EVIL TWIN PROJECT USING ESP8266 D1 MINI

TABLE OF CONTENTS

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.

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.

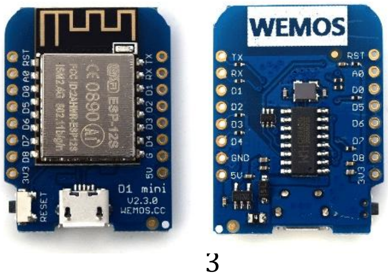
PROJECT GOALS AND OBJECTIVES

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.
- Raise awareness about network security risks.
- Educate on defensive measures against rogue networks.
- 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.
- This is the simplest and most common method for powering the board.

2. Powering via the 5V and GND Pins with Battery

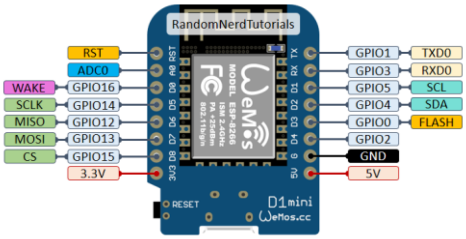
- If you're not using the micro-USB port, you can supply **5V directly** to the 5V and GND pins on the board.

- A regulated 5V supply (e.g., from a USB power bank, 3.7V LiPo with a boost converter, or a 6V battery pack with a 5V regulator) can be connected directly to the **5V pin** and **GND pin**.

The onboard voltage regulator converts the 5V to 3.3V for the ESP8266 D1 Mini chip.

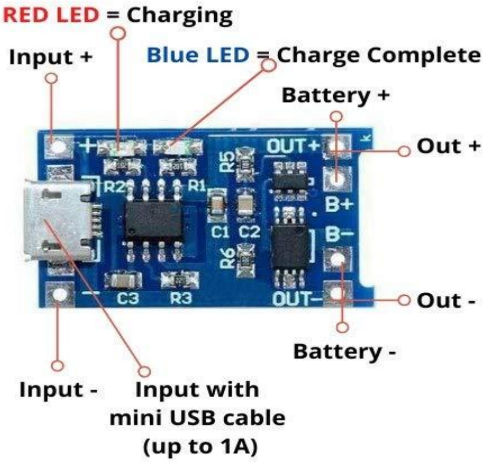
Connection:

- 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 WITH BATTERY 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

Tools and Resources

Arduino IDE:

Used for programming and flashing code onto the ESP8266 D1 Mini.
It allows the incorporation of required libraries, such as ESP8266WiFi, for developing functionalities needed in this project.

Source Code:

- The Evil Twin project can be accessed and downloaded here.
- Customizable code that enables an Evil Twin attack for testing purposes.

Hardware:

- ESP8266 /D1 Mini.
- USB cable for connection to your computer.

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 Necessary Libraries

1.Open Arduino IDE and go to Sketch > Include Library > Manage Libraries.

2. Install the following:

- **ESP8266WiFi.h**: Provides WiFi connectivity for ESP8266.
- Any additional libraries referenced in the project (check the .ino file for #include statements).

Step 3: Obtain the Source Code

1. Visit the GitHub repository: ESP8266 Evil Twin Project.
2. Download the .ino file.
3. Open the .ino file in Arduino IDE.

Step 4: Flash the Code onto the ESP8266

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.

Step 5: Power Up and Test

1. Disconnect and reconnect the ESP8266 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.

RESULTS AND OBSERVATIONS

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.

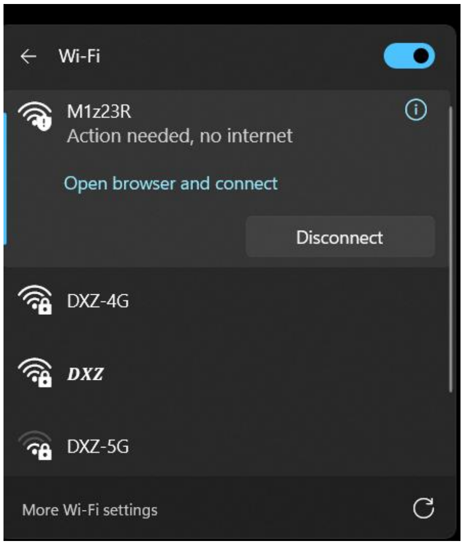
demonstrates how an ESP8266 D1 Mini can be utilized to create a rogue access point that impersonates a legitimate Wi-Fi network. By running custom code on the ESP8266 D1 Mini, the device broadcasts a cloned SSID identical to an existing network, deceiving nearby devices into connecting. Upon connection, 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.

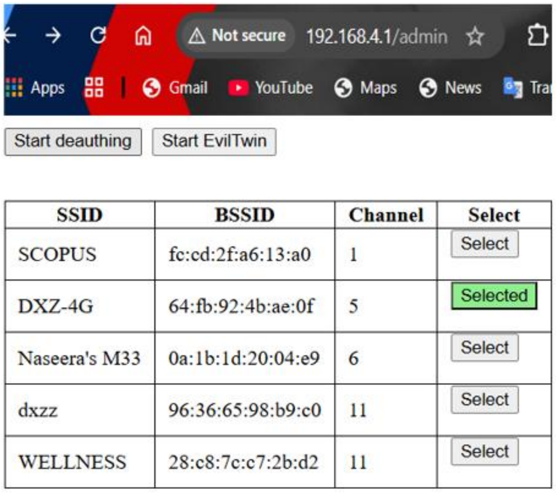
The project also highlighted key limitations of the attack. For instance, the attacker needs to be in close proximity to the targeted devices for effective execution, and many modern devices display security warnings when connecting to unsecured or unfamiliar networks, reducing the likelihood of unsuspecting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

STEPS TO EXECUTE THE EVIL TWIN ATTACK SIMULATION:

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

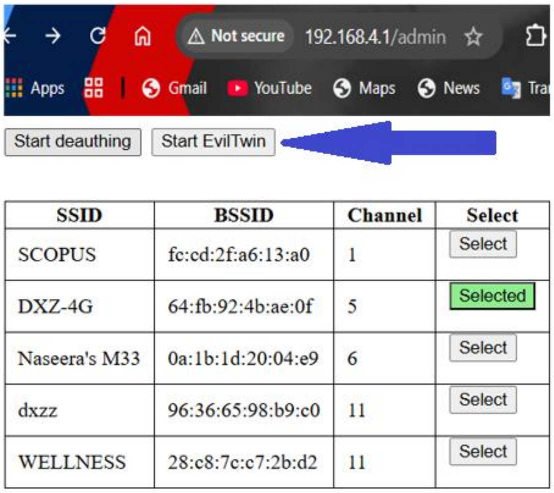


2. Use the web interface to select a target network from the refreshed list of available APs (updated every 30 seconds). Reload the page to view new Aps. or Open a browser and navigate to **192.168.4.1/admin** to access the control panel.



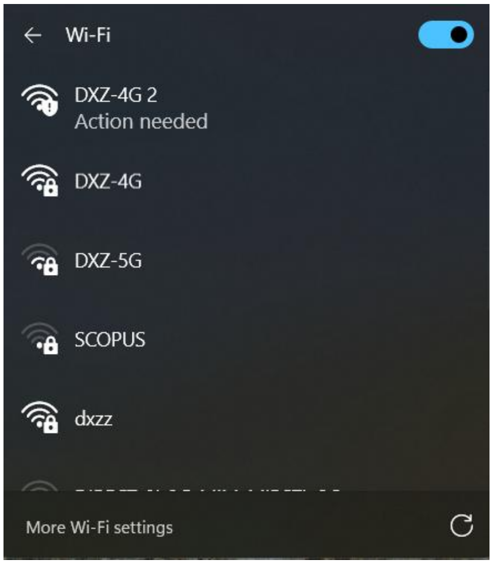
SSID	BSSID	Channel	Select
SCOPUS	fc:cd:2f:a6:13:a0	1	Select
DXZ-4G	64:fb:92:4b:ae:0f	5	Selected
Naseera's M33	0a:1b:1d:20:04:e9	6	Select
dxzz	96:36:65:98:b9:c0	11	Select
WELLNESS	28:c8:7c:c7:2b:d2	11	Select

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).

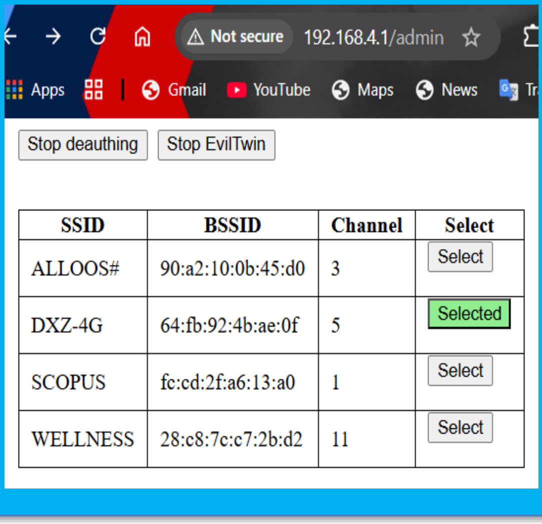


SSID	BSSID	Channel	Select
SCOPUS	fc:cd:2f:a6:13:a0	1	Select
DXZ-4G	64:fb:92:4b:ae:0f	5	Selected
Naseera's M33	0a:1b:1d:20:04:e9	6	Select
dxzz	96:36:65:98:b9:c0	11	Select
WELLNESS	28:c8:7c:c7:2b:d2	11	Select

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

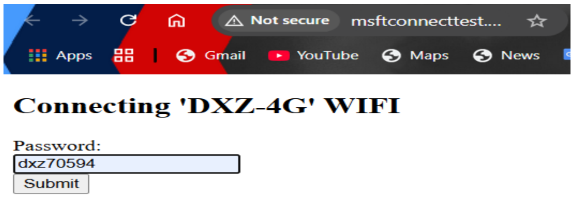


- Open a browser and navigate to **192.168.4.1/admin** to access the control panel. From here, manage the attack by **<u>STARTING OR STOPPING</u>** deauthentication of devices connected to the original AP.



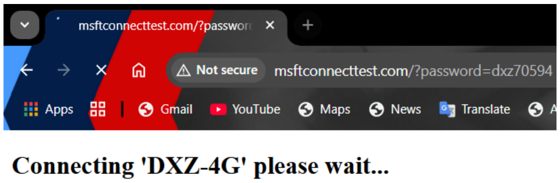
SSID	BSSID	Channel	Select
ALLOOS#	90:a2:10:0b:45:d0	3	Select
DXZ-4G	64:fb:92:4b:ae:0f	5	Selected
SCOPUS	fc:cd:2f:a6:13:a0	1	Select
WELLNESS	28:c8:7c:c7:2b:d2	11	Select

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



Connecting 'DXZ-4G' WIFI

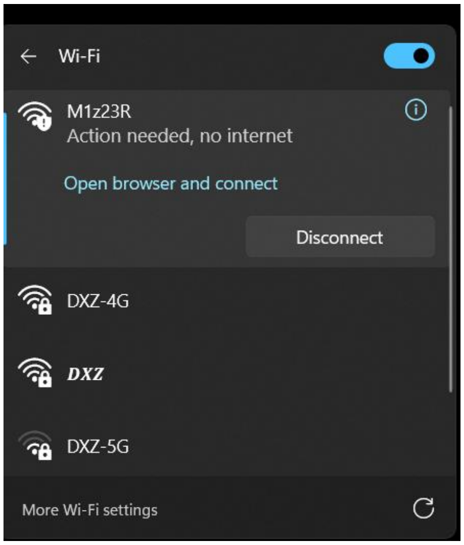
Password:
dxz70594
Submit


msftconnecttest.com/?passwor
Not secure
msftconnecttest.com/?password=dxz70594
Apps
Gmail
YouTube
Maps
News
Translate

Connecting 'DXZ-4G' please wait...

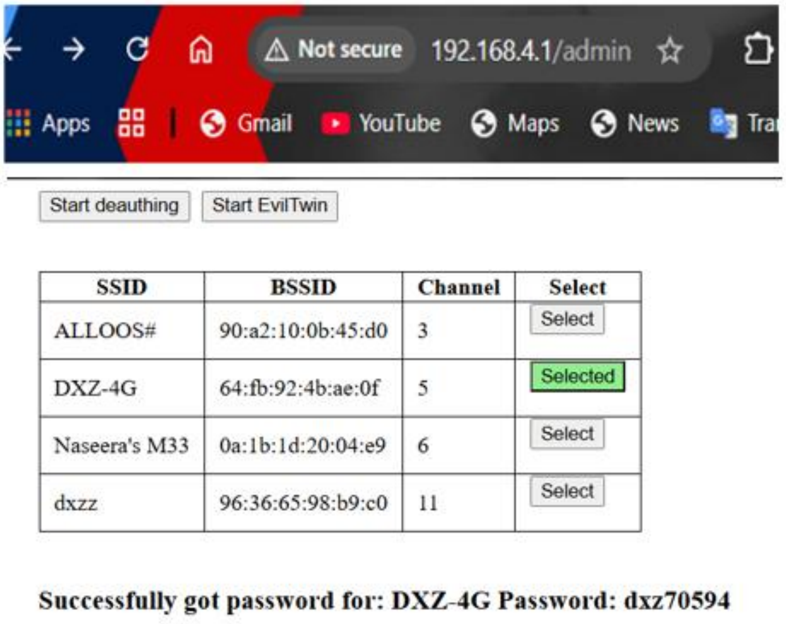
And the D1 Mini will restart, and the default SSID (**M1z23R**) will be restored.

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".



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

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.

Testing Results:
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.