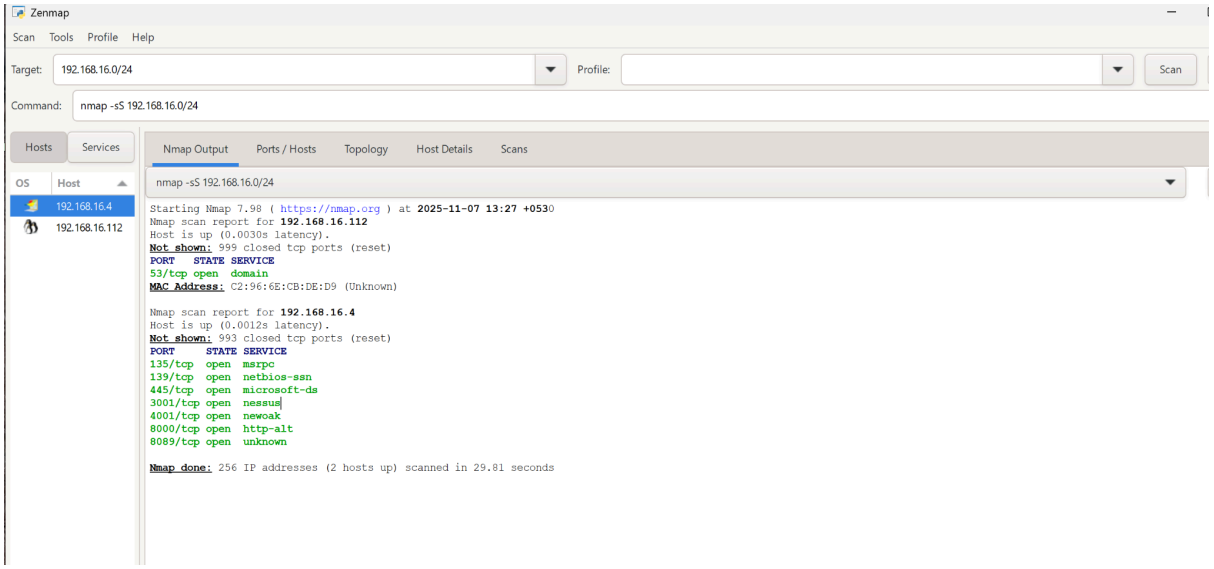
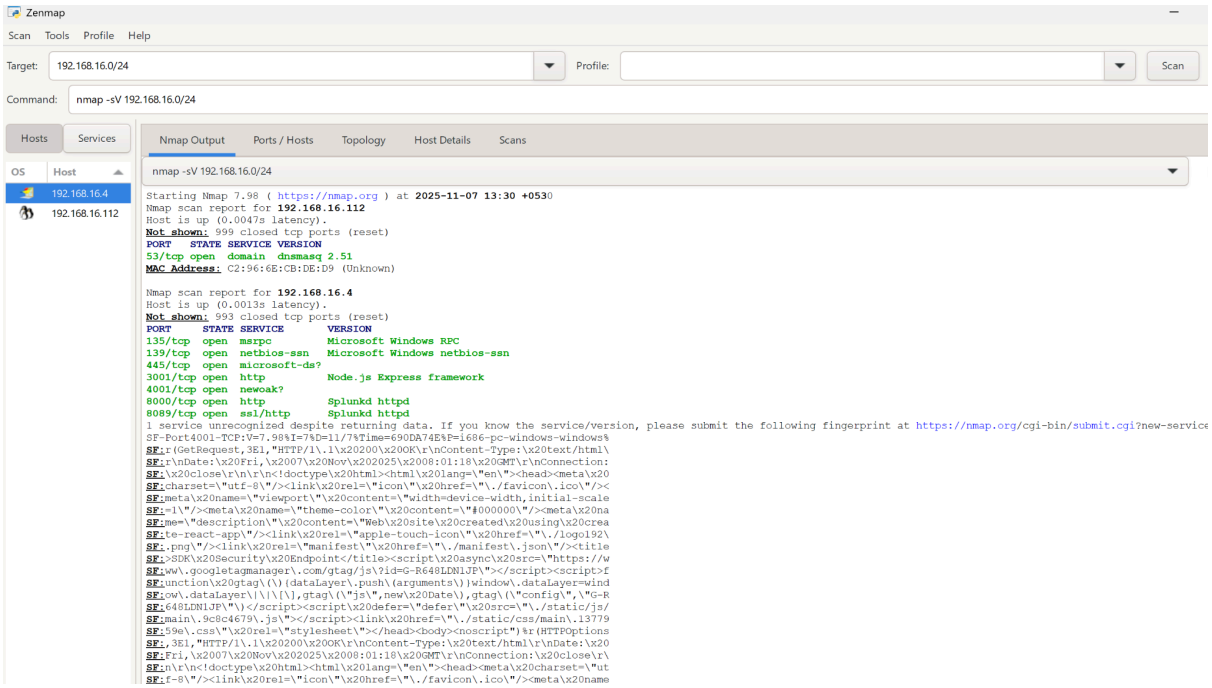
Scan Your Local Network for Open Ports using Nmap:



Port Scan (TCP SYN Scan):

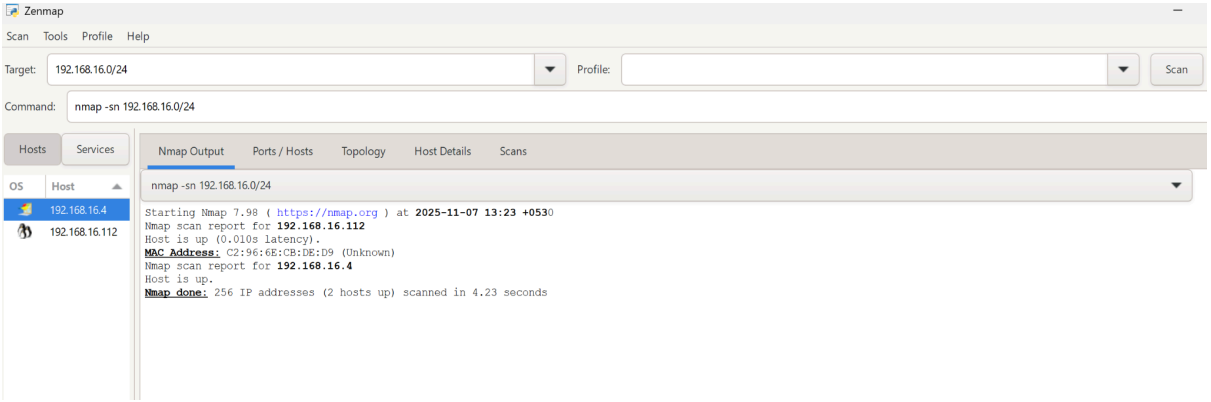
- **Command Used:** `nmap -sS 192.168.16.0/24`
- **Purpose:** To perform a "stealth" TCP SYN scan to check the state of the top 1000 common ports on the active hosts. The `-sS` flag is faster and stealthier than a full TCP Connect scan.
- **Result Analysis:**
  - **Host 1: 192.168.16.112**
    - **Port 53/tcp** is **open** (Service: `domain`). This is the standard port for DNS.
    - **999 closed ports** were not shown.
  - **Host 2: 192.168.16.4**
    - **Port 135/tcp** is **open** (Service: `msrpc`).
    - **Port 139/tcp** is **open** (Service: `netbios-ssn`).
    - **Port 445/tcp** is **open** (Service: `microsoft-ds`).
      - *Note: Ports 135, 139, and 445 are commonly associated with Windows Networking (SMB/CIFS).*
    - **Port 3001/tcp** is **open** (Service: `nessus`).
    - **Port 4001/tcp** is **open** (Service: `newoak`).
    - **Port 8000/tcp** is **open** (Service: `http-alt`).
    - **Port 8089/tcp** is **open** (Service: `unknown`).
    - **993 closed ports** were not shown.
  - The scan completed in **29.81 seconds**.



Service/Version Detection Scan:

- Command Used: `nmap -sV 192.168.16.0/24`
- Purpose: To perform service and version enumeration on the open ports detected in the previous scan. The `-sV` flag sends specific probes to determine the application name and version number running on the open port.
- Result Analysis (Focused on open ports):
    - Host 1: 192.168.16.112
        - Port 53 is open (Service: `domain`).
        - MAC Address: `02:9f:6c:3b:0e:09` (This is the same as the other host, suggesting they might be virtual interfaces on the same physical machine or that Nmap incorrectly assigned the MAC).
    - Host 2: 192.168.16.4
        - Port 135/tcp (Service: `msrpc`): Identified as Microsoft Windows RPC.
        - Port 139/tcp (Service: `netbios-ssn`): Identified as Microsoft Windows netbios-ssn.
        - Port 445/tcp (Service: `microsoft-ds`): Identified as Microsoft Windows netbios-ds.

- Port 3001/tcp (Service: `nessus`): Identified as Node.js Express framework.
- Port 4001/tcp (Service: `newoak`): Identified as `newoak` (still generic).
- Port 8000/tcp (Service: `uploaded http`): Identified as an uploaded http service.
- Port 8089/tcp (Service: `uploaded http`): Identified as an uploaded http service.
- Note: The detailed output for 8089/tcp shows HTML content (likely a login page or default index file), confirming a web server is running on that port.



Host Discovery (Ping Scan)

- **Command Used:** `nmap -sn 192.168.16.0/24`
- **Purpose:** To quickly determine which IP addresses in the subnet are actively responding (live). The `-sn` flag (Skip Port Scan) tells Nmap to only perform host discovery.
- **Result Analysis:**
  - **256 IP addresses** were scanned.
  - **2 hosts** were found to be **up** (active).
  - The live hosts are:
    - **192.168.16.112**
    - **192.168.16.4**
  - The scan completed in **4.23 seconds**.

Conclusion

The scanning successfully identified **two active hosts** on the `192.168.16.0/24` network. The host **192.168.16.4** appears to be a multi-service host, possibly running on a Windows OS (due to the netbios ports) and also hosting several web-related services (ports 3001, 8000, 8089). The service/version scan was successful in confirming the running applications on the open ports.