

CTF CHALLENGE: FORENSIC

By rwx4m

Deskripsi:

You are being given a task to forensic a hard drive, inside there is a zip file. can you solve this?

Analisis & penyelesaian:

Didalam file tantangan, terdapat file zip yang berisi 3 file “.bash_history, flag.zip, dan pass.txt”. Flag.zip di proteksi oleh kata sandi.

File bash_history: berisi history syntax yang dijalankan pada terminal linux

```
(gmt@gmt)-[~/../share/Trash/files/home]
$ cat bash_history
cat flag.txt
nano pass.txt
zip --password $(cat pass.txt | tr -d '\n') flag.zip flag.txt
cat pass.txt
truncate -s -2 pass.txt
cat pass.txt
rm flag.txt
history -a
```

File flag.zip: terdapat sebuah file flag.txt didalamnya yang dilindungi oleh kata sandi

```
(gmt@gmt)-[~/Downloads/home]
$ zipinfo flag.zip
Archive:  flag.zip
Zip file size: 231 bytes, number of entries: 1
-rwxr-xr-x  3.0 unx      37 TX stor 21-Apr-05 10:06 flag.txt
1 file, 37 bytes uncompressed, 37 bytes compressed:  0.0%
```

File pass.txt: berisi kata sandi yang digunakan untuk membuka file flag.zip

```
(gmt@gmt)-[~/Downloads/home]
$ cat pass.txt
5jsw75Zr2onylx631ltzy4ugah3jhlv
```

Jika diperhatikan, flag.zip sudah dipastikan memiliki file “txt” yang mempunyai isi (terlihat dari size yang ditampilkan) dan dapat disimpulkan itulah flag yang saya butuhkan. Untuk membukanya, dianalisis file bash_history yang memiliki petunjuk bahwa kata sandi dibuat sebelum pembuatan file zip(line 2). Pada line ke ketiga, terlihat bahwa pembuatan file flag.zip yang dibuat, memiliki kata sandi yang diambil dari pass.txt dan tidak mengambil baris baru (tr -d '\n') pada file tersebut. Kemudian setelah file zip berhasil dibuat, file pass.txt (yang berisi kata sandi yang benar) untuk membuka flag.zip, di hapus 2 karakter terakhir dari isi file tersebut. Yang berarti file pass.txt telah dihilangkan 2 karakter pada bagian terakhirnya.

CTF CHALLENGE: FORENSIC

By rwx4m

Proses Penyelesaian

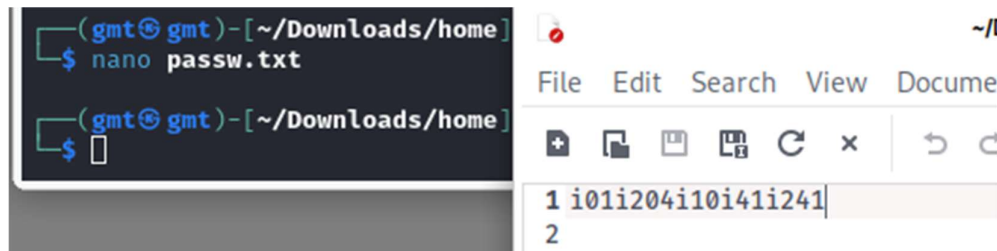
Dari 3 percobaan yang dilakukan dengan mencoba mengekstrak file "Flag.zip" menggunakan kata sandi asli dan mencoba menghapus 2 karakter terakhir ("v" dan "l"), didapati kata sandi yang saya coba dalam 3 kali percobaan, GAGAL.

```
(gmt@gmt)-[~/Downloads/home]
$ unzip -P 5jsw75zr2onylx631ltzy4ugah3jhlv flag.zip
Archive:  flag.zip
skipping:  flag.txt                                incorrect password

(gmt@gmt)-[~/Downloads/home]
$ unzip -P 5jsw75zr2onylx631ltzy4ugah3jhl flag.zip
Archive:  flag.zip
skipping:  flag.txt                                incorrect password

(gmt@gmt)-[~/Downloads/home]
$ unzip -P 5jsw75zr2onylx631ltzy4ugah3jh flag.zip
Archive:  flag.zip
skipping:  flag.txt                                incorrect password
```

Kemudian, mencoba Kembali memahami alur dan cara kerjanya. Melakukan percobaan pembuatan file baru berisi kata sandi random menggunakan **nano** dari **terminal** dan membukanya menggunakan **text editor**, maka didapati bahwa saat pembuatan kata sandi, baris baru otomatis akan ditambahkan pada baris ke 2 seperti contoh dibawah ini:



The image shows a terminal window on the left and a nano text editor on the right. In the terminal, the command `nano passw.txt` has been executed. The nano editor shows two lines of text: `1 i01i204i10i41i241` and `2`. The cursor is at the end of the second line.

Melalui uji coba ini, dapat disimpulkan bahwa saat melakukan penghapusan 2 karakter terakhir pada file `pass.txt` (`truncate -s -2 pass.txt`), baris baru (line 2) dan 1 karakter terakhir pada kata sandi, telah terhapus. Maka dipastikan kata sandi yang diperlukan hanya kurang 1 karakter saja pada bagian akhir untuk mendapatkan kata sandi yang benar dan membuka file `flag.zip` tersebut.

Percobaan saya lakukan secara manual dengan mencoba memasukan karakter terakhir dengan huruf abjad. Yang membuat saya yakin untuk dilakukan secara manual karena pada pola kata sandi, hurufnya tidak ada mengandung huruf kapital maka dipastikan semua bersifat huruf kecil atau angka.

CTF CHALLENGE: FORENSIC

By rwx4m

```
(gmt@gmt)-[~/Downloads/home]
$ unzip -P 5jsw75zr2onylx631ltzy4ugah3jhlve flag.zip
Archive:  flag.zip
  skipping: flag.txt                                incorrect password

(gmt@gmt)-[~/Downloads/home]
$ unzip -P 5jsw75zr2onylx631ltzy4ugah3jhlvf flag.zip
Archive:  flag.zip
  skipping: flag.txt                                incorrect password

(gmt@gmt)-[~/Downloads/home]
$ unzip -P 5jsw75zr2onylx631ltzy4ugah3jhlvg flag.zip
Archive:  flag.zip
  skipping: flag.txt                                incorrect password

(gmt@gmt)-[~/Downloads/home]
$ unzip -P 5jsw75zr2onylx631ltzy4ugah3jhlvh flag.zip
Archive:  flag.zip
  skipping: flag.txt                                incorrect password

(gmt@gmt)-[~/Downloads/home]
$ unzip -P 5jsw75zr2onylx631ltzy4ugah3jhlvi flag.zip
Archive:  flag.zip
  skipping: flag.txt                                incorrect password

(gmt@gmt)-[~/Downloads/home]
$ unzip -P 5jsw75zr2onylx631ltzy4ugah3jhlvj flag.zip
Archive:  flag.zip
  extracting: flag.txt

(gmt@gmt)-[~/Downloads/home]
$
```

Maka didapatkan, bagian terakhir yang hilang adalah huruf "j" untuk melengkapi kata sandi tersebut.

```
(gmt@gmt)-[~/Downloads/home]
$ cat flag.txt
flag{oh_y[REDACTED]_linux}
```

SEKIAN ^_^