

Forum:[Hack Forums](#)

Thread: [Decrypt WPA2 without brute force \(I'm a beginner\)](#)

n1x0nyx - January 29, 2021, 5:20 pm

hi everyone, is there any way to decrypt WPA2 passwords without brute force? or some different tool to crack wireless (I'm using Aircrack-ng). if not, is there any other way to crack wireless without capturing the handshake?

Thanks for your time reading.

pasnger57 - January 30, 2021, 1:35 pm

WPS pin was a ting back in 2010-2013 but it soly patched or just disabled in in 3 file attempts
2nd

aircrack-ng is Way way out of date (CPU cracking only) for running the wpa2 hash
you best using Hashcat whit some GTX 970s for better

3rd Question

i have to ask for clarification what are you running for Brut force mask or command you run ?

???????? ????? - February 3, 2021, 10:29 pm

The best programs and easy penetration

luddite - February 4, 2021, 10:22 am

there is another way left that can't be patched. most wireless client software will start probing from its list of profiles when the AP its connected to is turned off or they get deauthed.

with aireplay-ng deauth one client at a time,collect its probes in airodump-ng -w filename.

or use mdk3 or 4 with a blacklist for single AP macs. airodump creates several filename.xxx files

look at filename.csv,client probes are in the lower half. anything that looks like WPA key should

be tried with the AP listed in the same line. how do they get there? the end user creates a

profile for their home AP and enters the WPA key in place of the SSID. if not deleted this profile

comes up in rotation. about half of what I've got this way were for APs elsewhere.

it works best in busy areas,not high yield but its simple.

atrax0 - February 7, 2021, 7:56 am

(Feb 4, 2021 11:22 AM)luddite Wrote: [\[CITE\]](#) there is another way left that can't be patched. most wireless client software will start probing

from its list of profiles when the AP its connected to is turned off or they get deauthed.

with aireplay-ng deauth one client at a time,collect its probes in airodump-ng -w filename.

or use mdk3 or 4 with a blacklist for single AP macs. airodump creates several filename.xxx files

look at filename.csv,client probes are in the lower half. anything that looks like WPA key should

be tried with the AP listed in the same line. how do they get there? the end user creates a

profile for their home AP and enters the WPA key in place of the SSID. if not deleted this profile

comes up in rotation. about half of what I've got this way were for APs elsewhere.

it works best in busy areas,not high yield but its simple.

Hi, could you make a little tutorial. I tried it, but at the .csv there is not much to see.

luddite - February 8, 2021, 3:40 pm

Hi, could you make a little tutorial. I tried it, but at the .csv there is not much to see.

you need to let it run for hours to catch anything good,even in crowded airspace.
its better when deauthing is happening to one AP or all on the same channel.

the idea was discussed here a few years ago and forgotten,WPS was still working at the time.

<https://forums.kali.org/archive/index.php/t-24473.html>

airodump-ng wlan1 -w clientprobes -o csv
this will write one file with all the data you need.
clientprobes.csv will be in root and load into leaf or any text file reader.
in the lower half things like this will appear.

E8:E8:B7:4E:9F:93, 2019-04-07 17:18:43, 2019-04-07 17:25:46, -60, 5, (not associated)
,Oymqx5smhr2tlzni9k8w6jb,ATT292

this is what to look for. the client E8:E8:B7:4E:9F:93 got booted from ATT292 and started probing from its profile list that includes the WPA code the user entered instead of the ESSID.

one AP at a time using mdk3/4 and a blacklist (-b) or a single client with aireplay works best but takes longer. things have turned up even in long passive scans.

peppi200 - February 10, 2021, 8:58 am

Oymqx5smhr2tlzni9k8w6jb thats the wpa key ?

luddite - February 11, 2021, 11:22 am

(Feb 10, 2021 09:58 AM)peppi200 Wrote: [\[CITE\]](#) Oymqx5smhr2tlzni9k8w6jb thats the wpa key ?
yes,where there is only a WPA key you can search the csv file for a previous occurrence of that mac. all csv files should be saved and merged into a master file for reference.