

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



AIRCRAK-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



REAYER

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



AIRDGEDDON

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

- Passive Recon – kismet, airodump-ng
- Target Selection – channel, BSSID, clients
- Handshake / PMKID Capture – hcxdumpool
- Offline Cracking – hashcat + rulesets
- 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.

https://wiki.fortier-family.com/

Printed on 2026/09/22 12:14

// WIFI_PENTEST_TOOLKIT.SH

15 WIFI PENTEST TOOLS

Recon. Exploit. Persist. Harden.

DAILY RED TEAM

// offensive security

ACTIVE TOOLS: 15

UPDATED: 2025

KALI LINUX NATIVE

USE ON OWNED NETS ONLY

// CORE ARSENAL

01 /



AIRCRAK-NG

WEP/WPA/WPA2 cracking suite. Capture, replay and audit 802.11 traffic.

ESSENTIAL

02 /



HCXDUMPTOOL

Captures PMKIDs and handshakes from NIC in monitor mode. No client needed.

PREPARED

03 /



HASHCAT

GPU-accelerated hash cracking. WPA2 PMKID and handshakes cracked at maximum speed.

ESSENTIAL

04 /



BETTERCAP

Modern MITM, packet injection and WiFi scanning via a powerful Go framework.

ACTIVE

05 /



WIFITE2

Automated WPA/WEP/WPS attack framework wrapping the full aircrack-ng suite.

ACTIVE

06 /



FLUXION

Evil Twin and captive portal framework for WPA passphrase phishing attacks.

ACTIVE

07 /



KISMET

Passive 802.11 sniffer, wireless IDS and wardriving platform with GPS support.

RECON

08 /



AIRCRAK-NG

Death and disassociation attacks. Forces handshake capture on demand.

ACTIVE

09 /



HOSTAPD-WPE

Rogue AP for WPA-Enterprise impersonation and credential harvesting.

ENTERPRISE

10 /



EAPHAMMER

WPA-Enterprise GTC downgrade, EAP-PEAP and EAP-TTLS credential theft.

ENTERPRISE

11 /



HCXTOOLS

Converts pcap captures to hashcat-ready PMKID and HCCAPX hash formats.

UTILITY

12 /



MOK4

Beacon flooding, SSID spoofing, deauth floods and wireless DoS attacks.

ACTIVE

13 /



WPSCAN

Enumerates and brute-forces WPS PINs. Identifies known vulnerable router models.

ACTIVE

14 /



SCAPY

Python packet crafting and WiFi frame manipulation for custom exploit scripts.

SCRIPTING

15 /



PWNAGOTCHI

AI-driven passive wardriving device. Auto-captures WPA handshakes and PMKIDs.

AI-POWERED

// ATTACK VECTORS

- ▶ PMKID Capture (clientless)
- ▶ 4-Way Handshake Capture
- ▶ Deauthentication Flood
- ▶ Evil Twin + Captive Portal
- ▶ WPS Pixie-Dust Attack
- ▶ WPA-Enterprise GTC Downgrade
- ▶ Beacon / SSID Flooding
- ▶ MITM via ARP Poisoning

// PMKID ATTACK FLOW

- ▶ Enable monitor mode via airmmon-ng
- ▶ Capture PMKID with hcxdump tool
- ▶ Convert to hash with hcxtools
- ▶ GPU crack: hashcat -m 22000

hcxdump tool

 -

hcxtools

 -

hashcat

 -

CRACKED

// No client required - fastest modern method

// OPSEC CHECKLIST

- ▶ Monitor mode (airmon-ng check kill)
- ▶ MAC randomization via macchanger
- ▶ Route all traffic via VPN or Tor
- ▶ Use a dedicated pentest NIC
- ▶ No PII in wordlists or captures
- ▶ Obtain written authorization first
- ▶ Log all activity for the report
- ▶ Stay legal and ethical always

KNOWLEDGE IS POWER. AUTHORIZATION IS EVERYTHING.

DAILY RED TEAM

// think like the attacker - defend like the pro

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

Permanent link:
<https://wiki.fortier-family.com/cybersecurity/wifi>

Last update: 2026/09/20 11:16

Warnaud's Wiki - <https://wiki.fortier-family.com/>