ESP32 Security Testing Toolkit

A research project from the Department of Computer Science & Engineering

Indian Institute of Technology Jammu

Important Notice: This tool is intended for educational purposes and authorized security testing only. Unauthorized use may violate laws and regulations.

Project Supervision

Dr. Gaurav Varshney
Professor & Project Advisor
Department of Computer Science & Engineering

Ms. Rina Mishra
Teaching Assistant
Department of Computer Science & Engineering

Tool Capabilities

- **Network Discovery:** Scan and identify nearby wireless networks
- **Deauthentication Testing:** Assess network resilience against disconnection attacks
- **Security Analysis:** Evaluate WPA2 security strength (in development)
- **Persistent Testing Mode:** Continuous security assessment capability

Initial Setup Instructions

1. Power the ESP32 device using a USB cable or battery source
2. Wait for the device to initialize (LED indicator will show status)
3. Locate and connect to the wireless network `Rohit Wi-Pi`
4. Use the password `Rohit@123` when prompted
5. Open a web browser and navigate to `http://192.168.4.1`
6. Authenticate with the credentials provided by your administrator

Network Resilience Testing

1. From the web interface, select a target network from the discovered list
2. Choose `DOS` from the assessment type dropdown
3. Select `DEAUTH_ALL_CHANNELS` as the testing method
4. Set the duration (in seconds) for the assessment in the timeout field
5. Click **Begin Assessment** to start the test
6. Monitor the results in real-time through the interface

Security Protocol Analysis

1. Select a target network from the discovered list
2. Choose `HANDSHAKE` from the assessment type dropdown
3. Select either `Caputre Only Pasive` or `Deauth Passive` method
4. Set the desired duration for the capture process
5. Click **Begin Capture** to start the process
6. After completion, download the generated capture file
7. Analyze the results using security tools with this command:
   `aircrack-ng -w wordlist.txt -b TARGET_BSSID -e NETWORK_NAME capture.pcap`

Development Team

Team Member	ID
Rohit Tiwari	2024PCS0036
Uttam Patel	2024PCS0042