Local Network Port Scanning Guide

Objective:  
Learn to discover open ports on devices in your local network to understand potential network exposure and security risks.

# Tools Needed

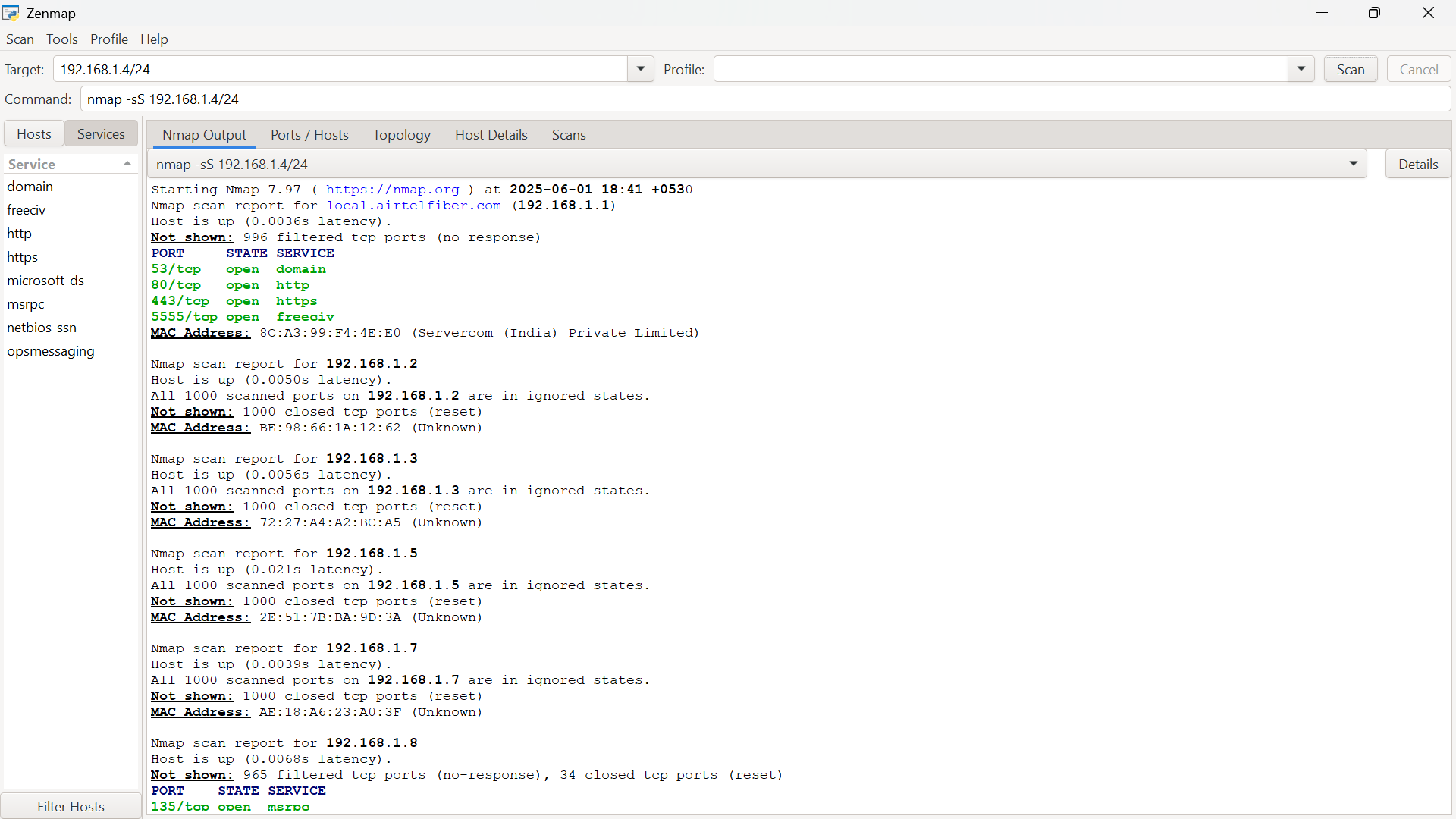
- Nmap (Free) – https://nmap.org/download.html

- Wireshark (Optional) – https://www.wireshark.org/

# Step-by-Step Guide

1. Install Nmap from the official website: https://nmap.org/download.html.
2. Find your local IP range:  
    - On Windows: Open Command Prompt and type `ipconfig`  
    - On macOS/Linux: Use `ifconfig` or `ip a`
3. Identify your subnet (e.g., if your IP is 192.168.1.4with a subnet mask of 255.255.255.0, your network is 192.168.1.4/24).
4. Open a terminal or command prompt and run the following Nmap command:  
    nmap -sS 192.168.1.4/24
5. Note down the IP addresses and open ports detected by the scan.
6. Optionally, use Wireshark to analyze network traffic and understand how Nmap communicates with other devices.
7. Research the common services running on those open ports. For example:  
    53/tcp open domain
8. 80/tcp open http
9. 443/tcp open https
10. 5555/tcp open freeciv
11. Identify potential security risks associated with open ports, such as unprotected remote access or exposed web services.
12. Save your scan results using Nmap options:  
     - Save as XML: nmap -sS 192.168.1.4/24 -oX scan\_results.xml

Here is the screenshot of the scan in nmap



You can see above the port numbers and their status.