■ Evil Twin Attack Manual

Overview

An Evil Twin AP (Access Point) is a malicious Wi-Fi hotspot that pretends to be a legitimate one. Victims unknowingly connect to it, exposing sensitive data such as credentials and browsing traffic. This manual provides both attacker-side and victim-side perspectives.

Attacker Side: Setting up Evil Twin AP

Step	Action
1	Install required tools: aircrack-ng, hostapd, dnsmasq, Wireshark, Bettercap.
2	Identify target network with `airodump-ng wlan0`.
3	Deauthenticate clients using `aireplay-ng --deauth`.
4	Create fake AP with same SSID using hostapd or airgeddon.
5	Configure DHCP/DNS with dnsmasq.
6	Set up SSL stripping/sniffing using Bettercap or Wireshark.
7	Monitor captured credentials and traffic.

Victim Side: Detection & Protection

Symptom	Check / Action
Duplicate Wi-Fi Name (SSID)	Avoid connecting if two networks with same name exist.
Unstable Connection	Frequent disconnects may indicate deauthentication attacks.
No HTTPS Lock ■	Beware if HTTPS sites show warnings or lack SSL lock.
Unexpected Captive Portal	Fake login pages may appear before real access.
Use VPN	Encrypt traffic to prevent sniffing.
Update Devices	Ensure latest patches to resist exploits.

■ Tips & Notes

- Attackers should use isolated lab environments only for testing. - Victims should verify networks before connecting and prefer mobile data when unsure. - Security tools like `wifiphisher` and `airgeddon` automate Evil Twin attacks. - Defensive tools: VPN, Intrusion Detection Systems, Wireless Security Monitors.