How to hack Wifi passwords using Wifiphisher

How to hack Wifi passwords quickly? Many WEP, WPA2, and WPS crackers take too much time and not all access points have WPS enabled. This article will show you a solution to get Wifi password without crack, it is Wifiphisher.

How to hack Wifi passwords quickly? Many WEP, WPA2, and WPS crackers take too much time and not all access points have WPS enabled. This article will show you a solution to get Wifi password without crack, it is Wifiphisher.

Wififisher creates a fake AP, then removes authentication or DoS users from the real AP. When confirming the fake AP with the same SSID, they will see a legitimate website searching for a password due to "firmware upgrade". When the user provides the password, you retrieve it and then allow them to use the evil twin as his AP without doubt.

In short, Wififisher does the following:

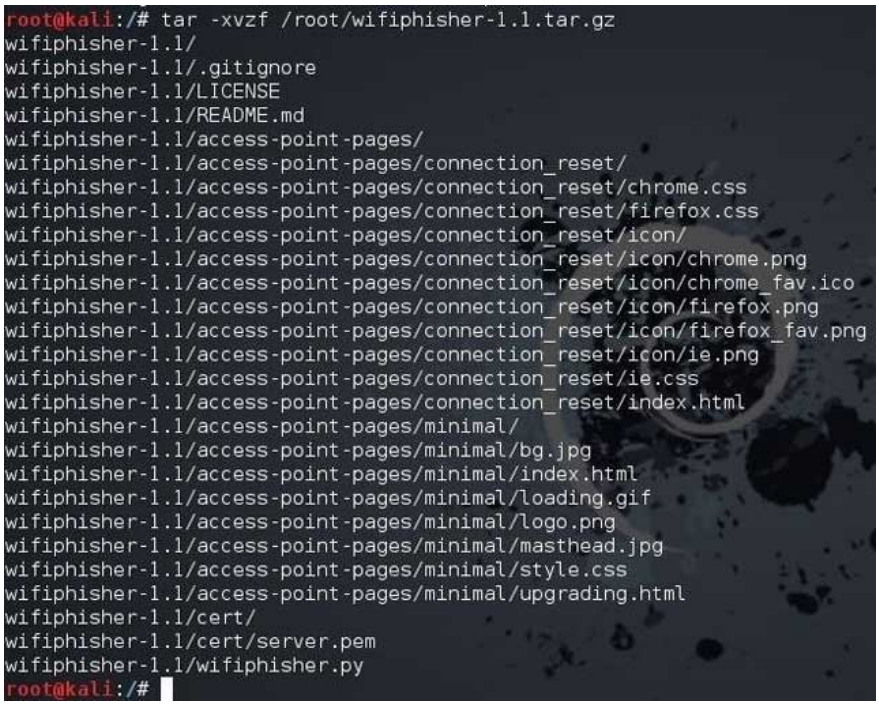
1. Quit authenticating users from their legitimate AP.
2. Allow users to authenticate with evil twin.
3. Providing the site to users on a proxy informs them that "software upgrade" is required and requires re-authentication.
4. Wifi passwords are transmitted to hackers and users continue to access the web without knowing what happened.

To do this, you need a Kali Linux distribution and two wireless adapters, one of which must have packet injection capability.

Step 1: Download Wifiphisher

To start, activate Kali and open a terminal window, then download Wifiphisher from GitHub and unzip.

potassium> tar -xvzf /root/wifiphisher-1.1.tar.gz



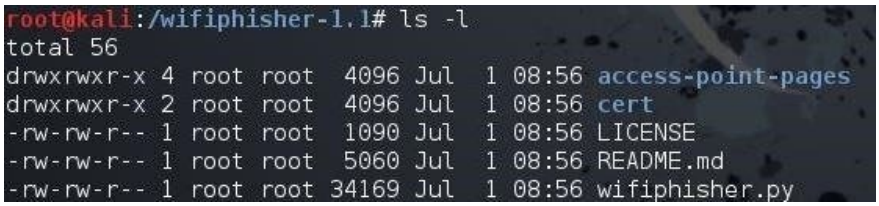
Step 2: Navigate to the directory

Next, navigate to the folder that Wifiphisher creates when extracting. In this field is */wifiphisher-1.1* .

Potassium> cd wifiphisher-.1.1

In the list, you will see the wifiphisher.py script here.

Potassium> ls -l



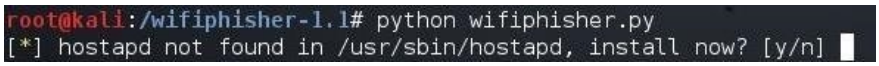
Step 3: Run the script

Run Wififisher script by typing:

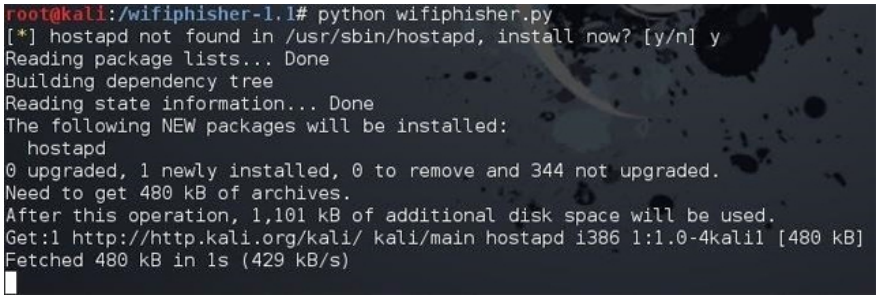
potassium> python wifiphisher.py

Note, here use the python interpreter, change the name of your interpreter.

1. More than 100 Python exercises have solutions (sample code)



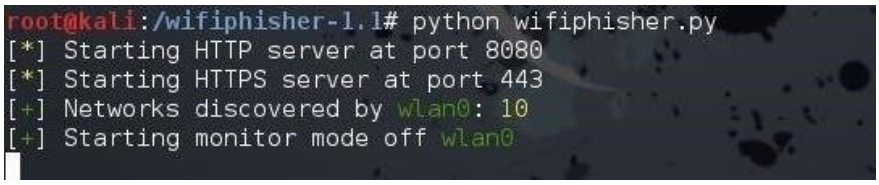
The first time you run the script, it may appear that you cannot find "hostapd" and prompt the user to install. Install by typing " **y"** , then it will proceed with hostapd installation.



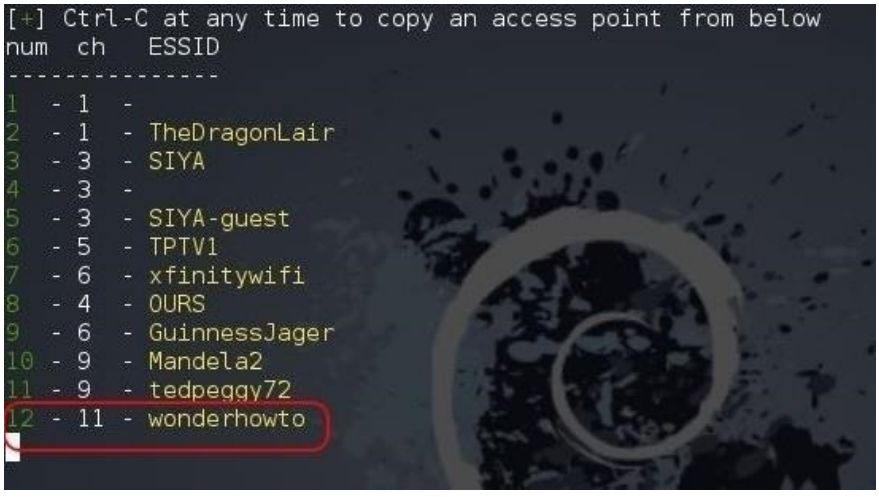
When finished, continue running the Wififisher script.

potassium> python wifiphisher.py

This time, it will launch the web server on ports 8080 and 443, then discover the available Wifi networks.

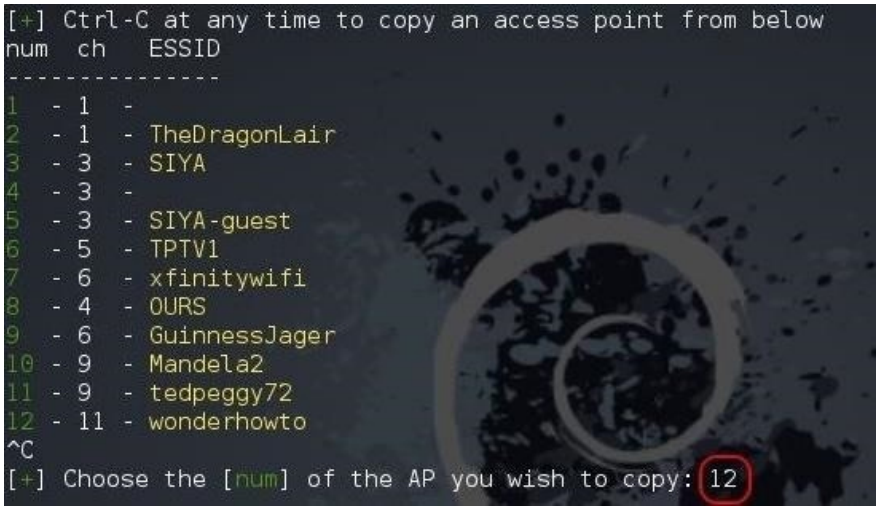


When completed, a list of Wifi networks will be listed. In this example will hack Wonderhowto network.

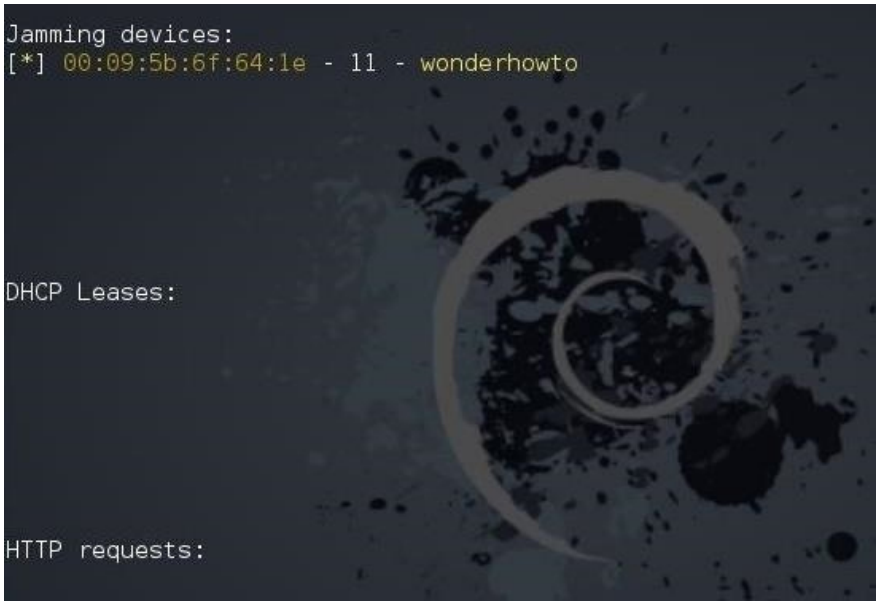


Step 4: Get the Wifi password

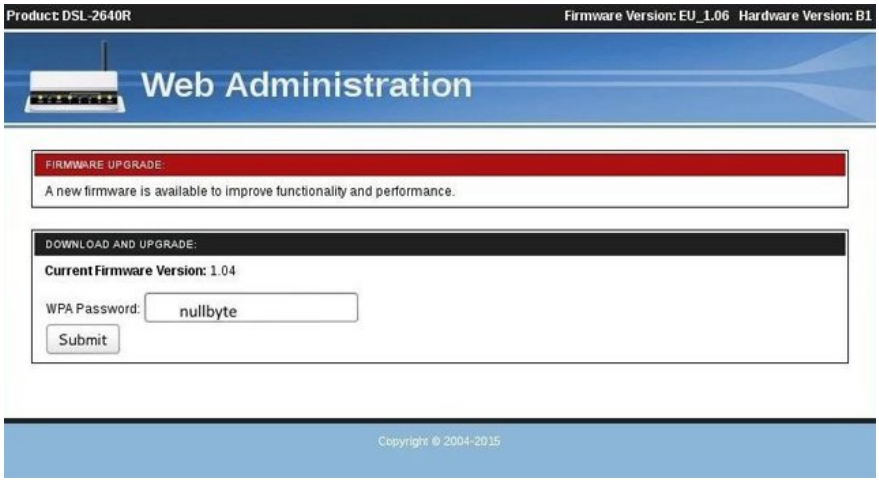
Press **Ctrl + C** and enter the number of APs you want to attack. In this case 12.



When you press **Enter** , Wifiphisher will display a screen like the one below that shows the interface being used and the AP's SSID being hacked and cloned.



Users have been removed from their AP authentication, so when they confirm the password, they will be redirected to the counterfeit access point that was copied. The proxy on the web server will issue a message about the firmware update to the router and ask the user to verify the password again.



When a user enters a password, Wifiphisher will be sent to you via the terminal, as shown below.

See more:

1. How to find Wi-Fi passwords of relatives

You finished reading the article "**How to hack Wifi passwords using Wifiphisher**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.