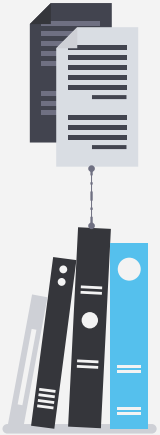
2024 is1ab 新生盃 CTF

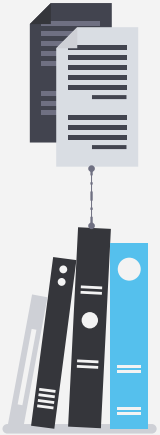
http://140.124.181.153

目錄

- Is they same?
- What is my password?
- 大駭客 Marco
- 好一隻可愛的貓
- huh?



Is they same?



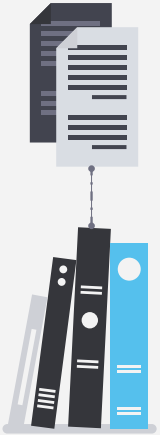
Welcome to the is they same? challenge!

In this challenge, you are required to input two strings.
These two strings must have different contents, but their MD5 hashes must be identical.
Additionally, both strings must start with "is1ab".

Input please transform by (",".join([str(i) for i in string]).encode()).
For example, if you're string is "is1ab", you're output will be "105,115,49,97,98".

Please input your string 1:
Please input your string 2:

md5

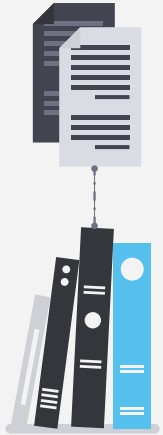


MD5 訊息摘要演算法（英語:MD5 Message-Digest Algorithm），一種被廣泛使用的密碼雜湊函式，可以產生出一個 128 位元（16 個位元組）的雜湊值（hash value），用於確保資訊傳輸完整一致。MD5 由美國密碼學家羅納德·李維斯特（Ronald Linn Rivest）設計，於 1992 年公開，用以取代MD4 演算法。這套演算法的程式在RFC 1321 中被加以規範。

1996 年後被證實存在弱點，可以被加以破解，對於需要高度安全性的資料，專家一般建議改用其他演算法，如SHA-2。2004 年，證實 MD5 演算法無法防止碰撞攻擊（英語:Collision_attack），因此不適用於安全性認證，如SSL 公開金鑰認證或是數位簽章等用途。

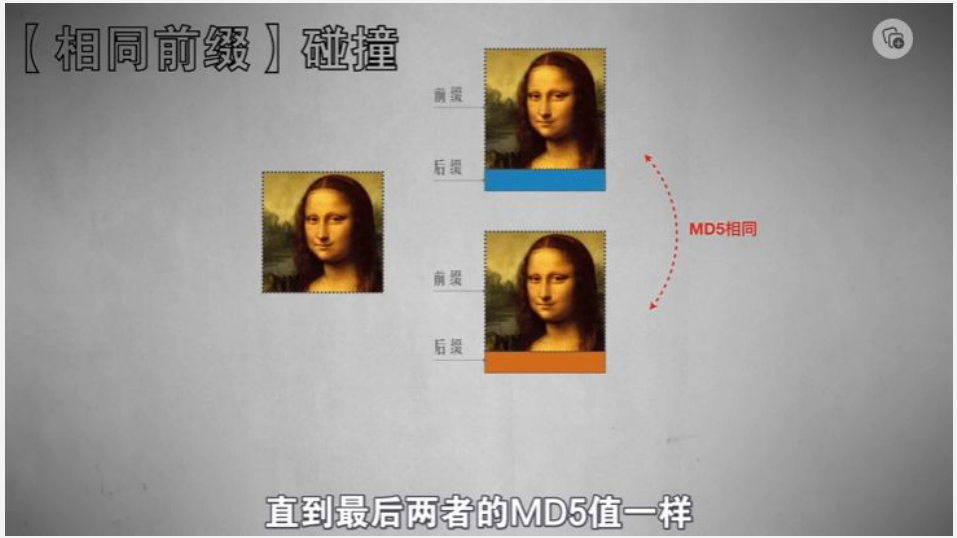
md5 攻擊

1. 原像攻擊：已知MD5，找出任意一個結果為該MD5 的原始內容
   a. 暴力攻擊次數高達2 ^ 128 種可能
2. 第二原像攻擊：已知內容及 MD5，找到第二個 MD5 相同的內容
3. 抗碰撞性：找出任意兩個MD5 相同的內容



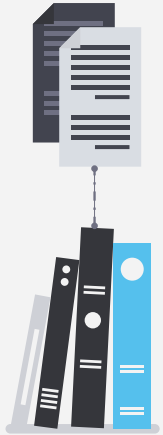
md5 碰撞攻擊

相同前綴碰撞：使用一份原始文件，產生兩份原文有差異但MD5 相同的文件
選擇前綴碰撞：前面內容不同，但MD5 相同



```
docker run --rm -it -v $PWD:/work -w /work -u $UID:$GID brimstone/fastcoll
--prefixfile input -o msg1.bin msg2.bin
```

將要使用的前綴放在input 中

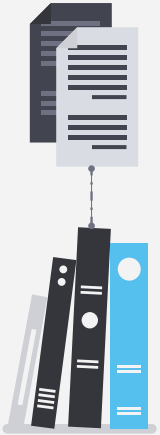


```
a@ubuntu:~/Desktop$ cat input
is1abCTF
a@ubuntu:~/Desktop$ sudo docker run --rm -it -v $PWD:/work -w /work -u $UID:$GID brimstone/fastcoll --prefixfil
e input -o msg1.bin msg2.bin
MD5 collision generator v1.5
by Marc Stevens (http://www.win.tue.nl/hashclash/)

Using output filenames: 'msg1.bin' and 'msg2.bin'
Using prefi
Using initi

Generating
Generating
Running time: 10.3833 s
a@ubuntu:~/Desktop$ cat msg1.bin
is1abCTF
◆◆◆?◆[A◆◆+◆|S◆◆◆e◆g◆x6◆◆◆4◆◆猸◆l◆◆l◆-y$◆◆◆#◆'lI◆<P◆◆j◆%*◆◆◆◆◆◆◆◆◆◆,◆Y◆m:◆X◆7◆◆◆qy◆{7◆)◆◆#◆L◆◆◆◆g◆◆◆◆O◆$◆◆◆◆nM◆4
a@ubuntu:~/Desktop$ cat msg2.bin
is1abCTF
◆◆◆?◆[A◆◆+◆|S◆◆ae◆g◆x6◆◆◆4◆◆猸◆l◆◆l◆◆y$◆◆◆#◆'lI◆<◆◆◆j◆%*◆◆◆◆◆◆◆◆◆◆,◆Y◆◆:◆X◆7◆◆◆qy◆{7◆)◆◆#◆L◆◆◆Vg◆◆◆◆O◆$◆◆◆◆◆M◆4
a@ubuntu:~/Desktop$ diff msg1.bin msg2.bin
Binary files msg1.bin and msg2.bin differ
```

```
a@ubuntu:~/Desktop$ diff -y msg1.bin msg2.bin
Binary files msg1.bin and msg2.bin differ
a@ubuntu:~/Desktop$ diff -y msg1.bin msg1.bin
```

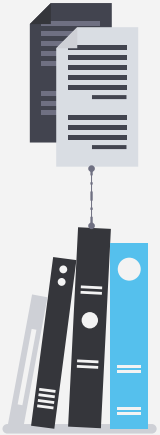
參考資料

MD5 - 維基百科，自由的百科全書
MD5 Collision Attack — SEED Security Labs | by Swetha
MD5为何不再安全
brimstone/fastcoll



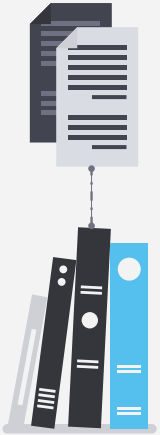
What is my password?

Rick 是個健忘的孩子，他常常忘記他的登入密碼，但還好他有把記憶體dump 出來的好習慣

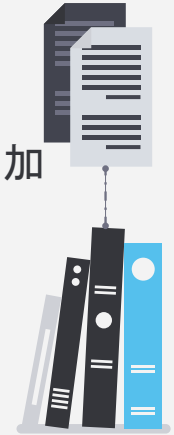


Pass the Hash (PtH)

攻擊者在獲得遠端主機的root 權限後，為了進行橫向移動，通常會先提取各用戶的 NTLM Hash，並利用 Pass the Hash 攻擊，模擬用戶登入其他主機。



NTLM Hash



在 Windows 中，密碼 Hash 目前稱之為 NTLM Hash，NTLM Hash 由明文經加密而來，加密流程如下：

1. 將明文密碼轉換成十六進制的格式
2. 轉換成 Unicode 格式，即在每個字節之後添加0x00
3. 對 Unicode 字符串作 MD4 加密，生成 32 位的十六進制數字

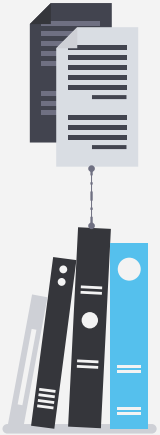
NTLM Hash 又分爲 LM hash和 NT hash，如果密碼長度大於 15，無法生成 LM hash。

NT hash 是目前 Windows 所使用的密碼儲存方式，有時會被誤稱為NTLM hash，可從 SAM 資料庫或 DC 的 NTDS 檔案中找到。這也是主要被利用進行pass-the-hash 攻擊的 hash。

Volatility 3

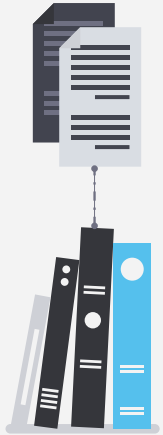
python .\vol.py -f DESKTOP-N5V28S9-20240617-122107.raw windows.info

windows.hashdump : Dumps user hashes from memory



參考資料

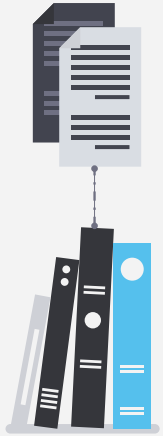
volatility3.plugins.windows.hashdump module — Volatility 3 2.11.0 documentation
[內網滲透]Pass the Hash(PtH)攻擊手法及防禦、偵測措施
破解 NTLM 密碼：深入 SAM 結構的內幕- TeamT5
CrackStation



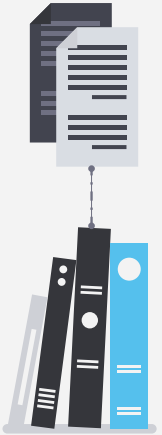
圖片隱寫

以前 meeting 時介紹過 wireshark

製作教學
Windows : copy test.jpg/b + flag.txt/a output.jpg
Linux : cat cover.jpg secret.zip > steg.jpg



大駭客 Marco



在未來的城市「新元都市」，科技與罪惡並存，霓虹燈下的陰影中隱藏著無數的黑暗交易。 Marco 是這座城市裡一名頂尖的駭客，專門替反抗組織與地下勢力執行高風險的任務。

某天，他接到了一個危險的任務 ——從一家名為「天穹集團」的大企業 內部，竊取一份機密文件。這份文件據 說包含了公司極機密的計畫，足以顛覆整個新元都市的權力結構。Marco 知道這次的任務非同小可，但高額的報酬與挑戰的誘惑讓他無法拒 絕。

經過數日的準備與精密的計劃， Marco 終於潛入了天穹集團的數據中心。在虛擬的防護網中，他如魚得水，迅速突破了層層防線，最終拿到目標文件。然而，正當他準備撤退時，警報突然響起，安全系統瞬間封鎖了出口。 Marco 一邊閃避著機械守衛的追擊，一邊急忙尋找出口，並在最後一刻搭乘了一輛飛行車逃離了現場。

在飛行車上，Marco 開啟了硬碟，準備檢 查他辛苦得手的機密文件。這時他驚恐地發現，由於剛才的猛烈撞擊與震動，硬碟竟然受損了！他辛苦得手的機密文件竟無法開啟。無論他怎麼嘗試，螢幕上顯示的都只是無法解讀的亂碼和錯誤訊息。這些檔案原本是他成功完成任務的唯一憑證，現在卻變成了他的最大麻煩。

在新元都市的地下世界裡流傳著一個傳 說：有一位神秘的修復師，能 夠修復任何數位損壞，甚至是最嚴重的資料腐壞。這位修復師行事低調，但名聲卻響徹整個黑市。Marco 別無選擇，只能冒險尋求這位修復師的幫助。

Marco 經過重重困難，找到了一條通往你 ——這位傳說中的修復師 ——的途徑。你精通資料修復技術，無論是被加密、損壞，還是被惡意 篡改的文件，你都能找到恢復它們的方法。在這個充滿黑暗與陰謀的城市中，你是唯一能 夠解開這些檔案的人。

當 Marco 帶著損壞的硬碟來到你的工作室，他知道這是他最後的希望。他知道，成功或失敗，未來的命運將取決於你手中的技術與智慧。

你接過硬碟，開始著手進行修復工作。時間緊迫，危險在不遠處逼近。 Marco 看著你專注的身影，心中充滿了緊張與期待。他不敢想像，如果這次修復失敗，他將面對怎樣的後果。

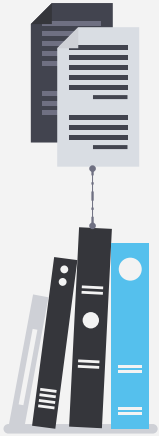
然而，你卻絲毫不為所動，專注地在虛擬界面上操作著，解開一層層加密與損壞的資料。這是你所擅長的領域，沒有什麼難題能 夠難倒你。Marco 默默地祈禱，希望這次能夠如他所願。

最終，你抬起頭，眼中閃爍著自信的光芒。你告訴 Marco，文件已經被成功修復，真相即將揭曉。在這一刻， Marco 明白，他的命運再度掌握在自己的手中，而這場危機背後的陰謀，才剛剛開始被揭開 .....

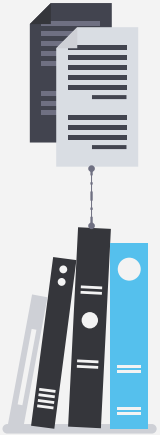
好一隻可愛的貓

一隻可愛的貓咪能藏有什麼壞心思

huh?



identify



ImageMagick 中的工具，用於獲得和格式化圖片

-format：允許自定義輸出格式
%s：圖片編號
%T：frame delay

identify -format "%s %T \n" huh.gif

參考資料

命令行工具:Identify - ImageMagick 中文
图像属性格式和打印- ImageMagick 中文