How to decrypt WiFi traffic in Wireshark

How to decrypt Wi-Fi traffic in Wireshark with kali linux

Walid Salame 7:48 PM

Decrypt WPA traffic in Wireshark

Let's start with the theory to understand why the process of decrypting WiFi traffic in Wireshark requires some effort and why one cannot simply decrypt any captured WiFi traffic even if there is a password from the Access Point.

When transmitting over WiFi, the traffic is encrypted using PTK (the Pairwise transient key can be translated as a Pair of Transition Key). At the same time, PTK is dynamic, that is, it is created anew for each new connection. Thus, it turns out that WiFi traffic for each connection in the same Access Point is encrypted with different PTK, and even for one Client after reconnection, PTK changes. To calculate PTK, you need data from a four-stage handshake, as well as a password from a WiFi network (in fact, you also need other information, such as the network name (SSID), but obtaining this data is not a problem).

Contents

The main thing you need to understand: to decrypt WiFi traffic, you need a four-landmark handshake. And not any, but exactly the one that happened to transmit the traffic that needs to be decrypted. But to use the captured handshake you need a password from the WiFi network.

So, to **decrypt WiFi traffic** is needed:

1. a handshake that occurred between the Client and the Access Point immediately prior to the exchange of decrypted information
    1. for this we need Monitor Mode WiFi adapter
2. password to connect to the Access Point

Next will be shown two examples of capturing WiFi traffic and its decryption. The first data capture is performed using Airodump-ng , and then the wireless traffic will be decrypted in Wireshark. In the second example, the data will be captured and decrypted using only Wireshark .

Capturing WiFi traffic in Airodump-ng

In order for the data to be suitable for decryption, it is necessary that the WiFi card does not switch channels, but to capture information on one channel on which the target Access Point operates. Therefore, we start by collecting information about the target access point.

We look at the names of wireless interfaces:

```
iw dev
```

We translate the INTERFACE into the monitor mode with commands like this:

```
sudo ip link set INTERFACE down
sudo iw INTERFACE set monitor control
sudo ip link set INTERFACE up
```

Change **INTERFACE** with your WiFi adapter name

Run airodump-ng with a command like:

```
sudo airodump-ng wlan0mon
```

For example, I want to capture and decrypt traffic for the Kali Access Point, which operates on channel 5.

Then I need to restart airodump-ng with a command like this:

```
sudo airodump-ng wlan0mon --channel CHANNEL --write FILE NAME
```

The **WPA handshake** inscription says that a four-stage handshake was captured. It means that:

- Now we can decrypt the WiFi data (**if we have the key to the WiFi network**)
- we can only decrypt data for a specific client (with which a handshake was made)
- we will be able to decrypt the data that was sent only after this captured handshake

Decryption of WiFi traffic in Wireshark

Open the capture file in Wireshark. In its original form, traffic looks like this:

That is, without decryption, we see only the MAC addresses of the data transfer participants, some types of packets, as well as data packets — in which the payload is encrypted.

Before decoding, make sure that there is a handshake, otherwise there is no point in continuing:

```
eapol
```

Before decoding, we need to make some changes in the IEEE 802.11 protocol settings.

Go to **Edit** → **Preferences** , expand the **protocol** section and select **IEEE 802.11** . The settings should be:

make sure you have the same settings as in the previous screenshot, click on the Edit button next to Decryption Keys (to add a WEP / WPA key):

Click the **Create** button . In the window that opens, in the **Key type** field, select **wpa-pwd** , enter the password for the WiFi network, and after the colon, enter the network name (SSID) and click OK.

For example, in my case, the password is qivxy17988, and the network name is Kali, then I enter:

```
qivxy17988:Kali
```

Click Apply :

Traffic will be decrypted:

Now there are visible DNS, HTTP requests and responses, as well as other network packets.

If traffic is captured not only for this network, but also for other networks operating on the same channel, or for this network but other clients for which no handshakes are taken, then this traffic will not be decrypted.

Capture WiFi in Wireshark

WiFi traffic can be captured directly in Wireshark.

But we first need to switch the WiFi card to the same channel as the target Access Point. This is done by commands like:

```
sudo ip link set INTERFACE down
sudo iw INTERFACE set monitor control
sudo ip link set INTERFACE up
sudo iw dev INTERFACE set channel
```

The subsequent decryption is performed in exactly the same way as shown above.

Conclusion

To decrypt WEP WiFi traffic, you only need to know the password.

Tags: Tutorials Wifi Hacking

Share it: Facebook Twitter G+ P in t

WANNA GET OUR AWESOME NEWS?

Sign up and get the best stories straight into your inbox!

Enter your email address...

Subscribe Now

* we won't spam you

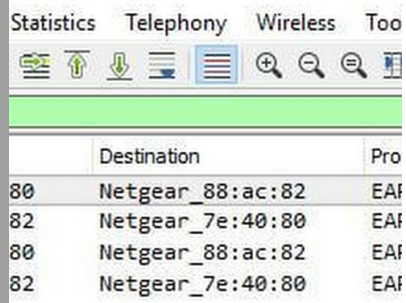
Next

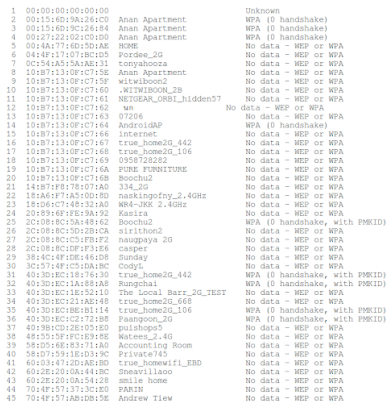
Intercept Passwords With Wireshark

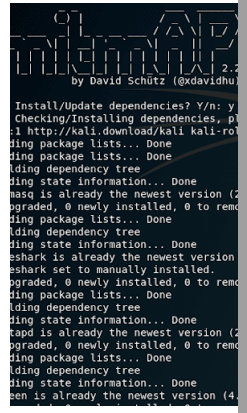
Previous

How to increase WiFi TXPower

Tutorials







WPA2 Half Handshake attack
Jun 08 2019

Hacking Wifi using PMKID and Aircrack-ng
Jun 08 2019

Hacking WiFi without users using PMKID attack
Jun 07 2019

Selective jamming of WiFi networks and clients
Jun 07 2019

mitmAP WiFi acce intercept passwor
May 31 2019

Post A Comment:

BLOGGER

0 comments:

Enter your comment...

Comment as: Google Accoun

Publish Preview

Social Widget

6.7K 22k 4.1K 3.9K

Popular Posts

Fix Kali Linux sources.list Repositories

Fix default repository First after installing a clean Kali Linux the sources.list contains only tow repository and they are ## Regul...

Useful Commands for Kali Linux

New to Kali Linux ? or to Linux world at all ... welcome to this new experience i'm sure you will enjoy once you start to try ... an...

Password dictionary

hi Guys how are you ? Looking for wordlist password ? password list ? ? they are all the same and you are on the right place :) ...

how to update Kali Linux and Fix update error

Kali Linux's the great Penetration testing system is like any other system in the world it need to be updated, Most of the update is not ...

infernal twin Automated Evil Twin Attack

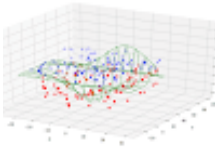
Automated Evil Twin Attack: infernal-twin Evil twin is a term for a fake WiFi access point, it appears to be a legitimate one offered on t...

Labels

- Android (5)
- Books (11)
- Cyber Security (4)
- Kali Linux (17)
- Linux (6)

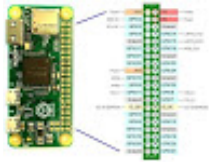
- Linux Commands (14)
- MITM (1)
- Network Administrator (3)
- Penetration Testing Tools (12)
- Raspberry Pi (132)
- Tutorials (11)
- Video Tutorials (29)
- WiFi Adapter (7)
- Wifi Hacking (40)

Recent | Random | Comment



What is data science

Sep 15 2019



Raspberry Pi Zero W Review

Sep 11 2019

Raspberry Pi Camera Board V2 Overview

Sep 10 2019

Raspberry pi zero w camera

Sep 10 2019

best laptop for Kali Linux

Aug 07 2019

A blog dedicated to Penetration Testing, Tutorials on hacking and security