How to Crack / Recover WEP/WPA/WPA2/WPS

Thank you for choosing Portable Penetrator.
This guide will help you understand how to recover WEP/WPA/WPA2 passwords.

https://www.secpoint.com/portable-penetrator.html

What is the difference on WEP WPA / WPA2 / WPS and how to crack it?

When you encounter a WiFi Network it is typically using WEP or stronger WPA/WPA2 Encryption

There are the following ways to crack / recover it:

**FIRST METHOD: WEP / WPA / WPA2 via WPS (WiFi Protected Setup) CRACKING**
Most Routers off the factories come with default enabled WPS WiFi Protected Setup.
This is a feature in routers that give a PIN Based authentication.

Typically there would be 10,000,000 possible combinations and therfore almost impossible to crack or take very long time. Due to a vulnerability discovered it can be possible with only 11,000 combinations to get the password.

When you get the WPS PIN you get both the full real encryption password for WEP WPA or WPA2.
The only requirement is that WPS Is enabled on the target router and there is a good signal.

So what you do is find a network and target it. You need to wait anywhere from 5 minutes to 30-60 minutes and you will start seeing a % bar for cracking like 0.2%, 0.5% 1% etc and this means it is vulnerable and it is cracking.
Then you just need to wait for it to finish and you will get a WEP WPA or WPA2 no matter how strong the key is. Even if it is long and complicated: L0n4ComPl!c4ated.

If after 60 minutes and you do not see a % like 0.2% or more it might indicate target Access Point do not have WPS enabled and you need use another way.
Video with real WPS cracking please see [https://www.youtube.com/watch?v=vuSEPROligM&feature=plcp](https://www.youtube.com/watch?v=vuSEPROligM&feature=plcp)
SECOND METHOD: WPA / WPA2 via Dictionary Attack
In this attack you need an access point with a good signal and users connected. -80 is very bad and -40 is extreme good.
So even -50 or -60 would be good.
Then you choose the access point and you can drop a WiFi bomb or target a specific user. Portable Penetrator will sent DE Authentication packets forcing the users to disconnect.

Typically Windows or other operating systems including mobile devices will think it is a connection error and just automatic reconnect. When this happen Portable Penetrator Sniffs the Connection Handshake.

This can take anywhere from 20 seconds to 2 hours depending on how many users connected, reconnection rate, signal strength.

After that you choose the word list dictionary file you want to use for cracking.
We have more than 1.1 billion entries for cracking. A typically I7 CPU can run with 2000 Cracks per second or more.
A quad core I7 will do 4000 or more per second. A WPA/WPA2 password is minimum 8 characters.

So if the word list password files contain 100 Million entries and for example 40 million are less than 8 characters it will skip those to optimize time.

We have many big word list dictionary files and language specific files as well you can choose from.

Now please notice if you run all the files and it says passphrase not found in dictionary word list it can indicate the password of target Access Point is more Complex and might not be in the 1.1+ Billion entries files.

This can be if the password is overly complicated @j3u*h*naij03%f.

In this case you need to attack another access point or use the WPS cracking technique if WPS is enabled on the router.
Video with real WPS cracking please see http://www.youtube.com/watch?v=CoZpoahF2As&feature=plcp

THIRD METHOD: WEP Cracking Only.

The WEP Encryption is an old type that is vulnerable in many ways and can be cracked fast.

The first way is via IVS cracking where you want to choose a network with a good signal strength -80 is very bad -40 is very good. So you can choose one with -60 or better.
Then you need in best cases 2-3 or more users connected.
Portable Penetrator will start to force traffic to the router and sniff existing traffic from the connected users to crack the password. This can take anywhere from 1 minute to several hours depending on how much traffic, signal strength, how many users connected.

The other way you can choose if the Fragmentation Technique where Portable Penetrator will sniff a packet from the Access Point and inject this to cause huge amount of traffic and via this technique crack the password even faster.
With WEP You will almost every time crack it since it is vulnerable technology.
Video with real WPS cracking please see: http://www.youtube.com/watch?v=Vk3cKvAYdNO&feature=plcp