

Forum:[Hack Forums](#)

Thread: [Crack WEP Key](#)

itsHaze - January 18, 2013, 7:54 pm

Any way to get into a locked WiFi network, via a brutforce or something? Obviously I'm new. Thanks!

Zonated - January 18, 2013, 7:56 pm

If it's a WEP key, you don't need to bruteforce. You can just get access by using airmon-ng in Backtrack 5.

icuruok - January 18, 2013, 7:57 pm

you can use linux based OS called backtack & use a program called air-crack ng. This program will allow you to crack any encrypted wep network. You can also crack WPA networks but you must use a brute list file which might not work.

Ignite - January 18, 2013, 7:57 pm

I recommend using backtrack if your looking to get into WiFi's. You can probably find a lot of tutorials on HF with the Search button, if not; Google is your friend.

itsHaze - January 18, 2013, 8:05 pm

Thanks everyone! I was just looking for a place to start.

dataconnect613 - January 18, 2013, 10:09 pm

If you want to crack WEP then use backtrack linux and use aircrack-ng. But if it is WPA i believe there is a way to bypass it if it has WPS activated. There might be a thread somewhere but the WPS bypass is just something i heard. Some routers have them on by default etc. But I believe it uses a bruteforce against possible pass-phrases WPS uses. Good luck.

Panoptic - January 19, 2013, 1:28 am

As everyone else has said, aircrack on BT5 works perfectly on WEP. Just search a tutorial on here, there are a hundred of them. Good luck.

ethhunt - January 19, 2013, 2:36 am

yes is aircrack is ideal for all forms of wifi authentication. WPA will be a bit more difficult. Success rate is based on your dictionary file or word list. WEP is RARELY used anymore. You probably wont see many people utilizing that type of encryption any longer because most ISP appointed technicians or tech support are going to recommend you use WPA/WpA2 for your security management.

but most def air-crack on bt5. Google [air-crack] and read some device drive types for cracking WiFi because you need a WiFi card you can put in monitor mode and most WiFi adapters that come already installed in most laptops wont work. So you will have to buy one. This is the one i use which allot of people use also over at backtrack forums.

"http://www.amazon.com/s/ref=nb_sb_ss_i_0_4/179-9766312-4228147?url=search-alias%3Daps&field-keywords=alfa+awus036h&sprexif=alfa%2Caps%2C662"

pretty cheap also. Before you can start cracking WiFi encryption remember you must have a compatible wireless card. Check out this site which clearly recommends the one most people use.

<http://www.raymond.cc/blog/best-compatible-usb-wireless-adapter-for-backtrack-5-and-aircrack-ng/>.

Also if you decide to purchase this WiFi remember to purchase the accessories. This card has few antennas that you could purchase also.

good luck.

pashabiceps - *January 19, 2013, 2:41 am*

How to Crack WEP/WPA/WPA2-PSK encrypted passwords:

<https://hackforums.net/showthread.php?tid=3048101>