Laboratorio 1 – seguridad ti

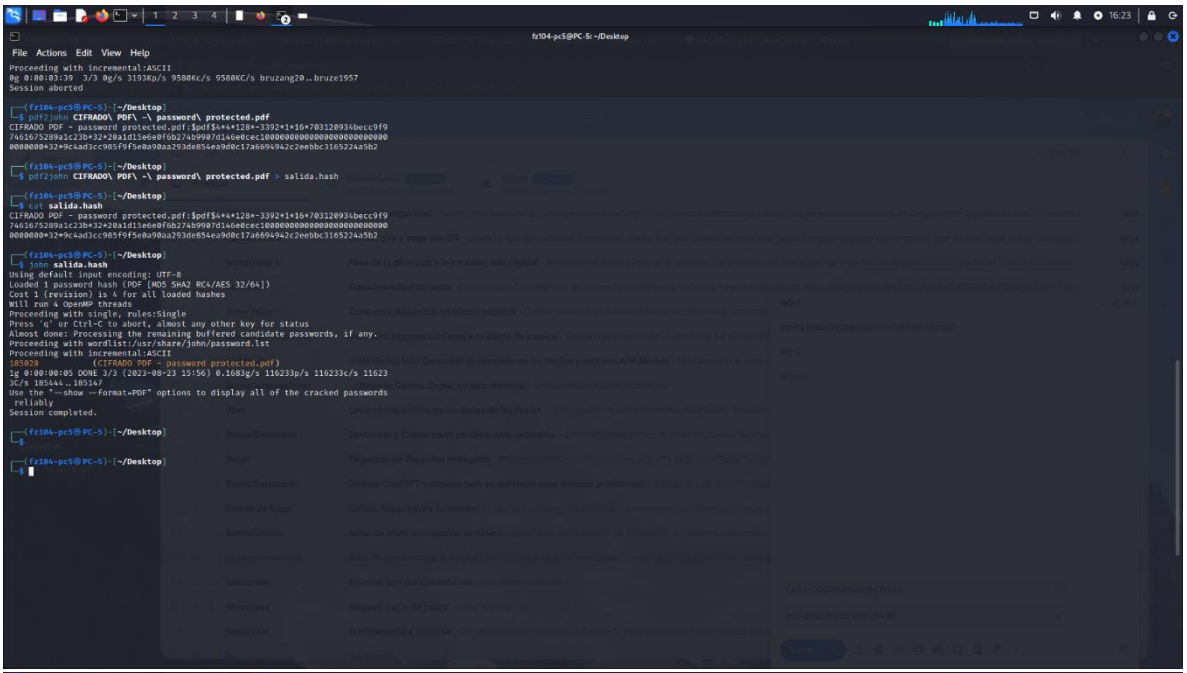
Integrantes: Diego Pandolfa, Carlos Araneda

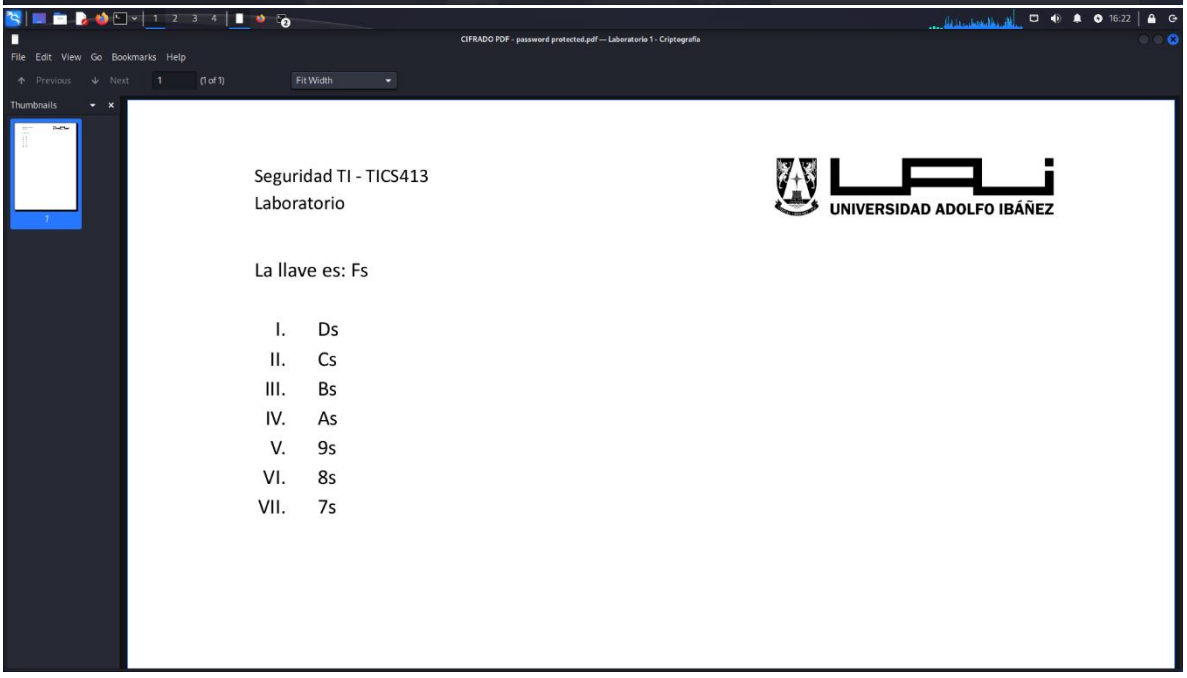
Grupo 1

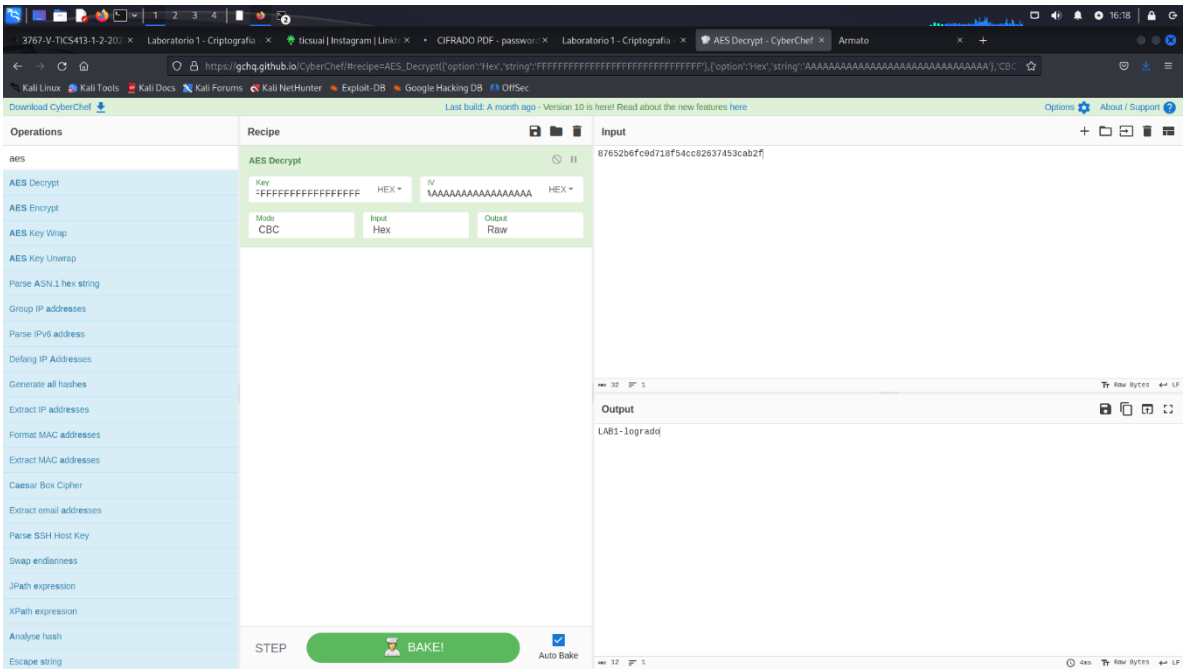
Pasos:

1. A través de la terminal y el comando cd llegamos al escritorio.
2. A través del link descargamos el pdf cifrado
3. Usando la herramienta pdf2john creamos un hash a partir del pdf cifrado
4. Usando la herramienta john sobre el hash pudimos encontrar que la contraseña era 185020
5. Insertamos esta contraseña en el pdf cifrado y logramos abrirlo
6. Luego ingresamos a cyberchef e insertamos el mensaje a desencriptar y como clave utilizamos 16 pares de F y para el parámetro IV usamos 16 pares de A, descifrando el mensaje que decía LAB1 – logrado.

A continuación se adjuntan imágenes de lo realizado.


File Actions Edit View Help
Proceeding with incremental:ASCII
0g 0:00:03:39 3/3 0g/s 3193Kp/s 9580Kc/s 9580KC/s bruzang20..bruze1957
Session aborted
(fz104-pc5㉿PC-5)-[~/Desktop]
$ pdf2john CIFRADO\ PDF\ -\ password\ protected.pdf
CIFRADO PDF - password protected.pdf:pdf4*4*128*-3392*1*16*70312093
$ pdf2john CIFRADO\ PDF\ -\ password\ protected.pdf > salida.hash
$ cat salida.hash
CIFRADO PDF - password protected.pdf:pdf4*4*128*-3392*1*16*70312093
$ john salida.hash
Using default input encoding: UTF-8
Loaded 1 password hash (PDF [MD5 SHA2 RC4/AES 32/64])
Cost 1 (revision) is 4 for all loaded hashes
Will run 4 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
Proceeding with incremental:ASCII
185929 (CIFRADO PDF - password protected.pdf)
1g 0:00:00:05 DONE 3/3 (2023-08-23 15:56) 0.1683g/s 116233p/s 116233c/s 11623
3C/s 185444..18514?
Use the "--show --format=PDF" options to display all of the cracked passwords
reliably
Session completed.


CIFRADO PDF - password protected.pdf — Laboratorio 1 - Criptografía
File Edit View Go Bookmarks Help
Previous Next 1 (1 of 1) Fit Width
Thumbnails
Seguridad TI - TICS413
Laboratorio
UNIVERSIDAD ADOLFO IBÁÑEZ
La llave es: Fs
I. Ds
II. Cs
III. Bs
IV. As
V. 9s
VI. 8s
VII. 7s


AES Decrypt - CyberChef
Armato
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Download CyberChef
Last build: A month ago - Version 10 is here! Read about the new features here
Options
About / Support
Operations
aes
AES Decrypt
AES Encrypt
AES Key Wrap
AES Key Unwrap
Parse ASN.1 hex string
Group IP addresses
Parse IPv6 address
Defang IP Addresses
Generate all hashes
Extract IP addresses
Format MAC addresses
Extract MAC addresses
Caesar Box Cipher
Extract email addresses
Parse SSH Host Key
Swap endianness
JPath expression
XPath expression
Analyse hash
Escape string
Recipe
AES Decrypt
Key
FFFFFFFFFFFFFFFF
HEX
IV
AAAAAAAAAAAAAAAA
HEX
Mode
CBC
Input
Hex
Output
Raw
STEP
BAKE!
Auto Bake
Input
87652b6fc0d718f54cc82637453cab2f
Output
LAB1-logrado