Passcape Wireless Password Recovery:
无线网络的密码恢复自动化

Passcape Software

1 无线网络的密码恢复自动化

1.1 摘要

目前的 无线网络标准 使用的是基于 PBKDF2-SHA1 算法 的经过测试的可靠散列函数，并将最小密码长度限制为8个字符。这两个简单而有效的限制大大增加了WPA密码对黑客攻击的强度。

1.2 恢复WPA密码

1.2.1 常规恢复方法

很容易计算出，如果我们把10,000 p/s作为一个普通CPU的密码猜测速度，那么要想通过一个简单的8位数密码的所有组合，大约需要三个小时。如果源密码除数字外还包含小写拉丁字符，则需要3265天。如果还有大写的字符，那么就需要692年！这也是一个很好的例子。结论是非常简单和明显的：当涉及到比数字密码更复杂一点的密码时，暴力攻击是完全无效和无用的。

因此，所有的现代密码恢复软件，除了简单的暴力攻击外，还有一些替代的密码猜测方法。最受欢迎的免费Hashcat工具有六种攻击方式：简单暴力、屏蔽、基于规则、字典、组合器和混合。Elcomsoft无线密码恢复有6种类似的. Passcape Wireless Password Recovery 有10种不同的恢复类型。

1.2.2 恢复大量WPA握手时面临的问题

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 But it's password may be incorrect, outdated, or simply never be found due to some peculiarities of a WPA/WPA2 handshake.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!

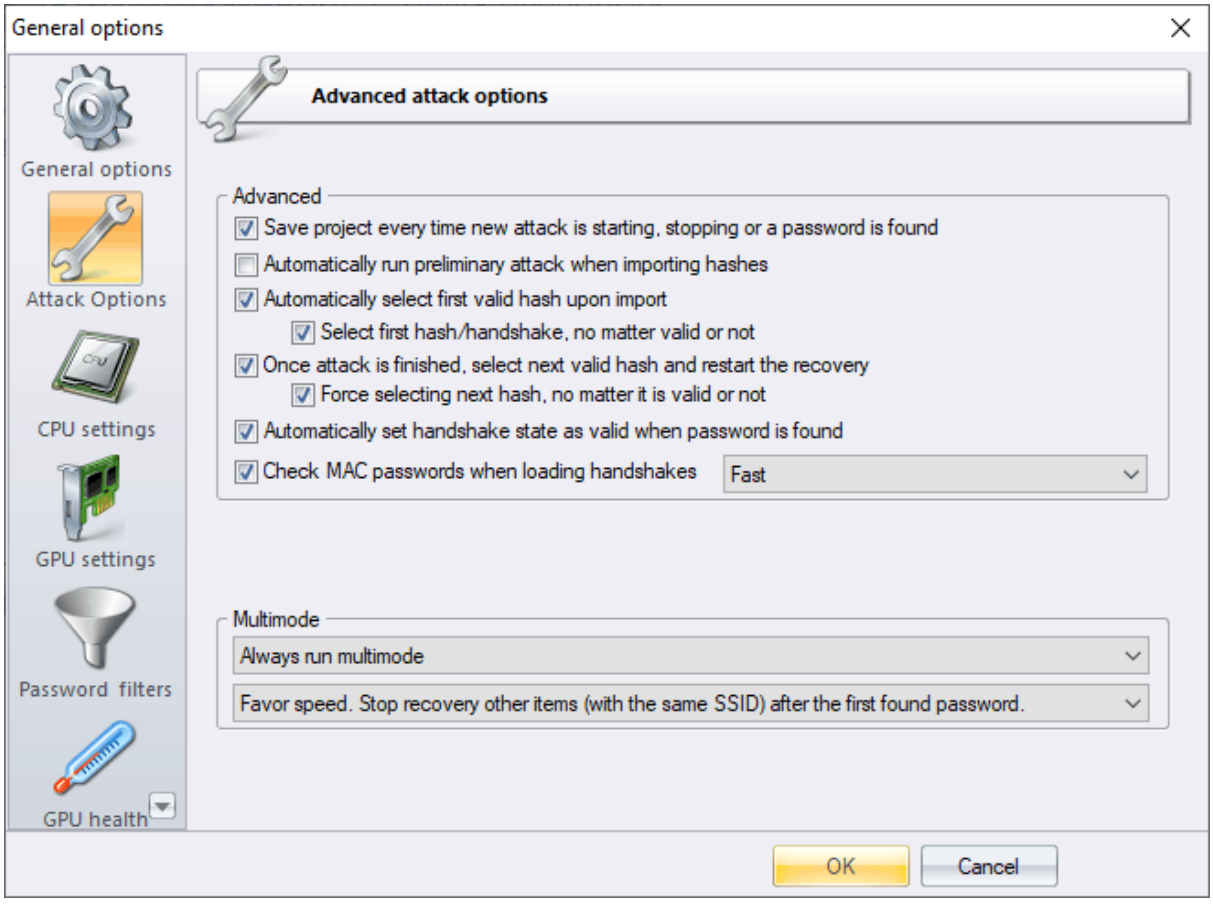
1.2.3 恢复WPA密码时的WIFIPR信息

让我们看一下一个简单的例子。该程序有30次握手，有三个不同的网络名称。在常规模式下，你必须对这30次握手的每一次都进行攻击。然而，当多模式设置开启时，程序会将这30条记录分成3部分，并将每一部分作为一个单项来运行。这使总搜索时间减少了10倍。

一个稍微复杂的案例。30次WPA和WPA2握手，以及PMKIDs，总共三个SSIDs。多模式也会为你做一些优化。WPA和WPA2握手将被同时处理(它们的SSID是相同的，没有速度损失)，所有项目将按网络名称和不同的BSSIDs分割。但最终的结果将取决于所选择的多模式。

在多模式下有三种操作模式可供选择.

1. 如果你选择了全面检查，程序会以牺牲恢复时间为代价，试图找到尽可能多的密码。这种模式一直持续到当前的攻击结束，或者在活动的SSID组中的所有项目的密码被找到。然后重新开始对下一组SSID的攻击。如果一个组由不同的类型(PMK哈希，握手，或PMKID)组成，多模式保证对每一个组都能启动。
2. 在快速检查中，在一组具有相同网络名称的握手中找到第一个密码后，其余项目(即使具有不同的BSSID)将被忽略。例如，列表中包含不同类型的条目。PMK，握手，和PMKID。在找到密码后，例如PMK记录，所有其他具有相同SSID的记录(无论是PMKID、握手还是PMK)将被跳过，多模式将把搜索切换到下一个具有不同SSID名称的组。
3. 智能搜索是最智能的模式。与前两种模式类似，该程序将整个网络列表按SSID名称分成若干组。每个组又按BSSID名称划分为子组。如果找到一个特定的SSID和BSSID子组的密码，程序会切换到另一个BSSID子组，以此类推。如果找到了PMKID的密码，所有其他具有相同SSID的PMKID条目，以及所有其他具有相同SSID和BSSID的握手将被跳过。



1.3 总结

多模式的设计主要是为了与下一个记录自动选择选项一起工作。如果它被设置了，那么对于结合了握手、PMKID、不同来源的PMK、不同的SSID和BSSID、WPA和WPA2等的大量网络列表的密码恢复过程，只需要选择一个多模式并发起一个首选攻击或一组攻击。该程序将负责其余的优化工作。

保持安全，把你的数据保存在安全的地方!