​hashcat高效破解wifi密码(比aircrack-ng快)

**(tip:本文所有操作在个人测试环境下运行,请不要用于违法行为)**

## ****准备工具:****

* 电脑
* kali-linux-2025.2系统(4G内存以上)

----在aircrack爆破时,**无线网络审计套件(**aircrack-ng)作为内置模组组件常用于一体化流程破解密码,但由于其早期主要以来于CPU以及对GPU优化性能不佳,在和专业密码恢复工具:**哈希破解器**(hashcat)破解速度上差距显著.因此在最后的wifi**爆破密码**中,使用hashcat为更优解.

## 一.监听抓包过程:

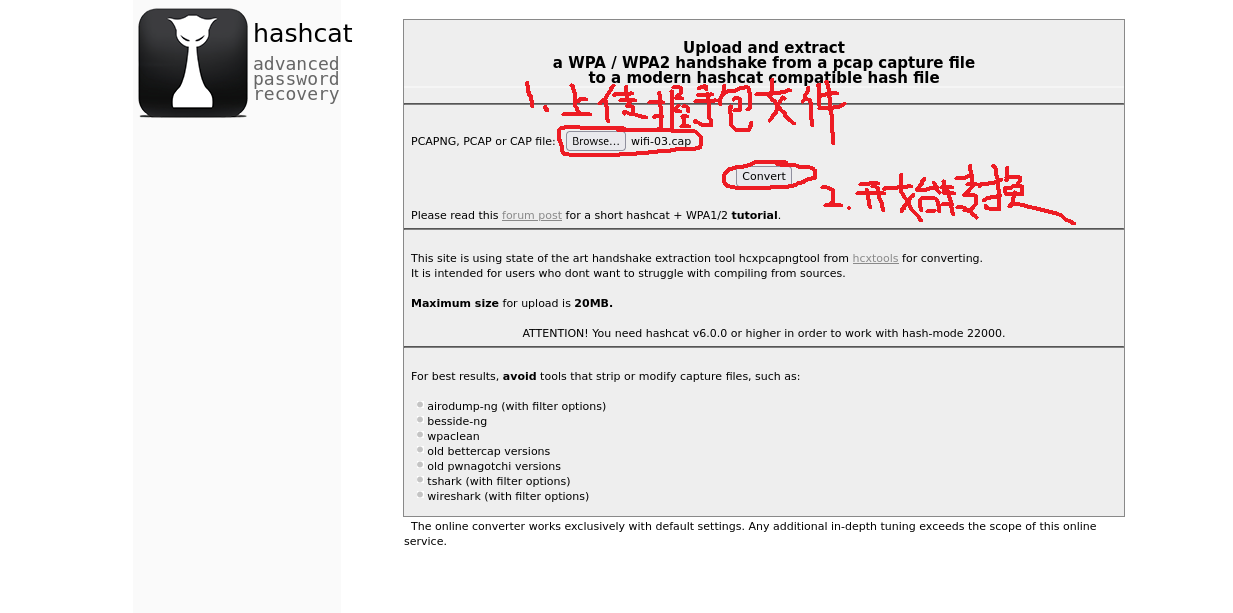
这里省略,网上教程很多,**在成功抓包以后即可进行下面流程**...

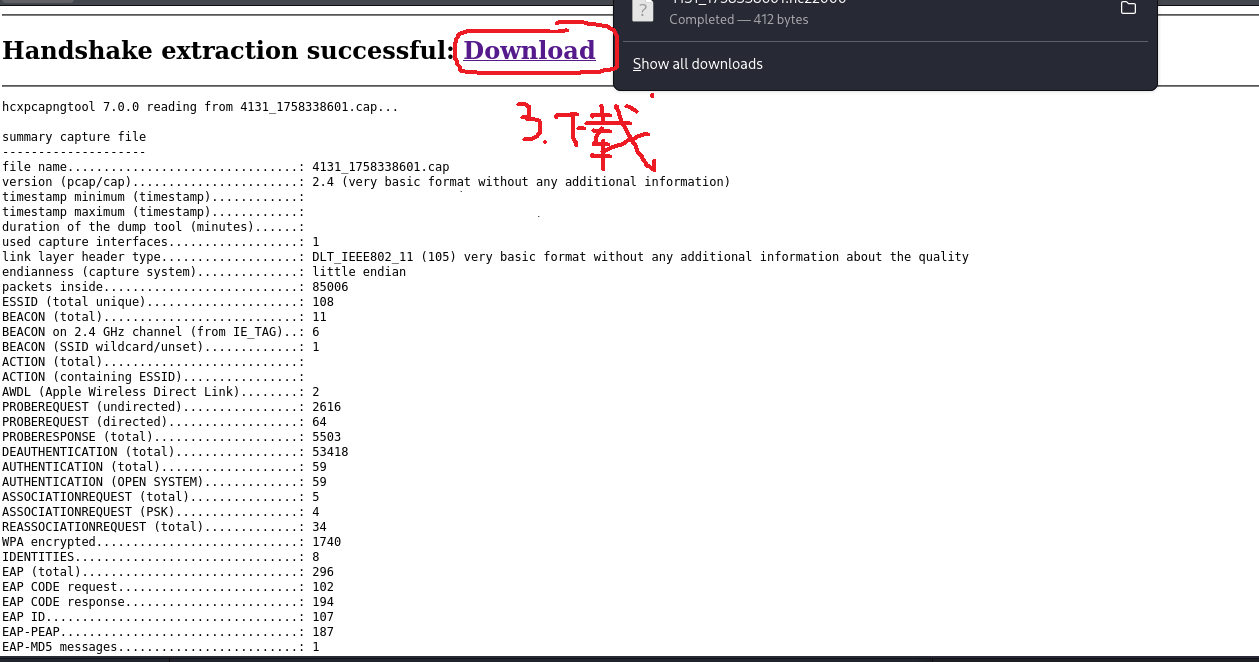
简单来说有四步:

1. 开启wlan监听模式
2. 扫描周边wifi
3. 监听目标wifi
4. 发送解除认证数据包让目标断网从而暴露握手包

## 二.转换cap包格式:

1. 打开[https://hashcat.net/cap2hashcat/](https://hashcat.net/cap2hashcat/" \o "https://hashcat.net/cap2hashcat/)页面
2. 将握手包转换为.hc22000文件

点击并拖拽以移动​编辑\

点击并拖拽以移动​编辑

## 三.hashcat爆破:

**1.字典攻击:(基础)**

hashcat -m 22000 -a 0 wifi.hc22000 ./wordlist.txt

点击并拖拽以移动

* -m 22000:指定哈希类型为WPA-PMKID-PBKDF2
* -a 0:使用预定义的单词列表尝试破解密码
* wifi.hc22000:要爆破的哈希文件
* ./wordlist.txt;你指定的字典文件(比如著名的rockyou.txt)

**2.字典+规则攻击:(推荐)**

hashcat -m 22000 -a 0 wifi.hc22000 ./wordlist.txt -r ./best64.rule

点击并拖拽以移动

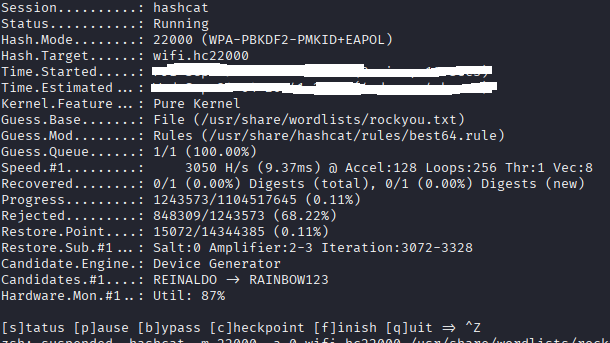
* ./best64.rule:指定的规则文件

**(如果要用规则攻击的话,指定攻击模式(-a)一定要是0或9,不然不能运行!)**

## ****实战测试:****

hashcat -m 22000 -a 0 wifi.hc22000 /usr/share/wordlists/rockyou.txt -r /usr/share/hashcat/rules/best64.rule

点击并拖拽以移动

点击并拖拽以移动​编辑

这里能否破解要看电脑性能、wifi密码强度和字典质量等多方面因素:)

## 代码优化方面:

* -O:启用内核优化模式
* -w:工作负载调优
* -K:内存加速(不稳定,我这个版本好像不支持,要根据具体情况来选择)
* -U:内核循环次数(不推荐,适合详细了解哈希算法后的微操)

### 示例:一个微调后的优化指令

hashcat -m 22000 -a 0 -O -w 4 wifi.hc22000 /usr/share/wordlists/rockyou.txt -r /usr/share/hashcat/rules/best64.rule

点击并拖拽以移动

## 附:hashcat简单介绍(转自ai回答)

Hashcat 是世界上最快、最先进的密码恢复（破解）工具，它支持使用 CPU 和主流的 GPU（显卡）来高速破解多种类型的密码哈希值。

### 核心特点

**速度极快**：Hashcat 的核心优势。它高度优化，能充分利用现代 GPU（特别是 NVIDIA 和 AMD）的数千个计算核心进行并行计算，破解速度远超只使用 CPU 的工具。

**多平台支持**：支持在 Windows、Linux、macOS 上运行。

**多种攻击模式**：提供了灵活多样的攻击方式来尝试破解密码。

**字典攻击**：使用预设的密码字典文件进行尝试。

**组合攻击**：将字典中的词条进行组合后尝试。

**掩码攻击**：当你对密码结构有所了解时（例如“知道以大写字母开头，后面是4个数字”），这种攻击效率极高。

**暴力攻击**：尝试所有可能的字符组合。理论上能破解任何密码，但耗时随密码长度指数级增长，不切实际。

**混合攻击**：结合字典和掩码规则，功能非常强大。

**支持哈希类型广泛**：支持破解超过 300 种常见的哈希算法，如 MD5、SHA1、SHA256、SHA512、NTLM（Windows）、WPA/WPA2（Wi-Fi）等。

**开源免费**：遵循 MIT 许可证，任何人都可以免费使用和审查其代码。

### 基本工作原理

**获取哈希值**：首先，你需要获得目标的密码哈希值（例如，从数据库泄露文件中提取，或从网络中抓取）。

**识别哈希类型**：确定这个哈希值是用哪种算法生成的（Hashcat 提供了 --example-hashes 参数来帮助识别，也有其他工具如 hash-identifier）。

**选择攻击模式**：根据你对目标密码的可能信息，选择最合适的攻击模式（如字典、掩码等）。

**开始破解**：Hashcat 会使用你提供的字典或规则，生成大量的候选密码，并用相同的算法计算其哈希值，然后与目标哈希进行比对。一旦匹配成功，密码即被破解。

#### ****hashcat常用命令****

-m 指定哈希类型

-a 指定破解模式

-V 查看版本信息

-o 将输出结果储存到指定文件

--force 忽略警告

--show 仅显示破解的hash密码和对应的明文

--remove 从源文件中删除破解成功的hash

--username 忽略hash表中的用户名

-b 测试计算机破解速度和相关硬件信息

-O 限制密码长度

-T 设置线程数

-r 使用规则文件

-1 自定义字符集 -1 0123asd ?1={0123asd}

-2 自定义字符集 -2 0123asd ?2={0123asd}

-3 自定义字符集 -3 0123asd ?3={0123asd}

-i 启用增量破解模式

--increment-min 设置密码最小长度

--increment-max 设置密码最大长度

​