



# WiFi Penetration Testing Tools



<https://cyberexam.io>

# Table Of Content

- 1. Configuration**
- 2. Information Gathering**
- 3. Rouge Access Point**
- 4. Cracking**
- 5. Decryption**
- 6. Packet Manipulation**
- 7. Blue Team**

# Configuration

## airmon-ng

The **airmon-ng** tool is a tool belonging to the aircrack-ng family. Using this tool, you can put the network card in monitor mode.

```
kali@kali:~  
File Actions Edit View Help  
root@kali:~# airmon-ng  
  
PHY      Interface      Driver      Chipset  
phy8      wlan0          rt2800usb    Ralink Technology, Corp. RT5370  
  
root@kali:~# airmon-ng start wlan0  
  
PHY      Interface      Driver      Chipset  
phy8      wlan0          rt2800usb    Ralink Technology, Corp. RT5370  
)  
        (mac80211 monitor mode vif enabled for [phy8]wlan0 on [phy8]wlan0mon  
        (mac80211 station mode vif disabled for [phy8]wlan0)  
  
root@kali:~#
```

# Configuration

## ifconfig, iw

It is a command used to view and configure wireless network cards. With this command, we can also put network cards in monitor mode.

```
kali@kali:~  
File Actions Edit View Help  
root@kali:~# ifconfig wlan0 down  
root@kali:~# iw wlan0 set monitor none  
root@kali:~# ifconfig wlan0 up  
root@kali:~# iw dev  
phy#8  
      Interface wlan0  
            ifindex 16  
            wdev 0x8000000003  
            addr 1c:hf:ce:1a:24:9a  
            type monitor  
            channel 10 (2457 MHz), width: 20 MHz (no HT), center1: 2457 MHz  
            txpower 30.00 dBm  
root@kali:~#
```

# Configuration

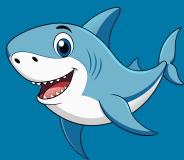
## ifconfig, iwconfig

The **iwconfig** command is used to configure wireless network cards. If you want to view detailed information about the wireless network cards installed in your system, you can use this command.

```
kali@kali:~  
File Actions Edit View Help  
root@kali:~# iwconfig  
lo      no wireless extensions.  
  
eth0    no wireless extensions.  
  
wlan0   IEEE 802.11 ESSID:off/any  
        Mode:Managed Access Point: Not-Associated Tx-Power=0 dBm  
        Retry short long limit:2 RTS thr:off Fragment thr:off  
        Encryption key:off  
        Power Management:off  
  
root@kali:~# ifconfig wlan0 down  
root@kali:~# iwconfig wlan0 mode Monitor  
root@kali:~# ifconfig wlan0 up  
root@kali:~# █
```

# Information Gathering

## Wireshark



**Wireshark** is a powerful tool in wireless network Pentest processes, used to capture and analyze traffic in monitor mode. It helps identify SSIDs, BSSIDs, encryption types, and can capture WPA/WPA2 handshakes for password cracking. It's also useful for detecting suspicious traffic or unauthorized devices.

The screenshot shows the Wireshark interface with the following details:

- Toolbar:** File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, Help.
- Search Bar:** Apply a display filter ... <Ctrl-/>
- Table Headers:** No., Time, Source, Destination, Yeni Kolon - Özel Filtre, Protocol, Length/Info.
- Selected Row (Frame 1):** 1 0.000000 HuaweiTe\_1b... Broadcast 802... 307 Beacon frame, SN=3639, FN=0, Flags=....
- Frame Details:** Frame 1: 307 bytes on wire (2456 bits), 307 bytes captured (2456 bits). IEEE 802.11 Beacon frame, Flags: .... IEEE 802.11 Wireless Management. Fixed parameters (12 bytes). Tagged parameters (271 bytes). Tags include: SSID parameter set: The Cyber Path, Supported Rates 1(B), 2(B), 5.5(B), 11(B), 6, 9, 12, 18, [Mbit/sec], DS Parameter set: Current Channel: 8, Traffic Indication Map (TIM): DTIM 0 of 0 bitmap, Country Information: Country Code TR, Environment Any, ERP Information, Extended Supported Rates 24, 36, 48, 54, [Mbit/sec], HT Capabilities (802.11n D1.10), HT Information (802.11n D1.10), Overlapping BSS Scan Parameters, Extended Capabilities (1 octet), Vendor Specific: Microsoft Corp.: WPA Information Element, RSN Information, Vendor Specific: Microsoft Corp.: WMM/WME: Parameter Element, Vendor Specific: Epigram, Inc.: HT Capabilities (802.11n D1.10).
- Hex Dump:** Shows the raw bytes of the selected frame:

0000	80 00 00 00 ff ff ff ff ff ff ff 80 13 82 1b f6 81	.....
0010	80 13 82 1b f6 81 70 e3 7e 31 55 16 00 00 00 00	.....p~1U.....
0020	64 00 11 04 00 00 0e 54 68 65 20 43 79 62 65 72 20	d.....Th e Cyber
- Bottom Status Bar:** packets.pcap, Packets: 8 · Displayed: 8 (100.0%), Profile: Default

# Information Gathering

## airodump-ng

**Airodump-ng** is used to collect information in wireless network penetration tests. With the Airodump-ng tool, you can analyze previously captured traffic. You can also perform real-time wireless network traffic analysis. It also makes traffic analysis much easier with its filtering options.

```
kali㉿kali: ~
File Actions Edit View Help
CH 12 ][ Elapsed: 0 s ][ 2020-07-18 04:17
BSSID          PWR  Beacons #Data, /s CH   MB   ENC CIPHER AUTH ESSI           MANUFACTURER
94:FE:9D:E8:09:49 -76      4     11    0   6   270   WPA2 CCMP   PSK  VodafoneNet-e80940 SHENZHEN GON
5C:63:BF:8A:84:70 -68      2     2     0   10  130   WPA2 CCMP   PSK  TurkTelekom_Yilmaz TP-LINK TECH
C8:54:4B:18:E7:70 -71      3     0     0   4   130   WPA  CCMP   PSK  TurkTelekom_ZKUU4 Zyxel Commun
E8:37:7A:D6:DF:D5 -69      2     0     0   2   130   WPA  CCMP   PSK  TTNET_ZyXEL_TAPP Zyxel Commun
98:E7:F5:AB:95:AD -57      1     1     0   7   130   WPA2 CCMP   PSK  Emni_12_3_2021 HUAWEI TECHN
3A:6B:1C:07:56:7B -75      2     0     0   1   270   WPA2 CCMP   PSK  SUPERBOX_Wi-Fi_3349 Unknown
1C:A5:32:E2:01:A9 -73      2     0     0   1   270   WPA  CCMP   PSK  VodafoneNet-e201a0 SHENZHEN GON
5C:63:BF:6F:3F:CA -77      3     0     0   10  130   WPA2 CCMP   PSK  TurkTelekom_T9FA9 TP-LINK TECH
BSSID          STATION          PWR  Rate   Lost   Frames Notes Probes
94:FE:9D:E8:09:49 6C:00:6B:0B:36:35 -1   1e- 0     0     11
5C:63:BF:8A:84:70 50:3E:AA:36:2A:D1 -1   0e- 0     0     1
5C:63:BF:6F:3F:CA F0:DB:F8:16:22:03 -80  0 - 1     0     1
Quitting...
root@kali:/home/kali# airodump-ng wlan0mon --manufacturer
```

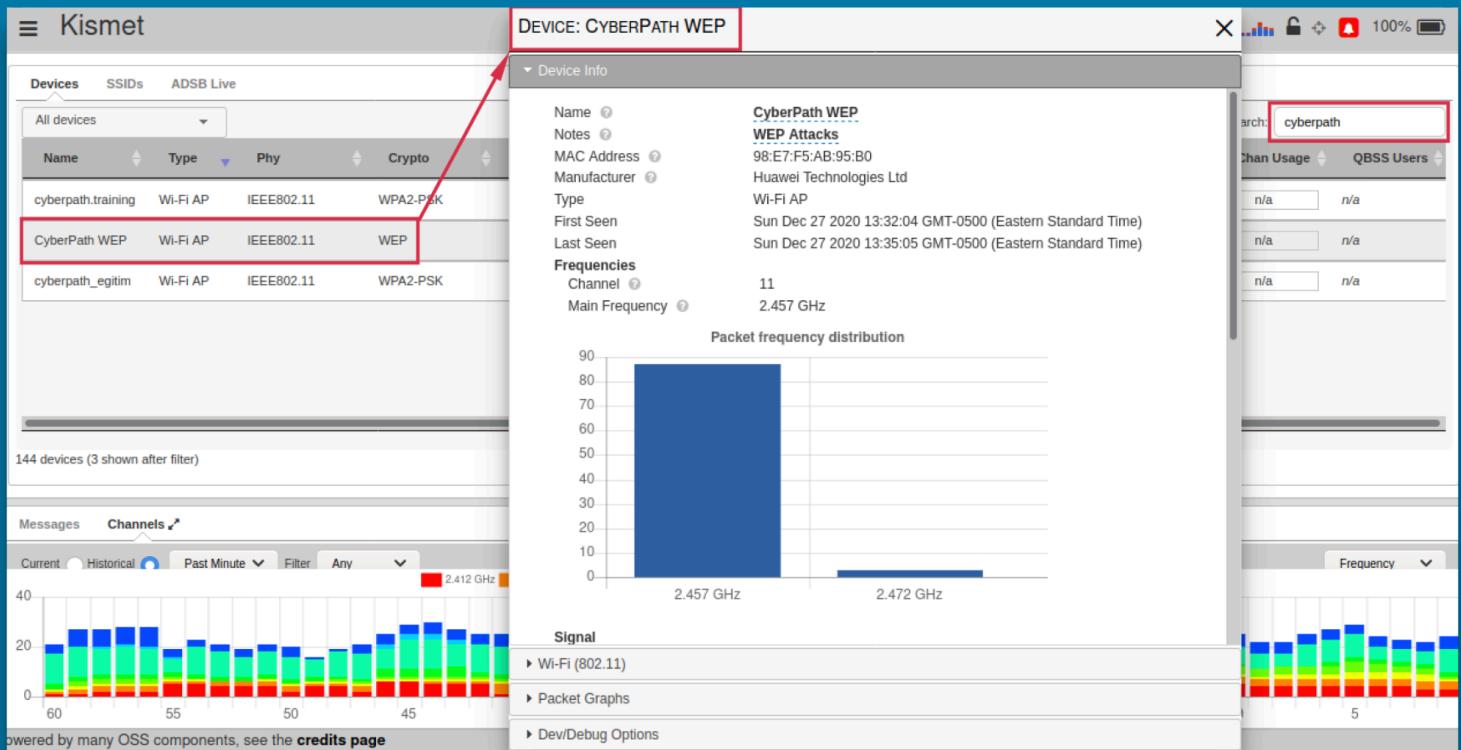
# Information Gathering

## KISMET

wifi attack detection



**Kismet** is a wireless network detector and sniffer used in Pentest processes to discover hidden networks, detect access points, and capture packets in monitor mode. It's valuable for identifying rogue devices, analyzing signal strength, and gathering data for further analysis or attacks like WPA handshake capture.



# Information Gathering

## Windows Commands (netsh)

When performing information gathering operations about wireless networks, if you do not have a wireless network adapter or a wireless network adapter that supports monitor mode, you can use the “**netsh**” command to gather information about nearby access points. You can use two different “**modes**” when performing information gathering operations with the “**netsh**” command. These are mode=ssid and mode=bssid scanning types.

```
PS C:\Users\besim\> netsh wlan show network mode=bssid

Interface name : Wi-Fi
There are 18 networks currently visible.

SSID 2 : cyberpath.training
Network type          : Infrastructure
Authentication        : WPA2-Personal
Encryption            : CCMP
BSSID 1              : 98:e7:f5:ab:95:ad
Signal                : 70%
Radio type            : 802.11n
Channel               : 9
Basic rates (Mbps)   : 1 2 5.5 11
Other rates (Mbps)   : 6 9 12 18 24 36 48 54

SSID 3 : cyberpath_egitim
Network type          : Infrastructure
Authentication        : WPA2-Personal
Encryption            : CCMP
BSSID 1              : 98:e7:f5:ab:95:ae
Signal                : 70%
Radio type            : 802.11n
Channel               : 9
Basic rates (Mbps)   : 1 2 5.5 11
Other rates (Mbps)   : 6 9 12 18 24 36 48 54
```

# Information Gathering

## Microsoft Network Monitor



In Windows systems, it is quite difficult and curious to collect information by putting the wireless network card in monitor mode. **Windows Network Monitor** solves this problem at this point.

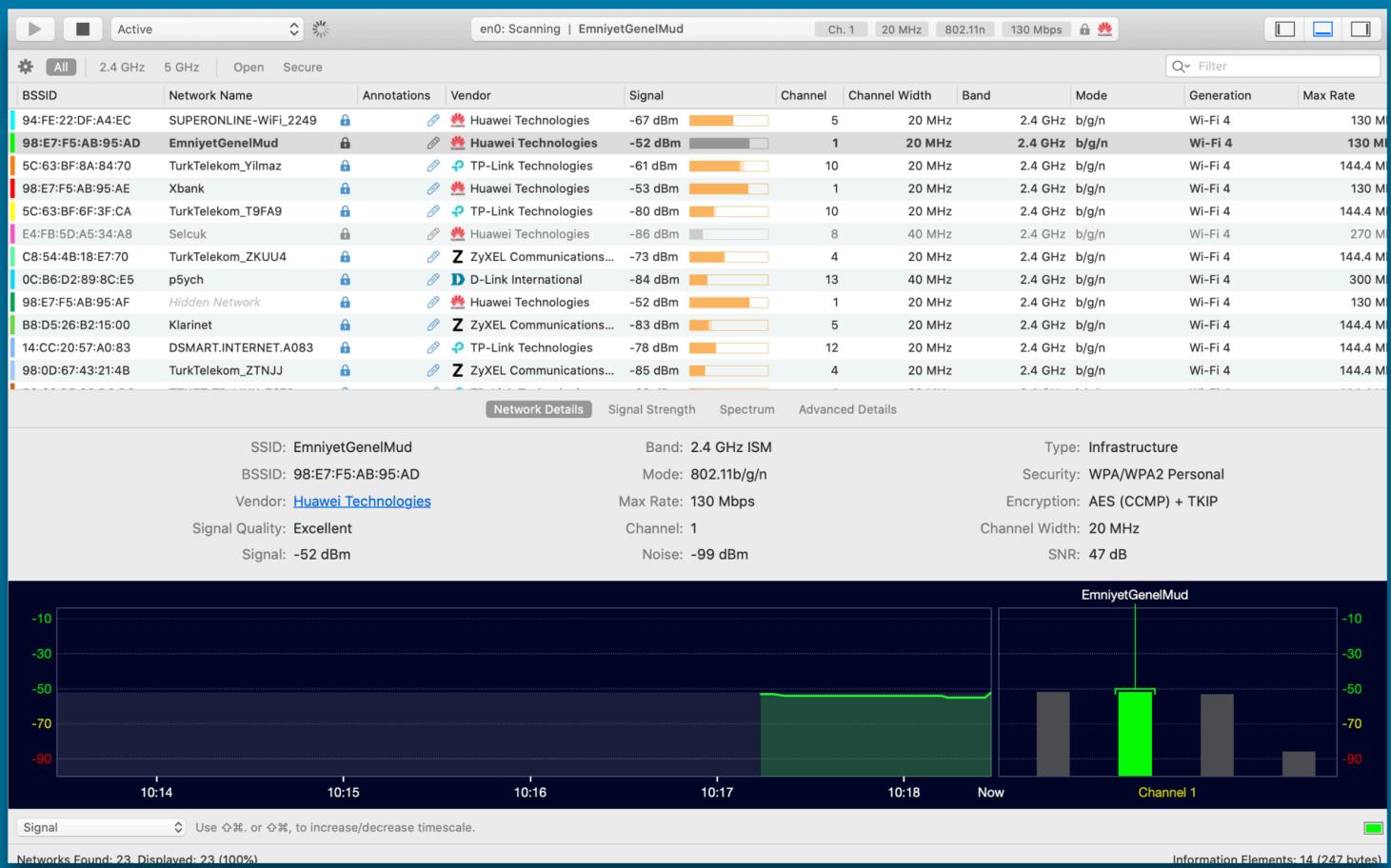
The screenshot shows the Microsoft Network Monitor interface. The main window displays a list of captured frames (Frame Summary) with columns for Frame Number, Time, Date, Local Adjusted Time, Offset, Process Name, Source, Destination, Protocol, Name, and Description. A red '1' highlights the first frame. The second frame is highlighted with a red '2'. The third frame is highlighted with a red '3'. The fourth frame is highlighted with a red '4'. The bottom right corner shows a hex dump of the selected frame (Frame Off: 0x000). The bottom status bar indicates: Version 3.4.2350.0, Displayed: 19, Dropped: 0, Captured: 10, Pending: 0, Focused: 6, Selected: 1.

# Information Gathering

## MacOS Network Monitor



**WiFi Explorer Pro** is a Wi-Fi scanner and analyzer for Mac designed to help WLAN and IT professionals design, verify, and troubleshoot wireless networks. When you first access the tool, you will see a panel like the one below. There may be slight differences depending on the version of the tool. However, the general design is as seen in the image below.



# Information Gathering

## MacOS Airport



The **airport command** is more powerful than just listing information on the current wireless network. It can change any wi-fi settings, network card settings, troubleshoot network problems, change the types of security used on a connection, log packets to a pcap file, join and connect to wireless networks, leave a wifi network, prioritize routers and networks, view signal strength and interference, adjust wi-fi hardware drivers, and perform a wide range of network troubleshooting functions. This is one of the most powerful ways to interact with the wireless card on a Mac.

```
MacBook-Pro:~ besimaltinok$ airport -I
    agrCtlRSSI: -62
    agrExtRSSI: 0
    agrCtlNoise: -100
    agrExtNoise: 0
        state: running
        op mode: station
    lastTxRate: 52
        maxRate: 144
lastAssocStatus: 0
    802.11 auth: open
        link auth: wpa2-psk
            BSSID: 98:e7:f5:ab:95:ad
            SSID: cyberpath.training
            MCS: 5
        channel: 11
MacBook-Pro:~ besimaltinok$
```

# Rouge Access Point

## hostapd-wpe

This package contains hostapd modified with hostapd-wpe.patch. It implements IEEE 802.1x Authenticator and Authentication Server impersonation attacks to obtain client credentials, establish connectivity to the client, and launch other attacks where applicable.

```
File Actions Edit View Help
[ /etc/hostapd-wpe ]
# hostapd-wpe ./FakeAP/FakeAP.conf
Configuration file: ./FakeAP/FakeAP.conf
Using interface wlan0 with hwaddr b6:eb:3b:fc:18:cf and ssid "TARGET"
wlan0: interface state UNINITIALIZED->ENABLED
wlan0: AP-ENABLED
```

# Rouge Access Point

## eaphammer

EAPHammer is a toolkit for performing targeted evil twin attacks against WPA2-Enterprise networks. It is designed to be used in full scope wireless assessments and red team engagements. As such, focus is placed on providing an easy-to-use interface that can be leveraged to execute powerful wireless attacks with minimal manual configuration. To illustrate just how fast this tool is, our Quick Start section provides an example of how to execute a credential stealing evil twin attack against a WPA2-EAP network in just commands.

```
root@kali:~# eaphammer -h
```



Now with more fast travel than a next-gen Bethesda game.

Version: 1.14.0  
Codename: Final Frontier  
Author: @s0lst1c3  
Contact: gabriel<at>transmitengage.com

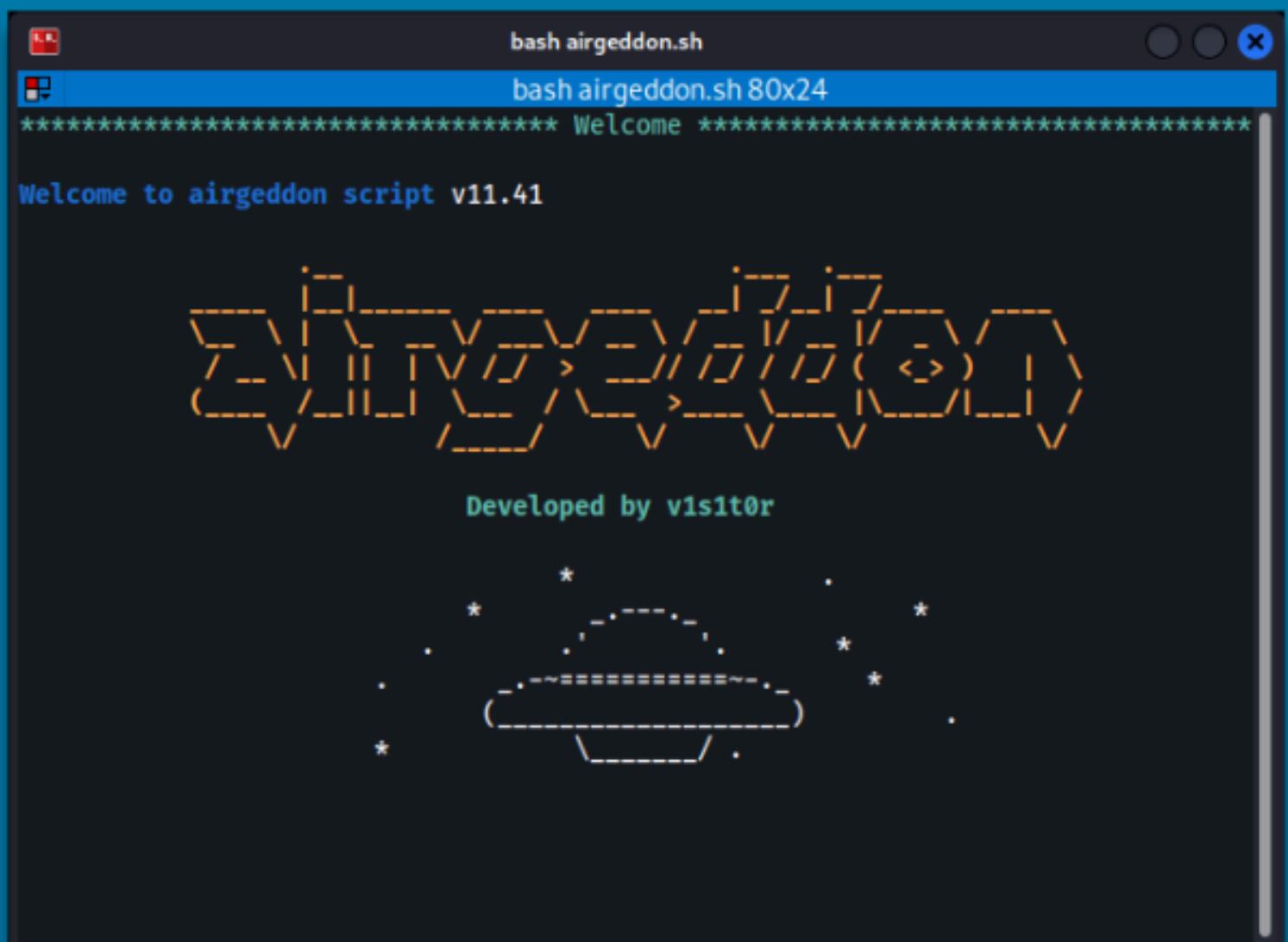
```
usage: eaphammer [-h] [--cert-wizard [{create,import,interactive,list,dh}]] |  
                  --list-templates | --create-template | --delete-template |  
                  --bootstrap | --creds | --pmkid | --eap-spray |  
                  --hostile-portal | --captive-portal-server-only |  
                  --captive-portal] [--debu] [--lhost LHOST] [-i INTERFACE]
```

# Rouge Access Point

# Support multi purpose

# airgeddon

Airgeddon is a multifunctional bash script used in wireless network Pentest processes. It supports WPA/WPA2 handshake capture, captive portal attacks, DoS attacks, and password cracking. Working with monitor mode-enabled adapters, it offers a user-friendly interface that simplifies executing various attack scenarios.



<https://cyberexam.io>

# CRACKING

## Aircrack-ng



Aircrack-ng is a widely used toolset in wireless network Pentest processes, focused on capturing and cracking WEP and WPA/WPA2 keys. It includes utilities for packet capture, deauthentication attacks, and password recovery using dictionary or brute-force methods. It's a core tool for Wi-Fi security assessments.

```
root@kali:/home/kali# aircrack-ng cyberpath-05.cap
Reading packets, please wait...
Opening cyberpath-05.cap
Read 9995 packets.

#       BSSID           ESSID          Encryption
1  5A:6E:FA:70:5F:0E  cyberpath_egitim    WPA (1 handshake)

Choosing first network as target.

Reading packets, please wait...
Opening cyberpath-05.cap
Read 9995 packets.

1 potential targets

Please specify a dictionary (option -w).

root@kali:/home/kali#
```

# DECRYPT

airedecap-ng



**airdecap-ng** is a tool used in wireless Pentest to decrypt WEP, WPA, and WPA2 encrypted capture files (PCAPs). After capturing the handshake or key, it allows the user to view the decrypted traffic for further analysis. It's especially useful for post-capture inspection of Wi-Fi communications.

```
root@kali:/home/kali# aircrack-ng cyberpath-05.cap
```

```
Reading packets, please wait...
```

```
Opening cyberpath-05.cap
```

```
Read 9995 packets.
```

#	BSSID	ESSID	Encryption
1	5A:6E:FA:70:5F:0E	cyberpath_egitim	WPA (1 handshake)

```
Choosing first network as target.
```

```
Reading packets, please wait...
```

```
Opening cyberpath-05.cap
```

```
Read 9995 packets.
```

```
1 potential targets
```

```
Please specify a dictionary (option -w).
```

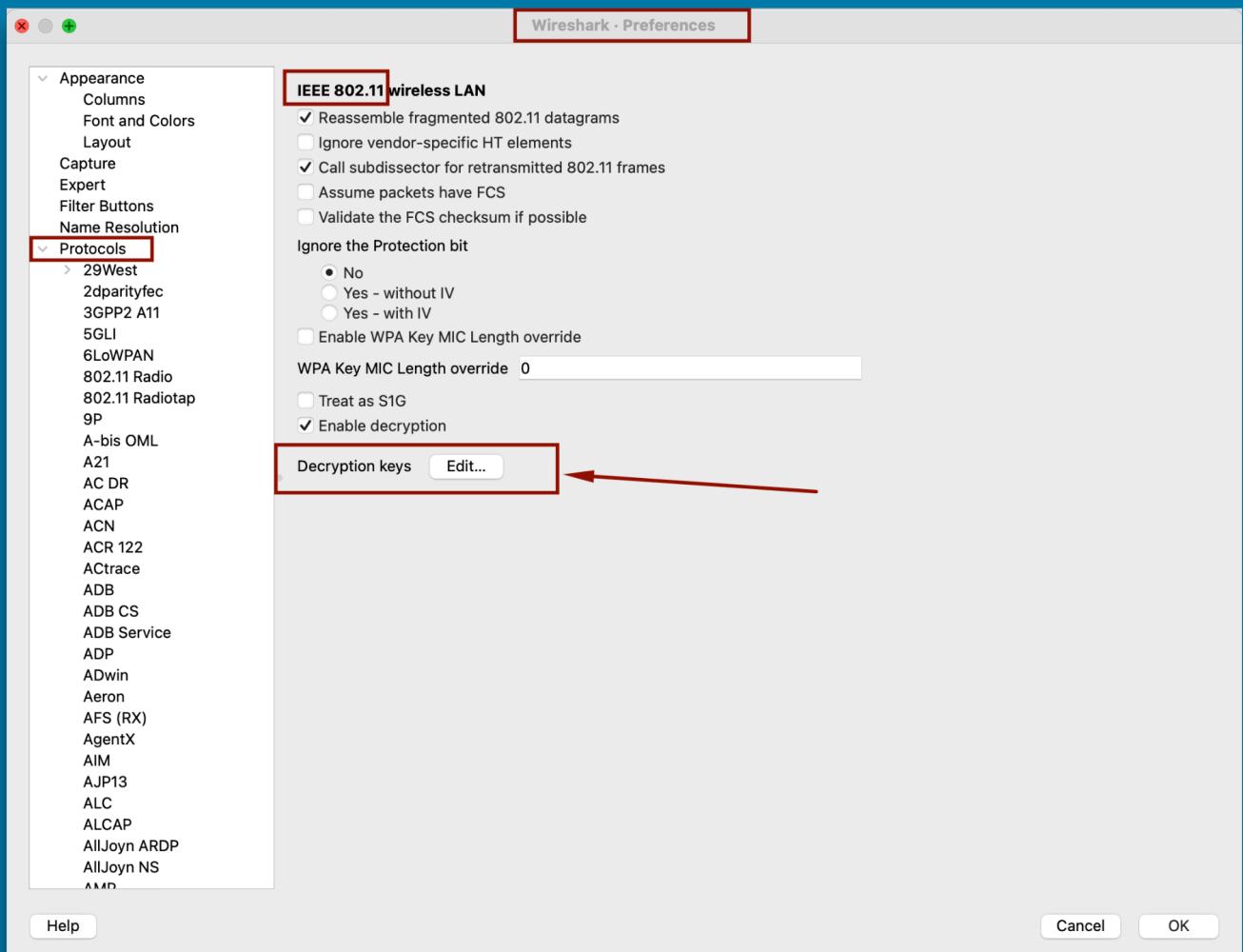
```
root@kali:/home/kali#
```

# DECRYPT

## Wireshark



**Wireshark** is a versatile network analysis tool that can decrypt WEP, WPA, and WPA2 wireless traffic when the correct key or a captured 4-way handshake is available. This feature is useful for analyzing encrypted sessions, inspecting sensitive data, and understanding communication patterns in wireless networks during Pentest operations.



# Packet Manipulation

Scapy



Scapy is a powerful Python-based interactive packet manipulation program and library.

It is able to forge or decode packets of a wide number of protocols, send them on the wire, capture them, store or read them using pcap files, match requests and replies, and much more. It is designed to allow fast packet prototyping by using default values that work.

```
Scapy v2.4.4
File Actions Edit View Help
└─(root💀kali㉿kali)-[~]
# scapy
INFO: Can't import PyX. Won't be able to use psdump() or pdfdump().

          aSPY//YASa
      apyyyyCY//////////YCa
      sY////////YSpcs  scpCY//Pp
ayp ayyyyyyySCP//Pp          syY//C
AYAsYYYYYYYYYY///Ps          cY//S
pCCCCCY//p          cSSps y//Y
SPPPP///a          pP///AC//Y
A//A          cyP///C
p///Ac          sC///a
P///YCpc          A//A
scffffp///pSP///p          p//Y
sY/////////y caa          S//P
cayCyayP//Ya          pY/Ya
sY/PsY///YCcc          aC//Yp
sc  sccaCY//PCypaapyCP//YSS
          spCPY//////YPSPs
          ccaacs

Welcome to
Version 2.4.4
https://github.com/secdev/scapy
Have fun!
To craft a packet, you have to be a
packet, and learn how to swim in
the wires and in the waves.
-- Jean-Claude Van Damme

using IPython 7.19.0
>>> █
```

# Blue Team

## WiPi-Hunter

**WiPi-Hunter** was developed to detect illegal wireless network activities. However, It represents more than a functional tool; it embodies an approach.. In fact, it represents a philosophy. From this project, new methods, innovative ideas, and different perspectives for detecting unauthorized wireless activities can be derived.



**WiPi-Hunter**  
The Swiss Army knife against Malicious WiFi activity  
68 followers · Monitor

**Pinned** Customize pins

 **PiKarma** Public :::  
Detects wireless network attacks performed by KARMA module (fake AP). Starts deauthentication attack (for fake access points)  
Python 253 ⚡ 46

 **PiSavar** Public :::  
Detects activities of PineAP module and starts deauthentication attack (for fake access points - WiFi Pineapple Activities Detection)  
Python 241 ⚡ 51

 **PiDense** Public :::  
Monitor illegal wireless network activities. (Fake Access Points), (WiFi Threats: KARMA Attacks, WiFi Pineapple, Similar SSID, OPN Network Density etc.)  
Python 542 ⚡ 85

 **Repositories**





**Start to learn  
Cyber Security**

<https://cyberexam.io>