CYBEREXAM

WiFi Penetration Testing Tools

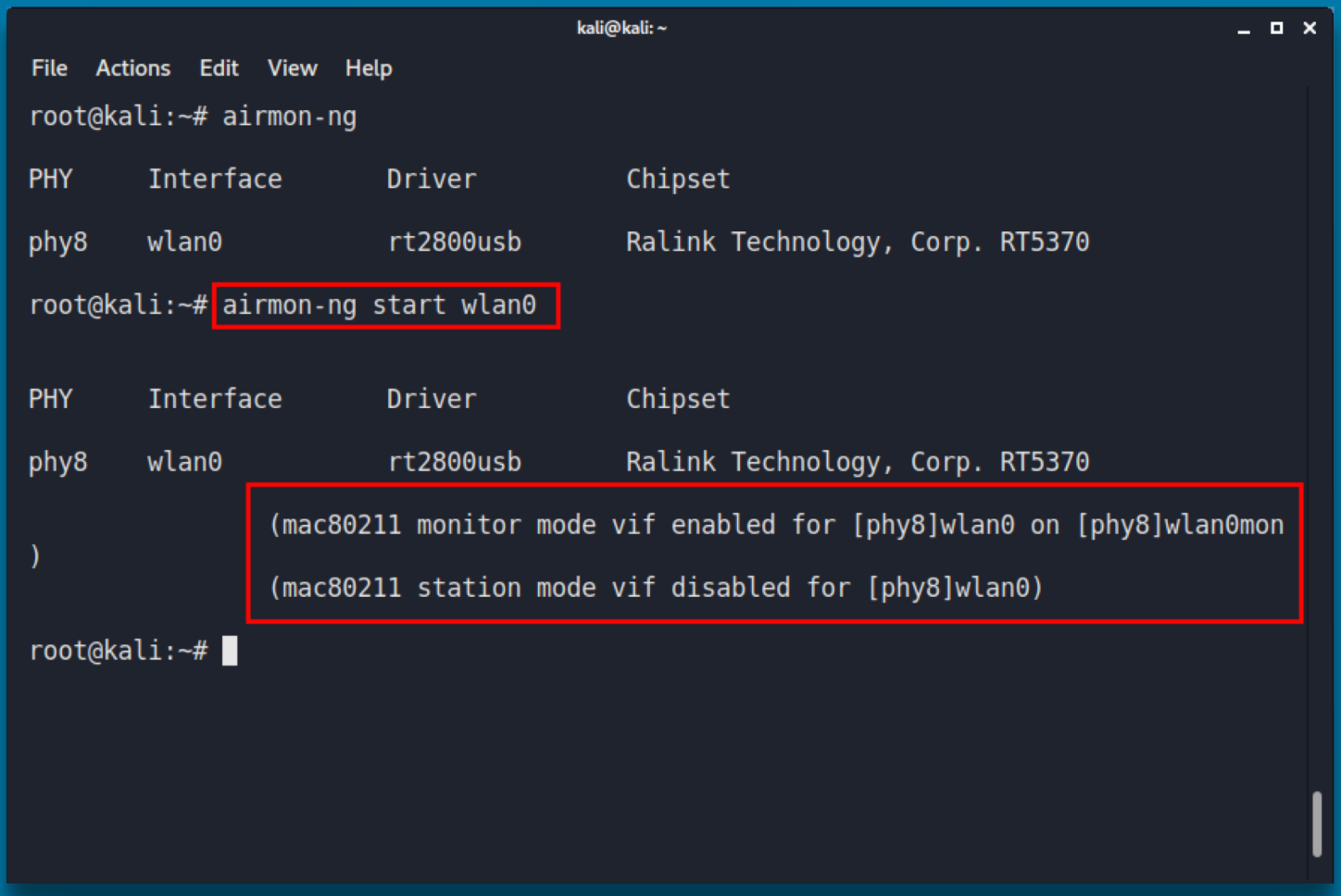
https://cyberexam.io

Table Of Content

Configuration

airmon-ng

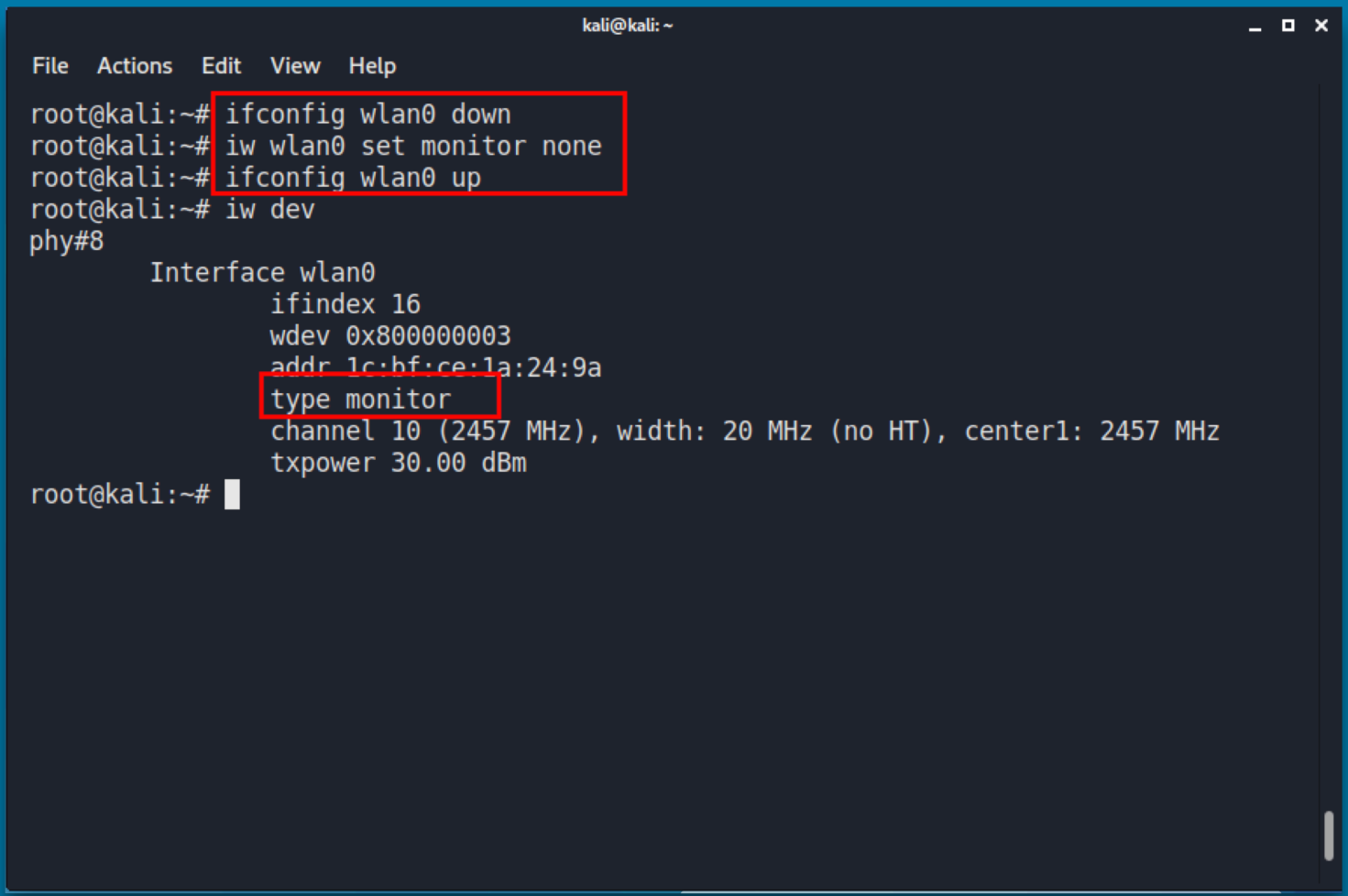
The **airmon-ng** tool is a tool belonging to the aircrack-ng family. Using this tool, you can put the network card in monitor mode.



Configuration

ifconfig, iw

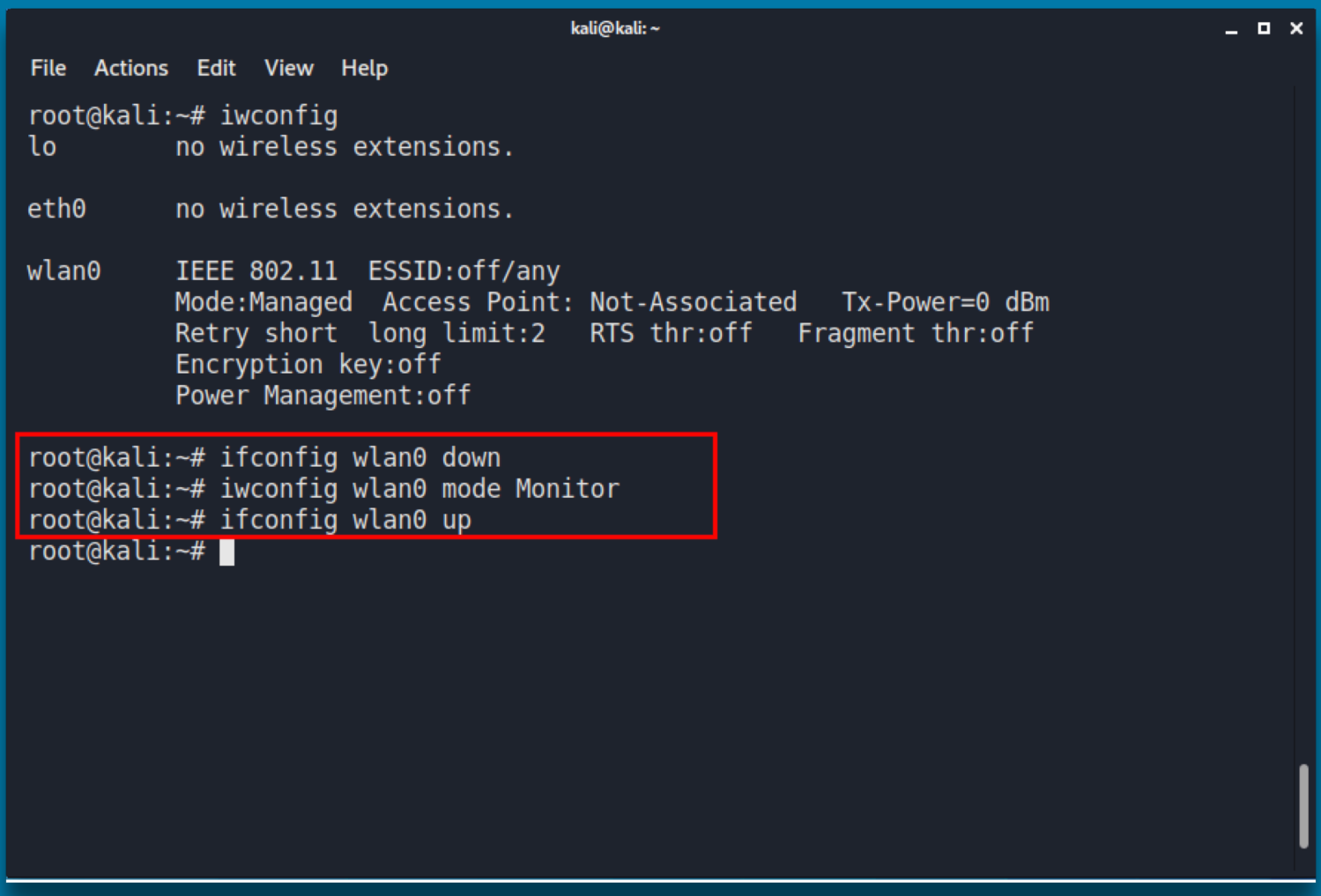
It is a command used to view and configure wireless network cards. With this command, we can also put network cards in monitor mode.



Configuration

ifconfig, iwconfig

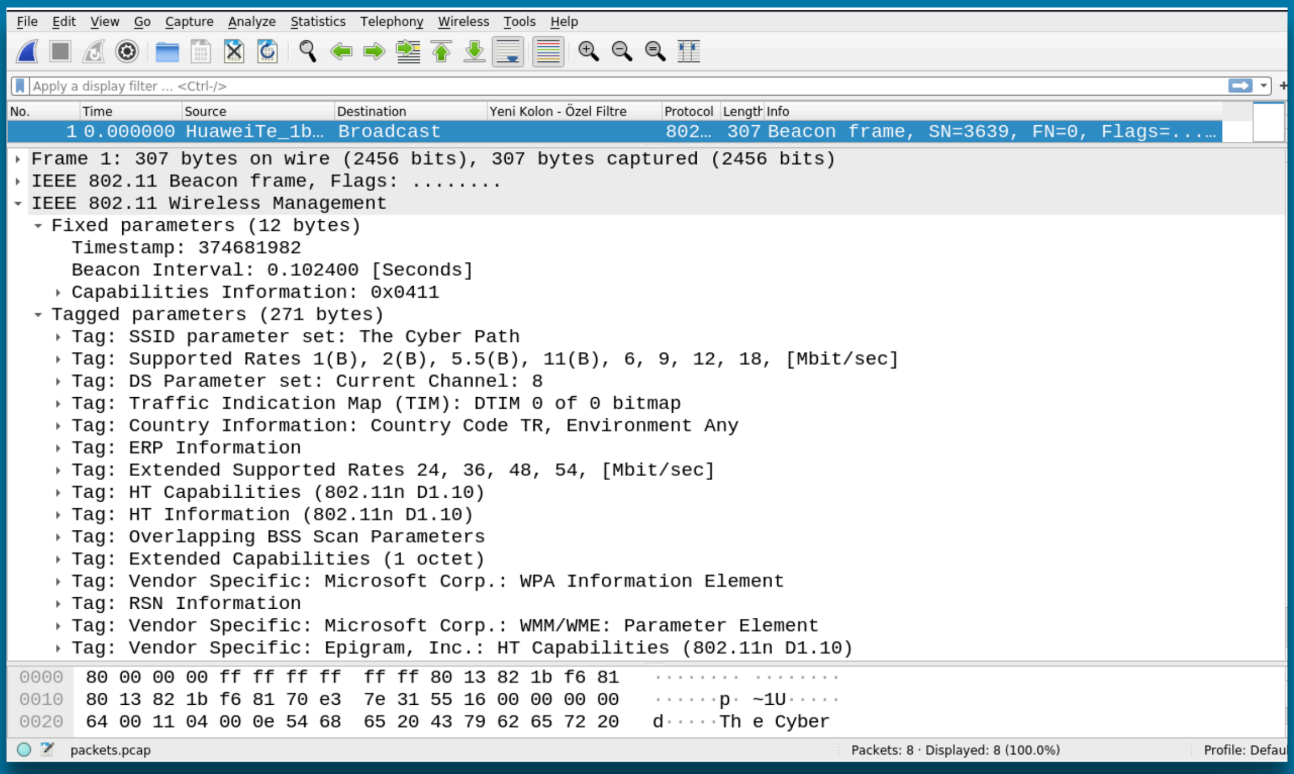
The **iwconfig** command is used to configure wireless network cards. If you want to view detailed information about the wireless network cards installed in your system, you can use this command.



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.

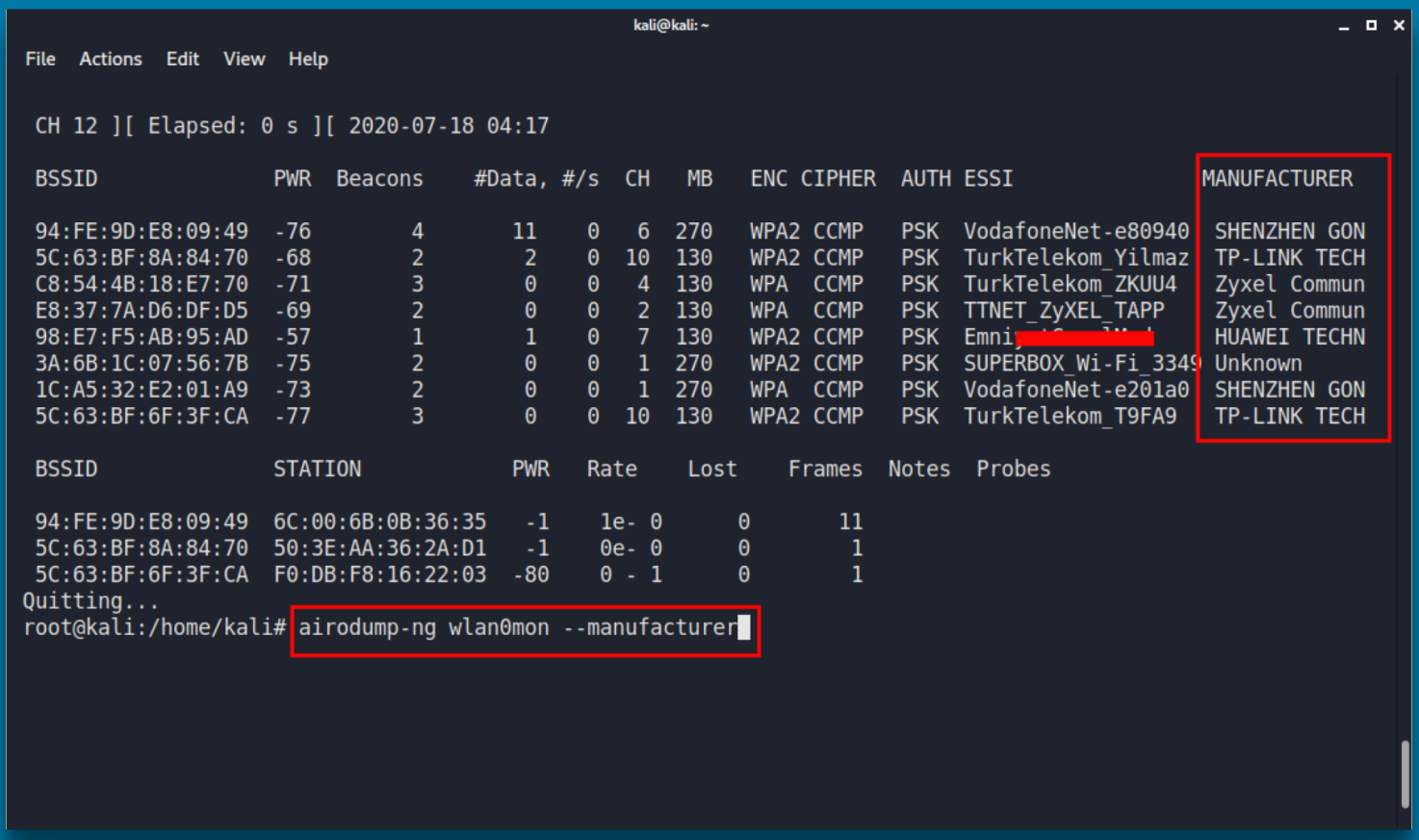


https://cyberexam.io

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.

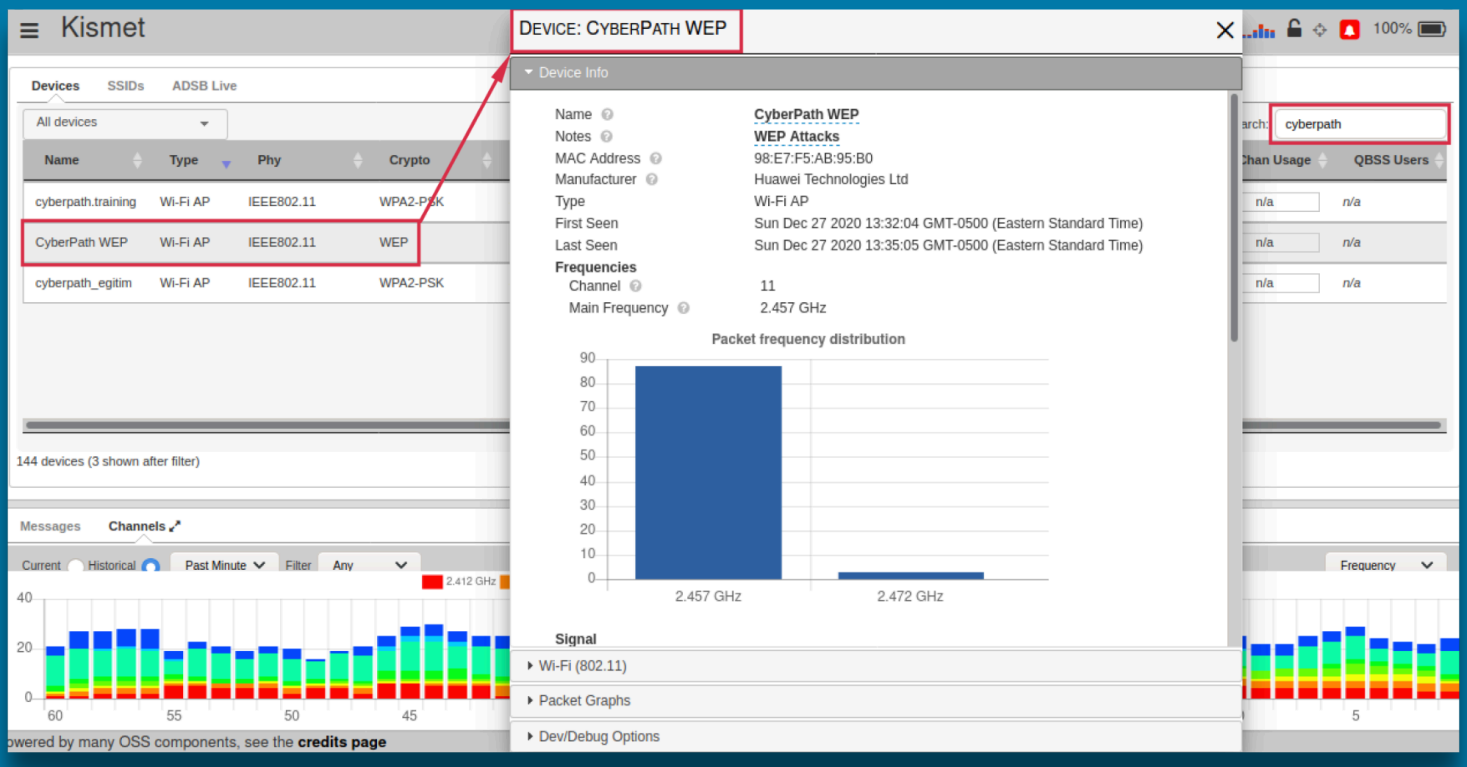


Information Gathering

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.



https://cyberexam.io

Information Gathering

Windows Commands (netsh)

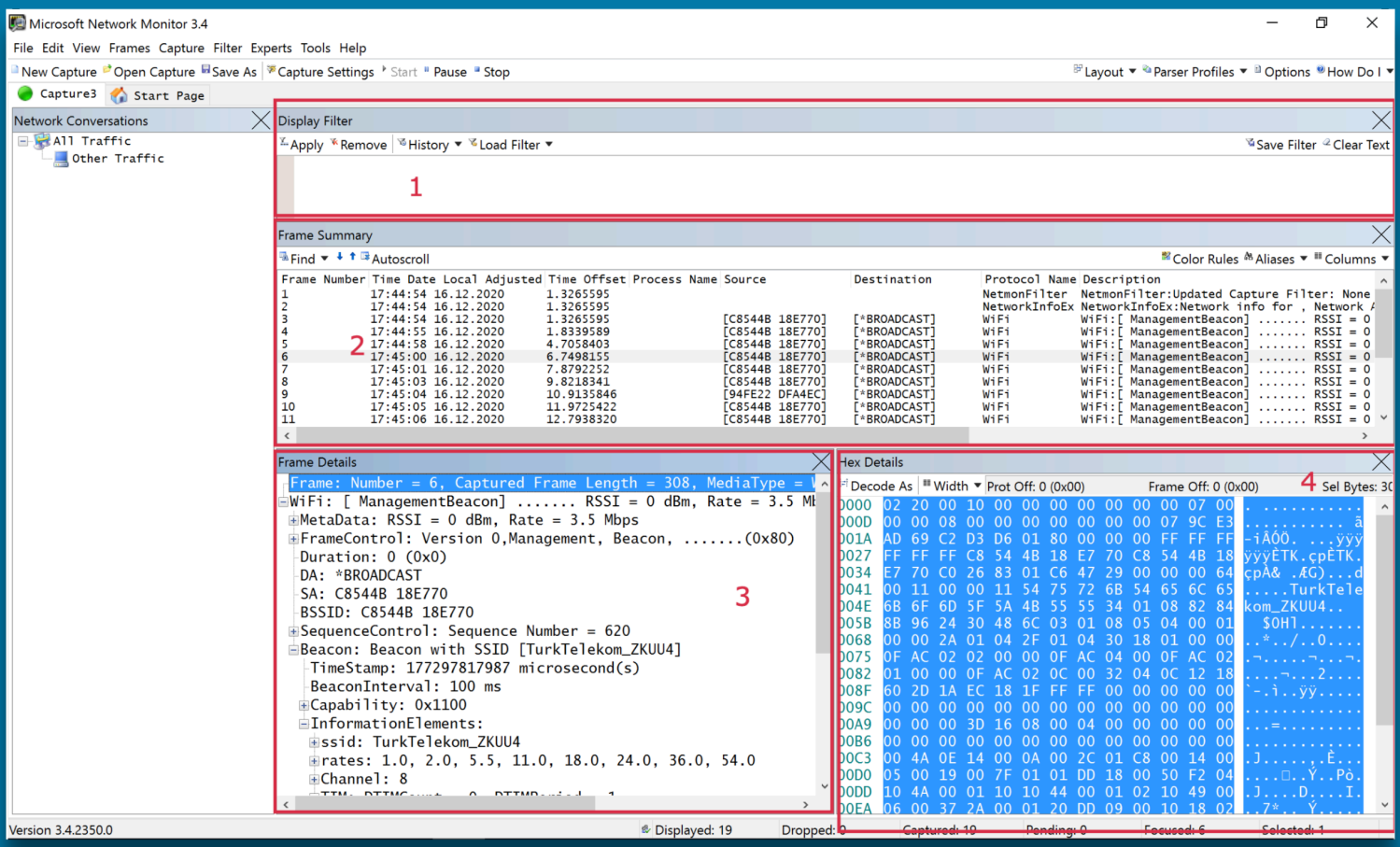
When performing information gathering operations about wireless networks, if you do not have a wireless network adapter or a wireless network adapter that supports monitor mode, you can use the "**netsh**" command to gather information about nearby access points. You can use two different "**modes**" 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.

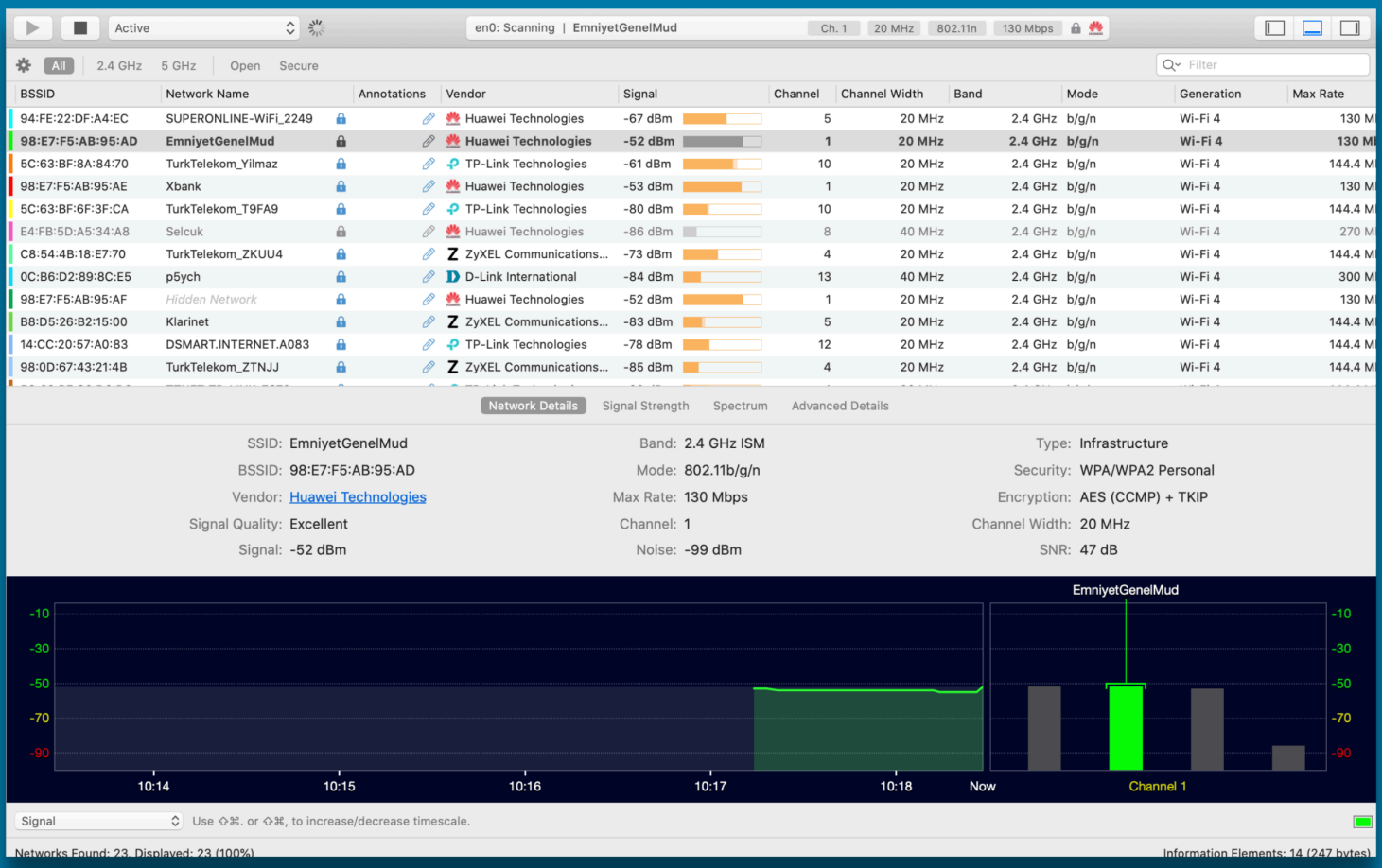


https://cyberexam.io

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.



https://cyberexam.io

Information Gathering

MacOS Airport

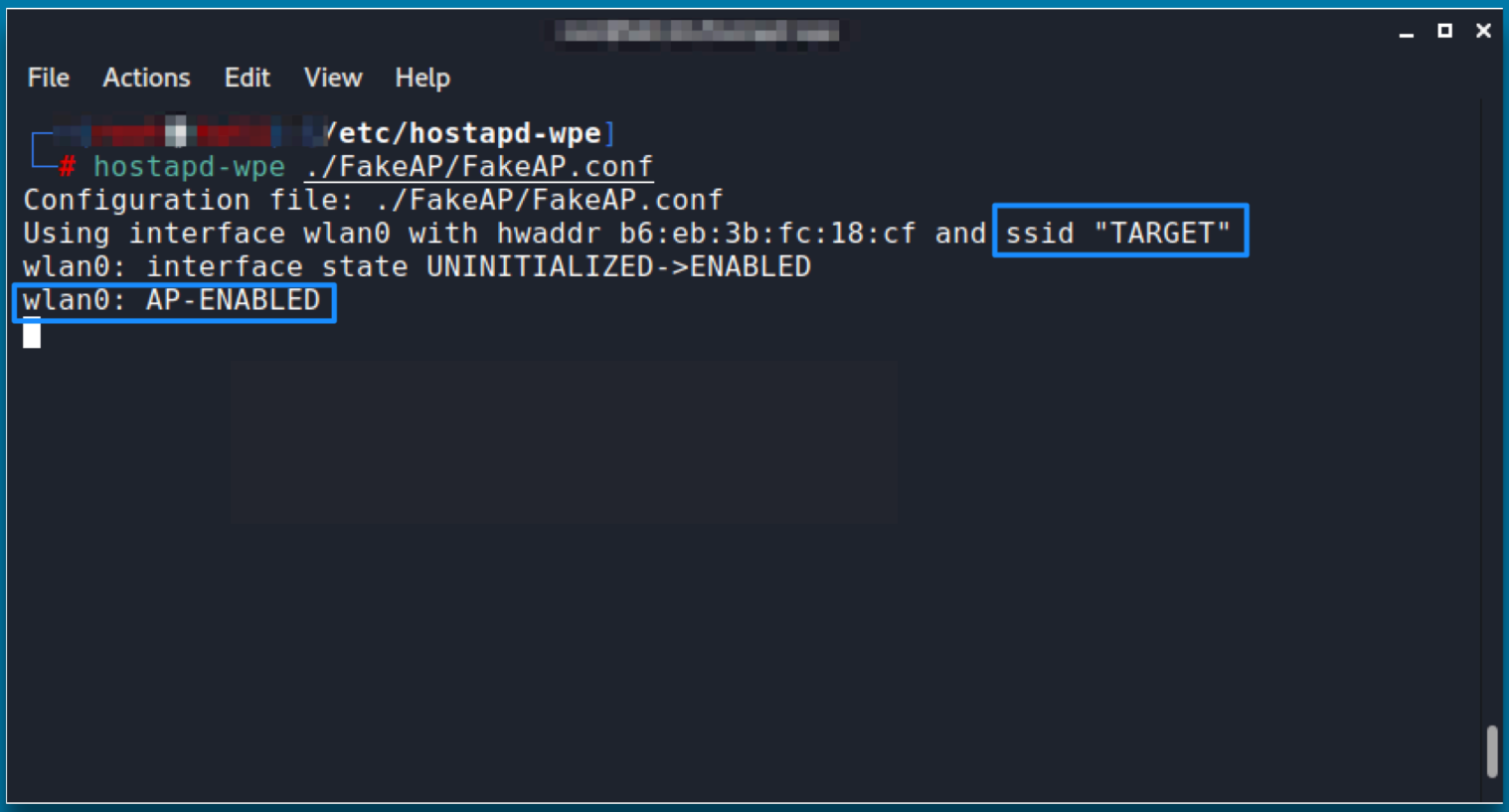
The **airport command** is more powerful than just listing information on the current wireless network. It can change any wi-fi settings, network card settings, troubleshoot network problems, change the types of security used on a connection, log packets to a pcap file, join and connect to wireless networks, 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

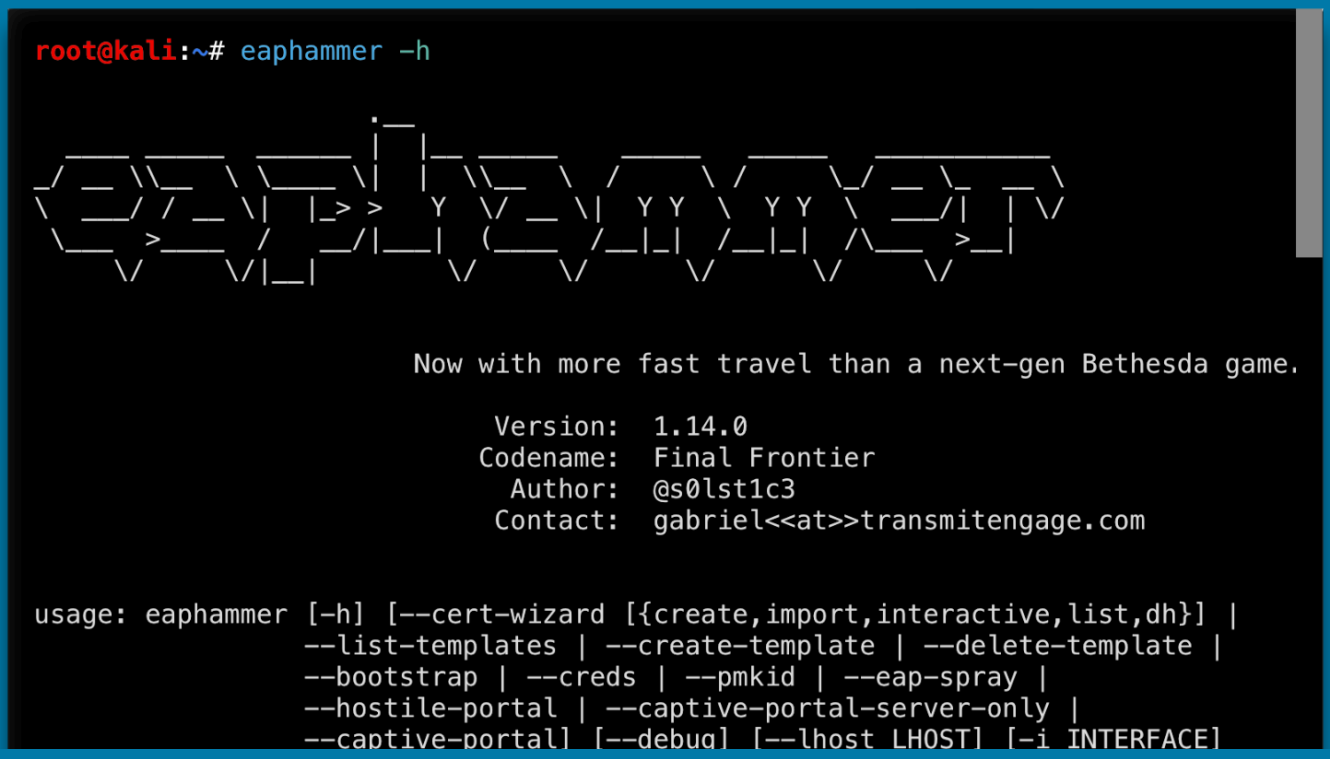
This package contains hostapd modified with hostapd-wpe.patch. It implements IEEE 802.1x Authenticator and Authentication Server impersonation attacks to obtain client credentials, establish connectivity to the client, and launch other attacks where applicable.



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 WPA/2-EAP network in just commands.

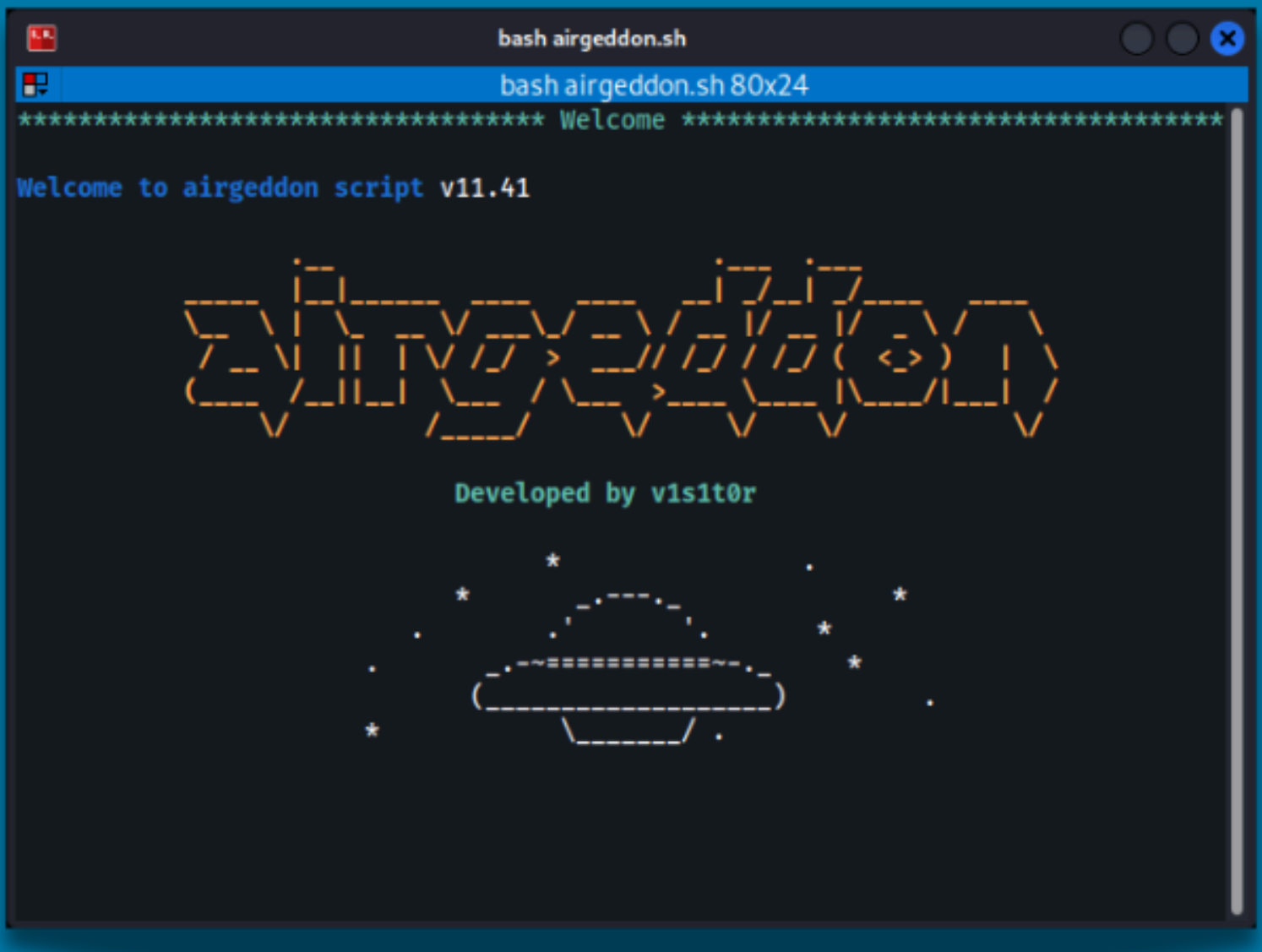


Rouge Access Point

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

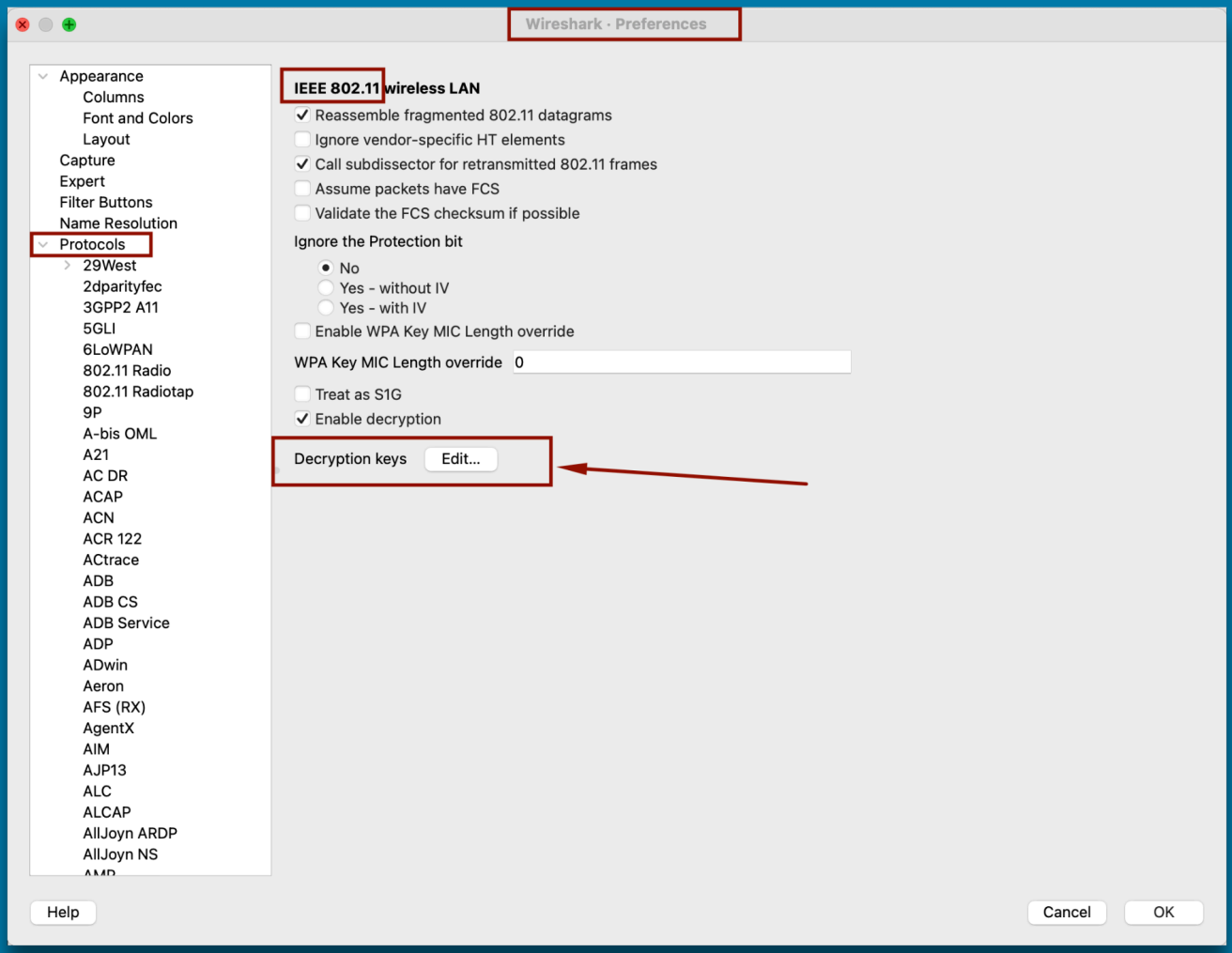
airdecap-ng is a tool used in wireless Pentest to decrypt WEP, WPA, and WPA2 encrypted capture files (PCAPs). After capturing the handshake or key, it allows the user to view the decrypted traffic for further analysis. It's especially useful for post-capture inspection of Wi-Fi communications.

```
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.



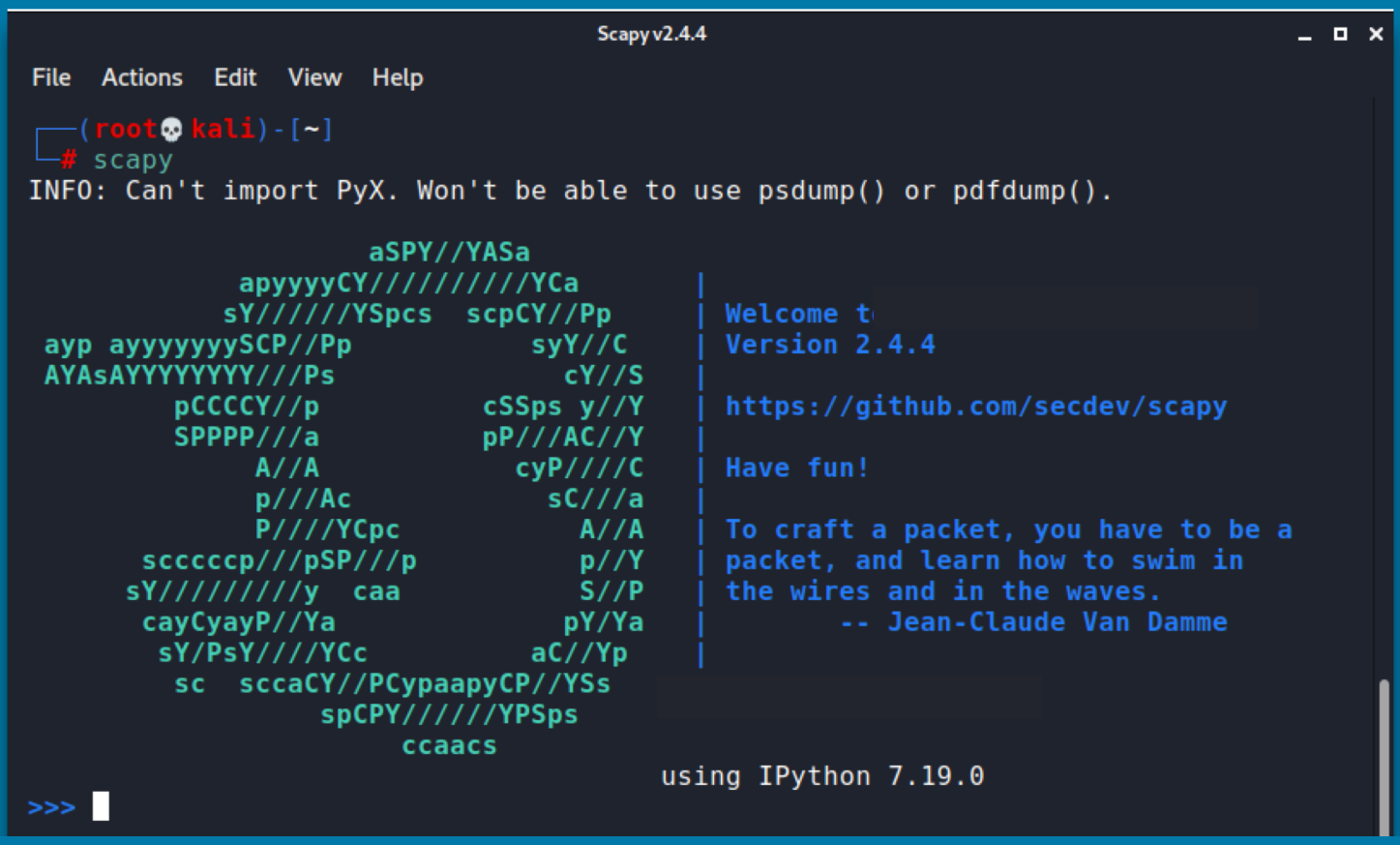
https://cyberexam.io

Packet Manipulation

Scapy

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

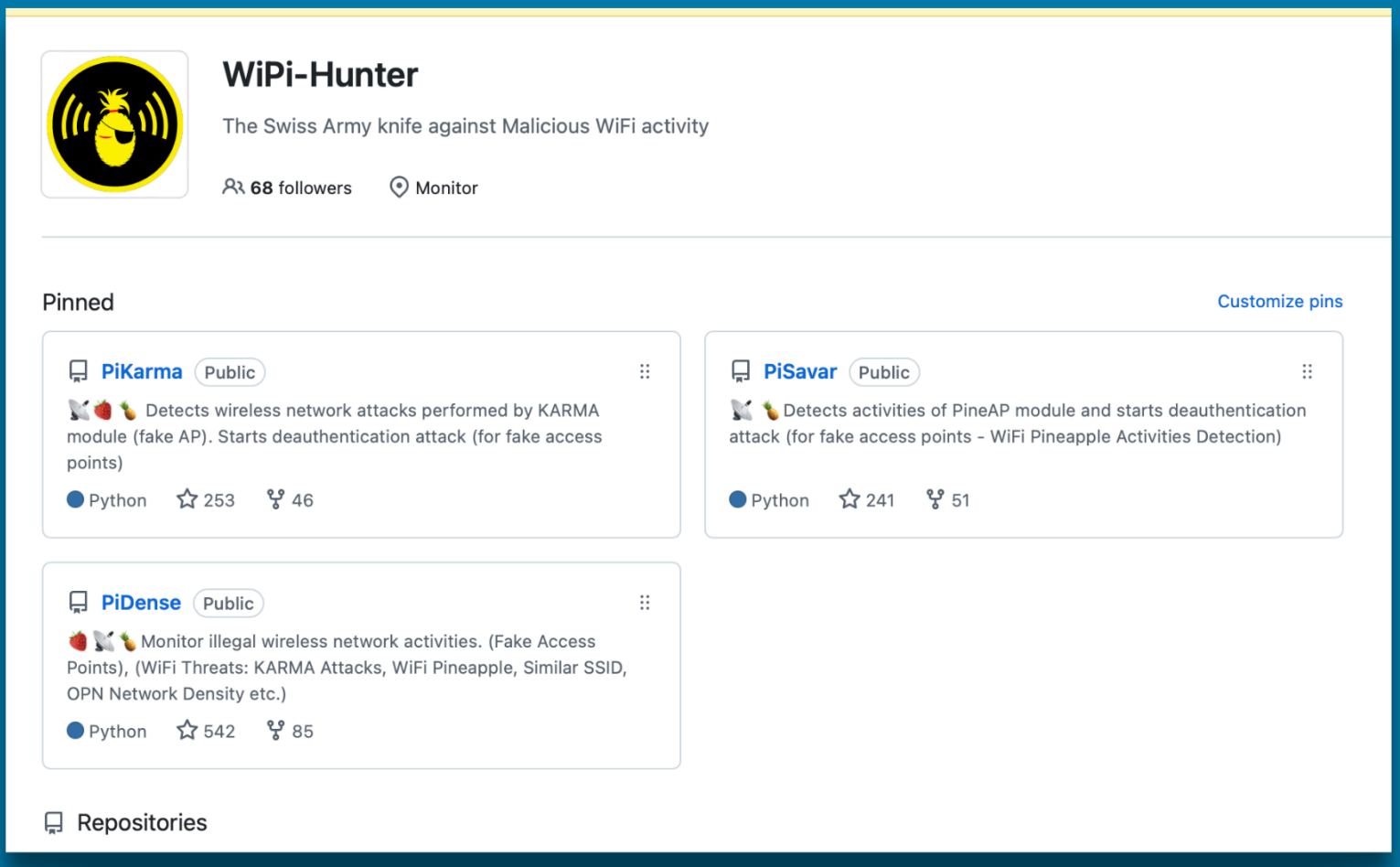
It is able to forge or decode packets of a wide number of protocols, send them on the wire, capture them, store or read them using pcap files, match requests and replies, and much more. It is designed to allow fast packet prototyping by using default values that work.



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.



https://cyberexam.io

Start to learn Cyber Security

https://cyberexam.io