1. descargar el pdf encriptado
2. abrimos el terminal para crear un documento .hash del pdf
3. ocupamos el metodo de fuerza bruta para poder descifrar la contraseña
4. ocupamos john … y el nombre del .hash que creamos del pdf
5. encontramos la contrasena
6. abrimos cyber chef
7. seleccionamos desencriptar AES/128
8. y lo logramos luego de descifrar bien el key y el IV (31 F y 31 A o 16 bytes en cada una)
9. finalmente nos entrego el mensaje LAB1-logrado

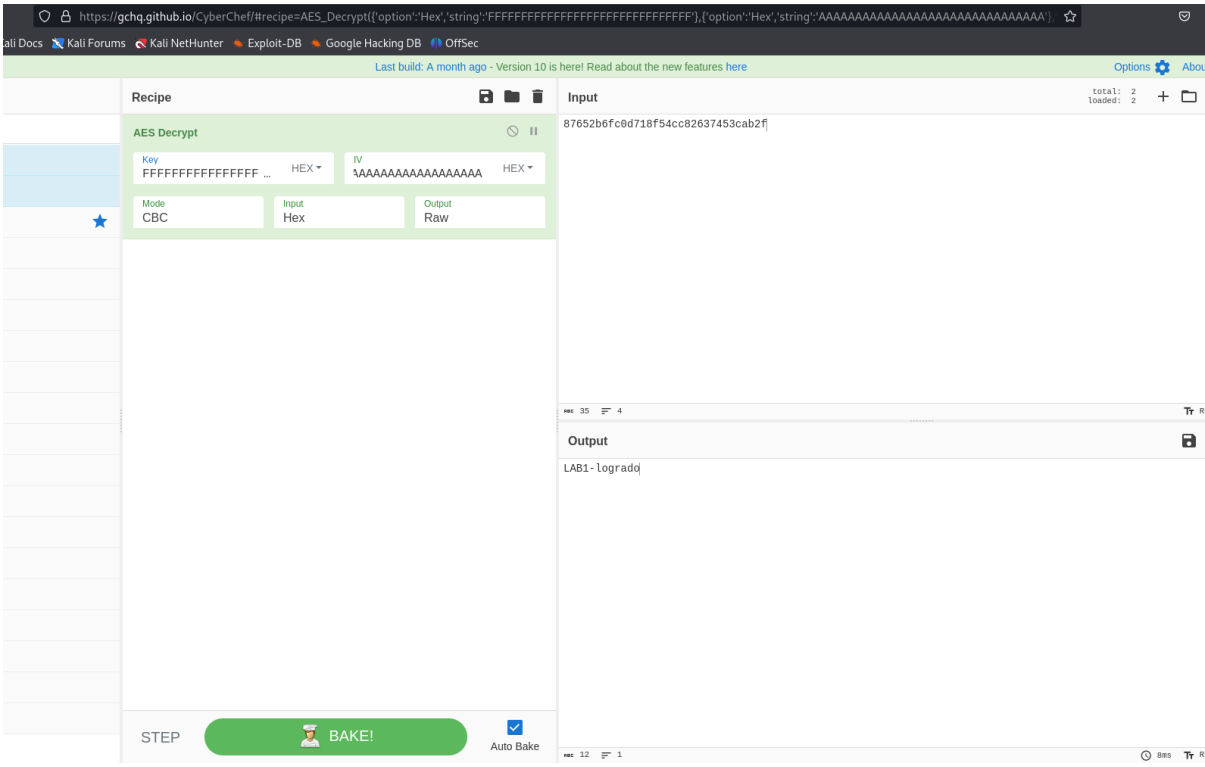
La llave es: Fs

I. Ds
II. Cs
III. Bs
IV. As
V. 9s
VI. 8s
VII. 7s

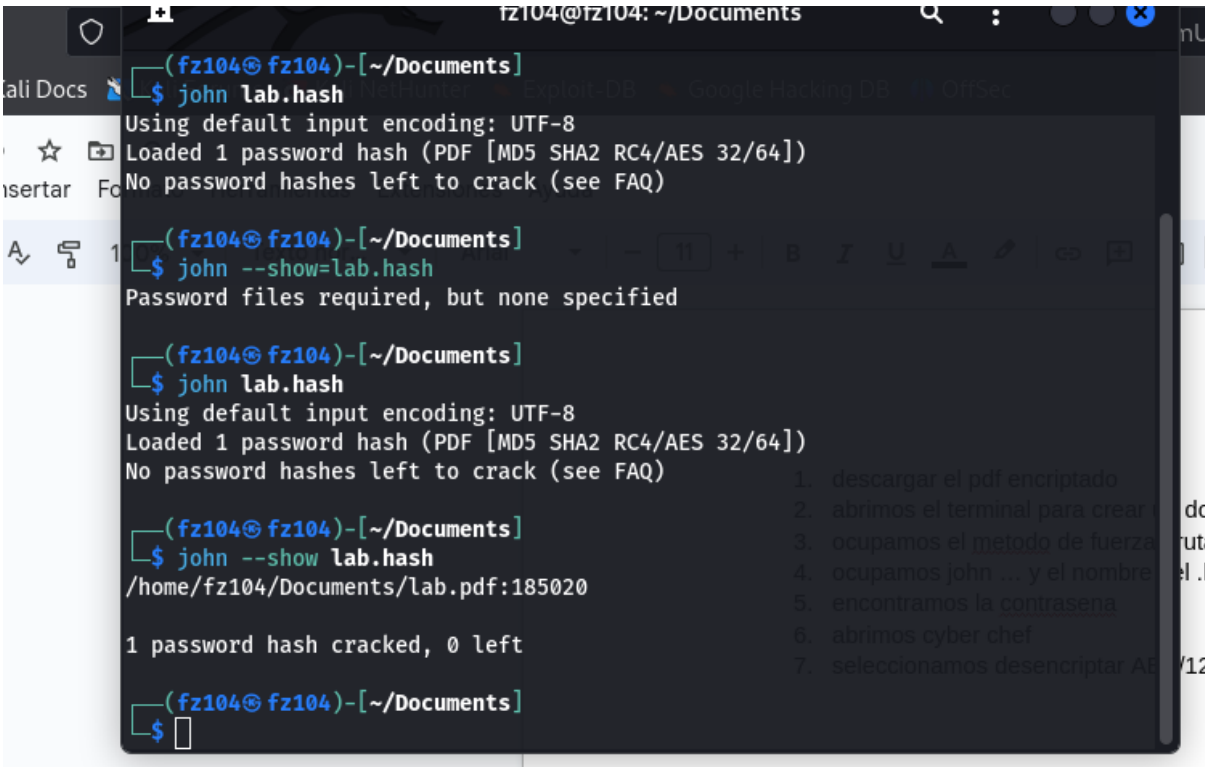
10.

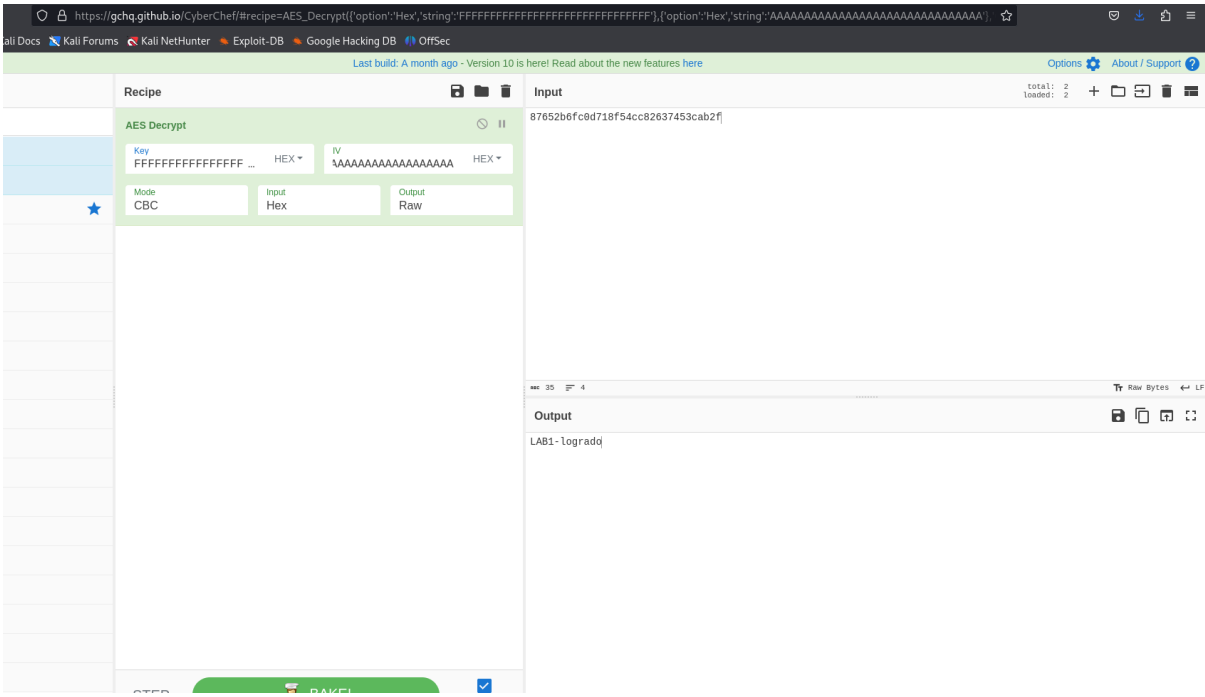
La llave es: Fs

I. Ds
II. Cs
III. Bs
IV. As
V. 9s
VI. 8s
VII. 7s


https://gchq.github.io/CyberChef/#recipe=AES_Decrypt({'option':'Hex','string':'FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF'},{'option':'Hex','string':'AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA'},
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Last build: A month ago - Version 10 is here! Read about the new features here
Options
Recipe
AES Decrypt
Key
FFFFFFFFFFFFFFFF ...
HEX
IV
AAAAAAAAAAAAAAAA
HEX
Mode
CBC
Input
Hex
Output
Raw
STEP
BAKE!
Auto Bake
Input
87652b6fc0d718f54cc82637453cab2f
Output
LAB1-logrado


fz104@fz104: ~/Documents
└─$ john lab.hash
stat: lab.hash: No such file or directory
┌──(fz104㉿fz104)-[~]
└─$ cd Documents
┌──(fz104㉿fz104)-[~/Documents]
└─$ john lab.hash
Using default input encoding: UTF-8
Loaded 1 password hash (PDF [MD5 SHA2 RC4/AES 32/64])
No password hashes left to crack (see FAQ)
┌──(fz104㉿fz104)-[~/Documents]
└─$ john --show=lab.hash
Password files required, but none specified
┌──(fz104㉿fz104)-[~/Documents]
└─$ john lab.hash
Using default input encoding: UTF-8
Loaded 1 password hash (PDF [MD5 SHA2 RC4/AES 32/64])
No password hashes left to crack (see FAQ)
┌──(fz104㉿fz104)-[~/Documents]
└─$
KALI LINUX
"the quieter you become, the more you are able to hear"


fz104@fz104: ~/Documents
(fz104㉿fz104)-[~/Documents]
$ john lab.hash
Using default input encoding: UTF-8
Loaded 1 password hash (PDF [MD5 SHA2 RC4/AES 32/64])
No password hashes left to crack (see FAQ)
(fz104㉿fz104)-[~/Documents]
$ john --show=lab.hash
Password files required, but none specified
(fz104㉿fz104)-[~/Documents]
$ john lab.hash
Using default input encoding: UTF-8
Loaded 1 password hash (PDF [MD5 SHA2 RC4/AES 32/64])
No password hashes left to crack (see FAQ)
(fz104㉿fz104)-[~/Documents]
$ john --show lab.hash
/home/fz104/Documents/lab.pdf:185020
1 password hash cracked, 0 left
(fz104㉿fz104)-[~/Documents]
$


Recipe
AES Decrypt
Key
HEX
IV
HEX
Mode
CBC
Input
Hex
Output
Raw
Input
87652b6fc0d718f54cc82637453cab2f
Output
LAB1-logrado