

Forum:[Hack Forums](#)

Thread: [\[ULTRA\] How to crack a WPA/WPA2/PSK WiFi Password ! \(Best Way, No Wordlist\)](#)

The Milkman - March 16, 2015, 3:19 pm

Hey Guys, after my recent tutorial about "How to hack into a paid hotspot" (<https://hackforums.net/showthread.php?tid=4690027>) I decided to write what will probably be my most successful tut' ever :

How to Find a WPA/WPA2/PSK WiFi Password !

For this, we'll use a break with the WPS protocol (if you don't know what it is, go there : http://en.wikipedia.org/wiki/WiFi_Protected_Setup

Needed :

- Kali linux
- External WiFi card
- 2/3 vacant years in case you get arrested and sent to jail

1 - Enable Monitor mode on your interface : `airmon-ng start wlan0` (it's possible that your interface isn't called wlan0, just replace it then.)

2 - We'll use a tool called "wash", used to perform a scan of all the routers you can reach in order to know if their WPS is secured or not (It'll be not for 99,8% of the routers all around the world.) : `wash -i mon0` (again, mon0 is my monitor interface but could be different for you)

3 - Then, copy the bssid adress of the target AP (obviously with "WPS secured : NO", and past it into this script : `reaver -i mon0 -b targetbssidadress -d 30 -S -N -vv`

4 - Then, just wait (could be 30 sec as it could be 3 or 4 decades) for the console to say something like : "WPS : blablabla", & "WPA : blablabla". Just copy/past the WPA text part into your network manager, as the victim wifi's password, then you're done !

Ps : This doesn't work with every unsecured (WPS talking) router, but it's quite often that it works within 5 minutes.

What, no replies !

Come on guys ! I took the time to write it oO

luljanek - March 18, 2015, 7:04 am

but what about WEP ?

Thanks in advance.

.BangsOnly - March 18, 2015, 7:48 am

Thanks for sharing. But I'm confused is this for secured networks or unsecured, I always thought unsecured networks don't need a password to connect to

The Milkman - March 18, 2015, 8:23 am

(Mar 18, 2015 07:48 AM)Ketam1ne Wrote: [\[CITE\]](#) Thanks for sharing. But I'm confused is this for secured networks or unsecured, I always thought unsecured networks don't need a password to connect to

It is for secured networks ! Reaver finds pins numbers, and when he gets the correct one he translates it (with the router) into the plain text password !

NoAccess123 - March 18, 2015, 11:32 am

Thanks for the Tut . will try when available time
=) =)

Articulate - March 18, 2015, 12:05 pm

Thanks for the tut. This helped me alot <3

Snapbytes - March 18, 2015, 12:07 pm

This only works in WPS and not in WPA/WPA2. Make your thread right.

The Milkman - March 18, 2015, 12:59 pm

(Mar 18, 2015 12:07 PM)demi.god Wrote: [\[CITE\]](#) This only works in WPS and not in WPA/WPA2.
Make your thread right.

It does work with WPA/WPA2 with WPS unsecured.