Hashcat

元動画のURL

この記事はゆっくりハッキングチャンネルの総当たり攻撃と辞書攻撃をHashcatを使ってパスワード解析をするに加筆したものになります。

hashとは？

- ハッシュ関数: 任意のデータから、別の値(多くの場合は固定長の)値を得るための関数のこと。
- 検索の高速化やデータ比較処理の高速化、改ざんの検出に使われる。

> 例えば、クラッカーがシステムに侵入し、システム内のファイルを改ざんした場合には、改ざん前のハッシュ値と比較することでどのファイルが改ざんされたかを判別することができます。

Hashcatとは

Hashcatは一般的にパスワード復号ツールに分類されており、MD5を始めとした**ハッシュ値を復号する**ことができます。 あるハッシュ値がわかっている場合に、辞書ファイルや総当り攻撃を使って大量のhashを生成し、それらを解析対象と比較することで、ハッシュ値のもとの値を解析します。

最近でいうと、twitterでAirDropの通信を盗聴してSHA-256ハッシュを取得することができれば、容易にもとの電話番号を解析できると話題に上がっていました。元ツイート

Hashcatの利点

- 100以上種類のhashタイプのオプションがあります。
- GPU計算に対応しているので高速実行可能です。

インストール

Linux系OSの場合

Ubuntu20.04やKali-Linuxではaptを使ってインストール可能です(他のLinuxディストリビューションでもパッケージ管理ソフトをつかってインストールできるかもしれないが未検証。)。

```
sudo apt install hashcat
```

公式Websiteからインストールを行う場合

1. hashcat公式サイトにアクセスし、「hashcat binaries」からDownloadをクリックしてダウンロードします。
2. 7zip等を使い、zipファイルを解答する。Windowsの場合はドライブ直下に解答するのがおすすめ。

ベンチマーク

まずは、hashcatが正しく動いているのを確認するために、ベンチマークを行います。ベンチマークによってhashレートという1秒あたりに何個のハッシュ値を解析できるのかが確認できます。

```
hashcat -m 0 -b #-mでhash-type0番(md5)を指定。-bはベンチマークモード
```

また、Windowsの場合はexeファイルを実行するので以下のようにコマンドを変更してください。

```
hashcat64.exe -m 0 -b
```

筆者の場合はGPUが搭載されていないパソコンで実行したため、場合にはNo devices found/left errorが表示されました。 この場合にはCPUを使ってハッシュ値の計算を行うため、コマンドの末尾に--forceをつけることでCPUを使って解析を行えます。

```
hashcat -m 0 -b --force
#実行結果
hashcat (v5.1.0) starting in benchmark mode...
Benchmarking uses hand-optimized kernel code by default.
You can use it in your cracking session by setting the -O option.
Note: Using optimized kernel code limits the maximum supported password length.
To disable the optimized kernel code in benchmark mode, use the -w option.

OpenCL Platform #1: The pocl project
====================================
* Device #1: pthread-11th Gen Intel(R) Core(TM) i7-1165G7 @ 2.80GHz, 4096/13685 MB

Benchmark relevant options:
===========================
* --force
* --optimized-kernel-enable

Hashmode: 0 - MD5

Speed.#1.........:   804.4 MH/s (9.81ms) @ Accel:1024 Loops:1024 Thr:1 Vec:16
```

```
Started: Sat May 22 15:27:49 2021
Stopped: Sat May 22 15:27:56 2021
```

これをみると、私のパソコンでは、1秒間に約804000000のハッシュ値を生成できるようです。いろいろなGPUのhashレートをgithubで公開している方がいらっしゃるので「hachcat hashrate」などで検索してみると面白いかもしれません。

Hashcatのオプションを確認する。

次にHashcatのオプションの確認の仕方を紹介します。

- Linux系OSの場合

```
man hashcat #マニュアルが表示される
hashcat -h #helpを表示
```

- Windowsの場合

```
hashcat64.exe -h
```

MD5のハッシュ値を作成して解析を行う

試しにabcdという値のハッシュ値を作成して、そのハッシュを復号する実験を行います。-nオプションをつけることで"abcd改行文字"ではなく、"abcd"のハッシュ値を生成するようにしています。

```
echo -n "abcd" | md5sum #-nオプションで改行コードを出力しないようにしている。
```

上のコマンドを実行するとabcdのハッシュ値e2fc714c4727ee9395f324cd2e7f331fが得られます。

hashcatを使って解析

今回はブルートフォースアタック(総当り攻撃)によって小文字のアルファベット4文字のハッシュを生成して、それがabcdのハッシュ値と一致しているかどうかでhashを復号していきます。?lは小文字の全てのアルファベットを表しており、今回は4文字の小文字アルファベットに総当たり攻撃をしています。(下のマスク表を参照)

> 筆者のPCにはGPUが搭載されていないため、コマンドの末尾に--forceオプションがついているが、GPUをお持ちの方は--forceを省いてください。

```
hashcat -m 0 e2fc714c4727ee9395f324cd2e7f331f -a 3 ?l?l?l?l --force # -a 3 アタック
```

すると、以下のようにhashが復号できているのが確認できます。

```
e2fc714c4727ee9395f324cd2e7f331f:abcd
```

一度解析したハッシュ値はhashcatに記録されるので、それを参照したい時は、--showオプションを使います。

```
hashcat -m 0 e2fc714c4727ee9395f324cd2e7f331f -a 3 ?l?l?l?l --force --show
```

辞書ファイルを使ったhashの解析を行う

rockyou.txt呼ばれるソシャゲ会社から流出した3200万件の平文パスワードリストを使って辞書攻撃を行っていきます。

```
hashcat -m 0 d41e98d1eafa6d6011d3a70f1a5b92f0 -a 0 ~/app/rockyou.txt  --force #-a (
```

無事ハッシュを複合することができました。

詳しいoptionの説明

Hashcatのマニュアル等の一部を抜粋しました。

アタックモード

0	辞書攻撃
1	Combination
3	Brute-force
6	Hybrid Wordlist + Mask
7	Hybrid Mask + Wordlist

マスク表

?l	abcdefghijklmnopqrstuvwxyz
?u	ABCDEFGHIJKLMNOPQRSTUVWXYZ
?d	0123456789
?h	0123456789abcdef
?H	0123456789ABCDEF

?s	各種記号
?a	?l?u?d?s(l,u,d,sのパターン)
?b	0x00 - 0xff

> 各種記号は!"#$%&'()+*,-./:;<=>?@[]^_`{|}~*の総称。