Hashcat

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**ことができる。

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。

Hashcatの利点

- 100以上種類のhashタイプのオプションがある。
- GPU計算に対応しているので高速。

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できた。(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する。
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、ベンチマークを行う。

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

GPUが搭載されていない場合にはNo devices found/left errorと表示される。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。

```
hashcat -m 0 -b --force #-b ベンチマークモード、-m 0 ハッシュタイプを指定する。0はMD5
```

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する。

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

hashcatのオプションを確認する。

Linux系OSの場合

```
mah 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hash値を作成して解析を行う

試しにabcdという値のhash値を作成して、そのハッシュを復号する実験を行う。

```
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が得られる。

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を復号する。 ?lは小文字の全てのアルファベットを表している。(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る。

```
e2fc714c4727ee9395f324cd2e7f331f:abcd
```

一度解析したhash値はhashcatに記録されるので、それを参照したい時は、--showオプションを使うとよい。

```
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う。

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

optionの説明

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!"#$%&'()+,-./:;<=>?@[]^_`{|}~