



# Crack the hash

## URL

<https://tryhackme.com/room/crackthehash>

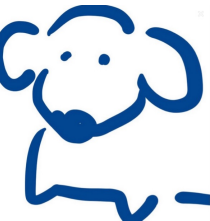


這個主題主要在探討各種的雜湊（hash）

雜湊的特性

- Input的長度無上限
- 使用相同的演算法，Output的長度就一致
- 不可逆性（不可從Output回推成Input）
- 唯一性（只要Input不同Output就不可能相同）

不同演算法有不同的特性跟Output結果，可以參考以下網址的例子  
[https://hashcat.net/wiki/doku.php?id=example\\_hashes](https://hashcat.net/wiki/doku.php?id=example_hashes)



## 雜湊辨識工具

線上：

<https://www.tunnelsup.com/hash-analyzer/>

線下：hash-identifier、hashid

## 雜湊辨識、破解工具

線上：

<https://hashtoolkit.com/>

<https://hashes.com/en/decrypt/hash>

<https://crackstation.net/>

線下：hashcat、john



```
└─# hash-identifier 'CBFDAC6008F9CAB4083784CBD1874F76618D2A97'
#####
#                                     #
#                                     #
#                                     #
#                                     #
#                                     #
#                                     #
#                                     #
#                                     #
#                                     #
#                                     #
#####
v1.2
By Zion3R
www.Blackexploit.com
Root@Blackexploit.com

Possible Hashs:
[+] SHA-1
[+] MySQL5 - SHA-1(SHA-1($pass))
```

```
└─# hashcat 'CBFDAC6008F9CAB4083784CBD1874F76618D2A97' /usr/share/password/rockyou.txt -m 100
```

( 第二題 )





```
└─# hashid \"$2y\\$12\\$Dwt1BZj6pcyc3Dy1FWZ5ieeUznr71EeNkJkUlypTsgbX1H68wsRom  
Analyzing '$2y$12$Dwt1BZj6pcyc3Dy1FWZ5ieeUznr71EeNkJkUlypTsgbX1H68wsRom'  
[+] Blowfish(OpenBSD)  
[+] Woltlab Burning Board 4.x  
[+] bcrypt
```

```
└─# cat /usr/share/password/rockyou.txt | grep -o '\\b[a-z]\\{4\\}\\b' > temp.list
```

這題可以看Hint  
考慮先把rockyou.txt中長度為4的小寫字母  
做成另外一份字典檔  
破解的速度會快很多，不然可能會破很久

```
└─# hashcat '$2y$12$Dwt1BZj6pcyc3Dy1FWZ5ieeUznr71EeNkJkUlypTsgbX1H68wsRom' temp.list -m 3200
```

( 第四題 )









```
# hashid '$6$aReallyHardSalt$6WKUTqzq.UQQmrm0p/T7MPpMbGNnzXPMAXi4bJmL9be.cfi3/qxIf.hsGpS41BqMhSrHVXgMpdjS6xeKZAs02.'  
Analyzing '$6$aReallyHardSalt$6WKUTqzq.UQQmrm0p/T7MPpMbGNnzXPMAXi4bJmL9be.cfi3/qxIf.hsGpS41BqMhSrHVXgMpdjS6xeKZAs02.'  
[+] SHA-512 Crypt
```

```
# cat /usr/share/password/rockyou.txt | grep -o '\.{6\}' > temp.list
```

這題可以先考慮先把rockyou.txt中長度為6的任何字元  
做成另外一份字典檔  
破解的速度會快很多，不然可能會破很久

```
# hashcat '$6$aReallyHardSalt$6WKUTqzq.UQQmrm0p/T7MPpMbGNnzXPMAXi4bJmL9be.cfi3/qxIf.hsGpS41BqMhSrHVXgMpdjS6xeKZAs02.' temp.list -m 1800
```

( 第八題 )

```
└─# hashid e5d8870e5bdd26602cab8dbe07a942c8669e56d6
Analyzing 'e5d8870e5bdd26602cab8dbe07a942c8669e56d6'
[+] SHA-1
[+] Double SHA-1
[+] RIPEMD-160
[+] Haval-160
[+] Tiger-160
[+] HAS-160
[+] LinkedIn
[+] Skein-256(160)
[+] Skein-512(160)
```

因為有Salt值，所以hashcat的hash type要選有Salt的SHA-1

```
└─# hashcat 'e5d8870e5bdd26602cab8dbe07a942c8669e56d6:tryhackme' /usr/share/password/rockyou.txt -m 160
```

( 第九題 )