Wireless Network Security Audit

Presenting Shashank, Sai Prasad
2320030343@klh.edu.in,2320030349@klh.edu.in

February 6, 2025

Abstract

This project is about testing the security of wireless networks using Kali Linux, a system designed for cybersecurity tasks. The aim is to know how secure Wi-Fi networks are by capturing and analyzing network data to find possible weaknesses.

How the Project Works:

- Setting Up the System – A special wireless adapter is used in monitor mode so it can capture Wi-Fi signals around it.
- Scan Networks – The program airodump-ng scans for and lists any available Wi-Fi networks and lists important details about them, including network names and security settings.
- Capture Login Credentials – In terms of security research, the project captures a WPA/WPA2 handshake-an exchange of data when a device connects to the Wi-Fi network.
- Force Devices to Reconnect – Aireplay-ng uses a simulated attack to temporarily take devices off a Wi-Fi connection, causing the devices to reconnect and generate a handshake.
- Analyzing the Data – It is checked that the handshake that was captured correctly recorded in the Wireshark. Then the Aircrack-ng is employed to test the strength of password by trying several possibilities from the wordlist.
- Restoring the Network – This time, once the test was over, it is switched to normal mode because there should be no more disconnections.

Why This Project Matters

It teaches how attackers will exploit weak Wi-Fi security. It emphasizes the need for strong encryption and passwords. It teaches practical ways to protect wireless networks from unauthorized access.