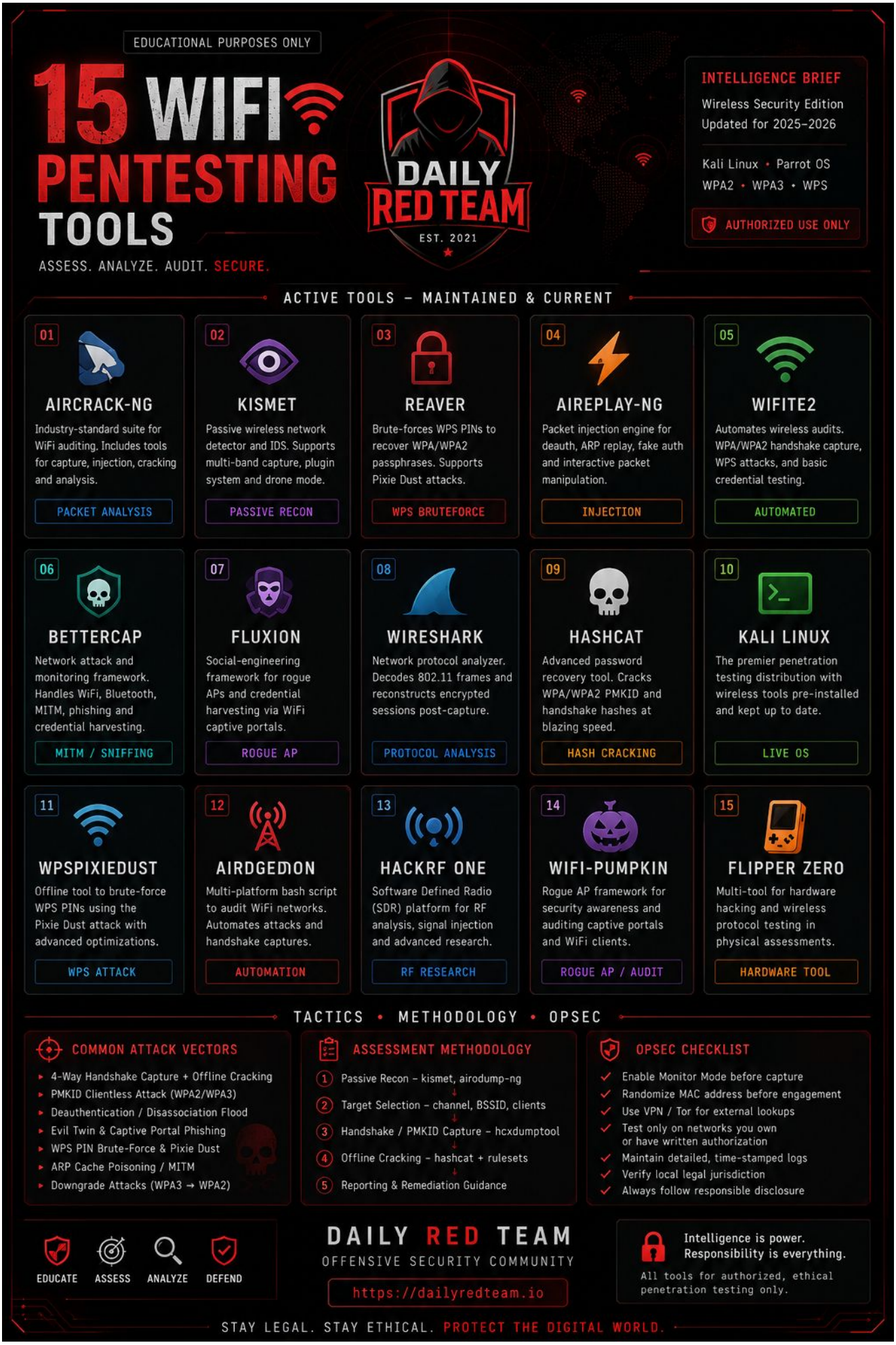
WiFi


EDUCATIONAL PURPOSES ONLY
15 WIFI PENTESTING TOOLS
ASSESS. ANALYZE. AUDIT. SECURE.
DAILY RED TEAM
EST. 2021
INTELLIGENCE BRIEF
Wireless Security Edition
Updated for 2025–2026
Kali Linux • Parrot OS
WPA2 • WPA3 • WPS
AUTHORIZED USE ONLY
ACTIVE TOOLS – MAINTAINED & CURRENT
01
AIRCRACK-NG
Industry-standard suite for WiFi auditing. Includes tools for capture, injection, cracking and analysis.
PACKET ANALYSIS
02
KISMET
Passive wireless network detector and IDS. Supports multi-band capture, plugin system and drone mode.
PASSIVE RECON
03
REAVER
Brute-forces WPS PINs to recover WPA/WPA2 passphrases. Supports Pixie Dust attacks.
WPS BRUTEFORCE
04
AIREPLAY-NG
Packet injection engine for deauth, ARP replay, fake auth and interactive packet manipulation.
INJECTION
05
WIFITE2
Automates wireless audits. WPA/WPA2 handshake capture, WPS attacks, and basic credential testing.
AUTOMATED
06
BETTERCAP
Network attack and monitoring framework. Handles WiFi, Bluetooth, MITM, phishing and credential harvesting.
MITM / SNIFFING
07
FLUXION
Social-engineering framework for rogue APs and credential harvesting via WiFi captive portals.
ROGUE AP
08
WIRESHARK
Network protocol analyzer. Decodes 802.11 frames and reconstructs encrypted sessions post-capture.
PROTOCOL ANALYSIS
09
HASHCAT
Advanced password recovery tool. Cracks WPA/WPA2 PMKID and handshake hashes at blazing speed.
HASH CRACKING
10
KALI LINUX
The premier penetration testing distribution with wireless tools pre-installed and kept up to date.
LIVE OS
11
WPSPIXIEDUST
Offline tool to brute-force WPS PINs using the Pixie Dust attack with advanced optimizations.
WPS ATTACK
12
AIRDGEDON
Multi-platform bash script to audit WiFi networks. Automates attacks and handshake captures.
AUTOMATION
13
HACKRF ONE
Software Defined Radio (SDR) platform for RF analysis, signal injection and advanced research.
RF RESEARCH
14
WIFI-PUMPKIN
Rogue AP framework for security awareness and auditing captive portals and WiFi clients.
ROGUE AP / AUDIT
15
FLIPPER ZERO
Multi-tool for hardware hacking and wireless protocol testing in physical assessments.
HARDWARE TOOL
TACTICS • METHODOLOGY • OPSEC
COMMON ATTACK VECTORS
4-Way Handshake Capture + Offline Cracking
PMKID Clientless Attack (WPA2/WPA3)
Deauthentication / Disassociation Flood
Evil Twin & Captive Portal Phishing
WPS PIN Brute-Force & Pixie Dust
ARP Cache Poisoning / MITM
Downgrade Attacks (WPA3 → WPA2)
ASSESSMENT METHODOLOGY
1 Passive Recon – kismet, airodump-ng
2 Target Selection – channel, BSSID, clients
3 Handshake / PMKID Capture – hcxdumptool
4 Offline Cracking – hashcat + rulesets
5 Reporting & Remediation Guidance
OPSEC CHECKLIST
Enable Monitor Mode before capture
Randomize MAC address before engagement
Use VPN / Tor for external lookups
Test only on networks you own or have written authorization
Maintain detailed, time-stamped logs
Verify local legal jurisdiction
Always follow responsible disclosure
EDUCATE ASSESS ANALYZE DEFEND
DAILY RED TEAM
OFFENSIVE SECURITY COMMUNITY
https://dailyredteam.io
Intelligence is power.
Responsibility is everything.
All tools for authorized, ethical penetration testing only.
STAY LEGAL. STAY ETHICAL. PROTECT THE DIGITAL WORLD.

From:
https://wiki.fortier-family.com/ - **Warnaud's Wiki**

Permanent link:
https://wiki.fortier-family.com/cybersecurity/wifi?rev=1789893996

Last update: **2026/09/20 10:46**