIox0MABz6wqyw-Ykjjffjsvs5w&csui=3)-based SMB which uses port 139. This makes it crucial for accessing shared resources across a network.

Port 902 is primarily used for VMware vSphere management, specifically for communication between the vSphere Client, ESXi hosts, and vCenter Server. It facilitates remote access, management tasks, and data exchange within VMware's virtualization environment.

Port 912 is primarily used for the APEX (Application Exchange Core) protocol, specifically for relaying messages within the protocol. It's an XML-based protocol used for instant messaging, and it also utilizes port 913 for related endpoint-relay services. Additionally, some SCADA (Supervisory Control and Data Acquisition) software, like [RealFlex RealWin](https://www.google.com/search?sca_esv=b0c8a5b5dae9aa98&cs=1&sxsrf=AE3TifPcLP793JGs3w3K1YIV6F2275vKyA%3A1754322247648&q=RealFlex+RealWin&sa=X&ved=2ahUKEwjFlvnSv_GOAxXO3TgGHeCNLksQxccNegQIBxAB&mstk=AUtExfCx3RC-D-HXgo46qwJWaC5xfpiKXS9rI9aRRX5DMJ1ZbNNE06jh_51t0Jr1qFDl4E4T7PMSPi6j6BqrmUZLMCS1KPCH2dHm8SxPqG0Lfbiv03dAnz1WG112CS1LPfATDR635W2bjjKpZPnpdBnOeIgosITx9VRMUNRDUq3jS4LQkMRBWgp91HRTP1_2aeGzHOENGNVo2PyEJE1ZJ4N8-O6BIq428akxq-GCc6QUXQDfc8KyPk1FQrn95ICuqM05SgvQkS-jFSepZ2hV5KTGSOGfujSF4SOlCNAQ2A780f4OqA&csui=3" \t "_blank), may use port 912 for its HMI (Human-Machine Interface) service.

Port 5357 is primarily used by Web Services on Devices (WSD) API (WSDAPI), a component of Windows that facilitates network device discovery and communication. Specifically, it allows devices like printers and scanners to advertise their services and capabilities to other devices on the same network, enabling automatic setup and use of these devices without manual configuration.

Port 8000 is commonly used as an alternative port for web development servers and API testing environments, often running over HTTP. It's frequently used by developers as an alternative to the default HTTP ports (80 for HTTP, 443 for HTTPS) when running local development servers or when specific port assignments are needed for testing or internal applications.

Port 8089 is primarily used as the default management port for Splunk instances. It is used by Splunk Enterprise, including deployment servers, search heads, and forwarders, for communication related to management and data forwarding.