# 使用Hashcat和在线工具破解NTLM Hash

## Hashcat介绍

Hashcat是一个密码恢复工具。直到2015年，它都有一个专有的代码库，但随后作为开源软件发布。版本适用于 Linux、OS X 和 Windows。哈希卡支持的哈希算法的示例包括 LM 哈希、MD4、MD5、SHA 系列和 Unix Crypt 格式，以及 MySQL 和 Cisco PIX 中使用的算法。

下载地址：`https://hashcat.net/hashcat/`

Hashcat的官网是Hashcat.net ,点击进去后会有两个下载选项，我们选择hashcat binaries，这个是直接可以在Windows下运行的

```
Usage: hashcat [options]... hash|hashfile|hccapxfile [dictionary|mask|directory]...

- [ Options ] -

 Options Short / Long           | Type | Description                                                | Example
================================+======+============================================================+=======================
 -m, --hash-type                | Num  | Hash-type, references below (otherwise autodetect)         | -m 1000
 -a, --attack-mode              | Num  | Attack-mode, see references below                          | -a 3
 -V, --version                  |      | Print version
 -h, --help                     |      | Print help
     --quiet                    |      | Suppress output
     --hex-charset              |      | Assume charset is given in hex
     --hex-salt                 |      | Assume salt is given in hex
     --hex-wordlist             |      | Assume words in wordlist are given in hex
     --force                    |      | Ignore warnings
     --deprecated-check-disable |      | Enable deprecated plugins
     --status                   |      | Enable automatic update of the status screen
     --status-json              |      | Enable JSON format for status output
     --status-timer             | Num  | Sets seconds between status screen updates to X            | --status-timer=1
     --stdin-timeout-abort      | Num  | Abort if there is no input from stdin for X seconds        | --stdin-timeout-abort=300
     --machine-readable         |      | Display the status view in a machine-readable format
     --keep-guessing            |      | Keep guessing the hash after it has been cracked
     --self-test-disable        |      | Disable self-test functionality on startup
     --loopback                 |      | Add new plains to induct directory
     --markov-hcstat2           | File | Specify hcstat2 file to use                                | --markov-hcstat2=my.hcstat2
     --markov-disable           |      | Disables markov-chains, emulates classic brute-force
     --markov-classic           |      | Enables classic markov-chains, no per-position
 -t, --markov-threshold         | Num  | Threshold X when to stop accepting new markov-chains       | -t 50
     --runtime                  | Num  | Abort session after X seconds of runtime                   | --runtime=10
     --session                  | Str  | Define specific session name                               | --session=mysession
```

## 使用hashcat破解NTLM Hash

```
hashcat -m 1000 NTLM HASH 字典 --force
```

```
570a9a65db8fba761c1008a51d4c95ab:Admin@123

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 1000 (NTLM)
Hash.Target......: 570a9a65db8fba761c1008a51d4c95ab
Time.Started.....: Wed Jul 20 15:01:49 2022, (0 secs)
Time.Estimated...: Wed Jul 20 15:01:49 2022, (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (C:\Users\DaoEr\Desktop\1.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:     2953 H/s (0.03ms) @ Accel:128 Loops:1 Thr:64 Vec:1
Recovered........: 1/1 (100.00%) Digests
Progress.........: 11/11 (100.00%)
Rejected.........: 0/11 (0.00%)
Restore.Point....: 0/11 (0.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: 123 -> hieowyrf

Started: Wed Jul 20 15:01:27 2022
Stopped: Wed Jul 20 15:01:50 2022
```

# 网站破解

https://www.cmd5.com/