Exploring WiFi Security Using ESP8266

Deauthentication & Evil Twin Attacks — Learning Through Hands-On Cybersecurity

Presented by:
Abdullah Khan
Inbisat Fayyaz
Adnan Aun Ali

Supervised by:
Sir Abdul Majid Jamil
Sir Muhammad Ammar
IBA — CICT

INTRODUCTION:

What is WiFi security?

Why is it important today?

Purpose of this experiment:

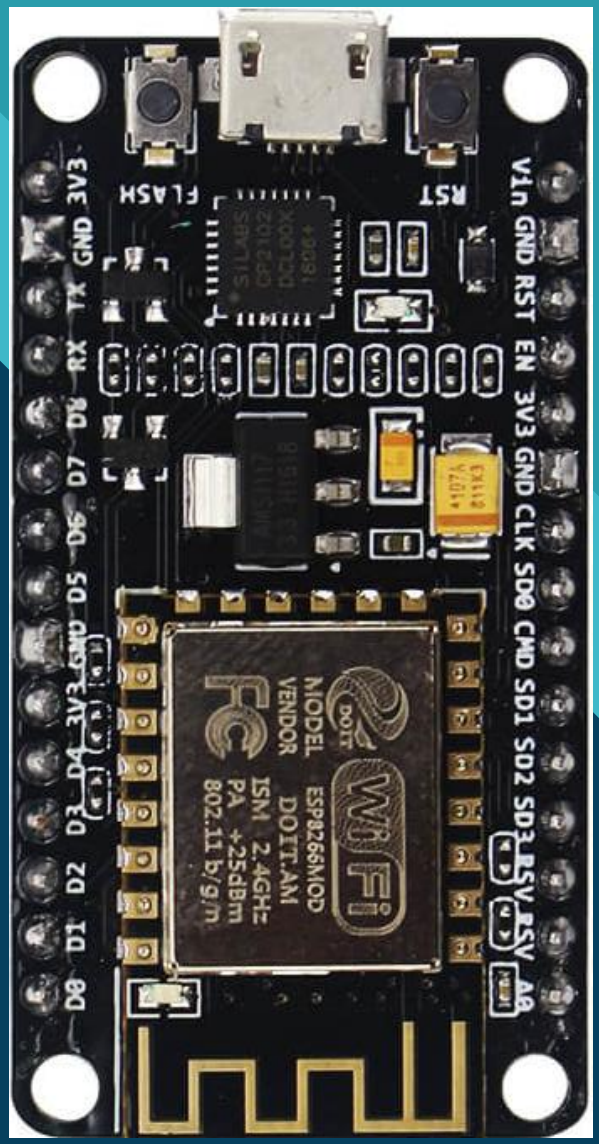
- To understand WiFi vulnerabilities
- To learn defensive measures
- To gain hands-on ethical hacking experience

Objectives of This Project:

- Understand ESP8266 packet handling
- Perform ethical WiFi security tests
- Study how attacks work
- Learn how to prevent these attacks
- Build foundational cybersecurity skills

What is ESP8266?

- Low-cost WiFi microcontroller
- Can send/deauth packets
- Can host fake AP (Evil Twin)
- Used widely in IoT security research



LAB SETUP

=> Devices used (2 ESP8266,2 Cables Laptop, Mobile)

=> Arduino IDE (For Integration on board)

=> WiFi network used (our own network)

Ethical rules followed:

✓ Only own WiFi

✓ Lab environment

✓ No third-party devices

Attack 1: Deauthentication Attack

- **Definition:**
  Disconnecting users by sending deauth frames.
- **Why it matters:**

  Can disrupt internet

  Used in advanced attacks

  Basis of Evil Twin attacks

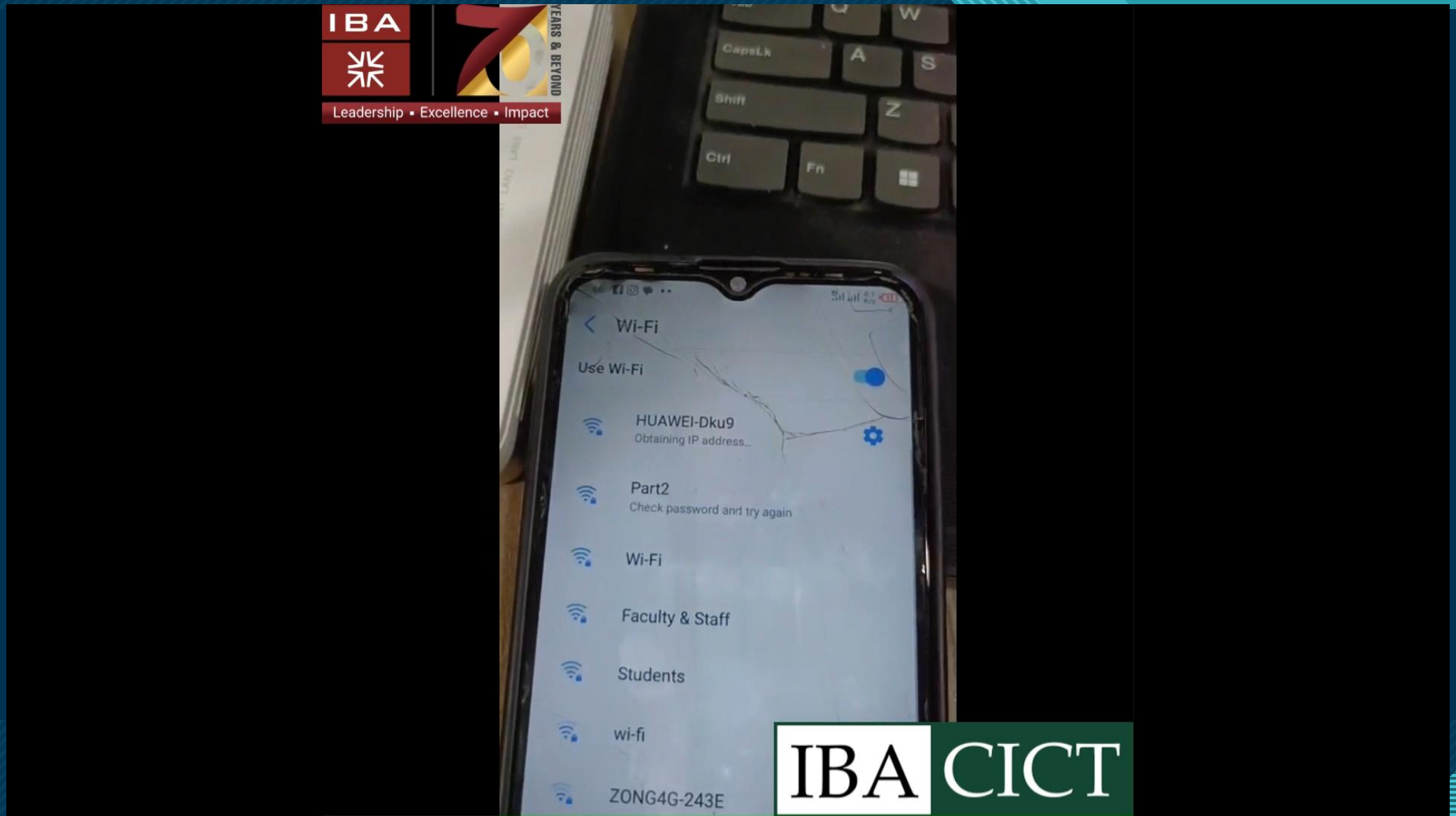
How We Performed the Deauth Test

Attack 2: Evil Twin Attack

- **Definition:**
  Creating a fake WiFi network that looks identical to the original to steal credentials.

- **Why dangerous:**
- Users connect accidentally
- Credentials can be captured
- Used in phishing & MITM attacks

How We Performed the Evil Twin Test



Thank You

Any Questions?