Ethical Hacking of Wifi Networks Using Raspberry Pi and Kali Linux

In this project, our goal is to understand the concepts of **ethical hacking** and **Wi-Fi network security**. We'll use a **Raspberry Pi** running **Kali Linux** and an external **USB Wifi adapter** to perform ethical penetration testing on Wi-Fi networks. This project will help you understand how to identify and secure vulnerabilities in Wi-Fi networks.

Materials Required

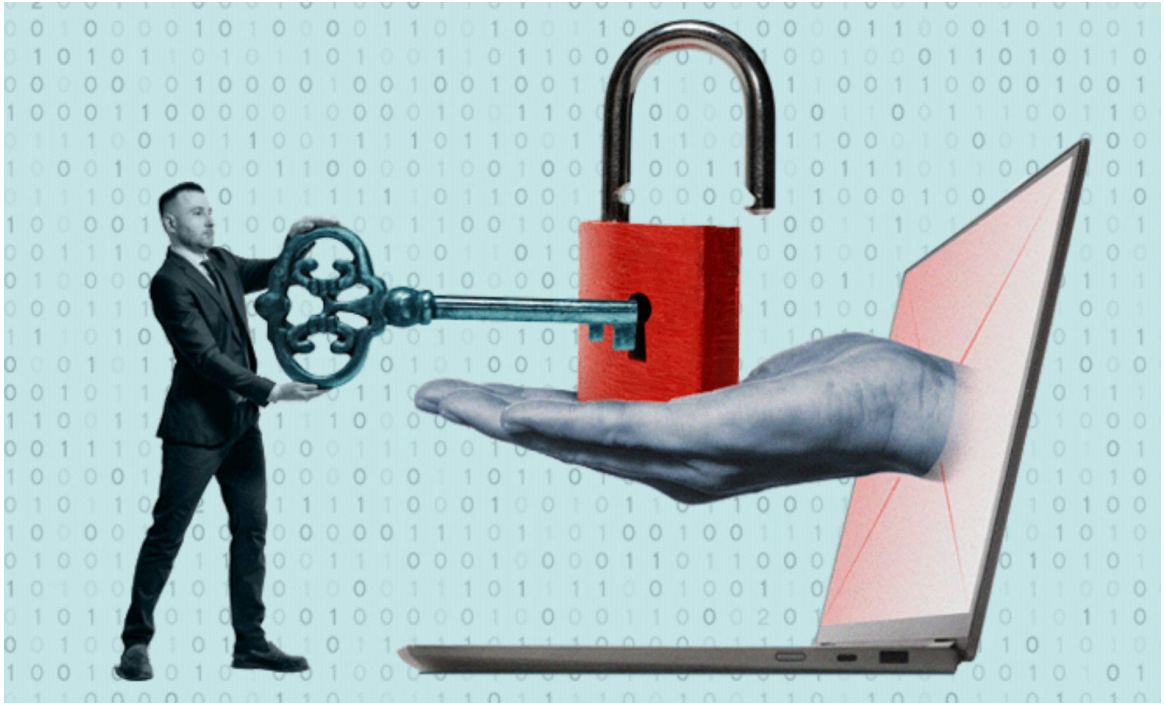
- **Raspberry Pi**
- **MicroSD Card**
- **USB Wifi Adapter** that supports

  Monitor Mode and **Packet Injection**

- **Keyboard, Mouse, and Monitor**

  (for setting up the Raspberry Pi)

- **Internet Connection**
- **Kali Linux** image for Raspberry Pi



Disclaimer

This document DOES NOT promote or encourage any illegal activities!

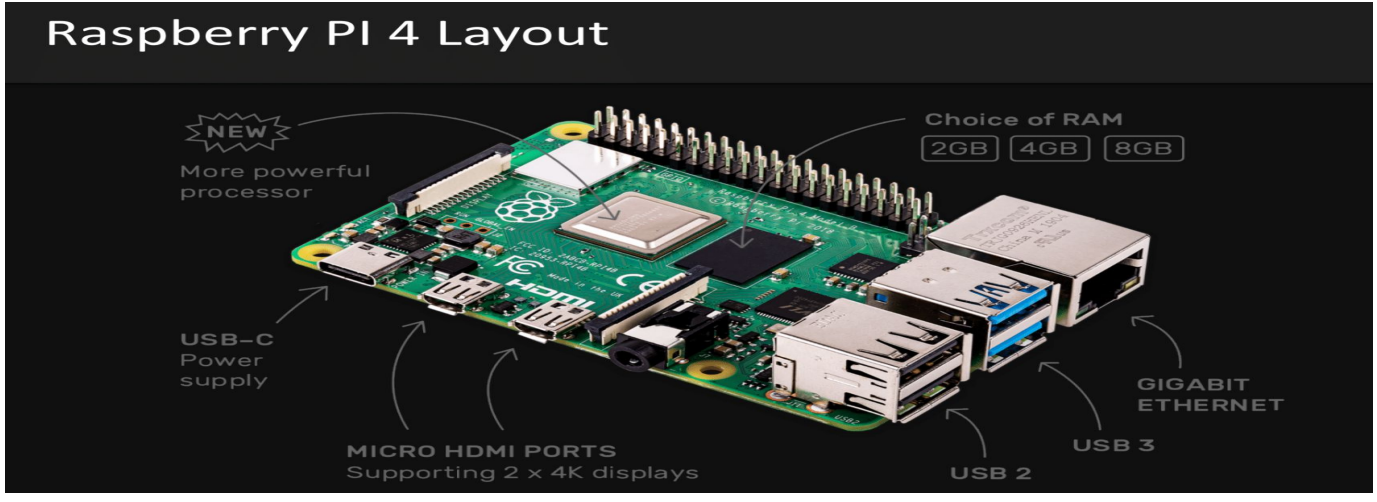
The content in this document is provided solely for educational purposes and to create awareness!

WARNING!

Overview of Kali Linux and Raspberry Pi

Kali Linux and Raspberry Pi for Security Testing

- **Kali Linux**: A penetration testing operating system with built-in tools for Wi-Fi network analysis.
- **Raspberry Pi**: A small, affordable computer that can run Kali Linux for ethical hacking purposes.
    - Ideal for portability and hands-on testing.
    - Great for setting up penetration testing labs.



What is Ethical Hacking?

Ethical Hacking: Testing with Permission

- **Definition**: Conducting authorized tests to find vulnerabilities.
- **Purpose**: Help network owners fix weaknesses before malicious hackers exploit them.
- **Legal Considerations**: Always obtain explicit permission before testing someone else's network.

Tools Used in Ethical Wifi Hacking

- **Fern-wifi-cracker** is a Wireless security auditing and attack software program written using the Python Programming Language and the Python Qt GUI library. The program is able to crack and recover WEP/WPA/WPS keys and also run other network based attacks on wireless or ethernet based networks
- **Wifite** is an automated tool for auditing wireless networks. It streamlines the process of cracking WEP, WPA, WPA2, and WPS-protected networks, leveraging tools like **aircrack-ng**, **reaver**, and **hashcat**. It's designed for ethical hacking and penetration testing, helping users find and exploit vulnerabilities in wireless networks.

Kali Linux in Raspberry Pi

Step 1: Download Kali Linux

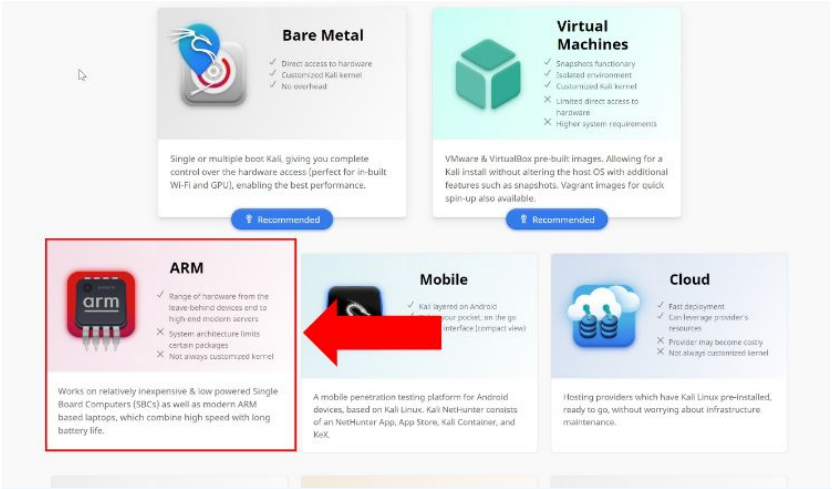
1. Go to the official **Kali Linux** website: https://www.kali.org/get-kali/ and download the image specifically for **Raspberry Pi**.
2. Choose the appropriate image based on your **Raspberry Pi model**.

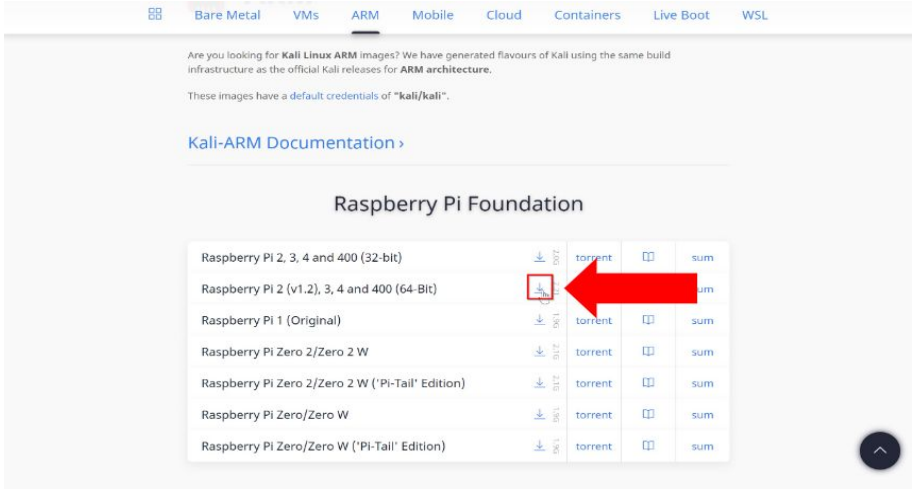
Step 2: Flash the Image to the MicroSD Card

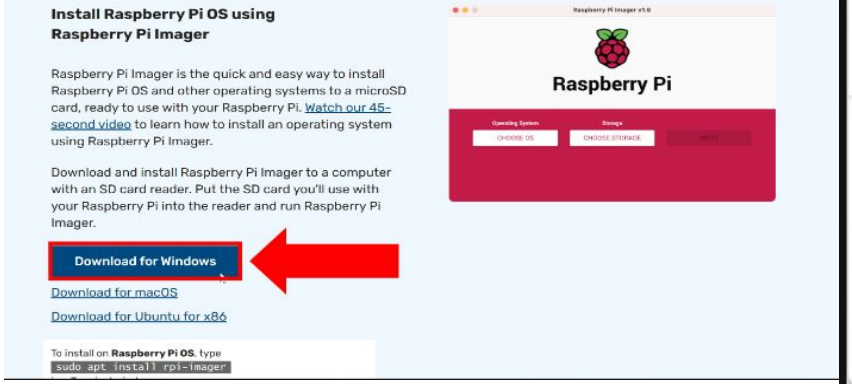
1. Use **Raspberry Pi Imager** to write the Kali Linux image to your **MicroSD card**:
    - In **Raspberry Pi Imager**, select **Kali Linux** image, choose the **SD card**, and click **Write**.

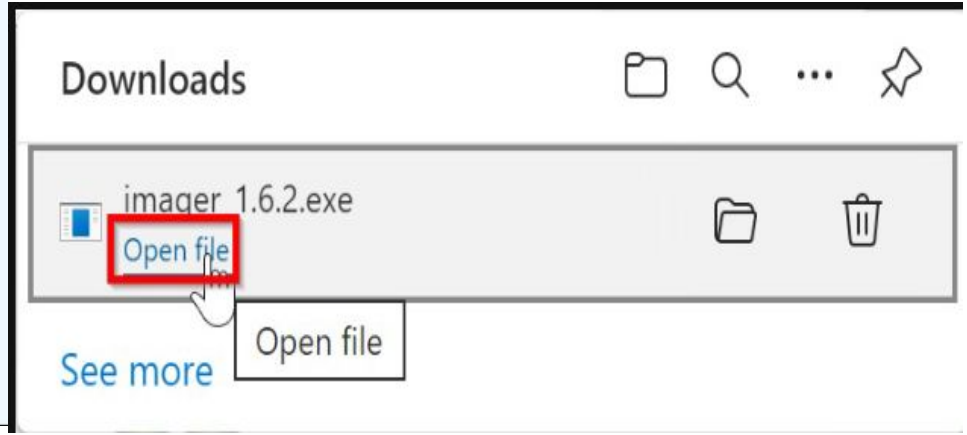
Step 3: Boot the Raspberry Pi

1. Insert the **MicroSD card** into the Raspberry Pi, then connect the **keyboard**, **mouse**, and **monitor**.
2. Power on the Raspberry Pi, and it will boot into Kali Linux.
3. Follow the on-screen instructions to set up your **username**, **password**, and **Wi-Fi settings**.


Bare Metal
Direct access to hardware
Customized Kali kernel
No overhead
Single or multiple boot Kali, giving you complete control over the hardware access (perfect for in-built Wi-Fi and GPU), enabling the best performance.
Recommended
Virtual Machines
Snapshots functionary
Isolated environment
Customized Kali kernel
Limited direct access to hardware
Higher system requirements
VMware & VirtualBox pre-built images. Allowing for a Kali install without altering the host OS with additional features such as snapshots. Vagrant images for quick spin-up also available.
Recommended
ARM
Range of hardware from the leave-behind devices end to high-end modern servers
System architecture limits certain packages
Not always customized kernel
Works on relatively inexpensive & low powered Single Board Computers (SBCs) as well as modern ARM based laptops, which combine high speed with long battery life.
Mobile
A mobile penetration testing platform for Android devices, based on Kali Linux. Kali NetHunter consists of an NetHunter App, App Store, Kali Container, and KeX.
Cloud
Fast deployment
Can leverage provider's resources
Provider may become costly
Not always customized kernel
Hosting providers which have Kali Linux pre-installed, ready to go, without worrying about infrastructure maintenance.


Bare Metal
VMs
ARM
Mobile
Cloud
Containers
Live Boot
WSL
Are you looking for Kali Linux ARM images? We have generated flavours of Kali using the same build infrastructure as the official Kali releases for ARM architecture.
These images have a default credentials of "kali/kali".
Kali-ARM Documentation ›
Raspberry Pi Foundation
Raspberry Pi 2, 3, 4 and 400 (32-bit)
Raspberry Pi 2 (v1.2), 3, 4 and 400 (64-Bit)
Raspberry Pi 1 (Original)
Raspberry Pi Zero 2/Zero 2 W
Raspberry Pi Zero 2/Zero 2 W ('Pi-Tail' Edition)
Raspberry Pi Zero/Zero W
Raspberry Pi Zero/Zero W ('Pi-Tail' Edition)
torrent
sum


Install Raspberry Pi OS using Raspberry Pi Imager
Raspberry Pi Imager is the quick and easy way to install Raspberry Pi OS and other operating systems to a microSD card, ready to use with your Raspberry Pi. Watch our 45-second video to learn how to install an operating system using Raspberry Pi Imager.
Download and install Raspberry Pi Imager to a computer with an SD card reader. Put the SD card you'll use with your Raspberry Pi into the reader and run Raspberry Pi Imager.
Download for Windows
Download for macOS
Download for Ubuntu for x86
To install on Raspberry Pi OS, type
sudo apt install rpi-imager
Raspberry Pi
CHOOSE OS
CHOOSE STORAGE


Downloads
imager_1.6.2.exe
Open file
Open file
See more

Installing Wi-fi Hacking Tools

To perform Wifi penetration testing, we need several tools. Fortunately, Kali Linux comes with many pre-installed, but you may need to install or update some additional tools.

- **Install Aircrack-ng -** Aircrack-ng is one of the most commonly used tools for **cracking WPA/WPA2** passwords through capturing handshakes.
- **Install Reaver -** Reaver exploits **WPS vulnerabilities** to recover the WPA password.
- **Install Wireshark-** Wireshark is a network protocol analyzer, which can capture packets and help you analyze network traffic.
- **Install PixieWPS -** PixieWPS can be used to recover WPS PINs offline after capturing the handshake.

Configuring the Wi-Fi Adapter

To use your Wi-Fi adapter for penetration testing, it needs to be set to **Monitor Mode**, which allows it to capture all wireless packets.

1. Identify the Wi-Fi Adapter

Plug in your **USB Wifi adapter** and check the network interfaces:

Wi-Fi interface will be typically be `wlan0` or `wlan1`.

2. Enable Monitor Mode

1. Turn off the interface:
2. Set the interface to **Monitor Mode**:
3. Turn the interface back on:
4. Verify that the interface is in **Monitor Mode**:

Ethical Hacking Techniques

Capturing WPA/WPA2 Handshakes

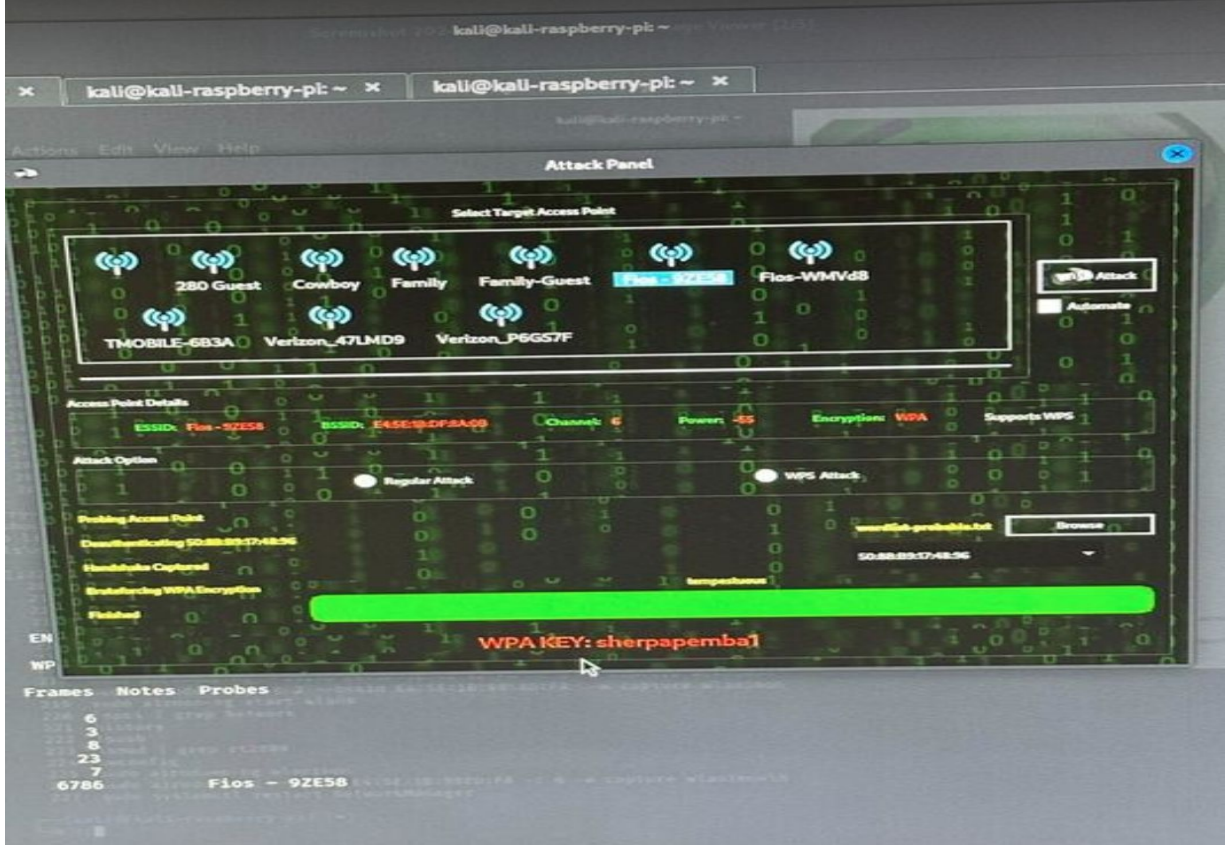
A **handshake** is a process that occurs when a device connects to a WPA or WPA2 secured Wi-Fi network. We can capture the handshake to later attempt to crack the password.

Scan for nearby Wi-fi networks
Capture the WPA handshake
Force a device to reconnect
If no handshake is captured, you can **deauthenticate** a device to force it to reconnect, capturing the handshake:
Crack the WPA password
Once the handshake is captured, you can attempt to crack the password

Exploiting WPS with Reaver

If the router supports **WPS (Wi-Fi Protected Setup)**, you can use **Reaver** to recover the WPA password by exploiting WPS vulnerabilities.

Run Reaver to attack WPS, Reaver will try to brute-force the **WPS PIN**, and once successful, it will reveal the WPA password.

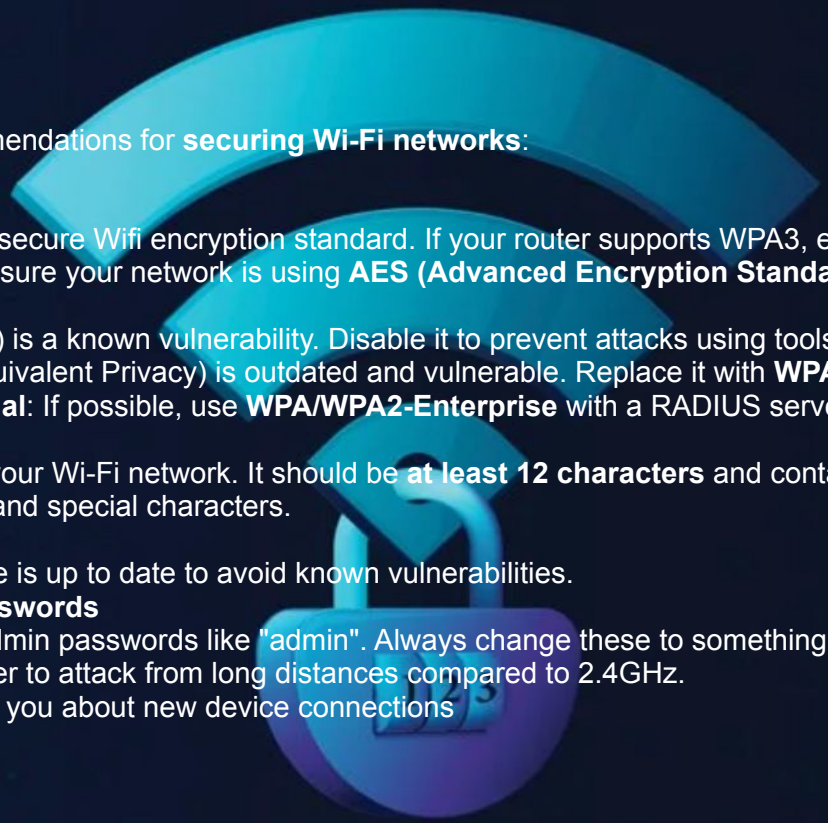

kali@kali-raspberry-pi: ~
kali@kali-raspberry-pi: ~
Attack Panel
Select Target Access Point
280 Guest
Cowboy
Family
Family-Guest
Fios-WMVd8
TMOBILE-6B3A
Verizon_47LMD9
Verizon_P6G57F
Attack
Automate
Access Point Details
Channel: 6
Power: -55
Encryption: WPA
Supports WPS
Attack Option
Regular Attack
WPS Attack
Browse
WPA KEY: sherpapemba1
Frames Notes Probes
6
3
8
23
7
6786 Fios - 9ZE58

Ethical Hacking Guidelines

Important Ethical Considerations

1. **Get Permission**:
   Always get explicit permission from the owner of the network before attempting any testing. Unauthorized access is illegal.
2. **Use Knowledge for Good**:
   Ethical hacking aims to identify and fix vulnerabilities, not to exploit them for malicious purposes.
3. **Stay Legal**:
   Only perform penetration testing on networks you own or have permission to test. Unauthorized hacking is against the law.

Securing Wi-Fi Networks



After testing, here are some recommendations for **securing Wi-Fi networks**:

1. **Use WPA3 Encryption**
   WPA3 is the latest and most secure Wifi encryption standard. If your router supports WPA3, enable it.
2. **Enable AES Encryption**: Ensure your network is using **AES (Advanced Encryption Standard)**
3. **Disable WPS**
   WPS (Wi-Fi Protected Setup) is a known vulnerability. Disable it to prevent attacks using tools like **Reaver**.
4. **Avoid WEP**: WEP(Wired Equivalent Privacy) is outdated and vulnerable. Replace it with **WPA3** or at least **WPA2**.
5. **Disable WPA/WPA2-Personal**: If possible, use **WPA/WPA2-Enterprise** with a RADIUS server for authentication.
6. **Use Strong Passwords**
   Set a **strong password** for your Wi-Fi network. It should be **at least 12 characters** and contain a mix of uppercase and lowercase letters, numbers, and special characters.
7. **Update Router Firmware**
   Ensure your router's firmware is up to date to avoid known vulnerabilities.
8. **Change Default Admin Passwords**
   Many routers have default admin passwords like "admin". Always change these to something secure.
9. Use 5GHz frequency is harder to attack from long distances compared to 2.4GHz.
10. Configure your router to alert you about new device connections

Conclusion

In this project, we gained hands-on experience in using Kali Linux on a Raspberry Pi to assess and test the security of Wi-Fi networks. We learned how to effectively utilize a range of powerful penetration testing tools, such as Fern-wifi-cracker , WIFITE, Aircrack-ng, Reaver, and Wireshark, to perform comprehensive network analysis and identify vulnerabilities. Specifically, we explored techniques for capturing and cracking WPA handshakes, exploiting weaknesses in the Wi-Fi Protected Setup (WPS) protocol, and analyzing network traffic to better understand how data flows over wireless connections. Through this process, we not only developed practical skills for ethical hacking but also gained a deeper understanding of the potential security risks that exist in wireless networks. Furthermore, we examined best practices and methods to help secure Wi-Fi networks against common attacks, improving our ability to both identify security flaws and implement effective countermeasures.

Key Takeaways:

- Ethical hacking is about identifying and securing vulnerabilities, not exploiting them.
- Always get **permission** before testing any network.
- Use strong security measures like **WPA3** with **SEA** encryption**,** use **strong passwords** or Unique wi-fi password, and **disabled WPS** and **WES** to protect your network.
- Configure the Router to alert about new device connections.