

WirelessDefence.org's Wireless Penetration Testing Framework

See <http://www.vulnerabilityassessment.co.uk> for the full Penetration Testing Framework

Wireless Penetration

Wireless Toolkit

Wireless Discovery

- [Aerosol](#)
- [Airfart](#)
- [Aphopper](#)
- [Apradar](#)
- [karma](#)
- [Kismet](#)
- [MiniStumbler](#)
- [Netstumbler](#)
- [Wellenreiter](#)
- [Wifi Hopper](#)
- [WirelessMon](#)

Packet Capture

- [Airopeek](#)
- [Airtraf](#)
- [Apsniff](#)
- [Cain](#)
- [Wireshark](#)

WEP/ WPA Password Attack Tools

- [Aircrack-ptw](#)
- [Aircrack-ng](#)
- [Aircrack](#)
- [Airsnot](#)
- [cowpatty](#)
- [wep attack](#)
- [wep crack](#)
- [Airbase](#)
- [wzcook](#)

Leap Attack Tools

- [asleep](#)
- [the leap cracker](#)
- [anwrap](#)

Frame Generation Software

- [Airobbler](#)
- [airpwn](#)
- [Airsnarf](#)
- [Commview](#)
- [fake ap](#)
- [void 11](#)

[wifi tap](#)

wifitap -b <BSSID> [-o <iface>] [-i <iface>] [-p] [-w <WEP key> [-k <key id>]] [-d [-v]] [-h]

Mapping Software

[Knsngem](#)

File Format Conversion Tools

[ns1 recovery and conversion tool](#)

[warbable](#)

[warkizniz](#)

warkizniz04b.exe [kismet.csv] [kismet.gps] [ns1 filename]

[ivstools](#)

IDS Tools

[WIDZ](#)

[War Scanner](#)

[Snort-Wireless](#)

[AirDefense](#)

[AirMagnet](#)

WLAN discovery

Unencrypted WLAN

Visible SSID

Sniff for IP range

MAC authorised

MAC filtering

Spoof valid MAC

[Linux](#)

ifconfig [interface] hw ether [MAC]

[macchanger](#)

Random Mac Address:- macchanger -r eth0

[mac address changer for windows](#)

[madmacs](#)

[TMAC](#)

[SMAC](#)

Hidden SSID

Deauth client

[1](#) [Aireplay-ng](#)

aireplay -0 1 -a [Access Point MAC] -c [Client MAC] [interface]

[2](#) [Commview](#)

Tools > Node reassociation

[3](#) [Void11](#)

void11_penetration wlan0 -D -t 1 -B [MAC]

WEP encrypted WLAN

Visible SSID

[WEPattack](#)

wepattack -f [dumpfile] -m [mode] -w [wordlist] -n [network]

[Capture / Inject packets](#)

Break WEP

[1](#) [Aircrack-ptw](#)

aircrack-ptw [pcap file]

[2](#) [Aircrack-ng](#)

aircrack -q -n [WEP key length] -b [BSSID] [pcap file]

[3](#) [Airsnot](#)

Channel > Start

[4](#) [WEPcrack](#)

perl WEPcrack.pl

./pcap-getIV.pl -b 13 -i wlan0

Hidden SSID

Deauth client

1  [Aireplay-ng](#)

aireplay -0 1 -a [Access Point MAC] -c [Client MAC] [interface]

2 [Commview](#)

Tools > Node reassociation

3  [Void11](#)

void11_hopper

void11_penetration [interface] -D -s [type of attack] -s [station MAC] -S [SSID] -B [BSSID]

WPA / WPA2 encrypted WLAN

[Deauth client](#)

Capture EAPOL handshake

WPA / WPA 2 dictionary attack

1  [cowPAtty](#)

./cowpatty -r [pcap file] -f [wordlist] -s [SSID]

./genpmk -f dictionary_file -d hashfile_name -s ssid

./cowpatty -r capture_file.cap -d hashfile_name -s ssid

2  [Aircrack-ng](#)

aircrack-ng -a 2 -w [wordlist] [pcap file]

LEAP encrypted WLAN

Deauth client

Break LEAP

 [asleap](#)

./asleap -r data/libpcap_packet_capture_file.dump -f output_pass+hash file.dat -n
output_index_filename.idx

./genkeys -r dictionary_file -f output_pass+hash file.dat -n output_index_filename.idx

 [THC-LEAPcracker](#)

leap-cracker -f [wordlist] -t [NT challenge response] -c [challenge]

802.1x WLAN

Create Rogue Access Point

 [Airsnarf](#)

Deauth client

Associate client

Compromise client

Acquire passphrase / certificate

wzcook

Obtain user's certificate

 [fake ap](#)

perl fakeap.pl --interface wlan0

perl fakeap.pl --interface wlan0 --channel 11 --essid fake_name --wep 1 --key [WEP KEY]

 [Hotspotter](#)

Deauth client

Associate client

Compromise client

Acquire passphrase / certificate

wzcook

Obtain user's certificate

 [Karma](#)

Deauth client

Associate client

Compromise client

Acquire passphrase / certificate

wzcook

Obtain user's certificate

./bin/karma etc/karma-lan.xml

 [Linux rogue AP](#)

Deauth client

Associate client

Compromise client

Acquire passphrase / certificate

wzcook

Obtain user's certificate

Resources

URL's

[Wirelessdefence.org](#)

[Wardrive.net](#)

[Wireless Vulnerabilities and Exploits \(WVE\)](#)

White Papers

[Breaking 104 bit WEP in less than 60 seconds](#)

[Weaknesses in the Key Scheduling Algorithm of RC4](#)

[802.11b Firmware-Level Attacks](#)

[Wireless Attacks from an Intrusion Detection Perspective](#)

[Implementing a Secure Wireless Network for a Windows Environment](#)

Common Vulnerabilities and Exploits (CVE)

Vulnerabilities and exploit information relating to these products can be found here: <http://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=wireless>

2007

[Multiple cross-site scripting \(XSS\) vulnerabilities in Cisco Secure Access Control Server \(ACS\)](#)

[Aruba Mobility Controllers and Alcatel-Lucent OmniAccess Wireless do not properly implement authentication and privilege assignment for the guest account](#)

[Heap-based buffer overflow in the management interfaces in Aruba Mobility Controllers and Alcatel-Lucent OmniAccess Wireless](#)

[Intel 2200BG 802.11 Wireless Mini-PCI driver allows remote attackers to cause a denial of service](#)

Wireless Assessment. The following information should ideally be obtained/enumerated when carrying out your wireless assessment. All this information is needed to give the tester, (and hence, the customer), a clear and concise picture of the network you are assessing. A brief overview of the network during a pre-site meeting with the customer should allow you to estimate the timescales required to carry the assessment out.

Site Map

RF Map

Lines of Sight

Signal Coverage

Standard Antenna

Directional Antenna

Physical Map

Triangulate APs

Satellite Imagery

Network Map

MAC Filter

Authorised MAC Addresses

Reaction to Non-Authorised MAC Addresses

Encryption Keys utilised

WEP

Key Length

Crack Time

Key

WPA/PSK

Pre-Shared Key, (PSK) where every user is given the same pass-phrase. WiFi Protected Access, (WPA / WPA2) improved authentication and encryption.

Temporal Key Integrity Protocol (TKIP)

TKIP. The Interim solution to replace the notoriously weak WEP.

Key

Attack Time

Advanced Encryption Standard (AES)

AES (a.k.a WPA2 and 802.11i). The preferred standard for the encryption for securing sensitive data.

Key

Attack Time

802.1x

Derivative of 802.1x in use

Access Points

ESSID

Extended Service Set Identifier (ESSID).

Broadcast ESSIDs

BSSIDs

Basic Service Set Identifier (BSSID).

Vendor

Channel

Associations

Rogue AP Activity

Wireless Clients

MAC Addresses

Vendor

Adhoc or Infrastructure Mode

ESSID Probes

Associations

Intercepted Traffic

Encrypted

Clear Text