Passcape Wireless Password Recovery: automating password recovery for wireless networks

Passcape Software

1 Automating password recovery for wireless networks

1.1 Abstract

The current wireless networking standard uses a well-tested and reliable hashing function based on the PBKDF2-SHA1 algorithm and limits the minimum password length to eight characters. These two simple but effective restrictions significantly increase the WPA passwords strength against hacking.

1.2 Recovering WPA passwords

1.2.1 Regular recovery methods

It is easy to calculate that if we take **10,000** p/s as a password guessing speed on an average CPU, it will take about **three hours** to go through all the combinations of a simple 8-digit password. If the source password contains lowercase Latin characters in addition to numbers, it will take **3265** days. If there are also uppercase characters, then **692 years**! The conclusion is quite simple and obvious: the brute-force attack is completely ineffective and useless when it comes to a little bit more complicated passwords than numeric ones.

Therefore, all modern password recovery software, in addition to the simple brute-force, has some alternative password guessing methods. The top popular and free **Hashcat** utility has six attacks: simple brute-force, mask, rule-based, dictionary, combinator, and hybrid. **Elcomsoft Wireless Password Recovery** has 6 similar ones. Passcape Wireless Password Recovery has 10 different recovery types.

1.2.2 Problems facing when recovering a big list of WPA handshakes

But one who ever tried to recover passwords for even a small list of wireless networks has probably faced a much more serious problem. The thing is that network dump files often contain dozens, hundreds, or even thousands of handshakes with the same network name. However, it is not always possible to figure out which of these handshakes is valid and which one is not. What should one do in such a case? To iterate through each and every one of the handshakes (with the same network name)? But it may take years. To try searching a password for a certain handshake? But it's password may be incorrect, outdated, or simply never be found due to some peculiarities of a WPA/WPA2 handshake.

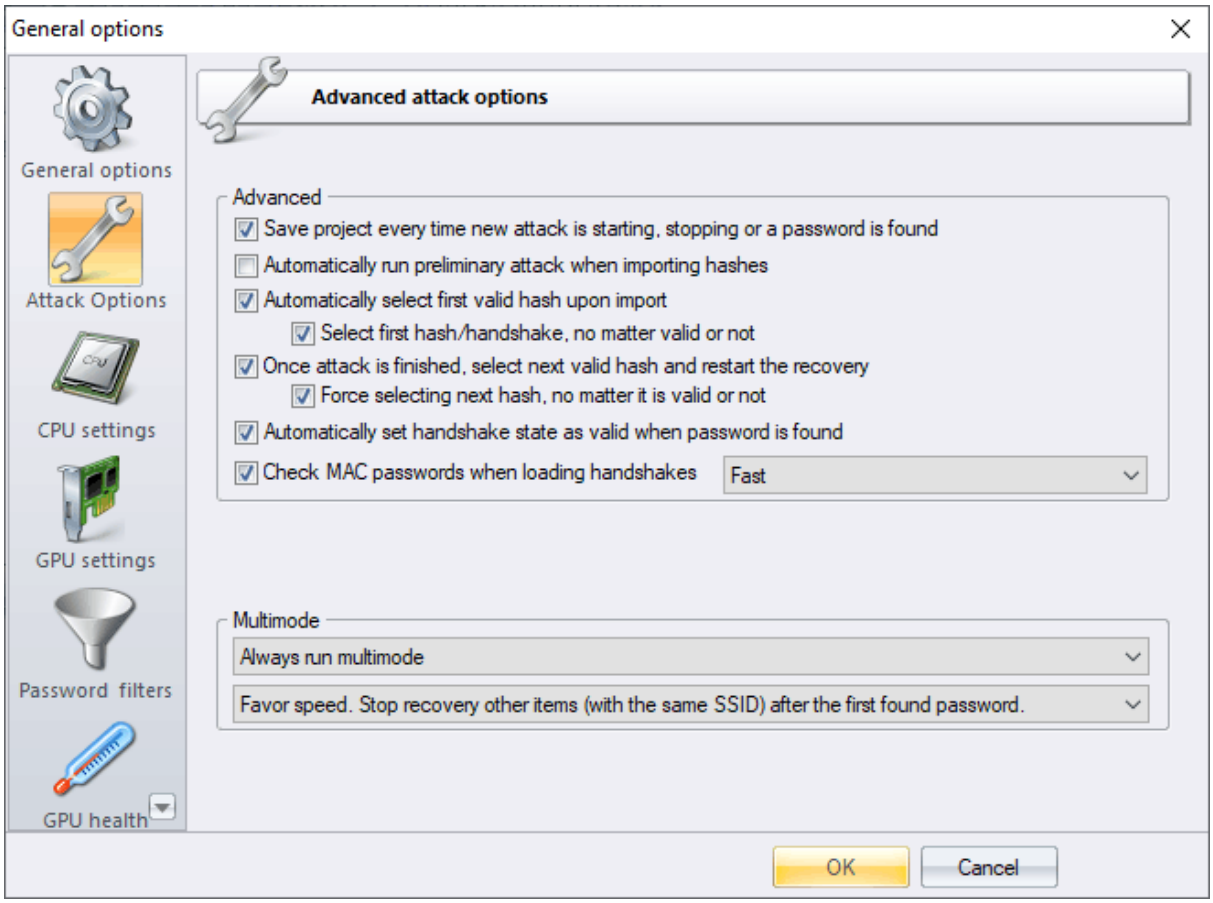
For such cases, **WIFIPR** has come up with a special algorithm that looks for passwords to all handshakes with the same SSID simultaneously, whenever it is possible. The spice of the algorithm is that the password search speed remains the same as if it is a single item!

1.2.3 WIFIPR intelligence when recovering WPA passwords

Let's take a look at a simple example. The program has 30 handshakes with three different network names. In a regular mode, you will have to run an attack on every one of the 30 handshakes. However, when a multi-mode set on, the program splits these 30 records into 3 parts and runs through each part as if it were a single item. This reduces the total search time by a factor of 10.
A slightly more complex case: 30 WPA and WPA2 handshakes, as well as PMKIDs, three SSIDs total. The multi-mode will also do some optimization for you: WPA and WPA2 handshakes will be processing simultaneously (with no speed loss of their SSID is the same), all items will be split by network name and different BSSIDs. But the final result will depend on the selected multi-mode.

There are three operating modes available in multi-mode.

1. If you select a **full check**, the program tries to find as many passwords as possible at the expense of recovery time. This mode continues until a current attack is over or the passwords for all items in the active SSID group are found. Then the attack restarts for the next group of SSID. If a group consists of different types (PMK hashes, handshakes, or PMKIDs), the multi-mode is guaranteed to be launched for each of them.
2. In a **quick check**, after the first password is found in a group of handshakes with the same network name, the remaining items (even with a different BSSID) will be ignored. For example, the list contains different types of entries: PMK, handshakes, and PMKID. After a password is found, for example, for the PMK record, all other records with the same SSID (whether PMKID, handshakes, or PMK) will be skipped and the multi-mode will switch the search to the next group with a different SSID name.
3. A **smart search** is the most intelligent mode. Similar to the previous 2 modes, the program splits the entire network list into groups by SSID name. Each group, in turn, is divided into subgroups by BSSID names. If a password is found for a specific SSID and BSSID subgroup, the program switches to another BSSID subgroup, and so on. If you find the password for the PMKID, all other PMKID entries with the same SSID, as well as all other handshakes with the same SSID and BSSID will be skipped.



1.3 Conclusion

Multi-mode is designed primarily to work in conjunction with the next record auto selection option. If it is set, the password recovery process for a large list of networks that combines handshakes, PMKID, PMK from different sources, with different SSIDs and BSSIDs, WPA and WPA2, etc., is reduced only to choosing a multi-mode and launching a preferred attack or a group of attacks. The program will take care of the rest of the optimization.

Stay safe and keep your data in a safe place!