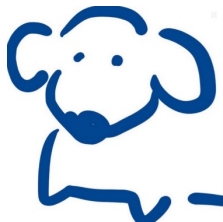
Crack the hash

URL

https://tryhackme.com/room/crackthehash

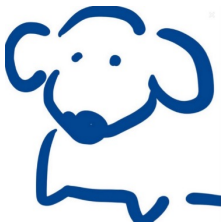


這個主題主要在探討各種的雜湊（hash）

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



雜湊辨識工具

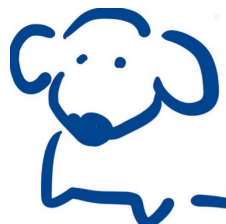
線上：
https://www.tunnelsup.com/hash-analyzer/

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 '48bb6e862e54f2a795ffc4e541caed4d'
   ##########################################################################
   #                                                                        #
   #                                                                        #
   #                                                                        #
   #                                                                        #
   #                                                                        #
   #                                                                        #
   #                                                                        #
   #                                                                v1.2    #
   #                                                             By Zion3R  #
   #                                                          www.Blackploit.com #
   #                                                         Root@Blackploit.com #
   ##########################################################################
--------------------------------------------------

Possible Hashs:
[+] MD5
[+] Domain Cached Credentials - MD4(MD4(($pass)).(strtolower($username)))
```

```
└─# hashcat '48bb6e862e54f2a795ffc4e541caed4d' /usr/share/password/rockyou.txt -m 0
```

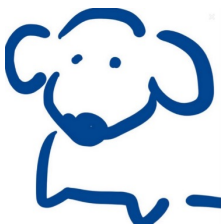
（第一題）


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

（第二題）


```
└─# hashcat '1C8BFE8F801D79745C4631D09FFF36C82AA37FC4CCE4FC946683D7B336B63032' /usr/share/password/rockyou.txt -m 1400
```

（第三題）



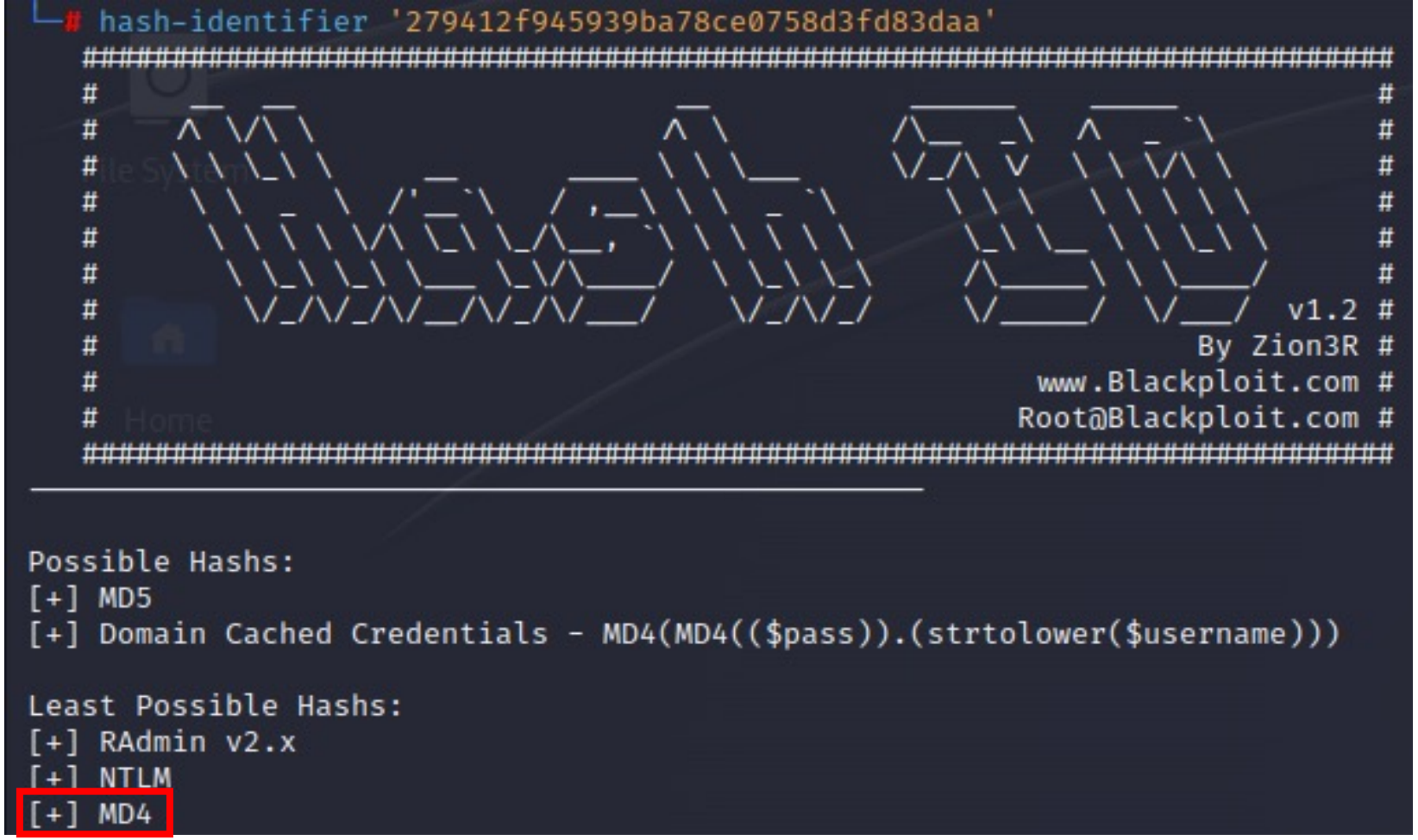
```
└─# hashid \$2y\$12\$Dwt1BZj6pcyc3Dy1FWZ5ieeUznr71EeNkJkUlypTsgbX1H68wsRom
Analyzing '$2y$12$Dwt1BZj6pcyc3Dy1FWZ5ieeUznr71EeNkJkUlypTsgbX1H68wsRom'
[+] Blowfish(OpenBSD)
[+] Woltlab Burning Board 4.x
[+] bcrypt
```

```
└─# 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）



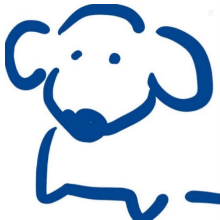
這題的答案不在rockyou.txt中，所以考慮使用線上平台來解（第五題）

```
└─# hash-identifier 'F09EDCB1FCEFC6DFB23DC3505A882655FF77375ED8AA2D1C13F640FCCC2D0C85'
   #########################################################################
   #                                                                  v1.2 #
   #                                                          By Zion3R #
   #                                                 www.Blackploit.com #
   #                                                Root@Blackploit.com #
   #########################################################################
--------------------------------------------------

Possible Hashs:
[+] SHA-256
[+] Haval-256
```

```
└─# hashcat 'F09EDCB1FCEFC6DFB23DC3505A882655FF77375ED8AA2D1C13F640FCCC2D0C85' /usr/share/password/rockyou.txt -m 1400
```

（第六題）



```
└─# hash-identifier '1DFECA0C002AE40B8619ECF94819CC1B'
   ##########################################################################
   #     __  __                     __           ______    ____            #
   #    /\ \/\ \                   /\ \__       /\__  _\  /\  _`\          #
   #    \ \ \_\ \     __      ____ \ \ ,_\      \/_/\ \/  \ \ \/\ \        #
   #     \ \  _  \  /'__`\   /',__\ \ \ \/         \ \ \   \ \ \ \ \       #
   #      \ \ \ \ \/\ \_\ \_/\__, `\ \ \_\ \_       \_\ \__ \ \ \_\ \      #
   #       \ \_\ \_\ \___ \_\/\____/  \ \__\ \_\     /\_____\ \ \____/      #
   #        \/_/\/_/\/__/\/_/\/___/    \/__/\/_/     \/_____/  \/___/  v1.2 #
   #                                                             By Zion3R #
   #                                                    www.Blackploit.com #
   #                                                   Root@Blackploit.com #
   ##########################################################################
--------------------------------------------------

Possible Hashs:
[+] MD5
[+] Domain Cached Credentials - MD4(MD4(($pass)).(strtolower($username)))

Least Possible Hashs:
[+] RAdmin v2.x
[+] NTLM
[+] MD4
```

```
└─# hashcat '1DFECA0C002AE40B8619ECF94819CC1B' /usr/share/password/rockyou.txt -m 1000
```

（第七題）

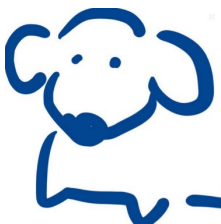
```
└─# hashid '$6$aReallyHardSalt$6WKUTqzq.UQQmrm0p/T7MPpMbGNnzXPMAXi4bJMl9be.cfi3/qxIf.hsGpS41BqMhSrHVXgMpdjS6xeKZAs02.'
Analyzing '$6$aReallyHardSalt$6WKUTqzq.UQQmrm0p/T7MPpMbGNnzXPMAXi4bJMl9be.cfi3/qxIf.hsGpS41BqMhSrHVXgMpdjS6xeKZAs02.'
[+] SHA-512 Crypt
```

```
└─# 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）