
PROJECT REPORT

EVIL TWIN
ESP8266 D1 MINI

Submitted by Dhanish

Table of Contents

INTRODUCTION AND STATEMENT OF CONFIDENTIALITY	3
DISCLAIMER	4
EXECUTIVE SUMMARY	5
APPROACH	6
SCOPE	7
OVERVIEW	8
PROJECT GOALS AND OBJECTIVES	9
COMPONENT	10
• ESP8266 D1 MINI	
• POWER INPUT OPTIONS	
TP4056 BATTERY CHARGING MODULE CONNECTION	11
SOFTWARE REQUIREMENTS AND INSTALLATION	12
• ARDUINO IDE	
• SOURCE CODE	
• HARDWARE	
OPERATION	15
WORKING MECHANISM OF THE EVIL TWIN ATTACK	16
STEPS TO EXECUTE THE EVIL TWIN ATTACK SIMULATION	17
RESULT AND OBSERVATION	21
DEFENSES AGAINST EVIL TWIN ATTACKS	22
MITIGATION STRATEGIES	23
DETECTION OF EVIL TWIN ATTACKS	25
FAKE WEB PAGE IMPLEMENTATION	26
CONCLUSION	27

INTRODUCTION AND STATEMENT OF CONFIDENTIALITY

With the growing reliance on wireless networks in today's interconnected world, ensuring Wi-Fi security has become a critical priority. Despite advancements in encryption protocols and authentication methods, vulnerabilities persist, particularly through attacks that exploit user trust in open or unsecured networks. One such threat is the Evil Twin attack, where a rogue access point mimics a legitimate Wi-Fi network, deceiving users into connecting.

This project explores the use of the ESP8266 D1 Mini, a compact and cost-effective microcontroller, to simulate an Evil Twin attack. By leveraging libraries like ESP8266WiFi, DNSServer, and ESP8266WebServer, the D1 Mini can create a rogue network, serve fake login pages, and intercept user credentials. The aim is to raise awareness about Wi-Fi vulnerabilities, educate users on proactive security measures, and contribute to the development of robust network defenses.

This project is designed solely for educational, research, and cybersecurity purposes, adhering strictly to applicable laws, ethical guidelines, and industry standards. All activities are conducted in controlled environments or with prior, explicit consent from network owners. There is no intent for unauthorized access, data theft, or malicious behavior.

Any data collected during testing or demonstrations is handled with the utmost confidentiality, retained only for educational purposes, and securely discarded afterward. Ethical conduct is maintained throughout the project's lifecycle, ensuring compliance with all legal and moral standards. This approach highlights the importance of cybersecurity awareness while ensuring ethical and responsible practices in addressing wireless network vulnerabilities.

DISCLAIMER

This project is strictly for cybersecurity research and education, aiming to demonstrate Wi-Fi vulnerabilities and to promote secure practices. All activities must comply with local and international laws. Any unauthorized misuse or unethical application of this project's tools or methodologies is not endorsed and will be the sole responsibility of the user. Participants agree to act lawfully and responsibly during all stages of implementation and testing.

EXECUTIVE SUMMARY

This project explores the vulnerabilities of wireless networks through the simulation of an Evil Twin attack using the ESP8266 D1 Mini microcontroller. The Evil Twin attack mimics legitimate Wi-Fi networks to deceive users into connecting, allowing attackers to intercept credentials and sensitive data. By leveraging this demonstration, the project raises awareness of Wi-Fi risks, educates on proactive security measures, and promotes the development of detection and mitigation strategies. Key outcomes include understanding the attack's mechanics, its limitations, and defenses, ensuring the emphasis on user safety and network security practices.

APPROACH

The project adopts a structured approach to simulate and analyze Evil Twin attacks. Hardware and software configurations allow the ESP8266 D1 Mini to mimic legitimate networks and serve deceptive content to connected devices. Through simulation, the vulnerabilities in Wi-Fi security are exposed, and effective defense mechanisms like strong encryption, VPNs, and proactive network monitoring are evaluated. This structured methodology not only highlights risks but also emphasizes user awareness and cybersecurity enhancements.

1. **Hardware Implementation:** The ESP8266 D1 Mini is configured to act as a rogue access point broadcasting a cloned SSID to mimic legitimate Wi-Fi networks.
2. **Software Configuration:** Libraries such as ESP8266WiFi, DNSServer, and ESP8266WebServer are utilized to redirect DNS traffic and serve a fake login page.
3. **Simulation and Testing:** The attack is demonstrated in controlled environments to analyse vulnerabilities and risks associated with such techniques.
4. **Défense Evaluation:** The project highlights mitigation strategies such as WPA3 encryption, VPNs, and network monitoring tools to safeguard against similar attacks.

SCOPE

This project aims to shed light on Wi-Fi vulnerabilities through the simulation of Evil Twin attacks. By employing the ESP8266 D1 Mini, it replicates real-world scenarios, enabling users to understand the risks associated with unsecured networks. The project serves as a training tool for cybersecurity professionals, focusing on the detection and mitigation of such attacks. All simulations are carried out in controlled environments to maintain ethical standards and uphold legal boundaries.

- **Demonstration of Mechanics:** The project reveals the working principles of Evil Twin attacks to highlight vulnerabilities in Wi-Fi networks.
- **Simulating Attacks:** Utilizes the ESP8266 D1 Mini to create realistic simulations, emphasizing risks in public and unsecured networks.
- **Education for Professionals:** Aims to train cybersecurity practitioners on detection and mitigation techniques for practical scenarios.
- **Ethical Boundaries:** Ensures all simulations are conducted within controlled environments and adhere to ethical guidelines.

Key Aspects of Scope
Explores Evil Twin attack mechanisms and Wi-Fi vulnerabilities.
Simulates real-world scenarios using the ESP8266 D1 Mini.
Provides cybersecurity training on detection and defines.
Maintains ethical and controlled implementation guidelines.

OVERVIEW

This project explores Wi-Fi vulnerabilities by simulating an Evil Twin attack using the ESP8266 D1 Mini microcontroller. In this attack, a rogue access point mimics legitimate Wi-Fi networks to exploit network weaknesses. By demonstrating how attackers can exploit these vulnerabilities, the project aims to help cybersecurity practitioners better understand the risks and enhance defence mechanisms. All activities are conducted in ethical, controlled environments, ensuring full compliance with relevant standards and regulations.

The ESP8266 D1 Mini successfully simulated an Evil Twin attack, exposing vulnerabilities of devices connecting to rogue networks. Observations highlighted that factors like proximity and modern device security warnings may limit the attack's success.

demonstrates how an ESP8266 D1 Mini can be utilized to create a rogue access point that impersonates a legitimate Wi-Fi network. By running custom code on the ESP8266 D1 Mini, the device broadcasts a cloned SSID identical to an existing network, deceiving nearby devices into connecting. Upon connection, the DNSServer library redirects DNS requests, and the ESP8266WebServer library serves a fake webpage, such as a login form, to simulate phishing scenarios and collect user input for demonstration purposes.

During testing, several devices connected to the rogue access point created by the ESP8266 D1 Mini without raising suspicion, effectively demonstrating the potential of an Evil Twin attack in controlled scenarios. Devices attempting to access websites or online services were redirected to a fake webpage, illustrating the significant risks to user data if such an attack were carried out maliciously. The D1 Mini performed reliably throughout the tests, maintaining stable operation with minimal interference from other nearby networks.

The project also highlighted key limitations of the attack. For instance, the attacker needs to be in close proximity to the targeted devices for effective execution, and many modern devices display security warnings when connecting to unsecured or unfamiliar networks, reducing the likelihood of unsuspecting connections.

PROJECT GOALS AND OBJECTIVES

The primary goals of this project are:

- To educate about Evil Twin attacks and demonstrate Wi-Fi security flaws.
- To simulate real-world scenarios using ESP8266 D1 Mini to create cost-effective solutions for understanding vulnerabilities.
- To inform better cybersecurity practices and develop strategies for detecting and mitigating such attacks.
- To raise awareness about network security risks.
- To educate on defensive measures against rogue networks.
- To utilize ESP8266 D1 Mini for realistic demonstrations.

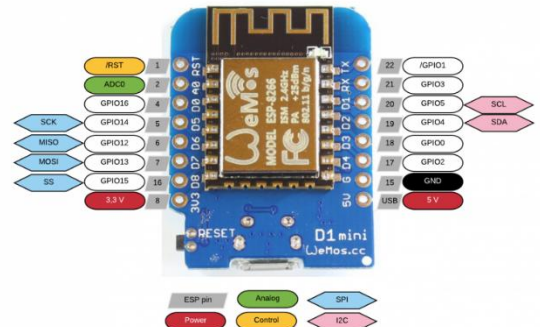
COMPONENTS

ESP8266 D1 Mini: The ESP8266 D1 Mini is the core hardware used in this project, offering powerful Wi-Fi capabilities to create rogue Wi-Fi networks and act as both a client and an access point. Its compact design, ease of programming, and versatility make it an ideal choice for penetration testing demonstrations.



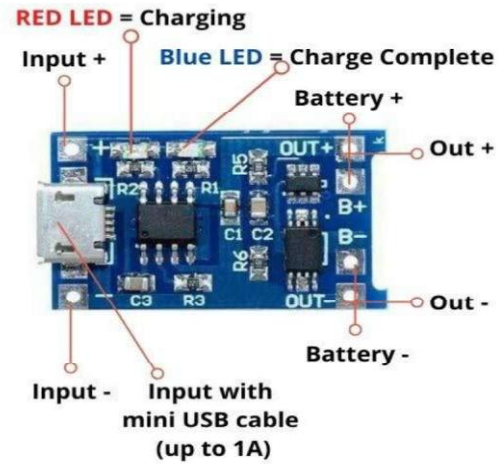
Power Input Options:

1. **Micro-USB Port:** The D1 Mini has a built-in voltage regulator and can be powered using a standard 5V USB adapter or a USB cable connected to a computer.
2. **Powering via the 5V and GND Pins with Battery:**
 - Battery Positive Terminal → 5V Pin
 - Battery Negative Terminal → GND Pin



(NOTE: USING A **TP4056** BATTERY CHARGING MODULE TO DIRECTLY POWER THE ESP8266 D1 MINI MAY DAMAGE THE BOARD. ENSURE PROPER VOLTAGE REGULATION AND CONNECTION TO AVOID DAMAGE.)

TP4056 BATTERY CHARGING MODULE CONNECTION



Wiring Steps:

1. Connect the Battery to the TP4056

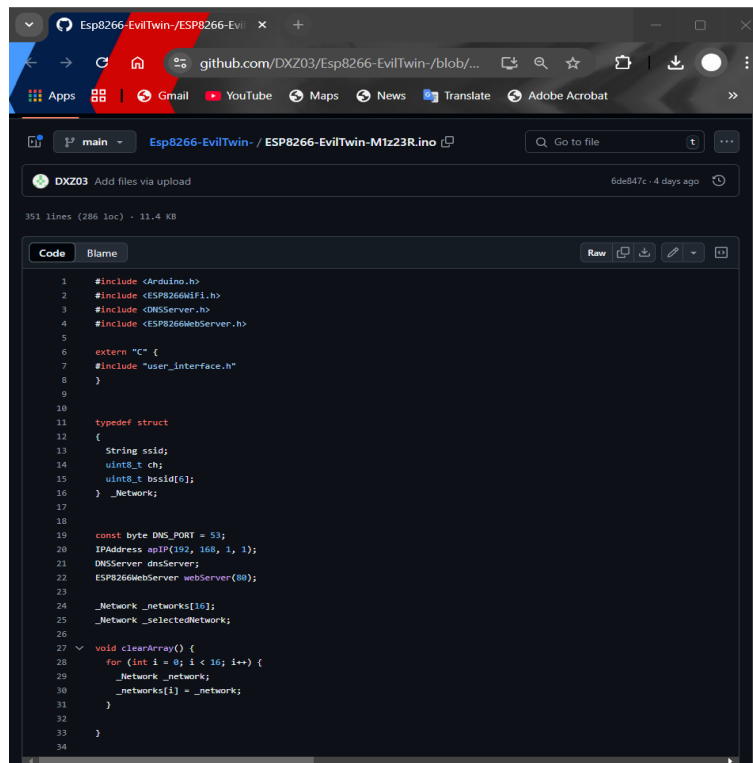
- **BAT+** on TP4056 → Positive terminal of the Li-Ion 3.7V battery.
- **BAT-** on TP4056 → Negative terminal of the Li-Ion 3.7V battery.

2. Powering the ESP8266 D1 mini

- Connect the **OUT+** of the TP4056 to the **5V/3.3V** pin of the ESP8266 D1 Mini.
- Connect the **OUT-** of the TP4056 to the **GND** pin of the ESP8266 D1 Mini.

SOFTWARE REQUIREMENTS AND INSTALLATION

- **Arduino IDE:**
 - Install and configure Arduino IDE with ESP8266 board support.
 - Used for programming and flashing code onto the ESP8266 D1 Mini.
- **Source Code:**
 - The Evil Twin source code can be accessed and downloaded [Link](#).



```
1 #include <Arduino.h>
2 #include <ESP8266WiFi.h>
3 #include <DNSServer.h>
4 #include <ESP8266WebServer.h>
5
6 extern "C" {
7 #include "user_interface.h"
8 }
9
10 typedef struct
11 {
12     String ssid;
13     uint8_t ch;
14     uint8_t bssid[6];
15 } _Network;
16
17
18
19 const byte DNS_PORT = 53;
20 IPAddress apIP(192, 168, 1, 1);
21 DNSServer dnsServer;
22 ESP8266WebServer webServer(80);
23
24 _Network _networks[16];
25 _Network _selectedNetwork;
26
27 void clearArray() {
28     for (int i = 0; i < 16; i++) {
29         _Network _network;
30         _networks[i] = _network;
31     }
32 }
33
34
```

- **Hardware:**
 - ESP8266 D1 Mini
 - USB cable for connection.

Installation Steps:

Step 1: Install Arduino IDE and ESP8266 Board Support

1. Download and install the Arduino IDE. <https://www.arduino.cc/en/software>
2. Add ESP8266 board support:
 - Open Arduino IDE and go to File > Preferences.
 - In "Additional Boards Manager URLs," add the following URL:
http://arduino.esp8266.com/stable/package_esp8266com_index.json
 - Go to Tools > Board > Boards Manager, search for "ESP8266," and install it.

Step 2: Install Required Libraries

1. Open Arduino IDE and go to Sketch > Include Library > Manage Libraries.
2. Install the following:
 - ESP8266WiFi.h: Provides WIFI connectivity for ESP8266.

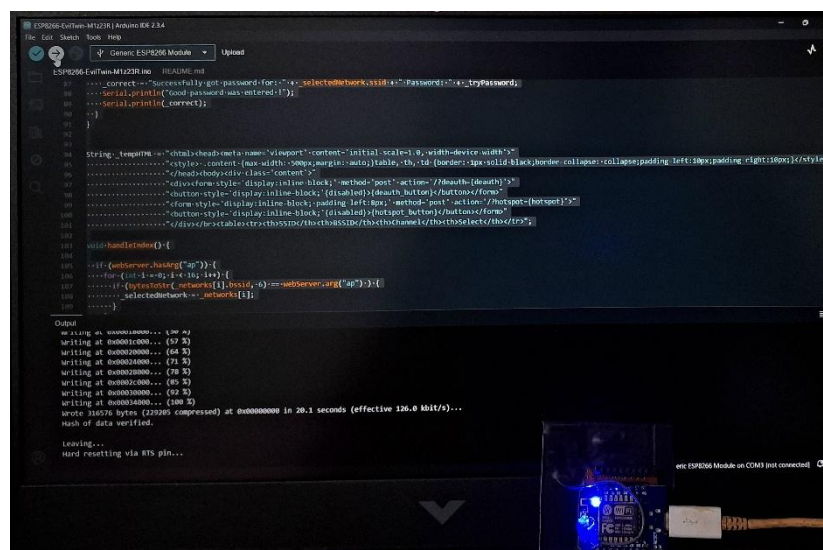
Step 3: Obtain the Source Code

1. Visit the GitHub Source Code and Download the Arduino file: [Link](#).
2. Open the file in Arduino IDE.

[illegible]

Step 4: Flash the source code onto the ESP8266 D1 Mini using Arduino IDE

1. Connect the ESP8266 D1 Mini to your computer using a USB cable.
2. In Arduino IDE, configure the following under Tools:
 - **Board:** Select **LOLIN(WEMOS) D1 R2 & Mini** (or appropriate ESP8266 model).
 - **Port:** Select the correct COM port.
 - **Flash Size:** Choose **4MB (1MB SPIFFS)**.
3. Click the **Upload** button to flash the code to the ESP8266 D1 Mini.



Step 5: Power Up and Test

1. Disconnect and reconnect the ESP8266 D1 Mini to power it on.
2. The ESP8266 will create a WIFI network with the configured SSID.
3. Connect a device to this network to simulate how the rogue access point operates.
 - This may include displaying a captive portal or fake login page, depending on the code's configuration.

OPERATION

Once configured, the ESP8266 D1 Mini broadcasts a cloned network SSID, attracting unsuspecting devices to connect. This setup enables controlled testing of data interception and spoofing methods, with system performance monitored using debugging tools.

The ESP8266 D1 Mini is configured with a custom Evil Twin attack script, using libraries such as **ESP8266WiFi**, **DNSServer**, and **ESP8266WebServer**. Once powered via a power bank, battery, or micro USB, the D1 Mini broadcasts a cloned SSID to mimic a legitimate network, enticing nearby devices to connect.

Upon connection, the **DNSServer** library redirects all DNS requests to the D1 Mini, where the **ESP8266WebServer** hosts a fake login page. This page prompts users to enter credentials, which are logged for analysis. The device can be monitored and managed through a web interface at **192.168.4.1/admin**, where attack parameters can be controlled.

The operation highlights the effectiveness of the Evil Twin attack, while also revealing limitations such as proximity requirements and modern device security prompts. This underscores the need for robust Wi-Fi security and user awareness.

WORKING MECHANISM OF THE EVIL TWIN ATTACK

1. Setting Up a Rogue Access Point (AP)

- The attacker configures a device (e.g., an ESP8266 module, laptop, or other Wi-Fi-enabled hardware) to act as a fake AP.
- The rogue AP is configured to mimic the SSID (network name) and, optionally, the security settings of a legitimate Wi-Fi network.
- Tools like ESP8266 or software such as Airbase-ng can make this setup easy for attackers.

2. Broadcasting the Fake Network

- The rogue AP begins broadcasting the cloned SSID.
- To increase effectiveness, attackers may configure the rogue AP with a stronger signal than the legitimate network, enticing users to connect to the fake one.

3. Deauthenticating Users from the Legitimate Network (Optional)

- Attackers may use a **deauthentication attack** to force users off the real network.
- Tools like aireplay-ng send deauth packets to disconnect users, making the rogue AP seem like the only available option.

4. Victim Connects to the Rogue AP

- When a user connects to the fake network, they are no longer interacting with the legitimate network but with the attacker-controlled device.
- The victim is unaware of the deception, as the SSID looks identical.

5. Capturing Credentials or Sensitive Data

Once the victim connects, the attacker can:

1. Create a Captive Portal

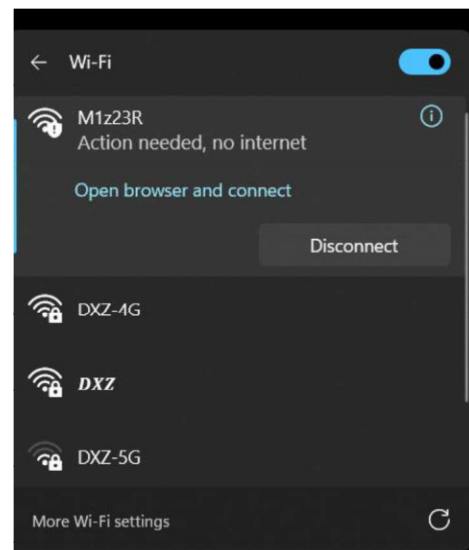
- Redirect the victim to a phishing page (e.g., a fake login page) that mimics the legitimate service (e.g., email, banking, or corporate networks).
- When the victim enters credentials, they are sent to the attacker.

6. Maintaining Control:

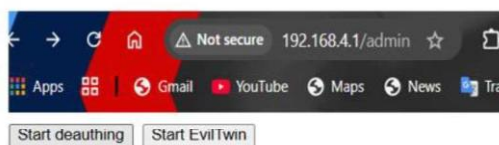
- The rogue AP remains active, logging user activity or continuously capturing sensitive data from connected devices.

STEPS TO EXECUTE THE EVIL TWIN ATTACK SIMULATION

Step:1 Connect to the rogue access point (AP) named **M1z23R** using the password **deauther** from your phone or PC.

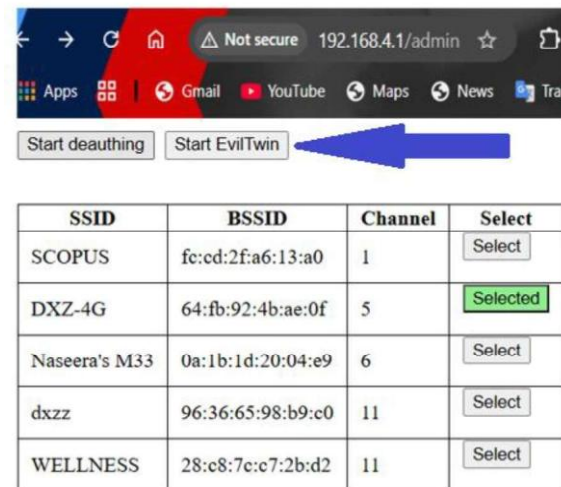


Step:2 Use the web interface to select a target network from the refreshed list of available APs (updated every 30 seconds). Reload the page to view new Aps. or open a browser and navigate to **192.168.4.1/admin** to access the control panel.



SSID	BSSID	Channel	Select
SCOPUS	fc:cd:2f:a6:13:a0	1	Select
DXZ-4G	64:fb:92:4b:ae:0f	5	Selected
Naseera's M33	0a:1b:1d:20:04:e9	6	Select
dxzz	96:36:65:98:b9:c0	11	Select
WELLNESS	28:c8:7c:c7:2b:d2	11	Select

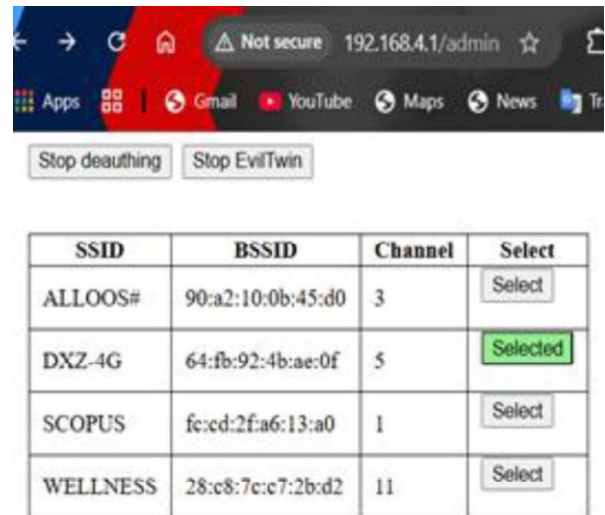
Step:3 Click the **Start Evil-Twin** button to clone the target network. A new AP with the same SSID as the target will be created, which will remain open (no password).



Step:4 Connect to the cloned AP and ensure your device selects "Use this network as is" (phrasing may differ by device).



- ❖ Open a browser and navigate to **192.168.4.1/admin** to access the control panel. From here, manage the attack by **STARTING OR STOPPING** deauthentication of devices connected to the original AP.

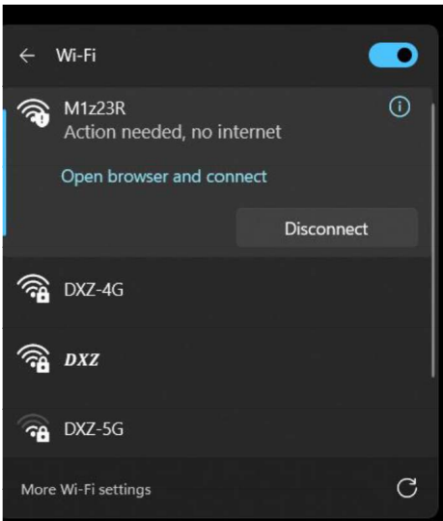


Step:5 Once a victim enters the correct password for the targeted network, the web entry like:



And the D1 Mini will restart, and the default SSID (**M1z23R**) will be restored.

Step:6 Reconnect to the rogue access point (AP) named **M1z23R** from your phone or PC.



The retrieved credentials will be displayed in the admin panel (Open a browser and navigate to **192.168.4.1/admin** to access the control panel) under a log entry like:

"Successfully got password for - SSID - Password".

← → ↻ 🏠 ⚠️ Not secure 192.168.4.1/admin ☆ 📄

📱 Apps 🗂️ | 📧 Gmail 📺 YouTube 📍 Maps 📰 News 🗣️ Translate

Start deauthing

Start EvilTwin

SSID	BSSID	Channel	Select
ALLOOS#	90:a2:10:0b:45:d0	3	Select
DXZ-4G	64:fb:92:4b:ae:0f	5	Selected
Naseera's M33	0a:1b:1d:20:04:e9	6	Select
dxzz	96:36:65:98:b9:c0	11	Select

Successfully got password for: DXZ-4G Password: dxz70594

RESULTS AND OBSERVATIONS

The ESP8266 D1 Mini successfully simulated an Evil Twin attack, exposing vulnerabilities of devices connecting to rogue networks. Observations highlighted:

- Effectiveness in mimicking legitimate SSIDs.
- Limitations such as proximity requirements and modern device security warnings.

DEFENSES AGAINST EVIL TWIN ATTACKS

1. User Awareness

- Avoid connecting to open or suspicious Wi-Fi networks.
- Verify Wi-Fi network names with trusted sources.

2. Encrypted Communication

- Use VPNs and HTTPS to protect sensitive data.

3. Secure Wi-Fi Networks

- Enable WPA3 or WPA2 encryption on legitimate networks.
- Disable SSID broadcasting for sensitive networks.

4. Network Monitoring

- Use tools to detect unauthorized access points and deauthentication attacks.

5. Two-Factor Authentication (2FA)

- Even if credentials are stolen, 2FA adds an additional layer of security.

The Evil Twin attack leverages social engineering and technical manipulation to impersonate legitimate Wi-Fi networks. It's particularly dangerous in public spaces like cafes, airports, or hotels. Awareness and the use of encryption are key to mitigating the risks of such attacks.

MITIGATION STRATEGIES

1. User Awareness

- **Educate Users**

- Encourage users to verify the Wi-Fi network's SSID and avoid connecting to open or suspicious networks.
- Avoid entering credentials into captive portals unless the network is trusted.

- **Use Known Networks Only**

- Manually select trusted networks rather than connecting to networks automatically.

2. Secure Network Configuration

- **Strong Encryption**

- Use WPA3 or WPA2-PSK with a strong password on all legitimate Wi-Fi networks.

- **Hide SSID**

- Disable SSID broadcasting for sensitive networks. While not foolproof, it makes cloning slightly harder.

- **MAC Filtering**

- Restrict devices that can connect to the legitimate network based on their MAC addresses.

3. Advanced Network Security

- **VPN Usage**

- Always use a Virtual Private Network (VPN) when connecting to public or unknown Wi-Fi. A VPN encrypts traffic, preventing attackers from intercepting sensitive data.

- **HTTPS Enforcement**

- Encourage the use of HTTPS for all web traffic. Tools like **HTTPS Everywhere** ensure secure connections, reducing the impact of MITM attacks.

- **Multi-Factor Authentication (MFA)**

- Implement MFA for all critical services so stolen credentials alone are not enough for attackers.

4. Detection and Prevention Technologies

- **Wireless Intrusion Prevention Systems (WIPS)**

- Detect and block rogue APs in real-time. Systems like **AirMagnet Enterprise** or **Cisco Prime Infrastructure** can enforce Wi-Fi security policies.

- **Firewalls and Network Access Controls:**

- Implement policies to block unauthorized devices or limit their network access.

5. Protect Against Deauthentication Attacks

- **802.11w Protected Management Frames (PMF)**

- Enable PMF on access points to prevent deauthentication attacks used to force users off legitimate networks.

6. Regular Audits

- Periodically scan for rogue APs using tools like:
 - **Aircrack-ng** for network analysis.
 - **Wigle.net** to map Wi-Fi networks and identify anomalies.
- Conduct penetration testing to identify vulnerabilities in network configurations.

DETECTION OF EVIL TWIN ATTACKS

1. Monitoring Wi-Fi Networks

- **Unusual SSID Behavior:**
 - Look for duplicate SSIDs in the same vicinity.
 - Use tools like **Wireshark**, **Acrylic Wi-Fi Analyzer**, or **Kismet** to scan networks and identify duplicate SSIDs with differing MAC addresses.
- **Signal Strength Anomalies:**
 - The signal strength of the rogue AP may be unusually high compared to the legitimate network due to proximity.

2. Inspecting Network Details

- Verify the **BSSID** (MAC address) of the access point:
 - Compare the AP's MAC address with the known address of the legitimate network.
 - Tools like **NetSpot** or **inSSIDer** can help identify discrepancies.
- Check for mismatched network encryption settings:
 - A legitimate WPA2-secured network suddenly appearing as an open network may indicate an Evil Twin.

3. Monitoring User Behavior

- Unexpected captive portals or login requests on previously known networks can indicate a rogue AP.
- Frequent disconnections from the legitimate network (caused by deauthentication attacks) are a warning sign.

FAKE WEB PAGE IMPLEMENTATION

A critical component of this simulation is the deployment of a fake login page hosted by the ESP8266 D1 Mini. Using the **ESP8266WebServer** library, the D1 Mini operates as a local web server, serving a deceptive HTML page to devices connecting to the rogue AP.

The web page mimics a typical Wi-Fi login interface, complete with input fields for usernames and passwords. Styled with basic CSS, the page is designed to appear trustworthy and lure unsuspecting users into entering sensitive credentials. When users submit the form, the data can either be logged locally on the D1 Mini or sent to a designated server for analysis.

TestingResults:

During testing, the ESP8266 D1 Mini successfully displayed the fake web page to connected devices. The login form functioned as intended, capturing user inputs without raising suspicion. The project demonstrated how attackers can exploit open networks to harvest sensitive information through phishing techniques.

Insights and Limitations:

- **Effectiveness:** The ESP8266 D1 Mini's ability to replicate legitimate SSIDs and serve deceptive content highlighted the dangers of connecting to unverified networks.
- **Limitations:** The attack requires the rogue AP to be within close proximity to the target devices, and modern devices often display warnings when connecting to unsecured networks, reducing the likelihood of success.

CONCLUSION

This project demonstrates practical and ethical methods to identify and address vulnerabilities in wireless networks, highlighting the security risks posed by rogue Wi-Fi networks. Utilizing the ESP8266 D1 Mini microcontroller, the project successfully simulates an Evil Twin attack by creating a fake Wi-Fi network that deceives devices into connecting. Through libraries like ESP8266WiFi, DNSServer, and ESP8266WebServer, the D1 Mini effectively mimics legitimate access points, intercepts DNS requests, and serves fake content to connected devices for demonstration purposes.

By showcasing the effectiveness of such attacks, this project emphasizes the critical need for robust security measures, including WPA3 encryption, VPN usage, and proactive security practices. The insights gained can inform better network monitoring and help develop strategies to detect and mitigate Evil Twin attacks.

Ultimately, this work serves as an educational tool for understanding wireless security vulnerabilities and a call to action for improving cybersecurity in our increasingly interconnected world. It underlines the importance of user awareness, strong encryption, and vigilance to mitigate risks associated with rogue networks.