

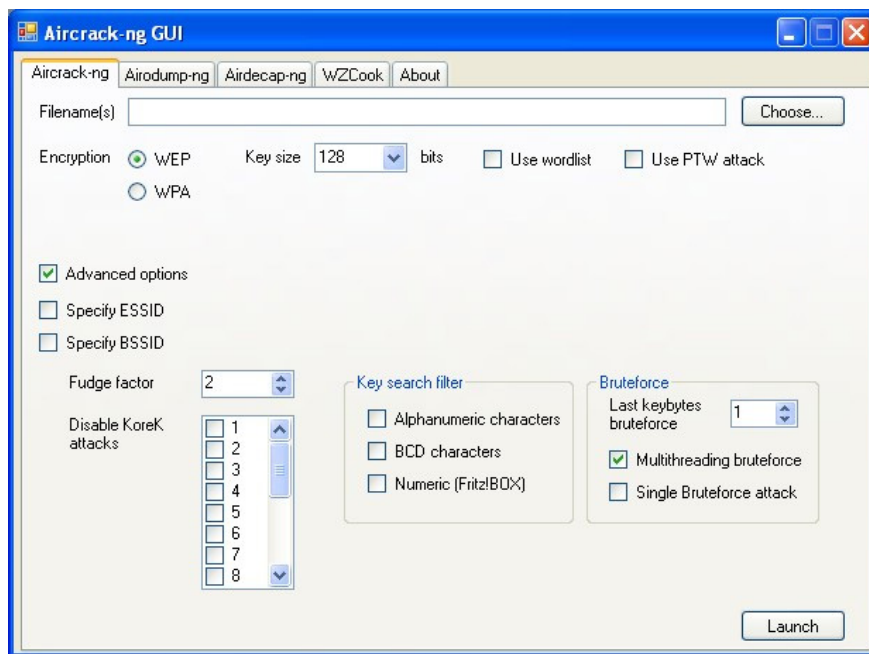
8 best Wifi analysis and hacking software

Pentest security analysis and security evaluation is an integral part of creating any kind of secure network. To create a secure network, developers use Wi-Fi hacking software to test wireless networks and make modifications. This article will introduce you to the best hacking and analyzing Wi-Fi tools.

Pentest security analysis and security evaluation is an integral part of creating any kind of secure network. To create a secure network, developers use Wi-Fi hacking software to test wireless networks and make modifications. This article will introduce you to the best hacking and analyzing Wi-Fi tools.

Note: It is illegal to try to fake someone's wireless or ethernet network without prior authorization. This list is prepared for educational purposes and you should test these software on the device you own.

1. AirCrack



If you have a basic knowledge of hacking or want to pursue or develop a career in this area, you may have heard about AirCrack software. This tool is written in C language, combined with many tools to access Wi-Fi network security.

Other tools in the AirCrack suite are used to monitor, attack, evaluate security and crack networks. With Aircrack-ng software, you can crack the 802.11 WEP and WPA-PSK key after getting enough data packets. For faster and more efficient attacks, you can perform standard FMS attacks, attack KoreK and attack new PTW.

1. How to hack Wifi password with Aircrack-Ng

AirCrack is a cross-platform tool, using the command line interface, compatible with Linux, Windows, OS X, and BSD.

Download : <https://www.aircrack-ng.org/>

2. Cain and Abel

If you're looking for a password recovery tool for Windows operating systems, then Cain and Abel are definitely the tools you need to find. Named after Adam and Eva's son, this tool retrieves the password using various methods such as network packet sniffing and brute force attacks, dictionary attack, and coding.

In addition, using this Windows Wi-Fi hacking software, you can record VoIP conversations, solve encrypted passwords, retrieve stored data and keep routing protocols for non-hacked purposes. breaking the law. One of the new features added to this useful tool is ARP support to block attacks on switching LANs and MITM attacks. As mentioned above, Cain and Abel are available for different versions of Microsoft Windows operating systems.

Download : <http://www.oxid.it/cain.html>

3. Fern WiFi Cracker



Fern WiFi Cracker is a tool used to analyze the network, find vulnerabilities and patch it to ensure the highest security. This software is written in Python programming language, it can run various network-based attacks such as on wired networks and wireless networks. The highlight of this software is that it can crack WEP / WPA / WPA2 / WPS standards, take up sessions, attack MITM, brute force attacks, etc. You can use Fern WiFi Cracker on Linux distributions.

1. Wireless security: Say NO to WEP and YES to WPA

Download : <https://github.com/savio-code/fern-wifi-cracker>

4. Reaver

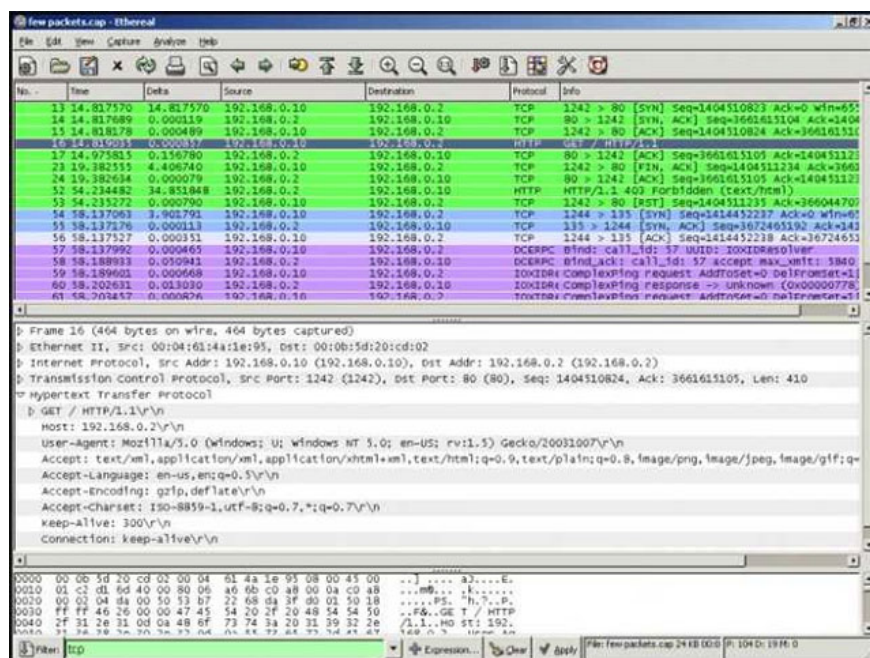


If you know the true power of Wi-Fi security, you can take some practical steps to make it safer and that is the purpose of the Reaver. This is an open source software and a free Wi-Fi password search can crack most of the current router's passwords. Reaver uses brute force attack for WPS PIN and receives WPA / WPA2 passwords again. It can recover pure text passwords in 4-10 hours. In real-world situations, you can get results faster.

Reaver can be installed on Linux distributions. This tool is also preinstalled in many hack distributions, including Kali Linux.

Download : <https://code.google.com/archive/p/reaver-wps/>

5. Wireshark



There is no doubt that Wireshark is the most popular network protocol analysis tool on the Internet. Although it does not directly help users recover plain text passwords, it helps you steal packets with the best possible way. This software can test hundreds of protocols and give the best results using offline analysis and online data retrieval.

In addition to retrieving data from wireless networks, Wireshark can also collect data directly from Bluetooth, Ethernet, USB, Token Ring, FDDI, etc. Wireshark tools are available for all major platforms, including Windows, Linux, OS X, Solaris, BSD, etc.

Download : <https://www.wireshark.org/>

6. Infernal Twin

Infernal Twin is an automated tool, used to assess Pentest wireless security. You can use this tool to automatically attack Evil Twin, creating a fake Wi-Fi hotspot to steal wireless communications packets. By using this tool, one can eavesdrop on users using phishing attacks (build a phishing system to steal sensitive information) and perform man-in attacks - the-middle to target predefined users. Using this Wi-Fi password hack tool, you can perform WPA2 / WEP / WPA security, wireless social engineering, automatically generate reports, etc.

The GPLv3-licensed security tool, written in the Python programming language, can be installed on Linux distributions and used for network testing and evaluation.

Download : <https://github.com/entropy1337/infernal-twin>

7. Wifisher

Wifisher is a WiFi security tool that has become popular in recent years. Hackers use this tool to perform automated and customized phishing attacks to infect victims or steal information. Wifisher does not use brute

force attack techniques, it is based on social engineering by redirecting all HTTP requests after performing an MITM attack using KARMA or Evil Twin.

Although Wifisher can be used on Linux distributions, Kali Linux is an officially supported operating system and all new features are supported on this platform.

Download : <https://www.wifisher.com/>

8. Hashcat / oclHashcat

```
Initializing hashcat v0.37 by atom with 8 threads and 32mb segment-size...
NOTE: press enter for status-screen
Added hashes from file C:/HashCat/hashes.txt: 1 (1 salts)
Activating quick-digest mode for single-hash
Charset...: abcdefghijklmnopqrstuvwxyz0123456789
Length...: 1
Index....: 0/1 (segment), 36 (words), 0 (bytes)
Recovered.: 0/1 hashes, 0/1 salts
Speed/sec.: - plains. - words
Progress..: 36/36 (100.00%)
Running...: ---:---:---
Estimated.: ---:---:---
Charset...: abcdefghijklmnopqrstuvwxyz0123456789
Length...: 2
Index....: 0/1 (segment), 1296 (words), 0 (bytes)
Recovered.: 0/1 hashes, 0/1 salts
Speed/sec.: - plains. - words
Progress..: 1296/1296 (100.00%)
Running...: ---:---:---
Estimated.: ---:---:---
Charset...: abcdefghijklmnopqrstuvwxyz0123456789
Length...: 3
Index....: 0/1 (segment), 46656 (words), 0 (bytes)
Recovered.: 0/1 hashes, 0/1 salts
Speed/sec.: - plains. - words
Progress..: 46656/46656 (100.00%)
Running...: ---:---:---
Estimated.: ---:---:---
dcb8e94ac7d0aadcb8a81d9c895ace5f4:fred
All hashes have been recovered
```

Although Hashcat is known as the fastest password crack tool in the world, it can be used perfectly for securing WPA / WPA2. Before you do that, you can use tools like Reaver to collect shared keys and decoded hash codes. If you want to hack Wi-Fi quickly, you can use oclHashcat's modern GPU. This is a cross-platform tool that can be used on Linux, Windows and macOS to recover passwords quickly.

Download : <https://hashcat.net/hashcat/>

There are many other WiFi security tools that you can use to ensure network security. Some other remarkable tools are: Wifite, KisMac, Bluepot, coWPAtty, Ghost Phisher.

See more:

1. How to hack Wifi passwords using Wifiphisher
2. Tips to use your cat hack WiFi neighbors password
3. How to know who is "using the temple" Wifi your home or not?

You finished reading the article "**8 best Wifi analysis and hacking software**" 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.