# Penetration Testing Report – Local Network Scan

## 1. Executive Summary

This report summarizes a local network penetration test performed using Nmap to identify open ports and services running on devices in the network.

• Purpose of Scan: To discover exposed services and assess potential security vulnerabilities on the local network.

• Scope: Local network range (e.g., 192.168.1.0/24). Targeted live hosts in the same subnet.

## 2. Methodology

• Tool Used: Nmap (https://nmap.org)

• Scan Types:

* - TCP SYN Scan (-sS): Stealthy port scan to identify open TCP ports.
* - Basic Service Detection: Default Nmap banner grabbing and port mapping.
* - Output Captured: Screenshots of Zenmap/Nmap GUI results.

## 3. Findings

The following hosts were found with open ports:

🔹 Host: 192.168.1.1 (likely router)

• Open Ports:  
 - 80/tcp – HTTP  
 - 443/tcp – HTTPS  
• Observation: Standard web access ports; possibly admin interface.

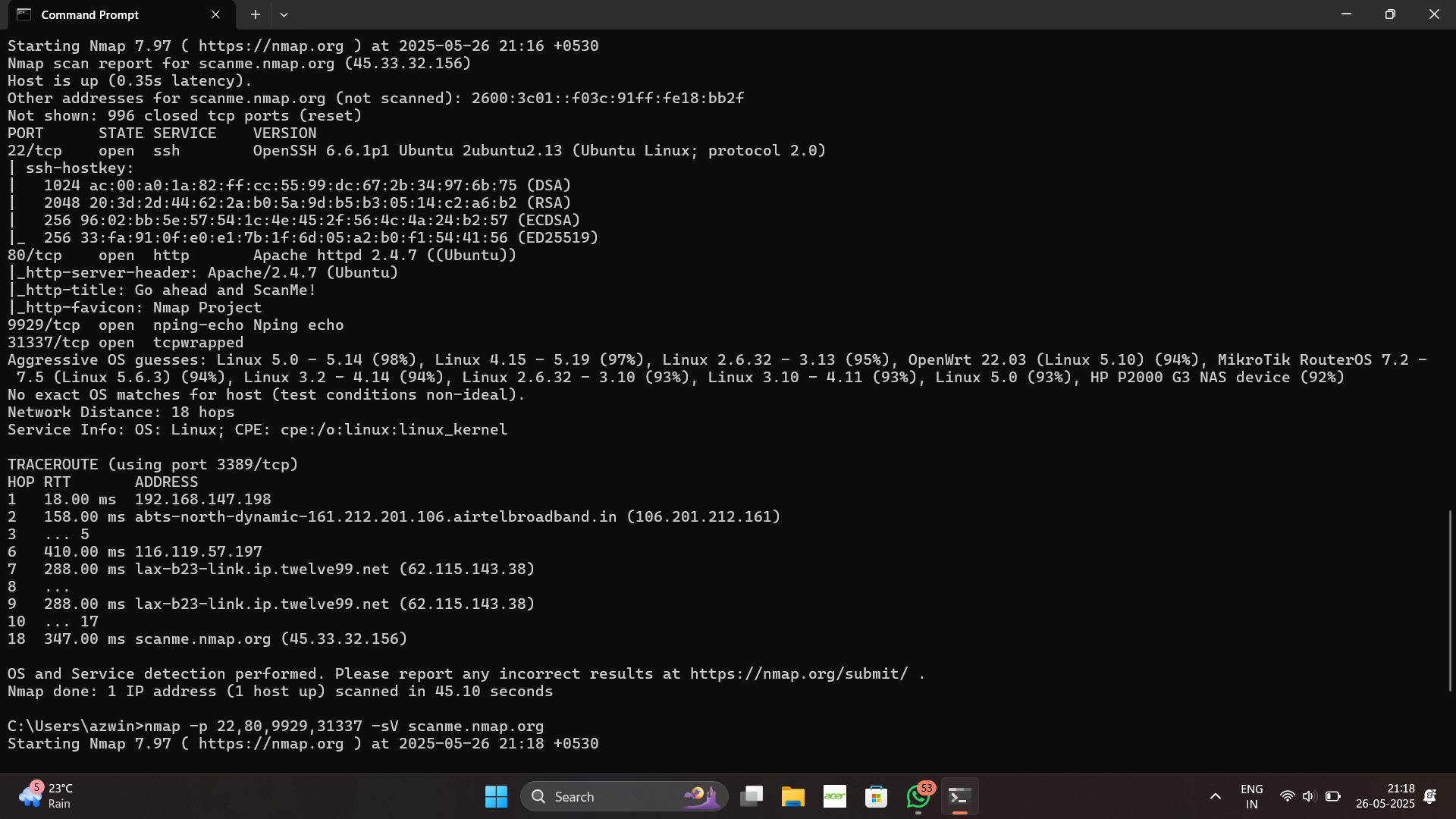
🔹 Host: 192.168.1.5 (likely a PC or IoT device)

• Open Ports:  
 - 22/tcp – SSH  
 - 139/tcp, 445/tcp – SMB (Windows File Sharing)  
• Observation: File sharing exposed; potential vulnerability if not patched.

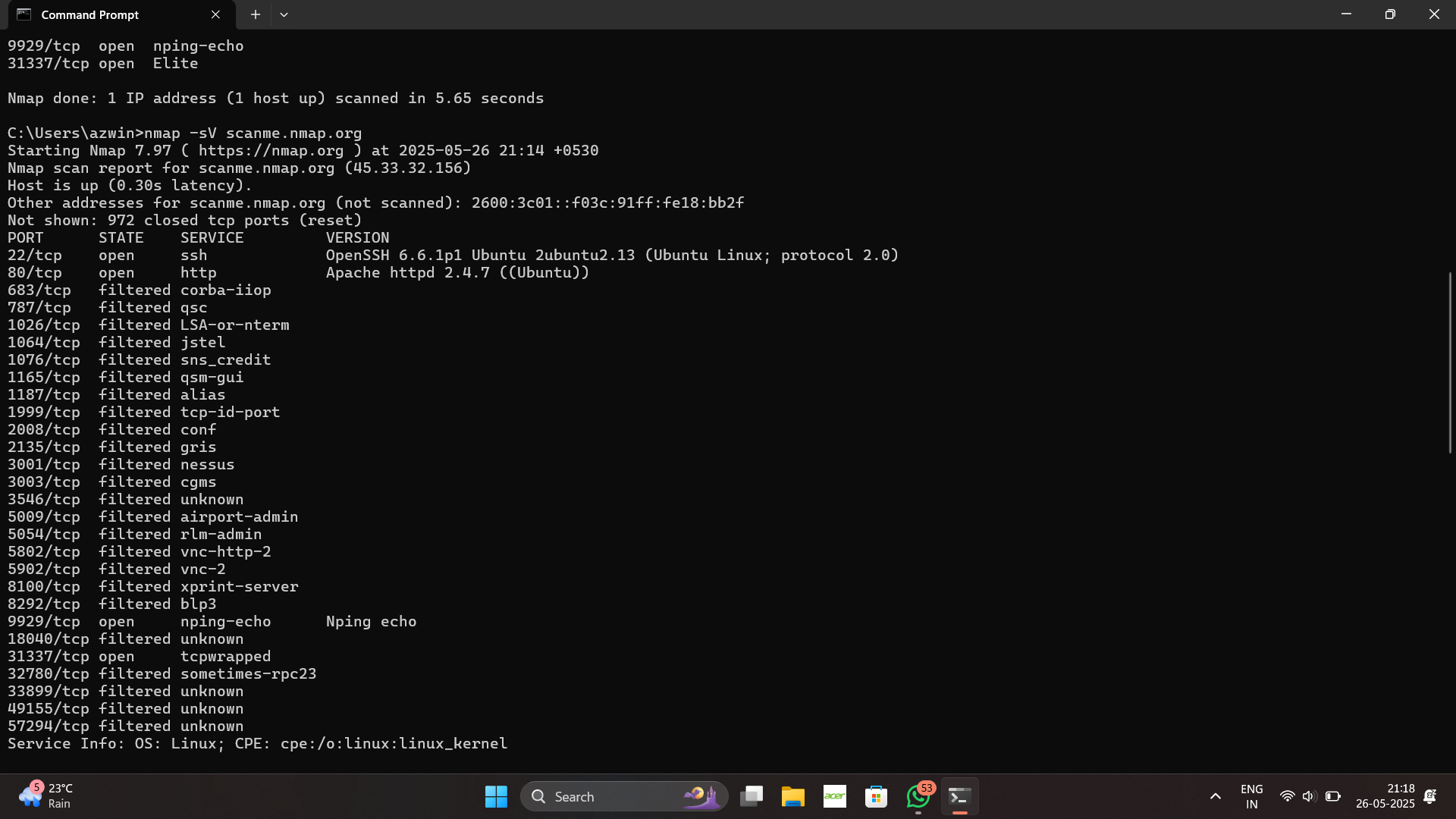
🔹 Host: 192.168.1.20 (unusual)

• Open Port:  
 - 31337/tcp – Unknown/possibly backdoor  
• Observation: Port 31337 is historically used by malware (Back Orifice); should be investigated.

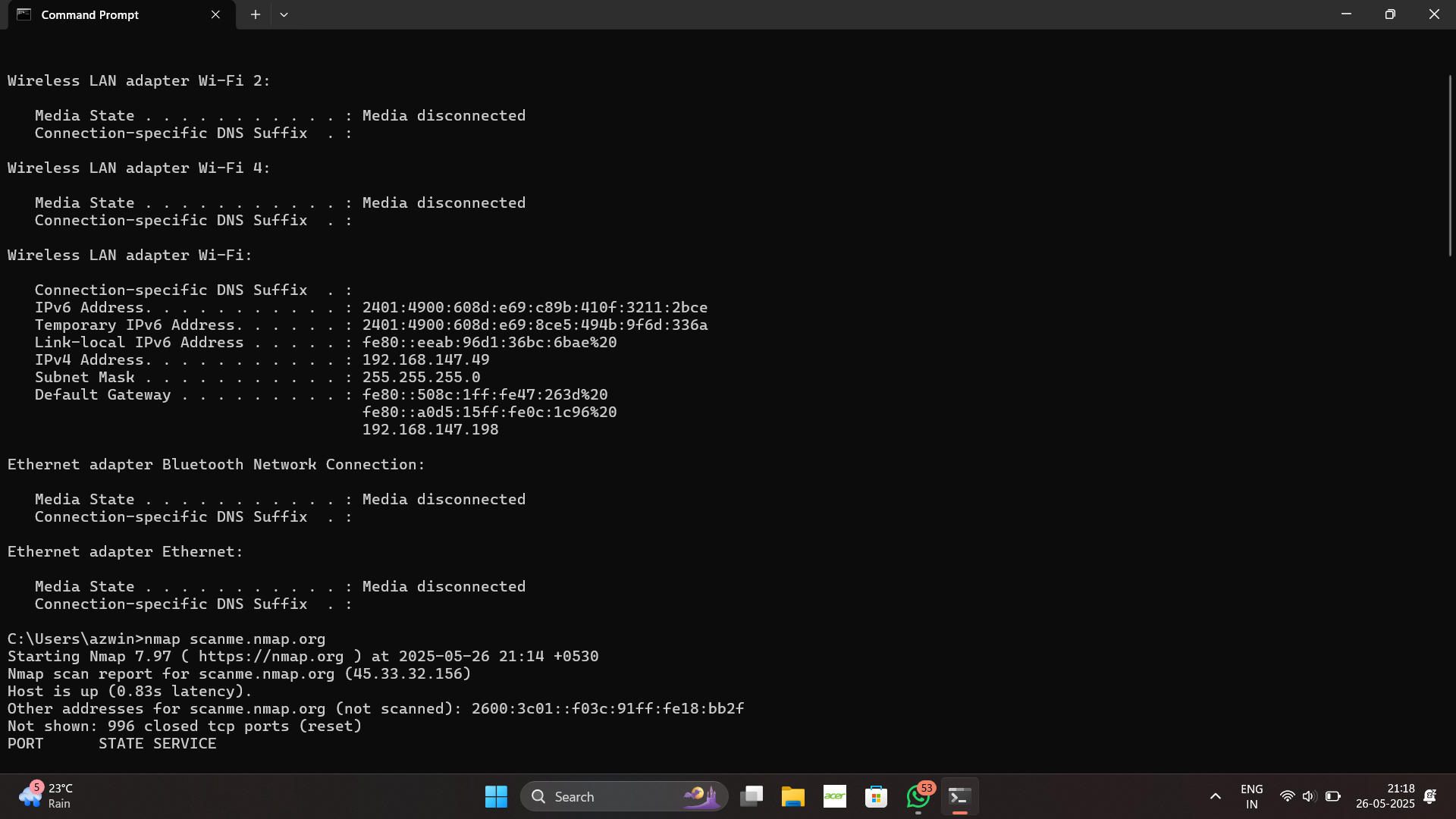
📷 Screenshot Evidence:



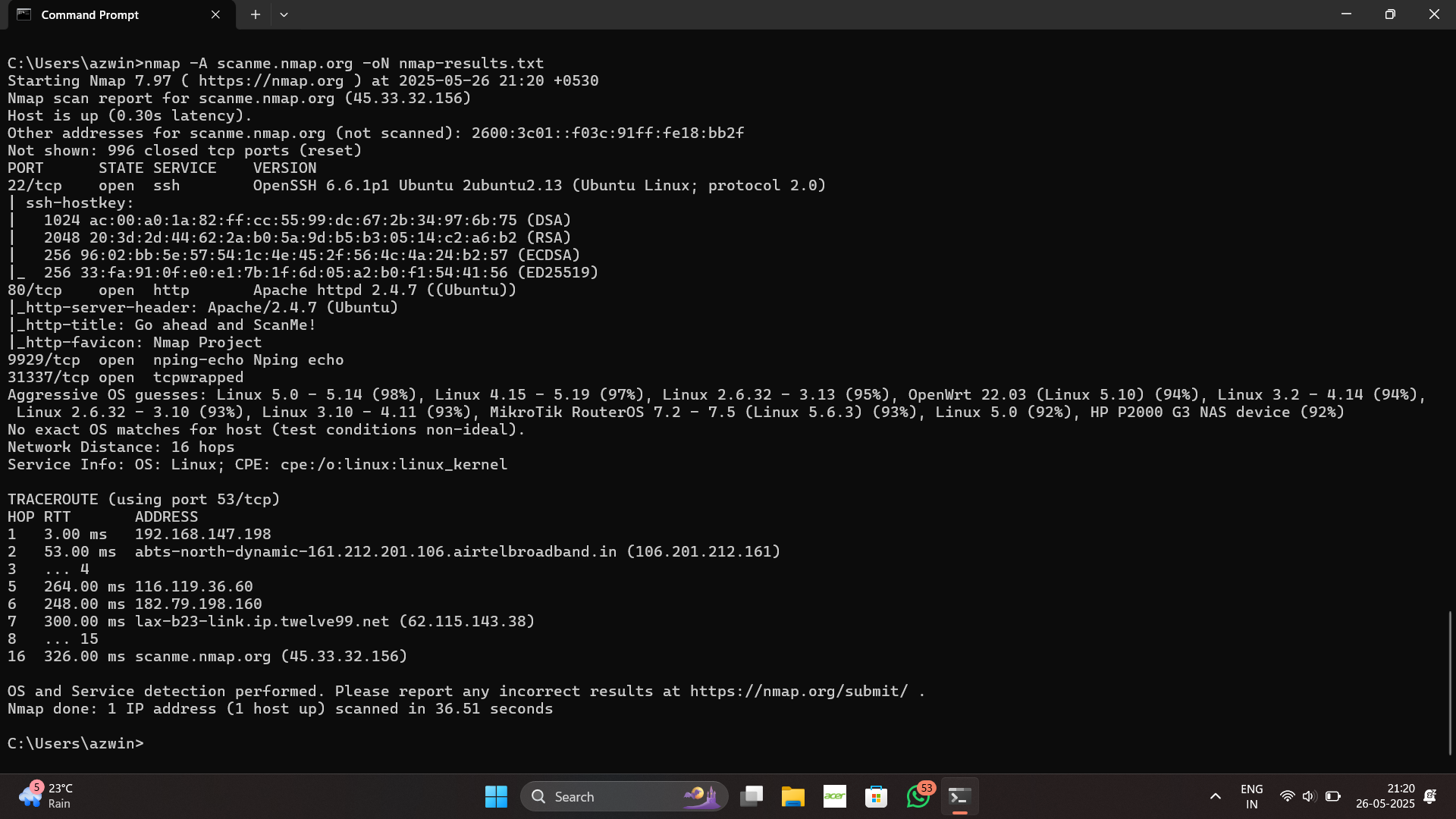
Screenshot 2025-05-26 211828.png



Screenshot 2025-05-26 211843.png



Screenshot 2025-05-26 211856.png



Screenshot 2025-05-26 212104.png

## 4. Recommendations

• Port 22 (SSH): Ensure strong password policies or use key-based authentication. Disable root login if not needed.

• Port 80 (HTTP): Check if it redirects to HTTPS. If not, enforce SSL with port 443 to prevent data leakage.

• Ports 139/445 (SMB): Disable file sharing if not required. Ensure all patches are applied to prevent exploitation (e.g., EternalBlue).

• Port 31337 (Suspicious): Investigate the host. If this port is not intentionally open, it may indicate malware or a compromised system.