



CAPTURE THE FLAG – TAKING LS

Autor: ETR00M

Github: <https://github.com/ETR00M/>

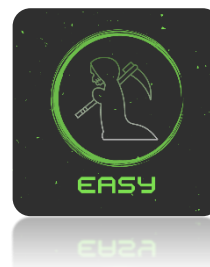
Linkedin: <https://www.linkedin.com/in/ls-anderson/>

Link da Challenge: <https://ctflearn.com/challenge/103>

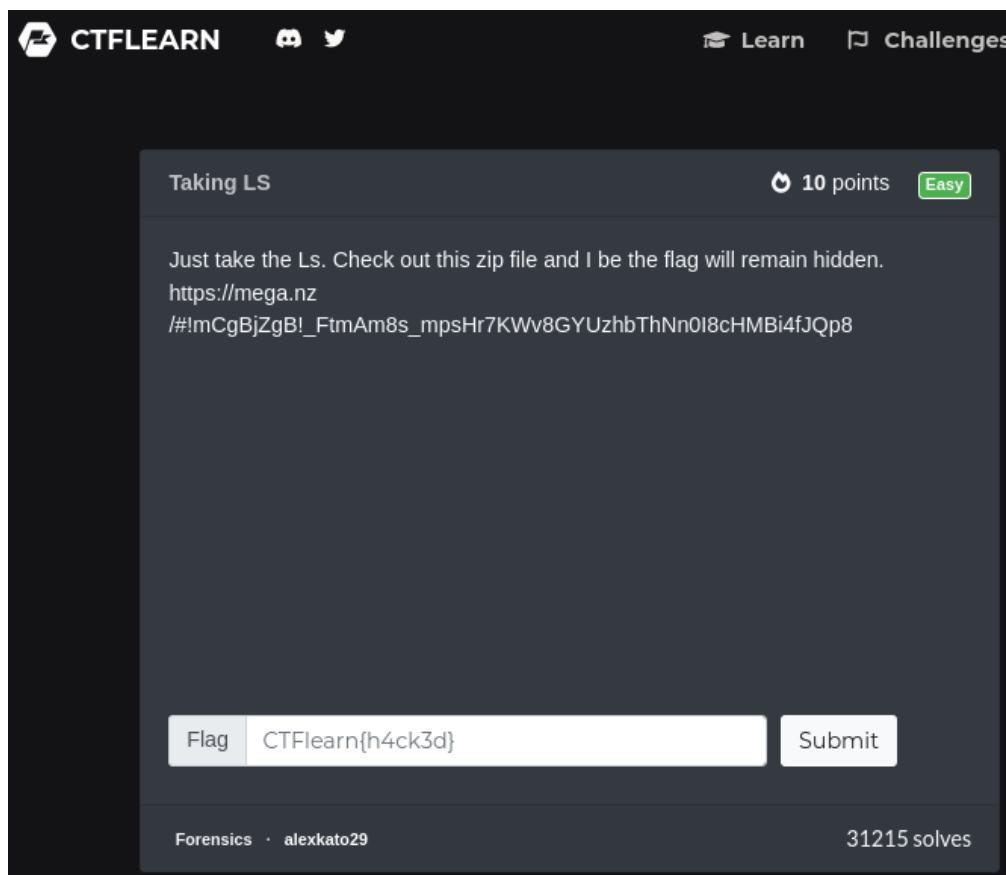
Nível: fácil;

Categoria: Forensics;

Tag: comandos Linux (ls), pensamento linear.

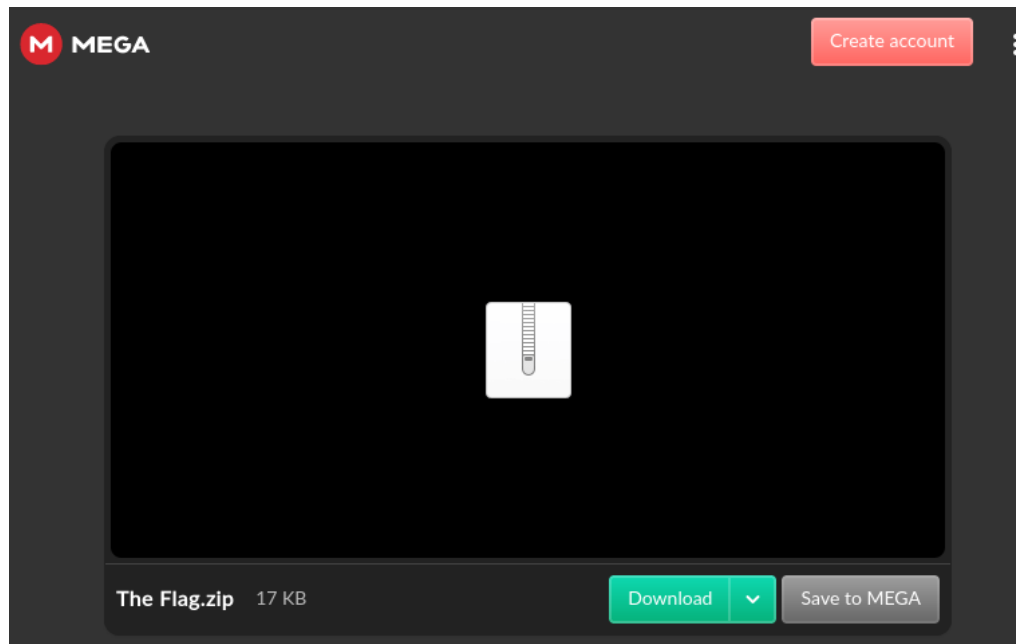


Neste desafio do **CTFLearn** precisamos localizar a *flag* escondida em diretórios e arquivos que podem ser baixados via link disponibilizado pelo autor. A partir da descrição da *challenge* nos é indicado que precisaremos conhecer o comando *ls* (*list*) para completá-lo, portanto o único conhecimento necessário é de comandos básicos de navegação em sistemas Linux.





O link de download nos leva a uma página do Mega, não é necessário criar conta para baixar o arquivo compactado “**The Flag.zip**”:



A partir deste ponto precisaremos utilizar comandos Linux básicos para navegação entre diretórios, listagem de conteúdos, manipulação de arquivos (descompactação e leitura), entre outros, caso não tenha familiaridade com essas ações recomendo o estudo desses assuntos.

Dicas de materiais para estudo:

- <https://guialinux.uniriotec.br/ls/>
- <https://guialinux.uniriotec.br/cd/>
- <https://guialinux.uniriotec.br/cat/>
- https://www.youtube.com/watch?v=ufWrWK0I2o0&ab_channel=B%C3%B3sonTreinamento
- https://www.youtube.com/watch?v=Bg4Iq3pnKj8&ab_channel=B%C3%B3sonTreinamentos
- https://www.youtube.com/watch?v=NamRiURAbmc&ab_channel=B%C3%B3sonTreinamentos

Primeiramente precisamos descompactar o arquivo para identificar seu conteúdo, como o diretório contém a extensão *.zip* utilizarei o *unzip* para descompactá-lo.



Comando: `unzip The\ Flag.zip`

```
(kali㉿kali)-[~/Downloads]
$ ls
'The Flag.zip'

(kali㉿kali)-[~/Downloads]
$ unzip The\ Flag.zip
Archive:  The Flag.zip
  creating: The Flag/
  inflating: The Flag/.DS_Store
  creating: __MACOSX/
  creating: __MACOSX/The Flag/
  inflating: __MACOSX/The Flag/._.DS_Store
  creating: The Flag/.ThePassword/
  inflating: The Flag/.ThePassword/ThePassword.txt
  inflating: The Flag/The Flag.pdf
  inflating: __MACOSX/The Flag/._The Flag.pdf

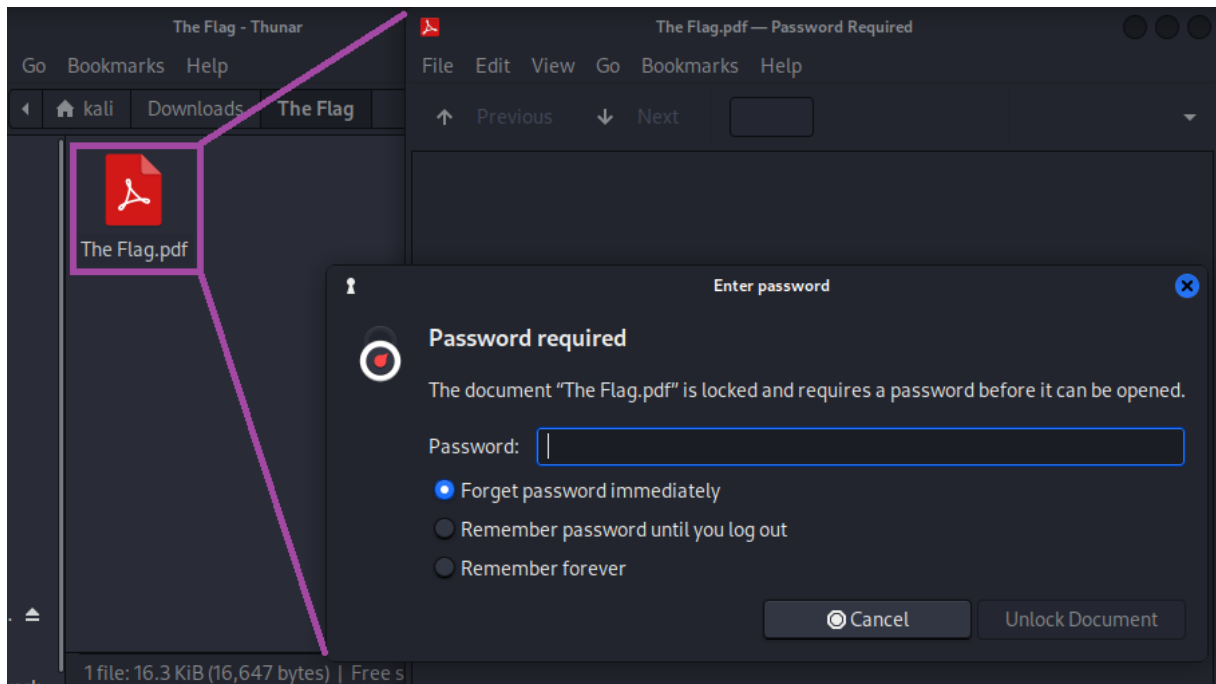
(kali㉿kali)-[~/Downloads]
$ ls -la
total 36
drwxr-xr-x  4 kali kali   4096 Feb  6 20:59 .
drwx----- 25 kali kali   4096 Feb  6 20:36 ..
drwxrwxr-x  3 kali kali   4096 Oct 30  2016 __MACOSX
drwxr-xr-x  3 kali kali   4096 Oct 30  2016 'The Flag'
-rw-r--r--  1 kali kali 17441 Feb  6 20:51 'The Flag.zip'

(kali㉿kali)-[~/Downloads]
$
```

Dentro do diretório “**The Flag**” temos um único arquivo visível nomeado como: “**The Flag.pdf**”, este arquivo possui controle de autenticação, sendo assim, quando é aberto solicita uma senha de acesso, que não temos no momento.

```
(kali㉿kali)-[~/Downloads]
$ cd The\ Flag

(kali㉿kali)-[~/Downloads/The Flag]
$ ls
'The Flag.pdf'
```



Como o objetivo deste CTF não é a quebra de senhas, e sim utilização de comandos básicos de Linux para localização da *flag*, faremos novamente a listagem de arquivos, porém desta vez, identificando arquivo ocultos, conforme abaixo:

Comando: `ls -la`

```
(kali@kali)-[~/Downloads/The Flag]
$ ls -la
total 40
drwxr-xr-x 3 kali kali 4096 Oct 30 2016 .
drwxr-xr-x 4 kali kali 4096 Feb 6 20:59 ..
-rw-r--r-- 1 kali kali 6148 Oct 30 2016 .DS_Store
-rw-r--r-- 1 kali kali 16647 Oct 30 2016 'The Flag.pdf'
drwxr-xr-x 2 kali kali 4096 Oct 30 2016 .ThePassword
```

Com isso, identificamos o arquivo “**DS_Store**” e o diretório “**ThePassword**” que estão ocultos (iniciam com “.”), como o nome do diretório “**ThePassword**” já indica que a informação que precisamos está em seu conteúdo vamos acessá-lo e coletar a senha de acesso ao *pdf*.

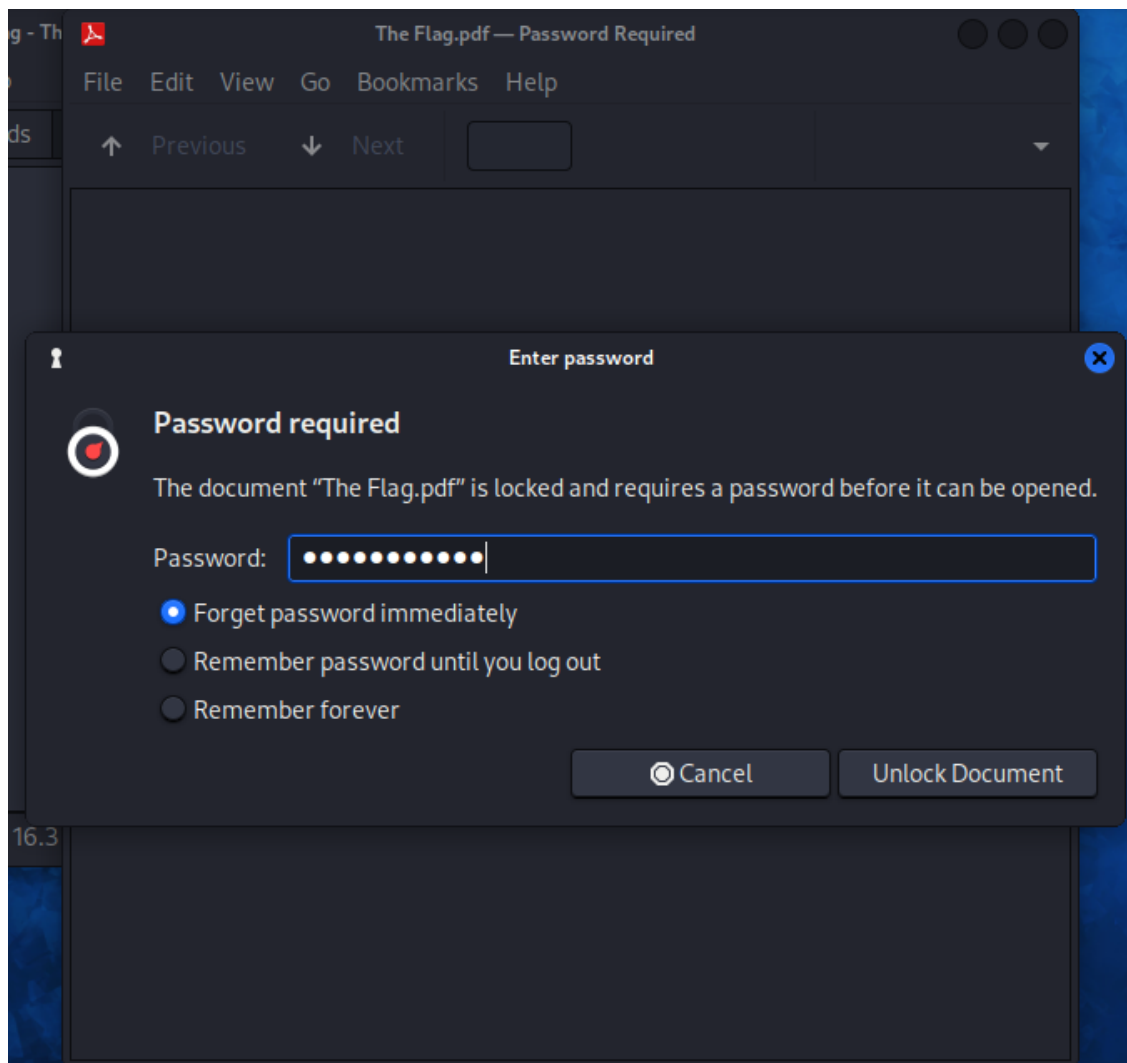


Comando: `cat ThePassword.txt`

```
(kali㉿kali)-[~/Downloads/The Flag/.ThePassword]
$ ls -la
total 12
drwxr-xr-x 2 kali kali 4096 Oct 30 2016 .
drwxr-xr-x 3 kali kali 4096 Oct 30 2016 ..
-rw-r--r-- 1 kali kali  42 Oct 30 2016 ThePassword.txt

(kali㉿kali)-[~/Downloads/The Flag/.ThePassword]
$ cat ThePassword.txt
Nice Job! The Password is "[REDACTED]".
```

Agora podemos verificar o conteúdo do arquivo *.pdf* e capturar a *flag* deste desafio.








Para concluir o desafio basta submetermos a *flag* na *challenge* correspondente na plataforma **CTFLearn**, conforme a seguir:

Here is the Flag:



 **CTFLEARN**  

Learn Challenges

Taking LS ✓ 10 points Easy

Just take the Ls. Check out this zip file and I be the flag will remain hidden.
https://mega.nz/#!/mCgBjZgB!_FtmAm8s_mpsHr7KWv8GYUzhbThNn0I8cHMBi4fJQp8

Flag

Solved

Forensics · alexkato29 31216 solves