Curated WiFi Arsenal

This project is based on the great work of 0x90/wifi-arsenal. I needed to go through the whole list of over 500 wifi-related projects listed there. I found the following limitations:

- by using submodules the project links are often not up-to-date, they are commit links
- the list lacks a categorization of projects
- there is no description of projects so that you have to click every bad-named project to evaluate usefullness

As I had to go through all the projects anyway I tried to fix this limitations and created a csv file which can be transformed into a README.md easily (shell-script inlcuded). And here it is. I hope it will help somebody. The categorization is not always easy/accurate (going through 500 projects was exhausting, concentration was gone eventually!). Please feel free to fix or add things and submit a pull request!

Keep track of changes made in the original 0x90/wifi-arsenal repo and were not added here yet.

Table of Contents

TOC created by gh-md-toc

General WiFi Information

- 802.11 frames - A starter guide to learn wireless sniffer traces
- 80211 Pocket Reference Guide - Cheat Sheet for 802.11
- 802.11p-wireless-regdb - Wireless regulatory database for CRDA
- 802.11 Wireless Networks: The Definitive Guide - Partly open chapters of O'Reilly 802.11 book
- Armory - The 802.11 Hacking Repo (Meta Information, Link collection)
- Awesome-wifi-security - A collection of awesome resources related to 802.11 security, tools and other things
- Call-for-wpa3 - Call for WPA3 - what's wrong with WPA2 security and how to fix it
- Known manufacturer MAC list -
- Wikipedia - IEEE802.11 site of Wikipedia

Noteworthy Tools of Different Categories

- Aircrack-ng - WiFi security auditing tools suite
- airgeddon - This is a multi-use bash script for Linux systems to audit wireless networks

- bettercap - bettercap is the Swiss Army knife for WiFi, Bluetooth Low Energy, wireless HID hijacking and Ethernet networks reconnaissance and MITM attacks
- Fern-wifi-cracker - Crack and recover WEP/WPA/WPS keys and also run other network based attacks on wireless or ethernet based networks
- karma - KARMA Attacks Radioed Machines Automatically (KARMA)
- kismet - Wireless network detector, sniffer, and intrusion detection system
- mdk3_6.1 - A fork and modification of the original MDK3
- Pwnagotchi - Pwnagotchi is an A2C-based "AI" powered by bettercap and running on a Raspberry Pi Zero W that learns from its surrounding WiFi environment in order to maximize the crackable WPA key material it captures (either through passive sniffing or by performing deauthentication and association attacks)
- pyrit - The famous WPA precomputed cracker, Migrated from Google
- Scapy - Python-based interactive packet manipulation program & library
- waidps - Wireless Auditing, Intrusion Detection & Prevention System
- Wifipumpkin3 - Powerful framework for rogue access point attack.
- WiFi-Pumpkin - Framework for Rogue Wi-Fi Access Point Attack
- Wireless-ids - Ability to detect suspicious activity such as (WEP/WPA/WPS) attack by sniffing the air for wireless packets
- zarp - Network attack tool centered around the exploitation of local networks

Attack/PenTesting

Denial of Service

- 80211mgmtDoS - 802.11 DoS Attacks based on unprotected Management frames
- airodump_mod - Improved version of airodump-ng with ability to kick-off a stations from AP
- android_packetspammer - Packetspammer sends unencrypted broadcast packets down a mac80211 wireless interface that should be set for Monitor mode
- apflood - Flood area with fake essids
- Curfew - 802.11w-2009 Auditor And Deauthentication Frame Spammer.
- dw - Small tool for sending 802.11 disassociation and deauthentication packets to specific clients.
- hwk - Hwk is a collection of packet crafting/network flooding tools
- JamWiFi - A GUI, easy to use WiFi network jammer for Mac OS X
- Mass-deauth-attack - A program that does Deauthentication Attack on every nearby wireless device

- Mass-deauth - A script for 802.11 mass-deauthentication
- mdk3_6.1 - A fork and modification of the original MDK3
- mdk4 - MDK4
- modwifi - Advanced Wi-Fi Attacks Using Commodity Hardware
- netattack - Python script that allows you to scan your local area for WiFi Networks and perform deauthentification attacks
- Scapy-deauth - Scapy based wifi Deauth
- ska - Framework for sniffing ieee80211 packets and generating deauth packets and sending raw packets.
- widowmaker - Widowmaker is an 802.11 DOS tool that exploits the Beacon time interval to outpace wireless access points. This (in theory) allows an attacker to deny service to a wireless access point by providing fake mac addresses to clients that are looking to authenticate with the legitimate access point
- wificurse - WiFi DoS attack tool created for educational purposes only. It works only in Linux and requires wireless card drivers capable of injecting packets in wireless networks
- WifiDeauth - A lightweight Wi-Fi auto deauthentication attack tool (libtins/C++)
- wifijammer - Continuously jam all wifi clients/routers
- WiFiJammer.py - Wireless Jammer to Disconnect Nearby Access-Points and Stations
- wifikicker - A tool to kick devices out of your network and enjoy all the bandwidth for yourself. It allows you to select specific or all devices and ARP spoofs them off your local area network
- wifikills - A python program to kick people off of wifi
- WiFi-Rifle - Creating a wireless rifle de-authentication gun, which utilized a yagi antenna and a Raspberry Pi
- wirelessjammer - Continuously jam all wifi clients and access points within range
- zizzania - Automated DeAuth attack

Encryption Attack

WEP/WPA/WPA2

- Eicrog - WEP key generator for predictable key weaknesses
- huawei_wifi - Wifi utilities for finding Huawei routers' default key
- Aircrack-ng - WiFi security auditing tools suite
- AircrackPy - Un simple modulo de automatización de crackeo de WPAKEY en Windows, además utiliza Google forms.
- airmode - AirMode is a GUI that can help you to use the Aircrack framework

- Airvengers - A GUI to pentest wifi Network, based on Aircrack-ng tools
- asleap - Recovers weak LEAP password. Pronounced asleep.
- autokwaker - Creating an auto cracker for 802.11 networks
- CapBreaker - Management tool for WPA hash cracking with a distributable software including WebUI.
- cenarius - Cenarius tool for crack Wi-Fi , crack wpa-psk , crack wpa2-psk , crack wep , crack wps pin and crack hidden AP . cenarius psk crack
- cherry - Distributed WPA/WPA2 cracker
- Cowpatty - Offline dictionary attack against WPA/WPA2 networks using PSK-based authentication (e.g. WPA-Personal)
- deauth_dot11decrypt - It sends deauth packet to all stations for getting keys in 4-way handshakes from stations already connected to an AP. When it detected 4-way handshakes between a station and an AP, it stops sending deauth packet to that station.
- dot11decrypt - An 802.11 WEP/WPA2 on-the-fly decrypter.
- Easy-HCX - Bash script using hcxdumptool, hcxtools and hashcat to collect WPA2 handshakes and/or PMKIDs, convert them to hashcat format and perform dictionary attacks to crack their passwords.
- Fern-wifi-cracker - Crack and recover WEP/WPA/WPS keys and also run other network based attacks on wireless or ethernet based networks
- HandShaker - Detect, capture, crack WPA/2 handshakes, WEP Keys and geotag with Android GPS
- hcxtools - Solution for capturing wlan traffic and conversion to hashcat formats (recommended by hashcat) and to John the Ripper
- Invasit-network - Automatizated bash script to invade WPA2 networks with wordlist method
- KeyGrab - Grabs and saves handshakes from WPA/WPA2 encrypted networks. Written for Kali Linux
- kismet-deauth-wpa2-handshake-plugin - Python plugin for Kismet to perform deauthentication to collect WPA2 handshakes
- krackattack-all-zero-tk-key - works with clients that install the all-zero TK in a KraCK attack!
- KrackAttack - An application that exposes and aims to raise awareness about Wi-Fi key reinstallation attacks
- krackattacks - KRACK attacks
- Krackattacks-pineapple - WPA2 Key reinstallation attack (KRACK) on the WiFi Pineapples
- krackattacks-poc-zerokey - Proof-of-concept of the KRACK attack against Linux and Android
- Krackattacks-scripts - KRACK attack scripts
- Krackattacks-Test-Vulnerability - Code for testing krackattacks

- KRACK - crack all zero tk
- krack - Proof of concept implementation of key reinstallation attack on WPA2 protected WiFi networks
- krackinfo - Vendor Response Matrix for KRACK WPA2 (Key Reinstallation Attack)
- krack-poc - Proof of concept for Krack attack using channel-based MitM
- KRACK-toolkit - Work in progress toolkit for KRACK attack
- marfil - Assess WiFi network security. It allows to split the work of performing long running dictionary attacks among many computers
- peapwn - Proof-of-concept implementation of the Apple relay attack in Python
- PINEAPPLE - Wifi Pineapple scripts
- piwifipineapple - script to automate the entire process on setting the raspberry pi up as a malicious hot spot for educational purposes
- Pmkid-extractor - Extract PMKIDs from a wifi capture to a hashcat-compatible format
- pyDot11 - Encrypt and Decrypt 802.11 on-the-fly
- pyrcrack - Python Aircrack-ng
- pyrit - The famous WPA precomputed cracker, Migrated from Google
- pythonAir - Flask/aircrack
- Thesis - "Master's Thesis: ""Identifying Software and Protocol Vulnerabilities in WPA2 Implementations through Fuzzing"" "
- uploadwpa - This module will upload a wpa handshake from a single capture file to an online hash cracker site
- WiFi-autopwner - Script to automate searching and auditing Wi-Fi networks with weak security
- WiFiBroot - A WiFi Pentest Cracking tool for WPA/WPA2 (Handshake, PMKID, Cracking, EAPOL, Deauthentication)
- Wifi-bruteforcer-fsecurify - Android application to brute force WiFi passwords without requiring a rooted device
- Wifi-cracker - Wifi Cracker is a great tool to use if you have forgotten your wifi password and need to figure it out. This application works well with WEP, WPA, WPA-PSK security types.
- wificracking - Crack WPA/WPA2 Wi-Fi Routers with Airodump-ng and Aircrack-ng/Hashcat
- Wifi-hacker - Shell Script For Attacking Wireless Connections Using Built-In Kali Tools. Supports All Securities (WEP, WPS, WPA, WPA2)
- wifite2 - Python script for auditing wireless networks
- wifite - An automated wireless attack tool
- Wifite-mod-pixiewps - Wifite with PixieWPS support

- Wifite-openwrt - Wifite for the WiFi Pineapple NANO + TETRA (Chaos Calmer - openWrt)
- Wireless_peeker - Tool to crack wireless encryption (WPA / WPA2) base on C99
- wpa2-enterprise-attack - Through these scripts it is possible to create Rogue or Fake Access Points and carry out an authentication downgrade attack against WPA and WPA2-Enterprise networks, obtaining passwords in hash format or cleartext (if GTC downgrade is successful).
- WPA2-HalfHandshake-Crack - Capture enough of a handshake with a user from a fake AP to crack a WPA2 network without knowing the passphrase of the actual AP
- wpa2hc - Quick script to automate converting WPA .cap files for Hashcat .hccap files.
- WPA2-KRACK - WPA2 KRACK
- wpa2own - Use hashcat to crack WPA2 PSK (Pre-Shared Key) passwords!
- Wpa-autopwn - WPA/WPA2 autopwn script that parses captured handshakes and sends them to the Crackq
- Wpa-bruteforcer - Attacking WPA/WPA encrypted access point without client.
- wpacrack - Open-source distributed Wifi-Protected Access (WPA) cracker
- WPA_DECRYPTION_MPI - WPA/WPA2 for cluster processing
- wpakey - monitor mode WPA1/WPA2 online password bruteforcer

WPS

- autoreaver - Automatically exported from code.google.com/p/auto-reaver
- bully - New implementation of the WPS brute force attack, written in C
- greaver - GUI for Reaver, WPS brute force tool
- HT-WPS-Breaker - HT-WPS Breaker (High Touch WPS Breaker)
- Krack-wps - attack networks with wps to corrupt their security using dictionary type pixywpa v3.0
- OneShot - Run WPS PIN attacks (Pixie Dust, online bruteforce, PIN prediction) without monitor mode with the wpa_supplicant
- Penetrators-wps - Experimental tool that is capable of attacking multiple WPS-enabled wireless access points in real time.
- phpreaver - A command line PHP script which uses the reaver WPS pin cracker to test multiple AP's with multiple WiFi adapters.
- Pixiewps-android - Pixiewps is a tool written in C used to bruteforce offline the WPS pin exploiting the low or non-existing entropy of some APs (pixie dust attack).
- pixiewps - An offline WPS brute-force utility
- PSKracker - An all-in-one WPA/WPS toolkit
- pyxiewps_WPShack-Python - Wireless attack tool written in python that uses reaver,

pixiewps and aircrack to retrieve the WPS pin of any vulnerable AP in seconds

- Reaver-ui - Hacky UI to wrap around reaver-wps
- Reaver-webui - Simple WebUI to crack wireless networks using reaver
- Reaver-wps-fork-t6x - Community forked version which includes various bug fixes, new features and additional attack method (such as the offline Pixie Dust attack)
- Reaver-wps - Brute force attack against Wifi Protected Setup
- wpscrack - Continuation of wpscrack originally written by Stefan Viehböck
- wpseyes - Tool for bruteforce Wi-Fi WPS
- wps - WPS related utilities
- WPSIG - Simple tool (written in Python) that does information gathering using WPS information elements.
- wpsoffline - PoC for routers vulnerable with WPS and deficiencies in their PRNG state
- Wps-scripts - WPS hacking scripts
- Wps-Ultimate-Cracker - This script will help help you to get the most of router in morocco by using pixiewps , reaver , aircrack-ng ,wifite

Others

- apbleed - Allows you to use existing heartbleed tools to test the RADIUS server
- eapmd5pass - An implementation of an offline dictionary attack against the EAP-MD5 protocol. This utility can be used to audit passwords used for EAP-MD5 networks from wireless packet captures, or by manually specifying the challenge, response and associated authentication information.
- haircrack - Automated aircrack/reaver/pyrit (An interface for aircrack/reaver/pyrit written in python. The interface itself may never get finished.)
- IKECrack - IKE/IPSec authentication crack tool. This tool is designed to bruteforce or dictionary attack the key/password used with Pre-Shared-Key [PSK] IKE authentication.
- Krackattacks-test-ap-ft - This script tests if APs are affected by CVE-2017-13082 (KRACK attack)
- PCAP-CRACKER - A python script file to decrypt encrypted IEE (802.11) Radio .pcap files captured via Wireshark for extraction and analyse
- wavecrack - Wavestone's web interface for password cracking with hashcat
- WifiBF - This is a wifi Brute Force. script undetectable and secure!
- wifite2-docker - Docker of Wifite2
- wifite2mod - This repo is a complete re-write of wifite, a Python script for auditing wireless networks
- wifite2-RPi3-nexmon - Wifite2 for Raspberry Pi 3

- wifiteintaller -
- Wpe-parse - This is a simple parsing script to convert output from hostapd-wpe (which makes John the Ripper-formatted logs) to Hashcat format.

Injection

- Aggr-inject - Remote frame injection PoC by exploiting a standard compliant A-MPDU aggregation vulnerability in 802.11n networks.
- Aircrack-db - A list of wireless cards tested with the dual-card injection test and in the field
- airown - Packet injection tool
- Airpwn-ng - New and improved version of airpwn
- litis-generator - Software for distributed statistical evaluation of IEEE 802.11 wireless networks using Linux mac80211 packet injection facility
- libfcap - Library for manipulate 802.11 frame in monitor mode
- libmoep - Allows for frame injection on monitor mode devices with per-frame radiotap options such as TX rate / MCS index and RTS/CTS protection
- Lorcon-examples - Various examples and patches for LORCON
- lorcon - A common injection and control library for wireless packet crafting
- lrc - Fast Wi-Fi hijacker in C, based on AirPwn ideas and LORCON
- moepdefend - Example monitoring/injection tool based on libmoep
- packetinjector - Packet analyzer and injector, written in JavaScript
- packetvector - 802.11 management packet injection tool based on packetspammer
- pylorcon2 - Pure Python wrapper for the LORCON library.
- wifitap - WiFi injection tool through tun/tap device
- wiwo - Wiwo is a distributed 802.11 monitoring and injecting system that was designed to be simple and scalable
- wperf - 802.11 frame injection/reception tool for Linux mac80211 stack

Rogue AP/Fake AP/ MITM

- Aerial - Multi-mode wireless LAN Based on a Software Access point for Kali Linux.
- AIRBASE-NG-SSLSTRIP-AIRSTRIP- - AIRBASE-NG + SSLSTRIP = AIRSTRIP
- cupid - Patch for hostapd and wpa_supplicant to attempt to exploit heartbleed on EAP-PEAP/TLS/TTLS connections
- eaphammer - Targeted evil twin attacks against WPA2-Enterprise networks. Indirect wireless pivots using hostile portal attacks.
- FakeAP - Create fake AP in Kali with 1 command

- FakeAP - Fake access point using dns spoof and ssl stripping
- fakeaps - Fake Access Points using Atheros wireless cards in Linux
- fluxion - Fluxion is the future of MITM WPA attacks
- FuzzAP - A python script for obfuscating wireless networks
- Hostapd-karma - DigiNinja patches to hostapd for rogue access points.
- hostapd-mana - A featureful rogue access point first presented at Defcon 22 by Dominic White (@singe) & Ian de Villiers @ sensepost (research@sensepost.com)
- Hostapd-wpe-extended - Modification and tools for using hostapd for rogue AP attacks impersonating WPA-Enterprise networks to steal user credentials
- Hostapd-wpe - Modified hostapd to facilitate AP impersonation attacks
- jfap - A simple 802.11 fake access point that supports open auth
- karma - KARMA Attacks Radioed Machines Automatically (KARMA)
- mana - Our mana toolkit for wifi rogue AP attacks and MitM
- mitmAP - A python program to create a fake AP and sniff data
- Mitm-helper-wifi - Make it easy and straight-forward to configure a Ubuntu virtual machine to act as a WiFi access point (AP)
- Mitm-rogue-WiFi-AP - MITM Attack Example Code with Rogue Wi-Fi AP
- openrtls -
- Platform-hostapd - Wireless access point for experimental-platform.
- PwnSTAR - PwnSTAR (Pwn SofT-Ap scRipt) - for all your fake-AP needs
- pyfi - Easy wireless access point fabricator
- refluxion - Refluxion -- MITM WPA attacks tool
- rogueap - Start a rogue access point with no effort, with support for hostapd, airbase, sslstrip, sslsplit, tcpdump builtin
- rogueDetect -
- roguehostapd - Hostapd fork including Wi-Fi attacks and providing Python bindings with ctypes
- rogue - An extensible toolkit providing penetration testers an easy-to-use platform to deploy Access Points during penetration testing and red team engagements
- RogueSploit - Powerfull Wi-Fi trap
- Rspoof - Wifi Automated Fake HotSpot Hijacking with aicrack-ng, airbase, ssl-strip, and dns spoof in Python
- Scapy-fakeap - Fake wireless Access Point (AP) implementation using Python and Scapy
- snifflab - Scripts to create your own MITM'ing, packet sniffing WiFi access point
- startools - To use a RasPi to do an Evil Twin attack and capture 802.1x RADIUS creds
- wifi_honey - Setting up four fake access points, each with a different type of encryption,

None, WEP, WPA and WPA2 and the seeing which of the four the client connects to

- wifimitm - Wi-Fi Machine-in-the-Middle: Automation of MitM Attack on Wi-Fi Networks
- wifiphisher - Automated victim-customized phishing attacks against Wi-Fi clients
- Wifipumpkin3 - Powerful framework for rogue access point attack.
- WiFi-Pumpkin - Framework for Rogue Wi-Fi Access Point Attack
- wifisoftap -
- Wifi_Trojans - Collection of wireless based bind and reverse connect shells for penetration testers

Sniffing

- Airodump-iv - A python implementation of airodump-ng
- Airodump-logger - Logging clients with airodump-ng
- Airport-sniffer - Very simple Wi-Fi sniffer and dump parser for built-in macbook AirPort Extreme card. Only native MacOS tools used.
- airpydump - Analyze Wireless Packets on the fly. Currently supporting three working Modes (Reader, Live, Stealth)
- airtraf - Wireless 802.11 network sniffer and analyzer
- bettercap - bettercap is the Swiss Army knife for WiFi, Bluetooth Low Energy, wireless HID hijacking and Ethernet networks reconnaissance and MITM attacks
- darm - Intelligent network sniffer for the masses
- datasamalen - Pick up wifi-probe requests
- DeSniffer - 802.11 wireless sniffer
- dot11sniffer - Sniffs 802.11 traffic and counts the number of active wireless devices in an area
- eap_detect - A simple script using the python library Scapy to detect the 802.1X authentication mechanism
- easy-bettercap - simple way to use bettercap
- geoprobe - geoprobe is a tool to sniff, collect and geolocate 802.11 ProbeRequests using WiGLE API.
- handshakeharvest -
- liber80211 - 802.11 monitor mode for Android without root
- libpcap-80211-c - Sniffs on a RFMON-enabled device for a beacon when compiled, linked and loaded
- mac80211-user - Intercept 80211 data frame and put it into userspace
- milicone - Investigating interaction with wireless communication traffic
- Mr-nosy - Liked to know about everything that was going on

- mupe - MUltiPath Estimator - Create statistical analysis of 802.11 Radiotap sniffs
- nabui - Not Another Bettercap UI
- Naive-project -
- Native-WiFi-API-Beacon-Sniffer - Tool that dumps beacon frames to a pcap file. Works on Windows Vista or Later with any Wireless Card
- ninjaberry - Ninjaberry: Raspberry Pi UI for @bettercap
- oculus - Lightweight tool to collect traces from wifi
- ofxSniffer - Wrapper for the libtins library. Libtins can be used to sniff network packages, or to generate network pacakages yourself.
- Peanuts - Peanuts is a free and open source wifi tracking tool. Based on the SensePosts Snoopy-NG project that is now closed.
- Phalloc-sniffer - With the ever increasing dependance on wireless solutions, it sometimes is useful to know the devices around you. This software aims to help know the MAC addresses of the devices that are leaving any sort of trace on the airwaves.
- phystats - Gather & plot ieee80211 counters from Linux debugfs
- probecap - A quick and dirty utility to capture and store WiFi probes.
- probehunter - Probe Request sniffer + Wigle
- probemon - Monitors 802.11 probe packets sent from roaming mobile devices. Developed using PyLorcon2.
- proberequest - Toolkit for Playing with Wi-Fi Probe Requests https://probequest.readthedocs.io/en/...
- probesniffer - A tool for sniffing unencrypted wireless probe requests from devices
- rifsniff - Remote Interface Sniffer
- ScapyGELFtoGraylog2 - Sniff some 802.11 packages and send the date and MAC with GELF UDP to Graylog2
- Scapy-wireless-scanner - Simple wireless scanner built using Scapy Library
- SSIDentity - Passive sniffing of 802.11 probe requests, stored in a central database.
- TCP-SeqNum - Means to sniff 802.11 traffic and obtain TCP session info using netfiter_queue. Use that data to construct a packet in scappy.
- wallofshame - Multi protocol sniffer, created for ChaosConstruction conference HackSpace
- Wall-of-Shame - A framework for capturing user credentials and sensitive device information.
- Watcher - Canari framework based Maltego transform pack that allows you to perform wireless sniffing within Maltego
- WiFi-802.11-Demo-Sniffer - This 802.11 sniffer written in Python provides a useful tool to raise awareness at the amount of data phones release for anyone to read.

- Wifi-harvester - For collecting probed SSID name by wireless devices, Access point detail and connected clients.
- wifijamMac - Allows you to select one or more nearby wireless networks, thereupon presenting a list of clients which are currently active on the network(s)
- Wifimon - Wi-fi 802.11 Beacon Frame sniffer
- Wifi-scan - Short python script scans for probe requests from whitelisted WiFi clients
- wifispy - Sniff Wifi traffic, log device addresses
- Wireless-info - Obtain information about wireless interfaces from MAC80211 stack
- Wireless-radar - DF and other tools to explore a 2.4GHz environment
- Wireless-Sniffer - A 802.11 wireless sniffer tool (c-based)
- wpasnff - This script allows you to decrypt and sniff packets for a specific WPA2 network based on BSSID you passed in input.

Wardriving

- Auto-Besside-Capturer - Capture WPA handshakes, using besside-ng. Auto upload to http://wpa-sec.stanev.org for cracking the password.
- MappingWirelessNetworks - Code, data, and (possibly) schematics for recording wireless network data around a city
- WAPMap - Parse Kismet .netxml output and then return a CSV file that can be uploaded to Google Maps Engine to map WEP or OPEN networks
- warcarrier - An NCURSES-based, all-in-one instrument panel for professional Wardriving
- WifiScanAndMap - A Linux Python application to create maps of 802.11 networks

Miscellaneous Attacking Tools

- 80211scrambler - Small collection of tools in Verilog for working
- airgeddon - This is a multi-use bash script for Linux systems to audit wireless networks
- airodump_mar_attack - Maroviher attack
- AirPirate - Android 802.11 pentesting tool
- airxploit - Wireless discovery and exploitation framework written in Python
- anubis - Captive wifi hotspot bypass tool for Linux
- AtEar - Wireless Hacking, WiFi Security, Vulnerability Analyzer, Pentestration
- beaconLeak - beaconLeak is an open source tool developed as a proof of concept of the beacon stuffing method as a covert channel. This channel allows command and control or data exfiltration using the wireless network card without association or authentication.
- BoopSuite - A Suite of Tools written in Python for wireless auditing and security testing.

- chap2aleap - Work with asleap+genk
- CloudCrackInstaller - Script which installs Crunch, Pyrit and Cowpatty on a running Amazon EC2 Cluster GPU Instance to crack WPA and WPA2 keys.
- Crippled - WPA/WPA2 Belkin.XXXX, Belkin_XXXXXX, belkin.xxx and belkin.xxxx router default key generator.
- eapeak - Analysis Suite For EAP Enabled Wireless Networks
- Easy-creds - Leverages tools for stealing credentials during a pen test
- evilportals - Evil Portals for the WiFi Pineapple
- FakeAuth - FakeAuthentication Network Attack framework written in python3, and made with poison
- FruityWiFi - Wireless network auditing tool
- hashcatch - Capture handshakes of nearby WiFi networks automatically
- Hijacker - Aircrack, Airodump, Aireplay, MDK3 and Reaver GUI Application for Android
- killosx - Use the Apple CoreText exploit (CVE-2012-3716) and launch an AP to affect all devices within wifi range
- KisMac2 - Free, open source wireless stumbling and security tool for Mac OS X
- LANs.py - Inject code, jam wifi, and spy on wifi users
- ManaToolkit - Mana Toolkit - Module for the WiFi Pineapples.
- Noon - Noon - The Swiss knife of wireless auditing.
- Null-packet-wifi-promt - Simple script to prompt responses from wireless devices with a known MAC address
- pinecone - Pinecone is a WLAN networks auditing tool, suitable for red team usage. It is extensible via modules, and it is designed to be run in Debian-based operating systems. Pinecone is specially oriented to be used with a Raspberry Pi, as a portable wireless auditing box.
- PiWAT - Wireless Attack Toolkit
- probequest - Toolkit for Playing with Wi-Fi Probe Requests
- Pwnagotchi - Pwnagotchi is an A2C-based “AI” powered by bettercap and running on a Raspberry Pi Zero W that learns from its surrounding WiFi environment in order to maximize the crackable WPA key material it captures (either through passive sniffing or by performing deauthentication and association attacks)
- Python-wireless-attacks - Wireless Attacks in Python (Based on blog series)
- scapy-dot11-toolkit - receive and send 802.11 management frames through python-scapy
- Sly-fi - Wifi pwnage automation
- smoothie - Web based wireless auditory tools
- WHAT-PRO - 802.11 Exploitation Tool for use with Kali 2. More tools available than WHAT or

WHAT Pi

- Wi-door - Wi-Fi Backdoors
- WIDSTT - Wireless Intrusion Detection Systems Testing Tool – test your WIDS by performing attacks
- wifibang - wifibang is a set of security tools which perform the main kinds of wifi attacks. Its most important feature is the user-friendly CLI which encourages users to use the script on mobile devices (like a smartphone, maybe associated with a raspberry).
- wifiBuddy - So the plan is to connect a RaspberryPi, a little Display (maybe even touch) and 2 wifi antennas – one for sniffing onw for attacking
- wifi-default-password - Bash script that tries all the default passwords for a particular wifi access point
- WiFiHunter - A WiFi Penetration Toolkit
- wifimonster - Wifi sniffing and hijacking tool
- Wifi-pentesting-guide - WiFi Penetration Testing Guide
- wifuzz - Access Point 802.11 stack fuzzer
- wifuzzit - A 802.11 wireless fuzzer
- WirelessMayhem - Wireless Mayhem is a python framework developed to automate wireless discovery and exploitation.
- wirespy - Framework designed to automate various wireless networks attacks (the project was presented on Pentester Academy TV's toolbox in 2017)
- wombat - An experimental Wi-Fi tracking system aiming at improving user awereness toward physical tracking technologies and at experimenting new privacy-preserving mechanisms.
- wtf - Wireless Test Framework. Collection of test suites for validating various wifi functionality on various wifi devices.
- zarp - Network attack tool centered around the exploitation of local networks

Information Gathering

- 3WiFi Database - Collect data from Router Scan log reports, search for access points, obtain its geolocation coordinates, and display it on world map
- access_points - Scan your WiFi and get access point information and signal quality
- Accumulation-rssi - Linux utility for accumulation of WiFi RSSI to text file. Using nl80211, Managed mode. Useful for experiments with WiFi (example, localization)
- airscan - Wi-Fi scanning utility for the Nintendo DS
- basiciw - Retrieve information such as ESSID or signal quality from wireless cards (Python module)

- Get-rssi - Linux utility for getting RSSI WiFi of APs to text file. Using Monitor mode, libpcap.
- IndoorPositionr - Indoor positioning using Android to provide the surrounding Access Points signals and guess the position
- Isniff-GPS - Passive sniffing tool for capturing and visualising WiFi location data disclosed by iOS devices
- rssi - Indoor localisation using RSSI. RSSI is received signal strength indicator in IEEE 802.11 beacon packet to announce the presence of WiFi
- whoishere - WIFI Client Detection - Identify people by assigning a name to a device performing a wireless probe request.
- Wifi-Dumper - Dump the wifi profiles and cleartext passwords of the connected access points on the Windows machine
- Wifi-monitor - Prints the IPs on your local network that're sending the most packets ack = 802.11 control frame acknowledgement or ...
- WIG - Tools for 802.11 information gathering.
- wraith - Wireless Reconnaissance And Intelligent Target Harvesting

Defense/Detection

- badkarma - BadKarma is a simple python script used to detect and disrupt rouge access points/honeypots using the karma attack such as the wifi pineapple
- eaphammer - Targeted evil twin attacks against WPA2-Enterprise networks. Indirect wireless pivots using hostile portal attacks
- eewids - Easily Expandable Wireless Intrusion Detection System
- etd - The Evil Twin Detector monitors for devices that are trying to spoof your existing wireless access points, if any are found a notification is sent by email and/or syslog over UDP.
- EvilAP_Defender - Protect your Wireless Network from Evil Access Points
- huntpineapples - WiFi Pineapple hunter from DC23
- kismetclient - A Python client for the Kismet server protocol
- kismet - Wireless network detector, sniffer, and intrusion detection system
- kismon - A GUI client for kismet
- KRACKDetection - Used to detect if the current version of wpa_supplicant is vulnerable to the KRACK attack. Developed using Debian 9.2
- krackdetector - Detect and prevent KRACK attacks in your network
- KrackPlus - with KrackPlus users can scan their devices to determine whether they are vulnerable to key reinstallation attacks, or attack those devices
- nzyme - Nzyme collects 802.11 management frames directly from the air and sends them to

a Graylog (Open Source log management) setup for WiFi IDS, monitoring, and incident response. It only needs a JVM and a WiFi adapter that supports monitor mode.

- Openwips-ng - Open source and modular Wireless IPS (Intrusion Prevention System)
- PiDense - Monitor illegal wireless network activities. (Fake Access Points)
- PiFinger - Searches for wifi-pineapple traces and calculate wireless network security score
- PiKarma - Detects wireless network attacks performed by KARMA module (fake AP). Starts deauthentication attack (for fake access points)
- PiSavar - Detects activities of PineAP module and starts deauthentication attack (for fake access points - WiFi Pineapple Activities Detection)
- Python-kismet - Python threaded listener to Kismet broadcasts
- RogueDetection - Rogue Access Point Detection and WIDS
- waidps - Wireless Auditing, Intrusion Detection & Prevention System
- Wave - 802.11 IDS, visualizer, and analytics platform for the web
- Wids-wips - Wireless intrusion detection and prevention system written in C and using kismet server as backend
- Wifi Miner Detector - Detecting malicious WiFi with mining cryptocurrency
- Wireless-forensics-framework - Automated Wireless Penetration Testing and Carrying out Wireless Forensics in Python
- Wireless-ids - Ability to detect suspicious activity such as (WEP/WPA/WPS) attack by sniffing the air for wireless packets
- wmd - Simple solution for the detection and location of Rogue Access Points.
- wspy - Python tool to create a wireless ids it detects which clients are connected to a network to allow the creation of usage patterns of a netowrk by the clients

Libraries/General Purpose Tools

- 80211p_raw - Raw socket utilities for 802.11p transmission
- 80211_raw - Sender and receiver for WiFi (IEEE802.11) network with raw sockets
- banjax - Library for low-level programming of IEEE 802.11 wireless network interfaces on the GNU/Linux operating system
- dot11anonymizer - Anonymizes 802.11 Layer 2 information found in capture files (BSSID, SSID, AP name, etc.)
- dot11er - Some tools for playing with IEEE802.11
- Frame-utils.js - A collection of utilities for processing streams of 80211 frames and radiotap headers.
- Gopacket-80211 - Extra gopacket layers for Radiotap and 802.11 (has been integrated in

Gopacket)

- itamae - 802.11 radiotap and MPDU parser
- Libairpcap-nl - Implementation of AirPcap library, targetting the NL80211 protocol.
- libuwifi - C library for parsing, generating and analyzing Wifi (WLAN 802.11) frames in userspace and related functions
- packetEssentials - An essential set of modules for working with the Scapy Library in Python
- packetparser - IEEE 802.11 packetparser
- pcap2xml - Convert 802.11 Packet Traces to XML and SQLITE Format
- PCS - Set of Python modules and objects that make building network protocol code easier for the protocol developer
- Probr-core - The core-component for generic WiFi tracking: remote device management, packet capturing, packet storage
- py80211 - Suite of libraries for parsing 802.11 packets as well as managing wireless cards and working with 802.11 information
- PyRIC - PyRIC (is a Linux only) library providing wireless developers and pentesters the ability to identify, enumerate and manipulate their system's wireless cards programmatically in Python.
- python3-wifi - Python WiFi is a Python module that provides read and write access to a wireless network card's capabilities using the Linux Wireless Extensions.
- Python-radiotap - Tiny lib for parsing radiotap/802.11 headers in python
- python-wifi - Python WiFi is a Python module that provides read and write access to a wireless network card's capabilities using the Linux Wireless Extensions.
- Qca-swiss-army-knife - Hosts a set of utilities that we use to debug / help with our driver development
- Radioparse - A WiFi protocol parser that can be used with radiotap packets and node-pcap
- Scapy - Python-based interactive packet manipulation program & library
- Wifi-scan - A nl80211 C/C++ library for monitoring signal strength of WiFi networks
- wifi-scripts - Misc scripts and tools for WiFi
- wireless - Dead simple, cross-platform Python library to connect to wireless networks

Visualization

- airview - A python web application compliment to py80211 which allows you to visualize the airwaves around you with your web browser.
- Sparrow-wifi - Next-Gen GUI-based WiFi and Bluetooth Analyzer for Linux
- speccy - Visualization tool for ath spectral scan

- Wifi-contour - A contour mapping program of wireless 802.11 signal strength
- Wifi-heatmap - Generate heatmaps of wifi coverage with Python
- wifiscanvisualizer - Wi-Fi Scan Visualizer by Pentester Academy
- Wifi-Signal-Plotter - A Python script for graphing and comparing the WiFi signal strengths between WiFi adaptors in Windows or Linux.
- wifivis - Visualize some mit wifi access point data
- wipi - Visualize the WiFi packages that are floating around us all the time.
- Wlan-stats - Tool chain using tshark to pull data from pcaps, further process them in python, and graph the output in R.

Localisation

- Find-lf - Track the location of every Wi-Fi device (📱) in your house using Raspberry Pis and FIND
- geowifi - This is a Geographic WiFi Positioning program written under the Linux.(it is also a WiFi Positioning API written for C language
- GrapplingHook - Open Source 802.11 Direction Finder
- gtaiad - Indoor Wi-Fi navigation prototype using triangulation
- Openwifimap-api - OpenWiFiMap database and its api
- Python Wi-Fi Positioning System - Python Wi-Fi Positioning System - Wi-Fi geolocation script using the Google Geolocation API
- whereami - Uses WiFi signals 📶 and machine learning to predict where you are
- Wifi-geolocation - Get your latitude/longitude via wifi access points
- Wifi-localization - Wifi Localization using a map and reference
- Wifi-locator - Determines physical location of station judging from 802.11 beacons' BSSID/Signal/Noise/Quality information.
- Wi-finder - Wi-Fi hotspot finder
- Wlan-pos - Location fingerprinting and triangulation engine for WLAN (IEEE802.11,aka WiFi) environment.

Configuration/setup

- 802.11p-iw - Wireless configuration tool (UNIX)
- agentapd - Agent of WiFi hardware
- AirLibre - Python API For UBNT AirOS Devices
- AtherosROMKit - Atheros ROM modding and recovery kit

- cac - A Centralized Adaptive Control algorithm that optimises the performance of IEEE 802.11 WLANs
- captiveportal - A captive portal that can be used on most linux distributions.
- cloudap - AP Manager in Cloud,AP Hardware on your side
- connme - Client for Hostapd
- crda - Central Regulatory Domain Agent
- create_ap - This script creates a NATed or Bridged WiFi Access Point.
- disable-802.11b-snmp - A tool to set 802.11 protocols on thousands of Access Points with SNMP.
- full_permissive_unlock_ath - This kernel patch enable all 2GHZ & 5GHZ channels (without restriction) for ath9k & ath5k forced to use buildin world regulatory
- FWAP - Minimal, very lightweight access point implementation
- hostapd - Python script to make using and configuring hostapd easier
- hostapd - User space daemon for access point and authentication servers
- hostapd-mana-openwrt - Hostapd-mana - build-files, and installation-files for OpenWRT
- Hostapd-with-WebID - WebID integrated hostapd
- Hostapd-wpe-openwrt - Hostapd-wpe (Wireless Pwnage Edition) packages for OpenWRT Barrier Breaker 14.07
- hotspotd - Simple daemon to create a wifi hotspot on Linux
- IEEE802.11-complete - IEEE802.11 protocol, including PHY, MAC, and rate adaptation approaches upon GNURadio/USRP software-defined radio platform
- Linux-wifi-tools - A set of Linux command line tools for managing and troubleshooting wifi
- monmob - Set of tools to provide monitor mode and raw frame injection for devices using broadcom chipsets bcm4325, bcm4329 and bcm4330
- nexmon - The C-based Firmware Patching Framework for Broadcom/Cypress WiFi Chips that enables Monitor Mode, Frame Injection and much more
- PyWiWi - Python Windows Wifi
- reghack - Replaces the regulatory domain rules in the driver binaries with less restrictive ones
- RegMon - RegMon is a Atheros WiFi card register monitoring tool for Linux OpenWrt
- remoteapd - Remote NL80211-Extent driver for Hostapd 2.0
- resfi - Framework supporting creation of RRM functionality in residential WiFi deployments
- rollmac - Automated WiFi limit evasion
- RT73-USB-Wireless- - Patched version of RT73USBWireless for Yosemite
- RTL8188-hostapd - Hostapd for Realtek RTL8188
- Wifi-ap - Library wrapper around hostapd and dnsmasq and their respective configuration

files that allows for programmatically creating access points in Debian-based Linux environments

- Wifi-configurator - Utility for command line configuration of hostapd
- Wifi-frequency-hacker - A modified frequency regulatory domain configuration that doesn't limit you.
- Wifi-txpower-unlocker - A bash script that generates a modified regulatory.bin to unlock the maximum WiFi TX power (on 2.4 Ghz) of the region BO
- WirelessConfig - A 802.1x Python wireless configuration tool with Cocoa wrappers

Monitoring

- como - CoMo is a passive monitoring system that supports arbitrary real time traffic queries
- horst - Lightweight IEEE802.11 wireless LAN analyzer with a text interface. Its basic function is similar to tcpdump, Wireshark or Kismet, but it's much smaller and shows different, aggregated information which is not easily available from other tools.
- scapybase - 802.11 monitor AP based on scapy
- Scapy-survey - 802.11 signal strength logger using Scapy
- sigmon - Modular WiFi/RF Monitoring and Analysis Implementation
- Wifi-linux - Simple python script to monitor access point signal strength.
- WiFiStat - Python tool to assess WiFi connection throughput and latency
- WiPy - Sends the WiFi signal strength from multiple clients to a central server. Built for Arch Linux ARM running on Raspberry pi 2
- WLAN-Monitoring - Monitor our vicinity to monitor wireless devices and traffic
- wmon - A Wireless Network Monitor with advanced measurement capabilities.

Miscellaneous/not sorted :)

- 80211ping - Linux command-line tool to ping 802.11 stations (e.g. any WiFi device)
- acs - Automatic Channel Selection utility
- Airfree-wt - Wireless Security Toolkit
- Ap-notify - An example of using the Linux kernel netlink protocol, specifically nl80211 via libnl/libnl-genl, to catch stations associating/disassociating with an 802.11 AP
- ath9k-4w-patch - Resources for increasing power of ath9k devices, such as TP-link WN722N
- Ath9k-nav - Linux kernel module to poll the NAV register on Atheros 9k series WLAN cards.
- bunny - Bunny is a wireless. meshing, darknet that uses 802.11 to hide its communications

- captiv8 - Captive Portal Evasion Tool
- Chura-Liya - A wireless interactive shell which utilizes 802.11 Management Frames to establish communication between two devices
- CODEX - Its like airgeddon but better!
- Connect-wifi - Dmenu based application for Linux that connects to the strongest open wireless network
- Cover-channel - Userland code for creating a covert channel in wireless broadcast medium
- disassociatedWiFi - DisassociatedWiFi creates a virtual network interface (using the Linux TUN/TAP device driver) which sends and receives ethernet frames over an 802.11 (WiFi) interface, that has been placed in monitor mode, and supports packet injection.
- FFT_eval - Aid open source spectrum analyzer development for Qualcomm/Atheros AR92xx and AR93xx based chipsets
- Frame-randomizer - Capture and randomize 802.11 Association Request frames
- FreeWifi - How to get free wifi
- Haiku-wifi - Turn your wireless router's extra radios into a public billboard!
- kismet2earth - Set of utilities that convert from Kismet logs to Google Earth .kml format
- kismeth2earth - Parsing Kismet logs to get collected data from wireless networks and generate a Google Earth map
- Kismet-to-KML - Converts kismet gps log files into kml files
- Mac-analyzer - Collects cross layer stats from ath9k
- Madwifi-be - Modified version of the madwifi driver allowing update of WME parameters for the BE access category
- Madwifi-hopping - Modified version of the Madwifi WLAN driver, that employs power-hopping for packet transmission
- make-a-new-mac80211-to-wirelessAP -
- netxml2kml - Converts netxml files from Kismet Newcore into KML or KMZ files for Google Earth
- openwifi - open-source IEEE802.11/Wi-Fi baseband chip/FPGA design
- Osx-wificleaner - Cleans out open wireless connections from OSX machine
- Osx-wifi-scan - Hacky wifi signal scanner for osx
- P4wnP1 - WiFi covert channel - Client agent (experimental Proof of Concept)
- parsecaps - Parse wpa.cap generated from besside-ng and create individual .caps for each network with a captured handshake.
- pcap80211analyzer - Not-so-smart 802.11 frame pcapng analyzer
- Probr-analysis - Analysis components for the probr WiFi tracking system
- py_DD_WRT_Remote_Mac_Adder - Python Script to remotely update mac filterlists of DD-

WRT routers with wl or atheros wifi drivers

- pykismetkml - Python script designed to export .gps and .xml files (in < Kismet RC1) to .kml files and .netxml files to .kml files in => Kismet RC2
- pykismetstats - Pykismetstats parses NetXML file generated by kismet and write statistics to CSV file.
- PyScapy - This is a package of using scapy.
- react80211 - Solution for mitigating the performance impairments of CSMA/CA protocols in multi-hop topologies based on the dynamic adaptation of the contention process experienced by nodes in a wireless network
- Rollmac - Automated WiFi limit evasion
- Scapy-rssi - Example of how to read RSSI values from wifi packaged using Scapy
- setbssid - Modify the MAC80211 layer in Linux Kernel
- skybluetero - 802.11b/g packet airtime consumption analyzer GUI for Linux
- sniffmypackets - Canari package for pcap file analysis within Maltego
- Snoopy-ng - Snoopy v2.0 - modular digital terrestrial tracking framework
- spectrum.py -
- Tools-Airgeddon - Tools Install Airgeddon Full
- VX - It might be fun to play tricks on somebody trying to crack your WEP protected router
- Wbc-utils - Couple of hacked together utils for use with the wifibroadcast system by befinitiv
- wi5-aggregation - Implementing and testing 802.11 frame aggregation (A-MPDU)
- WiFi-Analyzer - Analyzer 802.11 networks - android app [to refactor]
- wifi_based_population_estimator - This is a piece of glueware that sticks up different components from hardware detection to real-time web display.
- Wifi-beeper - Linux command-line tool to make WLAN frames audible
- wifidec - Repository for scriptz playing around with decoding elements of the Wifi stack (mainly Radiotap and 802.11 frames)
- wifi_decode - Wireless Key Dumper for Windows
- Wifidog-gateway - Repository for the wifidog-gateway captive portal designed for embedded systems
- Wifi-dump-analysis - Processing wireless traces from binary files written and read in custom format.
- wifi_dump_parser-v3 - Is the modified parser for the new data set collected using Wifi-dump
- wifi_dump-tmpfs - Dumps wifi data
- Wifiexplorer-sensor - WiFi Explorer Pro allows you to connect to a remote platform (e.g.

Raspberry Pi) and perform a passive Wi-Fi scan using a capable Wi-Fi adapter. When a remote sensor is used, the scan results are sent back to WiFi Explorer Pro for its visualization.

- wifi - [unmaintained] WiFi tools for linux http://pypi.python.org/pypi/wifi
- Wifi-mac-tracking - "Code and datasets for the paper entitled ""Non-cooperative 802.11 MAC layer fingerprinting and tracking of mobile devices"". "
- wifirxpower - Linux-based WiFi RX Power Grapher
- wifiScanMap - An other wifi mapping tool
- WiFi-scheduling - This project evaluates the efficiency and overhead of wireless network scheduling
- wifi_statistics - Linux kernel module to gather wifi statistics from peer and non-peer STAs
- wifitracker - Raspberry Pi Wifi Tracking API
- WifiTrafficAnalyzer -
- wifresti - Find your wireless network password in Windows , Linux and Mac OS
- wime - Wifi password recover tool for Windows, Linux, Mac.
- win32wifi - Python Windows Wifi
- wireless_half-mini - MacOS Airport Half Mini (WiFi and Bluetooth)
- WIRELESSINFO - Extract Important Data From Cisco Wireless Controllers
- wireless_RSSI -
- Wireless-tools - Wireless tools for Node.js
- wit - Command-line wifi manager for linux
- wobs - Detects near-by devices such as cell phones, tablets, and laptops. Does this through 802.11, Bluetooth, cell phone protocols, etc...