EvilTwinX: Understanding Rogue AP Attacks

EvilTwinX, a tool designed for educational purposes to simulate and analyze rogue access point (Evil Twin) attacks combined with captive portal phishing. Our goal is to empower cybersecurity researchers, red-teamers, and network defenders with insights into attack mechanics, detection strategies, and mitigation techniques to harden Wi-Fi networks.

Chapter 1

Executive Summary & Scope

EvilTwinX is a lab-only, educational tool illustrating how rogue APs and captive portals harvest WPA/WPA2 passphrases. It verifies these against captured handshakes, providing a safe environment for authorized testing. This report covers its design, components, test environment, observations, limitations, and defensive recommendations.

Primary Objectives

- *Reproducible PoC for Evil Twin + captive portal credential harvest.*
- *WPA/WPA2 handshake capture and passphrase verification.*
- *Automated logging and cleanup for safe, repeatable lab testing.*

Out of Scope

- *Unauthorized targeting of live networks.*
- *Offensive features beyond educational PoC needs.*
- *Integration with third-party cracking services.*

High-Level Methodology: The Three-Pronged Approach

EvilTwinX operates by observing, impersonating, and verifying, simulating a common attack chain to help defenders understand and counter such threats.

1. Observe

Put wireless radio in monitor mode, scan for APs and clients, and capture WPA/WPA2 handshake packets during client reconnections.

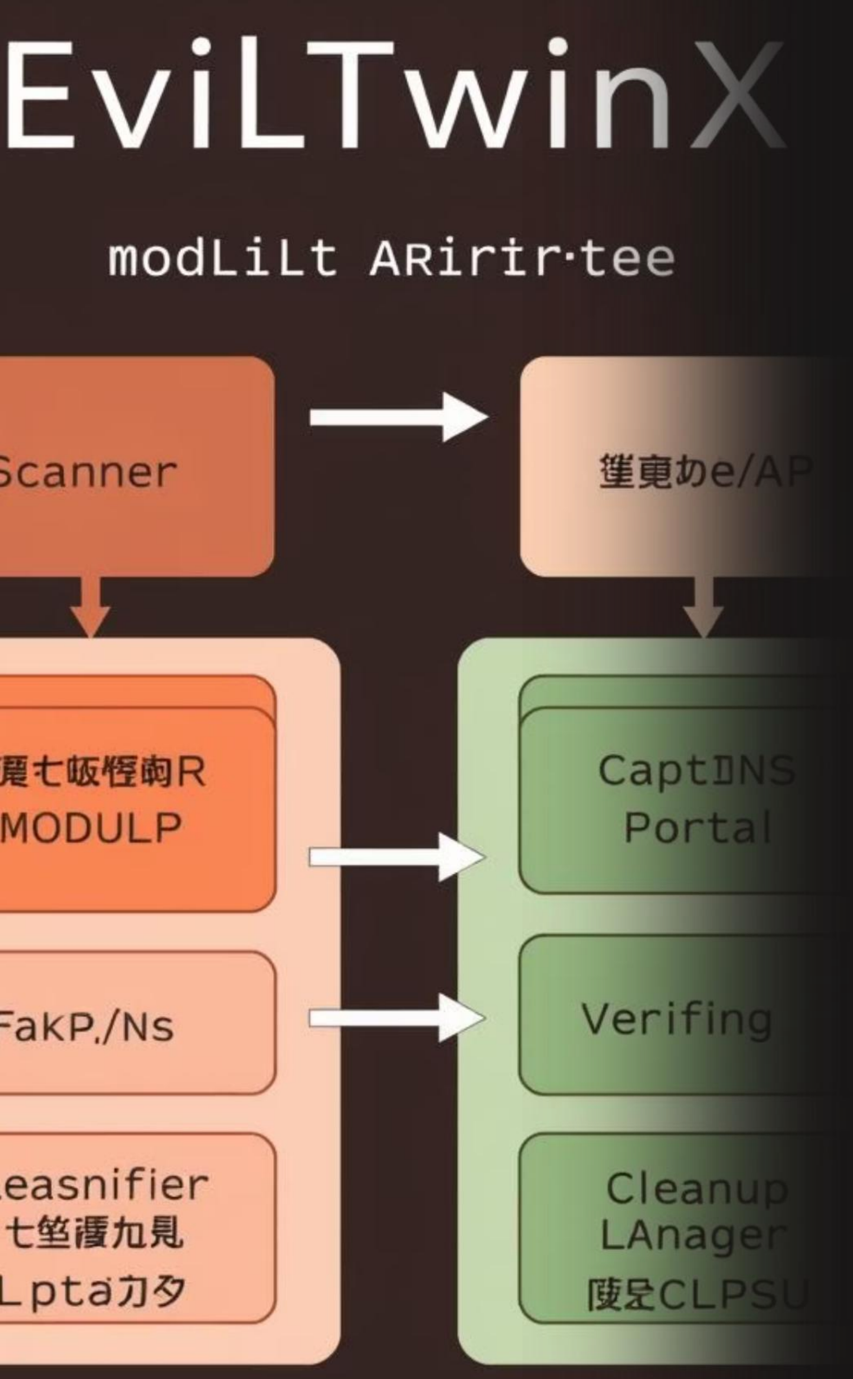
2. Impersonate

Create a fake AP with the legitimate SSID, provide DHCP/DNS, and serve a captive portal requesting the Wi-Fi password.

3. Verify & Close

Validate submitted passwords against captured handshakes. If correct, store securely, then terminate services and restore the environment.

This outline is for defensive research and education only, not for malicious use.



Chapter 2

Architecture & Components

EvilTwinX is built with modular components, each handling a specific function within the attack simulation process.

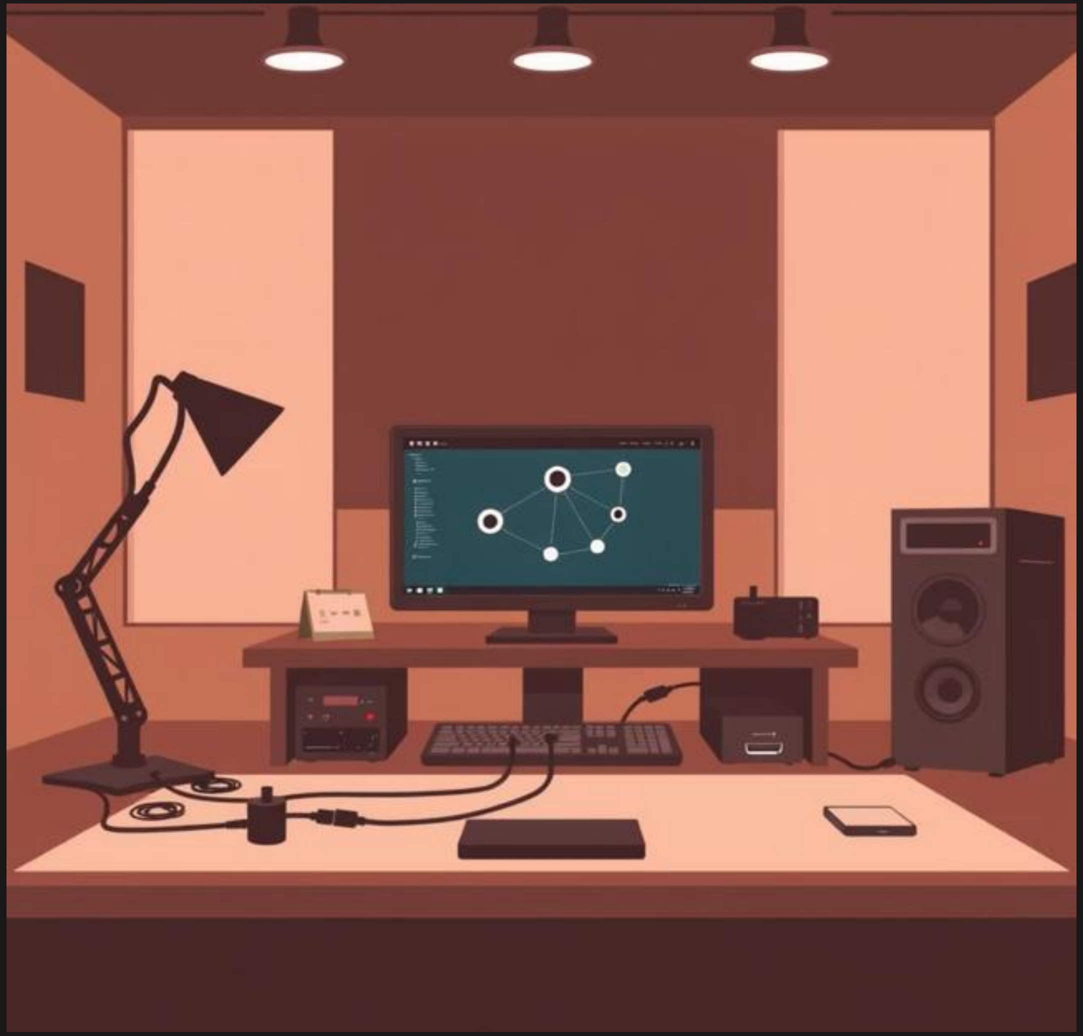
- ***Scanner / Handshake Capture:** Observes target APs/clients and records handshake packets.*
- ***Deauthentication Module:** Triggers client reconnections for handshake capture.*
- ***Fake AP (Evil Twin):** Broadcasts target SSID to attract clients.*
- ***DHCP/DNS Service:** Assigns IPs and resolves fake hostnames for the portal.*
- ***Captive Portal (PHP):** Serves login page, logs password submissions for verification.*
- ***Verifier:** Compares submitted passwords to captured handshakes.*
- ***Logging & Storage:** Records requests, attempts, and verified passphrases.*
- ***Cleanup Manager:** Reverts processes, iptables rules, and radio modes post-test.*

Controlled Test Environment

All EvilTwinX experiments are conducted in a strictly controlled lab environment using dedicated hardware to ensure safety a

Lab Setup

- **Host:** Debian-based Linux (Kali) with root access.
- **Radios:** Two USB Wi-Fi adapters (one for monitor/injection, one for AP mode).
- **Tools:** Standard open-source network utilities and a custom PHP captive portal.
- **Isolation:** RF-controlled room or low transmit power to avoid interference.



⚠ *Strictly for lab use: EvilTwinX is for authorised testing only. Deployment against third-party network is illegal and unethical.*

Chapter 3

Operational Flow & Observations

The operational flow demonstrates the step-by-step process of an Evil Twin attack, from setup to cleanup, highlighting key observations from lab tests.

01

Initialize & Scan

Prepare directories, reset files, set wlan0 to monitor mode, then scan for and select target AP.

02

Capture Handshake

*Run passive capture, trigger deauths to boost reconnects. **Observation:** Deauths increase success, but require active client reconnections.*

03

Launch Evil Twin & Phish

*Configure AP radio, start DHCP/DNS/Captive Portal. Log submitted passwords. **Observation:** Redirecting HTTP traffic requires careful iptables/dnsmasq config.*

04

Verify & Cleanup

*Validate password against handshake. If verified, save and cleanup. **Observation:** Verification is reliable with valid handshakes; cleanup reduces artifacts but requires explicit process termination.*

Limitations & Responsible Use

Understanding the limitations of EvilTwinX is crucial for accurate analysis and responsible deployment in lab environments.

Technical Limitations

- ***HTTPS & Captive Portal Detection:*** *Modern devices often bypass simple HTTP redirection, potentially showing warnings or bypassing the portal entirely.*
- ***Handshake Dependency:*** *Verification requires a complete and valid handshake capture for the specific SSID/client.*
- ***Dual-Band Complexity:*** *Simultaneous 2.4 GHz and 5 GHz attacks demand multiple capable adapters and intricate channel planning.*

Ethical & Legal Constraints

- ***Authorized Testing Only:*** *EvilTwinX is strictly for lab use on networks you own or have explicit, written permission for.*
- ***Scope & Consent:*** *Always define clear scope, timing, and acceptance criteria with network owners before any engagement.*
- ***Data Handling:*** *Securely delete all captured credentials post-testing; never publish, share, or reuse real credentials.*

Chapter 4

Defensive Recommendations

Mitigating Evil Twin attacks requires a multi-layered approach spanning user education, robust network configurations, and advanced detection mechanisms.

User & Policy

- *Educate users on Wi-Fi authenticity verification.*
- *Enforce connection to trusted SSIDs via device management.*

Network Config

- *Prioritize WPA3 for enhanced security.*
- *Implement 802.1X (Enterprise) with EAP.*
- *Enable Management Frame Protection (802.11w).*

Detection & Logging

- *Monitor for deauth spikes and association events.*
- *Correlate unusual DHCP/DNS activity for portal hostnames.*
- *Deploy Rogue AP detection (WIDS/WIPS).*

Key Recommendations for Defenders & Researchers

To effectively counter sophisticated Wi-Fi attacks, defenders must focus on robust authentication, continuous monitoring, and multi-factor security.

- ***Deploy Enterprise Wi-Fi (WPA2/WPA3-Enterprise):*** *Utilize server authentication (certificates) to significantly reduce captive-portal credential theft risks.*
- ***Monitor Management Frames:*** *Establish thresholds and alerts for high volumes of deauthentication packets to detect potential attacks.*
- ***Multi-Factor Authentication (MFA):*** *Implement MFA for all critical services to prevent account takeover even if Wi-Fi PSKs are compromised.*
- ***Wireless NAC & Continuous Monitoring:*** *Employ wireless network access control solutions and integrate continuous monitoring for anomalous behavior.*

Future Work & Closing Remarks

EvilTwinX serves as a powerful educational tool. Our future enhancements aim to further improve its utility for defensive research and training.

Enhancements

- *Multi-adapter orchestration for dual-band attack simulation.*
- *Automated lab mode for reliable client/portal simulation.*
- *Configurable portal templates for defensive testing realism.*
- *Telemetry and reporting features (logs, timelines, metrics).*
- *Installer with dependency checks and capability warnings.*

Conclusion

> *EvilTwinX demonstrates real-world Wi-Fi phishing concepts in a controlled lab. Its true value lies in improving detection, hardening networks, and educating users — not facilitating unauthorized access. Use this tool responsibly and only with explicit permission.*

THANK YOU..