How to hack your own WiFi network

One way to increase your understanding of WiFi security is to try to hack the network. But you absolutely should not intrude on the company or neighbor's network.

One way to increase your understanding of WiFi security is to try to hack the network. But you absolutely should not intrude on the company or neighbor's network. Instead, hack 'ethically' and try to legally access WiFi (done in cooperation with the network owner) so you can help you learn more about the strengths. and limitations of wireless security. Understanding the potential WiFi vulnerabilities can help you better protect managed networks and ensure a safer connection when you access other wireless networks.

Do you know how to hack your own WiFi network . yourself?

1. Start with a WiFi stumbler
2. WiFi sniffer
3. Tools to reveal WiFi network details
4. Linux distribution for testing hack and penetration testing
5. Full force with a hardware tool

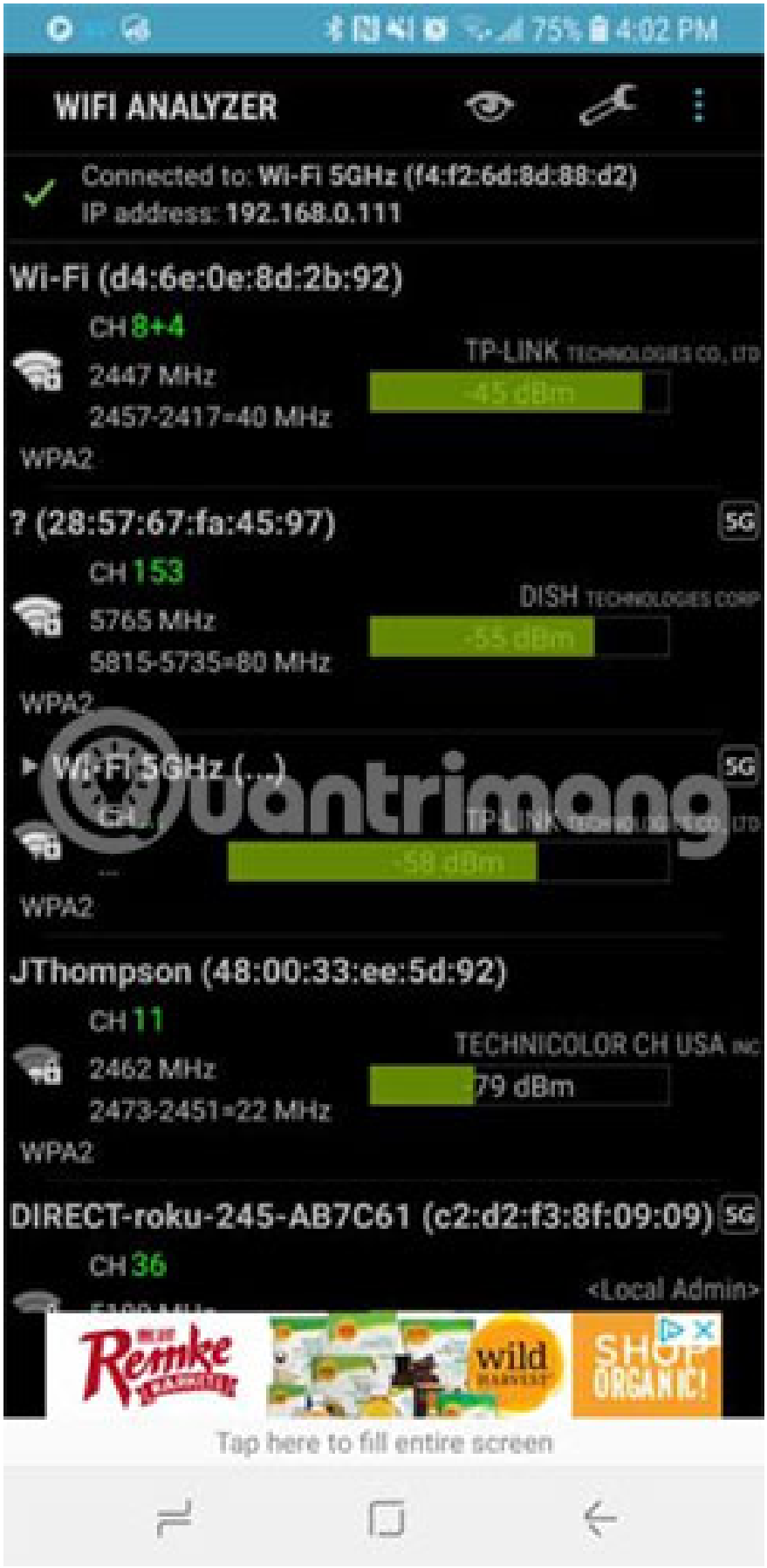
Start with a WiFi stumbler

WiFi stumbler is a software application that will help find wireless networks in close proximity. These are the simplest tools to add to the pen test toolkit. WiFi stumbler allows you to see nearby access points and details about them, such as signal level, security type / encryption and MAC address.

Using a stumbler, you can find networks that use weak security protocols, such as WEP or the original version of WPA, as well as reveal phishing access points set up by people who can Open your network to attack. Even with access points set with hidden SSID, some stumblers can also quickly reveal that SSID.

An example of stumbler is Vistumbler, an open-source Windows application that displays basic access point details, including accurate authentication and encryption methods, that can reveal SSIDs as well as signal levels. . Vistumbler also displays signal level charts and channel usage. Vistumbler is very customizable and offers flexible configuration options. Vistumbler supports access point names to help distinguish them. This feature also helps detect fake access points. Vistumbler supports GPS logging and tracking directly in the app with Google Earth.

If you do not want to use a laptop and have a mobile device, consider using AirPort Utility on an iOS device or download the application on Android.


75% 4:02 PM
WIFI ANALYZER
Connected to: Wi-Fi 5GHz (f4:f2:6d:8d:88:d2)
IP address: 192.168.0.111
Wi-Fi (d4:6e:0e:8d:2b:92)
CH 8+4
2447 MHz
2457-2417=40 MHz
TP-LINK TECHNOLOGIES CO., LTD
-45 dBm
WPA2
? (28:57:67:fa:45:97)
5G
CH 153
5765 MHz
5815-5735=80 MHz
DISH TECHNOLOGIES CORP
-55 dBm
WPA2
Wi-Fi 5GHz (...)
5G
-58 dBm
WPA2
JThompson (48:00:33:ee:5d:92)
CH 11
2462 MHz
2473-2451=22 MHz
TECHNICOLOR CH USA INC
79 dBm
WPA2
DIRECT-roku-245-AB7C61 (c2:d2:f3:8f:09:09)
5G
CH 36
<Local Admin>
Remke
wild HARVEST
SHOP ORGANIC!
Tap here to fill entire screen

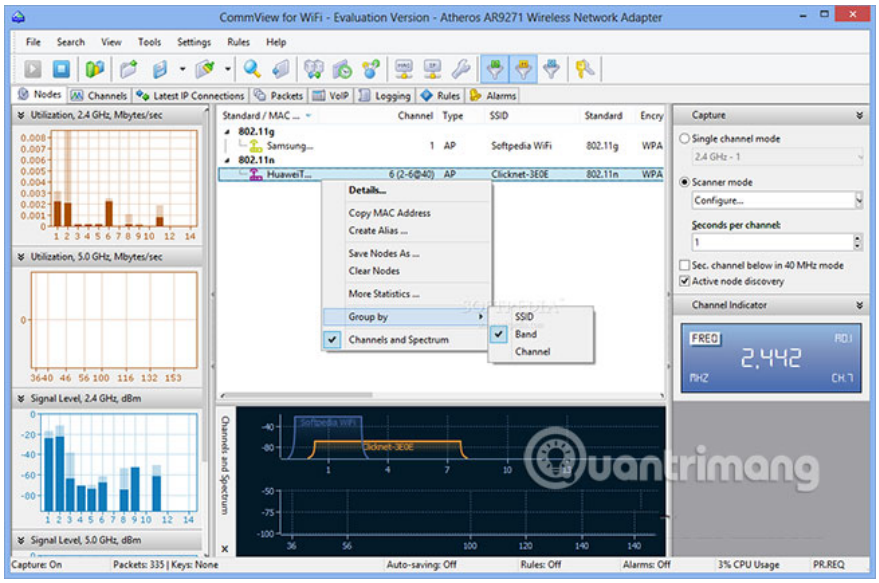
Wifi Analyzer's mobile option is a free Android app that you can use to find access points on smartphones or tablets based on Android. Wifi Analyzer lists basic details of access points on the 2.4GHz band and supported devices on the 5GHz band.

You can export the access point list (in XML format) by sending it to an email or other application or taking a screenshot. Wifi Analyzer also has charts that display channel signals, history and usage ratings. Besides, Wifi Analyzer also has a signal measurement feature to help find access points.

WiFi sniffer

WiFi sniffer (a portable tool to locate the nearest wireless connection). Instead of just taking network details, sniffer captures and displays, even analyzing raw packets sent over waves. Traffic can be imported into other tools, such as an encryption cracking tool. Some sniffer also include functions to perform analysis or unlocking. In addition, some sniffer only search and report on certain network traffic, such as having sniffer designed to disclose clear written password sent.

CommView for WiFi is a popular commercial WiFi analyzer and WiFi sniffer, offering a 30-day limited trial version. CommView for WiFi has a stumbler feature to display network details, plus statistics and channel usage. CommView for WiFi can monitor IP connections and record any VoIP session. This tool also allows you to capture and view raw packages.

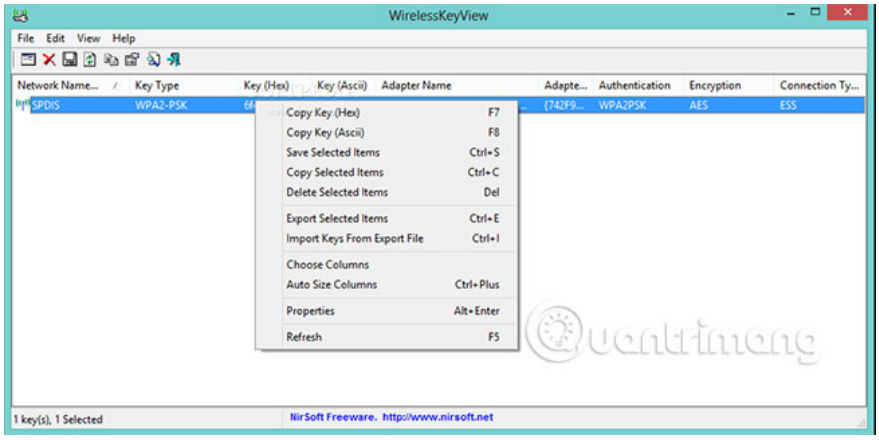


If connected to a WiFi network, you can enter the PSK passphrase to display the decrypted packages. You can also set visible data filtering rules and set alerts to track fake devices. Other interesting features include a traffic builder, node reorganization to automatically start the client and rebuild TCP to better track captured data (in text or pictures).

Kismet is an open source WiFi stumbler, packet sniffer and intrusion detection system that can run on Windows (with WSL framework), Mac OS X, Linux and BSD. Kismet displays access point details, including the SSID of "hidden" networks. It can also capture raw wireless packages, then you can import Wireshark, TCPdump and many other tools. In Windows, Kismet only works with CACE AirPcap wireless adapters due to limitations on Windows drivers. However, Kismet supports multiple wireless adapters in Mac OS X and Linux.

Tools to reveal WiFi network details

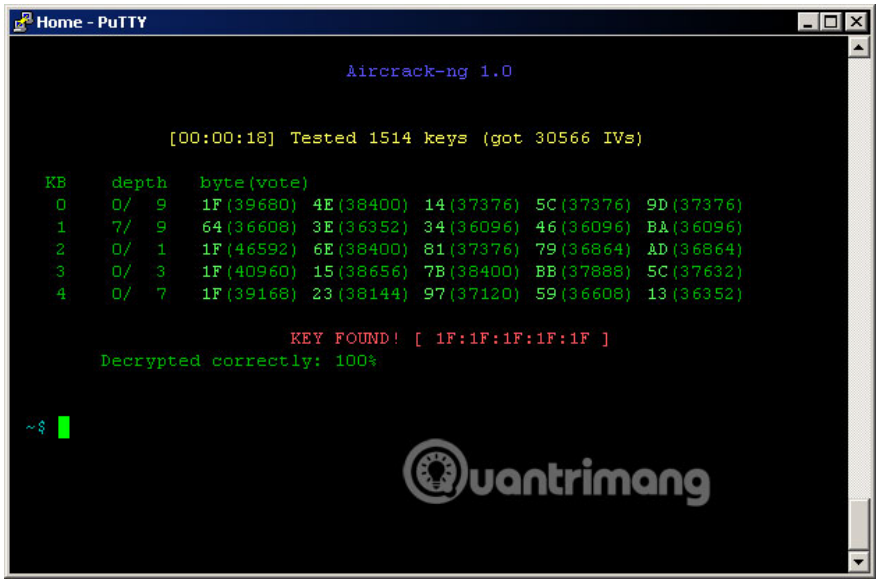
WirelessKeyView from NirSoft (*reference link: http://www.nirsoft.net/utils/wireless_key.html*) is a simple but neat tool, listing all WEP, WPA and WPA2 keys or passphrases store on the Windows computer that you run.



Although it is quite easy to find the key saved in Windows 7 and earlier versions through the regular Windows GUI, but to Windows 10, things have become more difficult. WirelessKeyView quickly produces an exportable list of all saved networks, regardless of the version of the operating system.

Tools like WirelessKeyView can reveal how a device contains sensitive information, in addition to regular, compromised or stolen documents. These tools also show the importance of using 802.1x authentication, in which users will have separate login information for WiFi and not easy to encounter this type of problem.

Aircrack-ng.org is an open source toolkit that performs WEP and WPA / WPA2-Personal unlocking tasks.



Aircrack-ng runs on Windows, Mac OS X, Linux and OpenBSD. This tool can also be downloaded as a VMware and Live CD image. You can view WiFi networks around, including hidden SSIDs.

Linux distribution for testing hack and penetration testing

One of the most popular distributions for pen test is Kali Linux. In addition to installing a regular Linux operating system on your computer, you can create a bootable disk directly, download VMware or VirtualBox images. Kali Linux contains many security and forensic tools, such as Kismet and Aircrack-ng tools. You can use one of these tools to pen test WiFi.

Some other WiFi tools included in Kali Linux are Reaver to hack networks through unsafe WPS PINs, FreeRadius-WPE, to perform man-in-the-middle attacks targeting 802.1X authentication and Wifi Honey for creating a honey pot, attracting clients to connect to a fake AP in the hope of gaining client traffic and performing man-in-the-middle attacks.

Full force with a hardware tool

If you're really serious about wireless security and want to try to find out which vulnerabilities exist, you must know about WiFi Pineapple. This is a hardware-based solution specifically designed to test WiFi and pen test. You can scan, target, block and report on many wireless threats and weaknesses.

WiFi Pineapple looks a lot like a regular router and includes web GUI.

You can do things like view client details of each access point, send authentication packages and automatically create fake access points by mimicking nearby SSIDs to simulate man-in attacks. -the-middle. You can also collect other people's browsing data and fake DNS responses to confuse users or send them to fake websites.

WiFi Pineapple currently offers two hardware options: a pocket-sized NANO band that costs between $ 99.99 (2.300.000VND) and a dual-band TETRA like router that costs from $ 199.99 (4.6 million VND).

tips and guides. Thank you for reading and for following us regularly.