

解題過程，請依現場環境調整 IP

試題敘述

- 被 A 集團派到 B 集團當臥底的小華每天都會回傳不同的梗圖給 A 集團，然而最近卻被 B 集團主管小南發現了異樣，小華只好緊急收拾脫逃
- 小南在調查小華遺留下的資訊時，發現了一套小華與 A 集團約定好的加密規則，規則指出傳遞的資訊是用 AES(CBC)加密，且需要的條件可以在當次傳送的圖片中找到，另外小南觀察到小華有把密碼重複密碼重複使用的習慣。
- 你是否能利用這些遺留的資訊，幫助小南解開小華逃跑前傳出去的梗圖中藏有什麼秘密？



解題步驟 1:

使用 Kali 工具 binwalk 進行分析，於圖片目錄下右鍵開啟 terminal 介面進行操作

輸入：`binwalk gandalf2.jpg`

結果：觀察圖片結構，可看出藏有兩壓縮檔

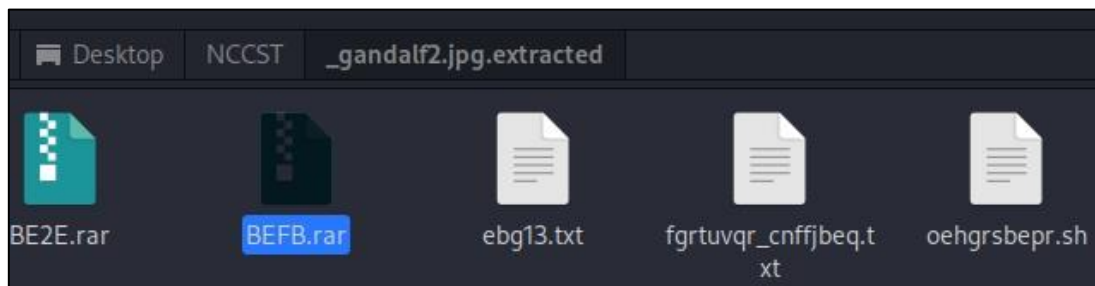
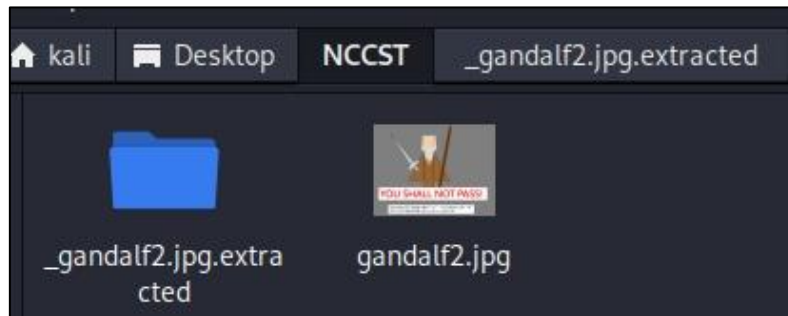
```
(kali@kali)-[~/Desktop/NCCST]
$ binwalk gandalf2.jpg
```

DECIMAL	HEXADECIMAL	DESCRIPTION
0	0x0	JPEG image data, JFIF standard 1.01
48686	0xBE2E	RAR archive data, version 5.x
48891	0xBEFB	RAR archive data, version 5.x

輸入：`binwalk -e gandalf2.jpg`

將壓縮檔拆開，產生_gandalf2.jpg.extracted 資料夾，進入_gandalf2.jpg.extracted 資料夾可看到含有 5 個檔案。

```
(kali@kali)-[~/Desktop/NCCST]
$ binwalk -e gandalf2.jpg
```

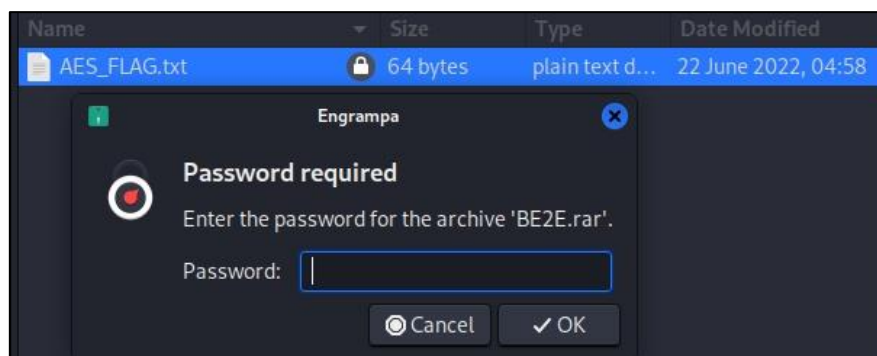


補充說明

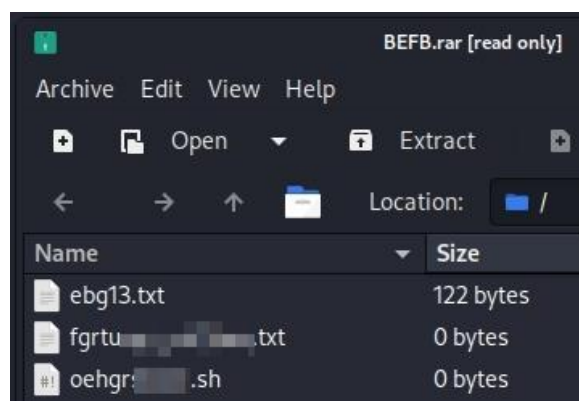
- Binwalk 是一種快速、易於使用的工具，用於分析、逆向工程和提取韌體檔案。
(refer to <https://github.com/ReFirmLabs/binwalk>)
- 參數介紹：-e, --extract：自動提取已知文件類型

解題步驟 2:

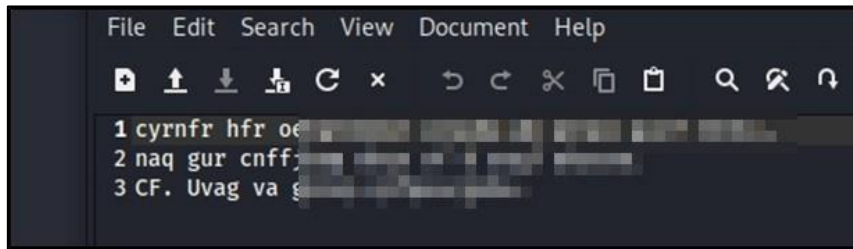
- 觀察拆出之檔案，試著解壓縮壓縮檔 BE2E，發現壓縮檔 BE2E 要密碼才能解開



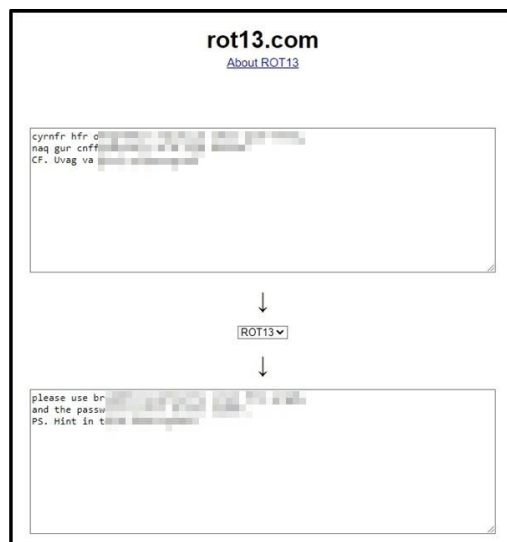
- 第二個壓縮檔 BEFB 已經拆開出 3 檔案，觀察發現僅 ebg13.txt 文件大小不為 0



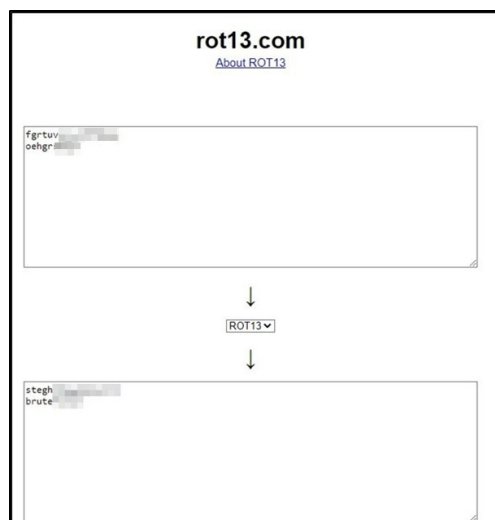
- 開啟 ebg13.txt 文件，發現 ebg13.txt 內有密文
 {cyrnfr hfr xxxxxxxxxxx xxxxxx xx xxxxx xxxx xxxxx,
 naq gur cnffxxxx xxxx xx x xxxx xxxxxx.
 CF. Uvag va xxxxx xxxxxxxxxxxxxx. }



- 觀察其他檔案名稱後，發現檔案名稱 ebg13 發現是字串 rot13 經過 rot13 加密後得到，所以使用 rot13 解開，得到明文
 {please use xxxxxxxxxxx xxxxxx xx xxxxx xxxx xxxxx,
 and the passxxxx xxxx xx x xxxx xxxxxx.
 PS. Hint in xxxxx xxxxxxxxxxxxxx. }



- 再次使用 rot13 解開其他檔案之檔名分別為
 {fgtruxxxx_xxxxxxxxx}.txt → {stegxxxx_xxxxxxxxx}.txt 與
 {oehgrxxxx}.sh → {brutexxxxx}.sh，得到提示為要寫程式破解並使用 stexxxxx 工具



補充說明

ROT13 是一種簡單的字母替換密碼，用字母表中的第 13 個字母替換一個字母。因為基本拉丁字母有 26 個字母(2x13)，因此可以使用相同的算法進行編碼和解碼。(refer to <https://en.wikipedia.org/wiki/ROT13>)

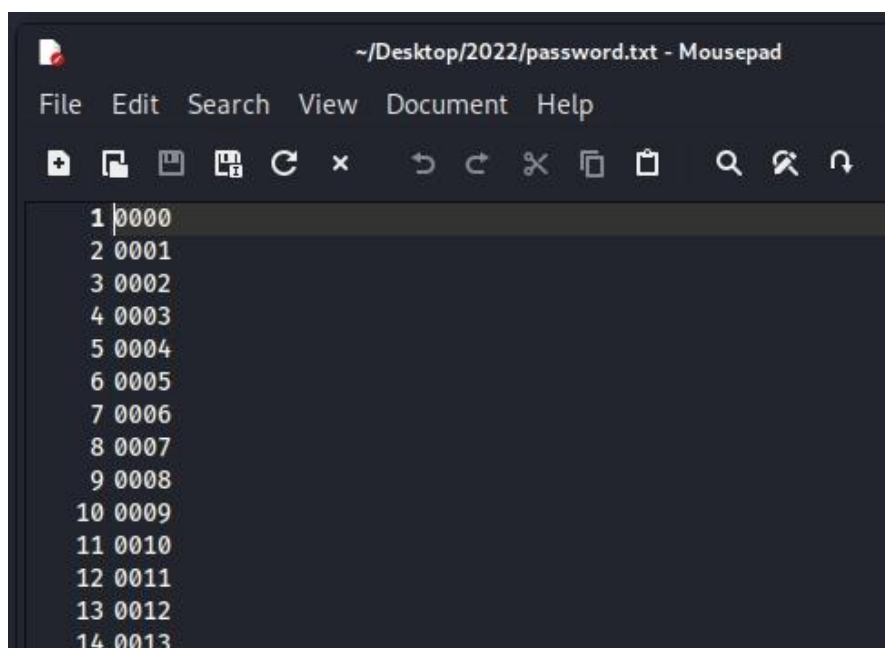
解題步驟 3:

依據提示，密碼為 8 位數字，根據提目中”密碼重複密碼重複”的提示，僅需製作 4 位數字之字典檔案重複使用

輸入：`crunch 4 4 0123456789 -o password.txt`

結果：製造一個 4 位數字之字典檔 `password.txt`

```
(kali㉿kali)-[~/Desktop/NCCST]
$ crunch 4 4 0123456789 -o password.txt
Crunch will now generate the following amount of data: 50000 bytes
0 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 10000
crunch: 100% completed generating output
```

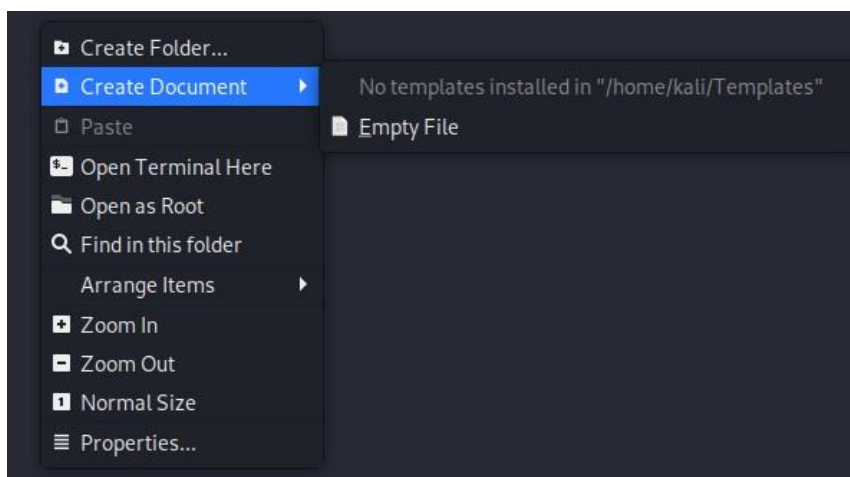


補充說明

- Crunch 是一個詞表生成器，您可以在其中指定標準字符集或用於生成詞表的任何字符集。詞表是通過一組字符的組合和排列來創建的。您可以決定字符數和列表大小 (refer to <https://www.kali.org/tools/crunch/>)
- 參數介紹：
 - min-len：最小長度字符串
 - max-len：最大長度字符串
 - charset string：選用特定字符集，如果留空，則將使用默認字符集
 - o wordlist.txt：指定結果輸出文件名稱，例如:wordlist.txt

解題步驟 4:

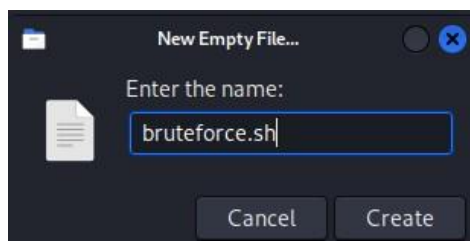
- 因 stexxxxx 工具指令並無支援使用字典檔案破解，需自行撰寫一個程式碼重複執行破解動作，於空白處按右鍵選擇 Create Document 選擇 Empty File



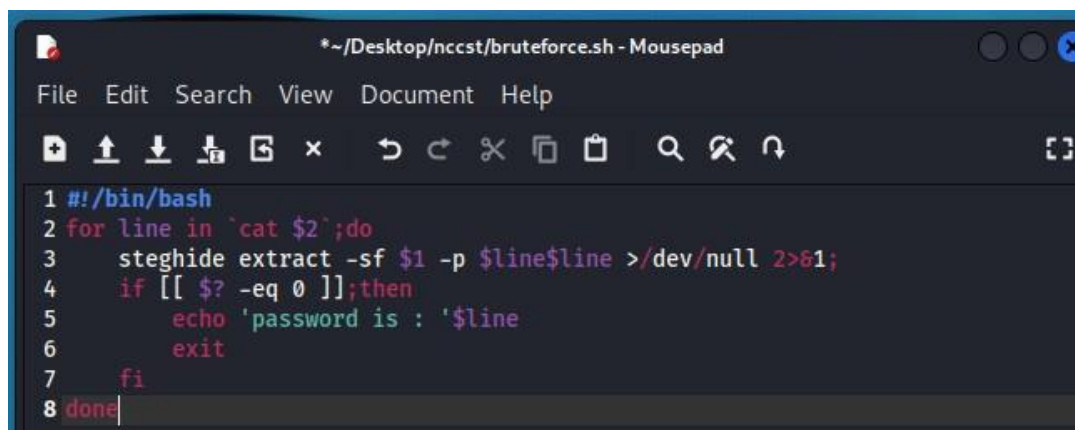
- 新增檔案名稱

輸入：bruteforce.sh

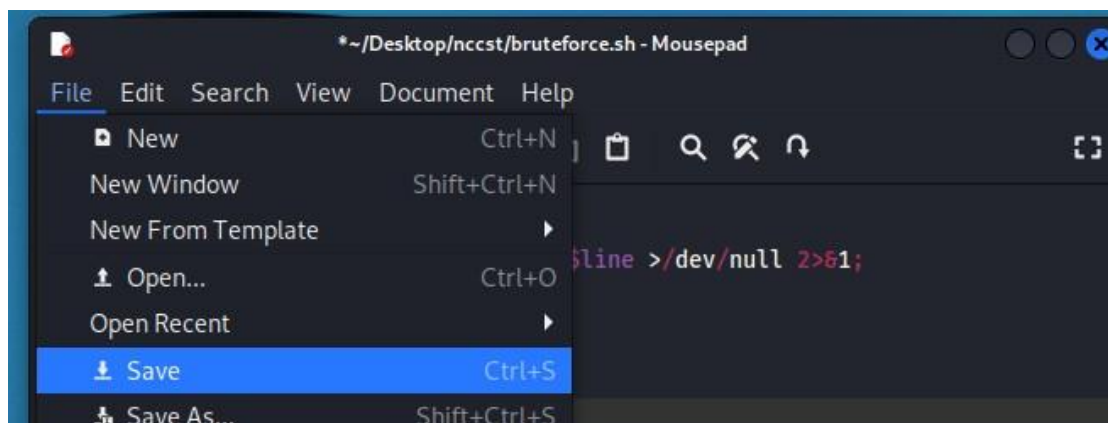
動作：按下 Create 建立



- 動作：滑鼠左鍵點兩下開啟該文件，輸入下列程式碼

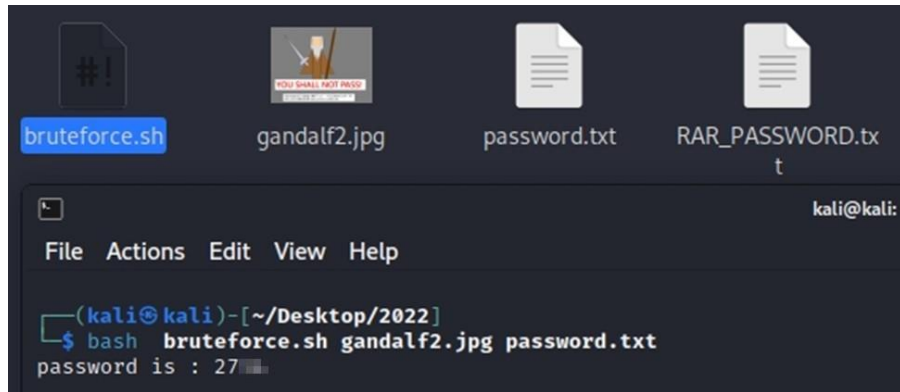


- 動作：按 File 再按 save 保存

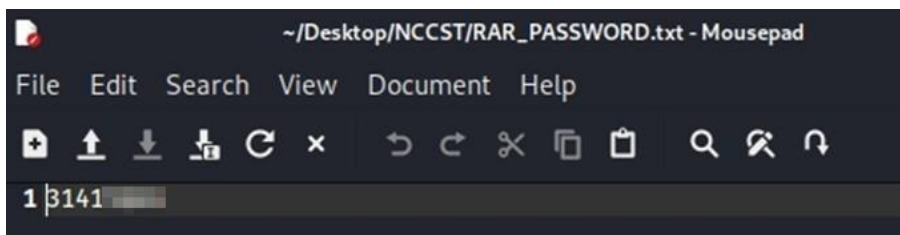


- 在 terminal

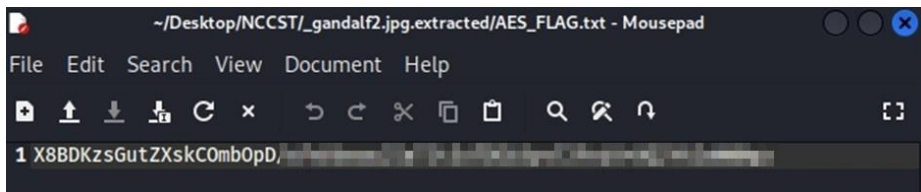
輸入：`bash bruteforce.sh gandalf2.jpg password.txt`



- 破解圖片的密碼為 27xx，並得到 RAR_PASSWORD.txt，內容為 3141xxxx



- 利用其內容解開壓縮檔 BE2E，得到 AES_FLAG 密文



補充說明

- Stexxxxx 是一種隱寫術程序，它將數據文件的位隱藏在另一個文件的某些最低有效位中，從而使數據文件的存在不可見且無法證明
- 參數介紹：extracting options
 - sf, --stegofile: 要從哪張圖提取資料
 - p, --passphrase: 用甚麼密碼去提取資料

解題步驟 5:

得到 AES_FLAG.txt 的密文後，需要 AES_KEY 與 IV 才能解開，已知每天的訊息都是用不同梗圖回傳，代表梗圖也藏了訊息，使用台詞 YOUSHALNOTPASS! 為金鑰



還愛重複利用密碼，因此把過程中的密碼重新利用，IV 為前面解出之密碼相加
27xx27xx3141xxxx，最後使用 AES 解密工具解開，得到

CSC{There_is_an_XXXXXXX, _XXXX_XXXXXXX}



The screenshot shows the 'totools.site' AES online encryption/decryption tool. The interface includes a header with the site name and a subtitle '(totools 最好用的在線工具集合)'. Below the header are navigation links: '編碼解碼', '加密解密', '哈希算法', '代碼格式化', and '語言處理'. A secondary navigation bar lists encryption methods: 'DES', 'RC4', '3DES', 'RSA', 'AES', and 'Rabbit'. The main section is titled '請輸入要進行加密或解密的數據'. The input field contains the text 'X8BDKzsGutZXskCOmbOpD'. Below the input field are settings for '模式' (CBC), '填充' (pkcs7padding), '密鑰' (YOUSHALNOTPASS!), 'iv' (27xx27xx3141), '輸出' (base64), and '字符集' (utf8). There are buttons for 'AES加密', 'AES解密', '交換', and '清空', along with a link to '各語言中的實現方法'. The '加密或解密的結果' field shows the output: 'CSC{There_is_an_XXXXXXX, _XXXX_XXXXXXX}'.

補充說明

- AES 是一種區塊加密標準(refer to <https://zh.wikipedia.org/wiki/%E9%AB%98%E7%BA%A7%E5%8A%A0%E5%AF%86%E6%A0%87%E5%87%86>)
- 線上 AES 工具 <https://totools.site/AES>