

# Task 1: Scan Your Local Network for Open Ports

Local IP address range 192.168.0.119/24

Command used sudo apt scan -l

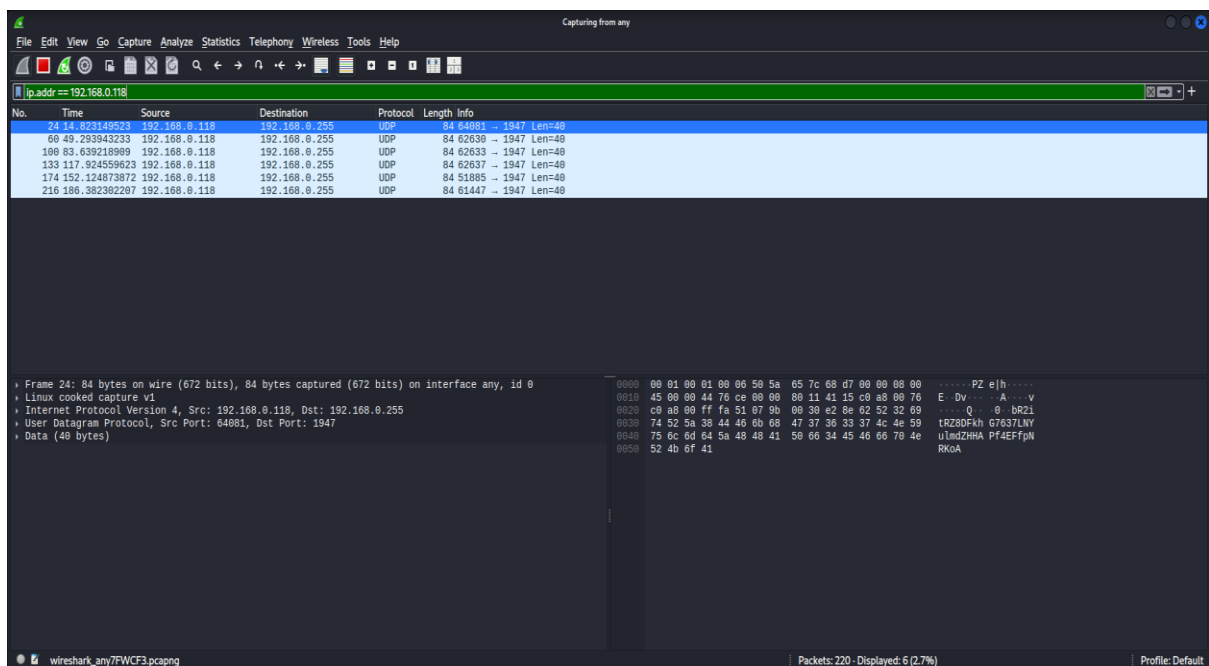
Run: nmap -sS 192.168.0.118

```
shish@kali: ~  
Session Actions Edit View Help  
TRACEROUTE  
HOP RTT ADDRESS  
1 215.25 ms 192.168.0.117  
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 243.33 seconds  
  
shish@kali:~$ sudo arp-scan -l  
Interface: eth0, type: EN10MB, MAC: 08:00:27:2c:24:7b, IPv4: 192.168.0.119  
WARNING: Cannot open MAC/Vendor file ieee-oui.txt: Permission denied  
WARNING: Cannot open MAC/Vendor file mac-vendor.txt: Permission denied  
Starting arp-scan 1.10.0 with 356 hosts (https://github.com/royhills/arp-scan)  
192.168.0.1 7a:fc:ce:b1:05:75 (Unknown)  
192.168.0.100 9c:a2:fa:37:7c:fd (Unknown)  
192.168.0.181 f8:b6:d2:5e:9f:7e (Unknown)  
192.168.0.118 50:5a:65:7c:68:d7 (Unknown)  
192.168.0.109 da:08:5a:39:18:f8 (Unknown: locally administered)  
  
5 packets received by filter, 0 packets dropped by kernel  
Ending arp-scan 1.10.0: 256 hosts scanned in 2.180 seconds (117.43 hosts/sec). 5 responded  
  
shish@kali:~$  
$ nmap -sS 192.168.0.118  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-28 21:55 IST  
Nmap scan report for 192.168.0.118  
Host is up (0.00077s latency).  
Not shown: 999 filtered tcp ports (no-response)  
PORT STATE SERVICE  
3306/tcp open mysql  
MAC Address: 50:5A:65:7C:68:D7 (AzureWave Technology)  
Nmap done: 1 IP address (1 host up) scanned in 12.09 seconds  
  
shish@kali:~$  
$ nmap -sS 192.168.0.181  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-28 21:56 IST  
Nmap scan report for 192.168.0.181  
Host is up (0.0035s latency).  
All 1000 scanned ports on 192.168.0.181 are in ignored states.  
Not shown: 1000 filtered tcp ports (no-response)  
MAC Address: F8:B4:D2:5E:9F:7E (D-LINK International)  
Nmap done: 1 IP address (1 host up) scanned in 32.95 seconds  
  
shish@kali:~$  
$ nmap -sS 192.168.0.100  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-28 21:57 IST  
Nmap scan report for 192.168.0.100  
Host is up (0.011s latency).
```

Find the open port 3306 - mysql

## Analyzing a packet capture using Wireshark

Here used packet filtering to capture the packet using wireshark.



**Open Port:** 3306 (MySQL Database Service)

**Risk Level:** High (if accessible externally)

**Potential Threats:** Unauthorized data access, brute-force attacks, SQL injection through exposed DB, data interception.

**Recommendations:** Restrict access, enable encryption, apply authentication hardening, and regularly patch MySQL.