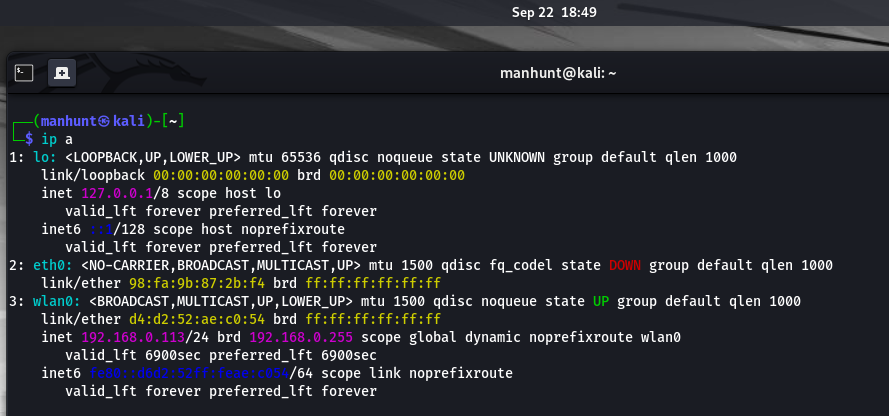
## **PAVAN GC** 22-09-2025 **Task 1 Report:** **Scan Your Local Network for Open Ports Nmap — Network Mapper**

**Definition:**  
Nmap (Network Mapper) is an open-source command-line utility for network discovery and security auditing. It identifies live hosts, open ports, running services, and (optionally) OS versions on IP networks.

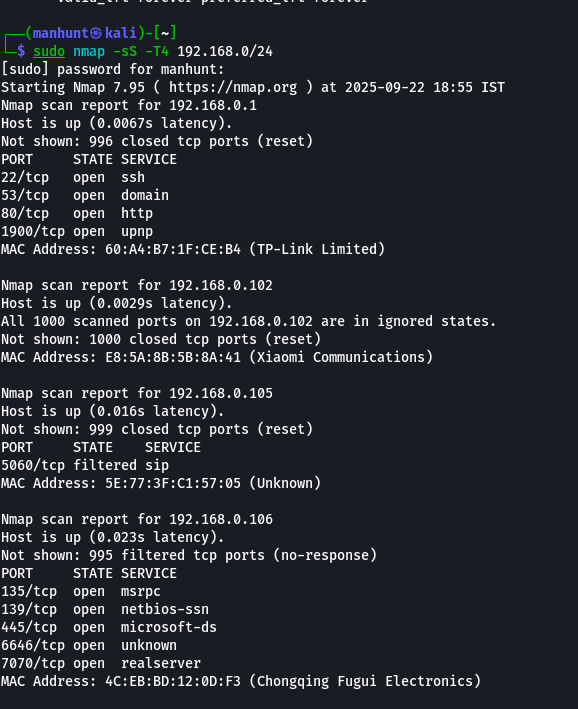
**Primary Purpose:**  
Rapidly map the network perimeter and internal hosts to understand which services are exposed and to perform vulnerability reconnaissance.

**Common Use-Cases**

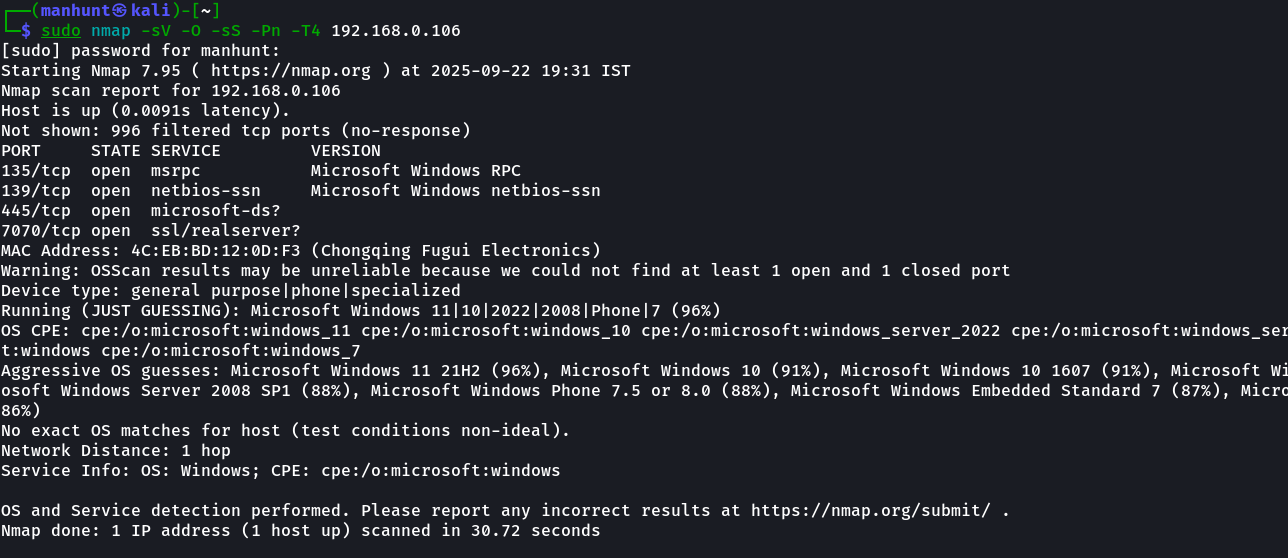
* Host discovery and inventory (ping sweep, ARP discovery)
* Port scanning (TCP SYN, connect, UDP)
* Service and version detection (-sV)
* OS fingerprinting (-O)
* Exporting scan results for reporting (-oN, -oX, -oA)

****

## **Command:** ip a **Description:** Displays the system’s network interfaces and assigned IP addresses. Shows loopback (lo), Ethernet (eth0 – down), and Wi-Fi (wlan0) with the local IP 192.168.0.113. This helped identify the subnet (192.168.0.0/24) for scanning.



**Command:** sudo nmap -sS -T4 192.168.0.0/24  
**Description:** Conducted a **TCP SYN scan** on the local network. Multiple devices were detected:

* 192.168.0.1 (TP-Link router) → open SSH, DNS, HTTP, UPnP.
* 192.168.0.102 (Xiaomi device) → filtered SIP port (5060).
* 192.168.0.106 (Windows host) → open SMB/RPC-related ports.

**Command:** sudo nmap -sV -sS -Pn -T4 192.168.0.106  
**Description:** Detailed scan of a Windows host. Found open services:

* RPC (135), NetBIOS (139), SMB (445), RealServer (7070), Unknown (666).

Service detection identified the OS as **Microsoft Windows (various versions possible)**.  
This reveals potentially risky services like SMB and RPC that should be patched/secured.  
  
**Potential Security Risks From Open Ports:**

I researched the common services you found in your scans and identified the main security risks and recommended mitigations for each. I used the ports and services visible in your screenshots:

* **192.168.0.1** — 22/tcp (ssh), 53/tcp (domain/DNS), 80/tcp (http), 1900/udp (UPnP)
* **192.168.0.102** — 5060/tcp (SIP — filtered)
* **192.168.0.105** — no open ports detected (from scan)
* **192.168.0.106** — 135/tcp (msrpc), 139/tcp (netbios-ssn), 445/tcp (microsoft-ds / SMB), 666/tcp (unknown service), 7070/tcp (realserver)

Below is a compact, professional analysis you can add to your report or notes.

**1) Common services found — quick reference & what they do**

**22/tcp — SSH (Secure Shell)**

* Purpose: Remote command-line login and secure file transfer (scp/sftp).
* Typical software: OpenSSH, Dropbear.

**53/tcp — DNS (domain)**

* Purpose: Hostname resolution (DNS over TCP for zone transfers or large responses).
* Typical software: BIND, dnsmasq, Microsoft DNS.

**80/tcp — HTTP**

* Purpose: Unencrypted web server traffic (web admin pages, device interfaces).
* Typical software: nginx, Apache, device web interfaces.

**1900/udp — SSDP / UPnP**

* Purpose: Simple Service Discovery Protocol used by UPnP for device discovery and automatic port forwarding.
* Typical on: routers, smart devices, media servers.

**5060/tcp — SIP (Session Initiation Protocol)**

* Purpose: VoIP signaling (call setup for SIP phones/softphones). Port 5060 usually uses UDP, but TCP is also possible. Filtered indicates firewall or device behaviour.
* Typical software: Asterisk, SIP phones, softswitches.

**135/tcp — MSRPC / RPC Endpoint Mapper**

* Purpose: Windows RPC service (used to locate RPC services like DCOM, Netlogon endpoints).
* Typical on: Windows hosts, networked printers, file servers.

**139/tcp — NetBIOS-SSN**

* Purpose: NetBIOS session services (legacy Windows file/printer sharing and name service).
* Typical on: older Windows SMB or devices exposing NetBIOS.

**445/tcp — Microsoft-DS / SMB over TCP**

* Purpose: Modern Windows file and printer sharing (SMB); also used for domain services and many remote operations.
* Typical software: Microsoft SMB server, Samba on Linux.

**666/tcp — Unknown (non-standard)**

* Purpose: Not reserved for a single common service — could be a proprietary service or misconfigured app. Needs investigation.
* Action: Identify service with -sV or banner grab.

**7070/tcp — RealServer / Streaming / Alternate HTTP**

* Purpose: Often used by streaming/media servers (RealServer/RTSP-like), sometimes by web services on alternate ports (or RealNetworks servers).
* Typical software: older RealMedia servers, custom streaming apps.

**2) Security risks for each open port & why they matter**

**SSH (22)**

* **Risks**: Brute-force or credential-guessing attacks, weak passwords, outdated OpenSSH vulnerabilities (rare but possible), exposed SSH with password auth increases risk of account compromise.
* **Impact**: Full system compromise or lateral movement if attacker gains credentials.
* **Mitigation**: Use key-based auth only, disable password auth, restrict allowed users, change default port (optional), enable fail2ban/connection rate limits, keep software updated.

**DNS (53)**

* **Risks**: DNS cache poisoning (if server misconfigured), zone transfer (AXFR) exposing internal hostnames if misconfigured, software vulnerabilities in DNS server.
* **Impact**: Traffic interception, reconnaissance, domain/host disclosure.
* **Mitigation**: Disable zone transfers to unauthorized IPs, use access controls, run DNS only on intended authoritative hosts, patch server.

**HTTP (80)**

* **Risks**: Exposed web admin panels with default/weak credentials, unencrypted traffic leaking credentials/sessions, outdated web server or web app vulnerabilities (RCE, XSS, SQLi).
* **Impact**: Credential theft, admin takeover, remote code execution.
* **Mitigation**: Disable or limit web admin to LAN or trusted IPs, apply HTTPS (TLS) for web interfaces, change default creds, patch web server and device firmware.

**UPnP / SSDP (1900/udp)**

* **Risks**: UPnP can auto-open router ports, allowing external exposure of internal services. Many devices implement UPnP insecurely; vulnerabilities allow lateral control or port mapping exploitation.
* **Impact**: Unexpected internet exposure of internal services, remote exploitation.
* **Mitigation**: Disable UPnP on router if not needed; if needed, restrict to trusted devices or segment IoT devices on guest network.

**SIP (5060)**

* **Risks**: SIP servers with default credentials or lack of authentication can be abused for toll fraud, call interception, or DDoS. SIP messages in cleartext can leak sensitive call metadata.
* **Impact**: Financial loss, privacy breaches, service disruption.
* **Mitigation**: Use SIP over TLS (SIPS) if possible, restrict signaling to trusted IPs, require strong auth, monitor for anomalous call traffic.

**MSRPC (135), NetBIOS (139), SMB (445)**

* **Risks**: SMB & NetBIOS historically have had many severe vulnerabilities (e.g., EternalBlue, SMBv1 issues), exposure leads to remote code execution, credential theft (NTLM relay/hashes), and ransomware propagation.
* **Impact**: High — lateral movement, file theft, ransomware.
* **Mitigation**: Disable SMBv1, restrict SMB to necessary hosts, apply patches, use firewall to block 139/445 from untrusted networks, enable SMB signing where possible, enforce strong credentials and principle of least privilege.

**Unknown service (666)**

* **Risks**: Unknown services are dangerous because they may be unpatched, custom, or misconfigured and could have vulnerabilities or default credentials.
* **Impact**: Varies — could be low to critical depending on service.
* **Mitigation**: Identify the service (nmap -sV, banner grab, connect with nc), research it, patch/remove if unnecessary.

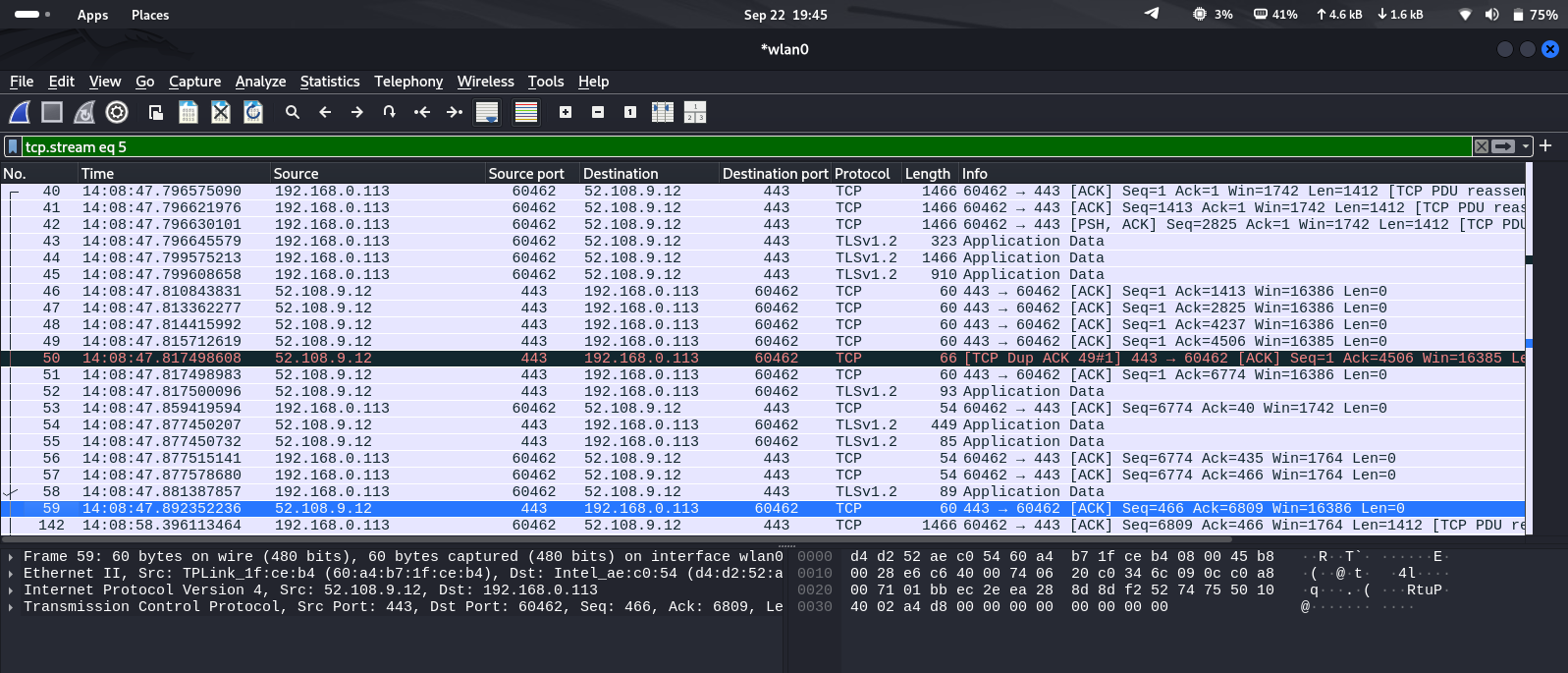
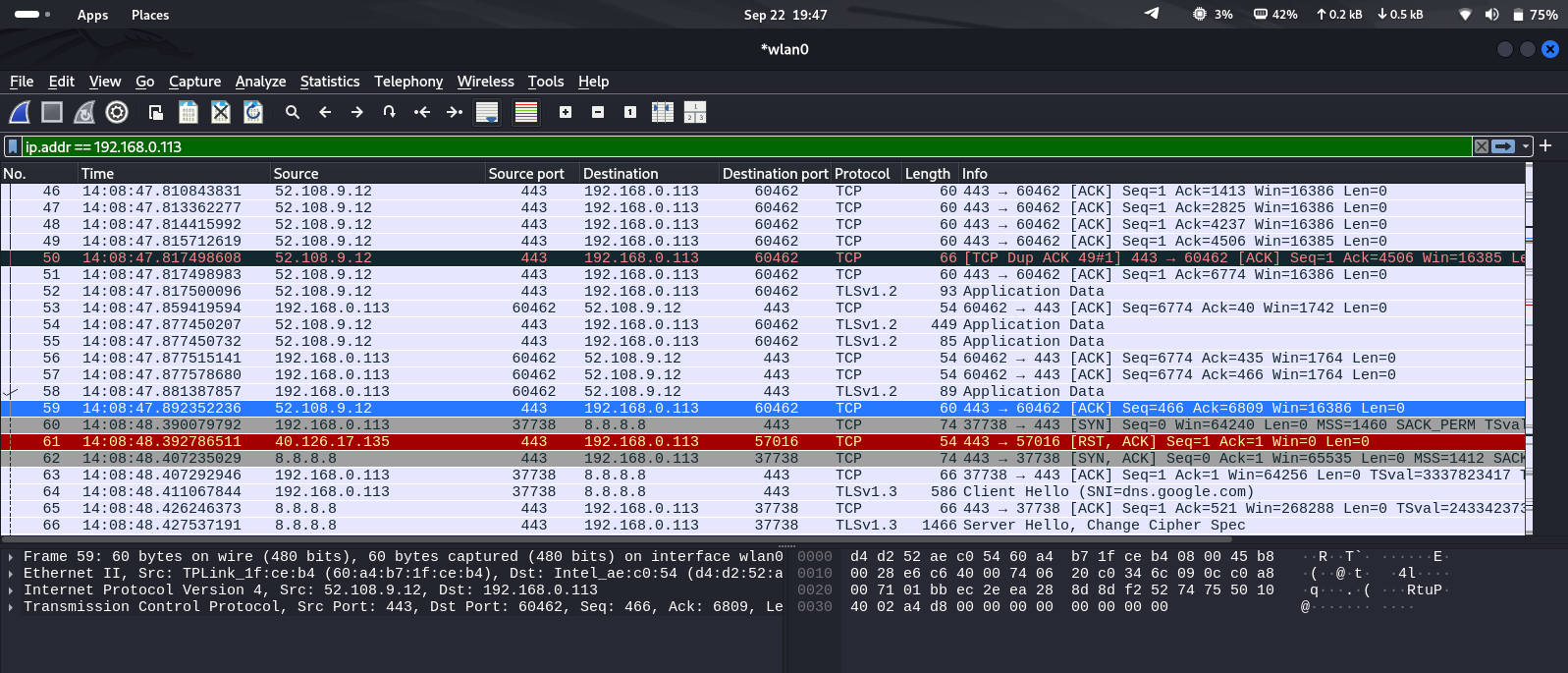
**Wireshark — Packet Analyzer**

**Definition:**  
Wireshark is a graphical, open-source network protocol analyzer that captures and inspects packets on a network interface, letting you examine protocol-level details and conversations between hosts.

**Primary Purpose:**  
Deep packet-level analysis to troubleshoot network issues, investigate suspicious traffic, or validate what a service/scan actually transmits and receives.

**Common Use-Cases**

* Capture and inspect TCP/UDP/ICMP and application-layer protocols (HTTP, DNS, SMB, SIP, etc.)
* Follow TCP streams to view full request/response payloads
* Analyze malformed packets, retransmissions, or suspicious behavior
* Extract files or credentials from unencrypted traffic (for testing only)



These screenshots show a Wireshark capture session analyzing network traffic involving the IP address 192.168.0.113, focusing on TCP and TLSv1.2 protocols, with detailed packet information displayed for forensic inspection.

**Key Features of the Session**

* The Wireshark interface highlights captured packets between source and destination IPs, including packet number, time, protocol, length, and info fields with sequence and acknowledgment numbers.
* Filters like "ip.addr==192.168.0.113" and "tcp.stream==5" are set, narrowing the displayed traffic to relevant packets for investigation.
* The lower pane shows decoded packet details down to the byte level, aiding protocol and payload examination for digital forensics.