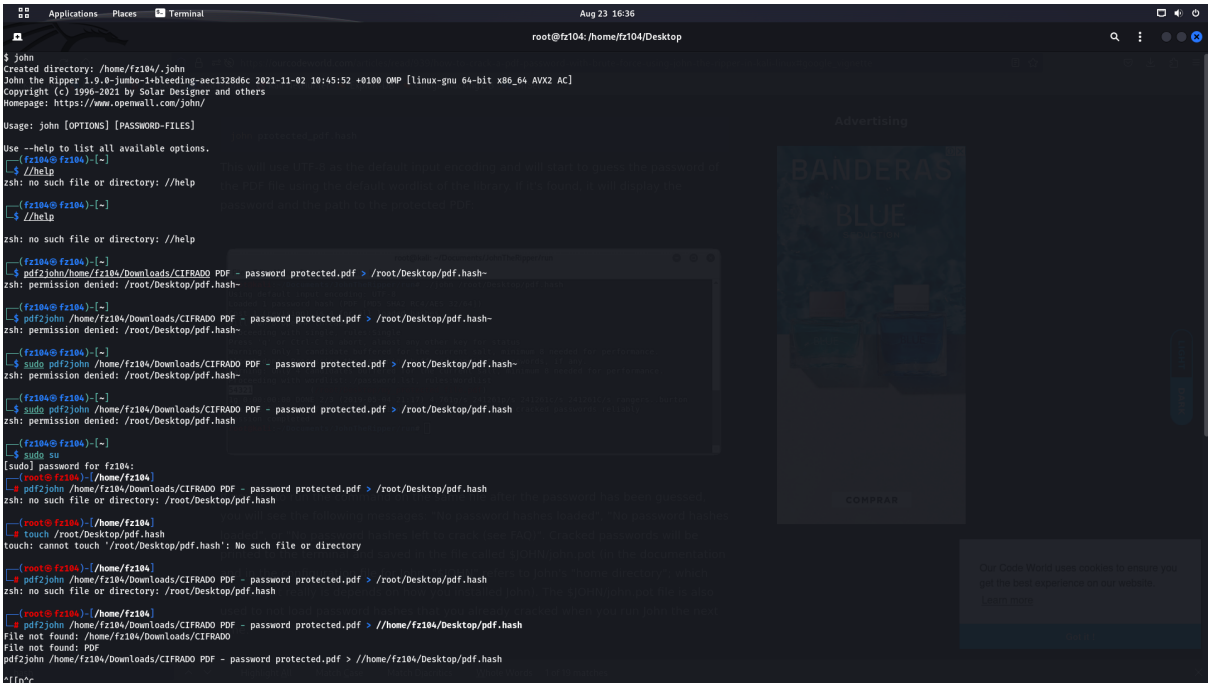
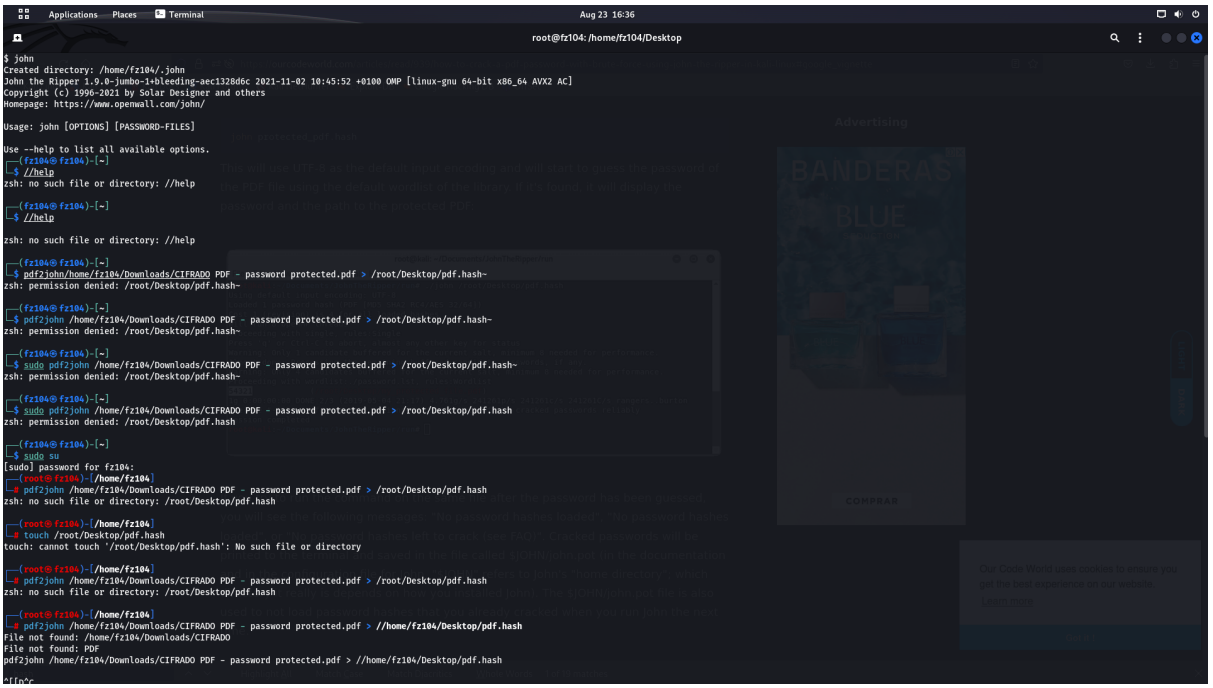
Informe Experiencia 1
Seguridad TI

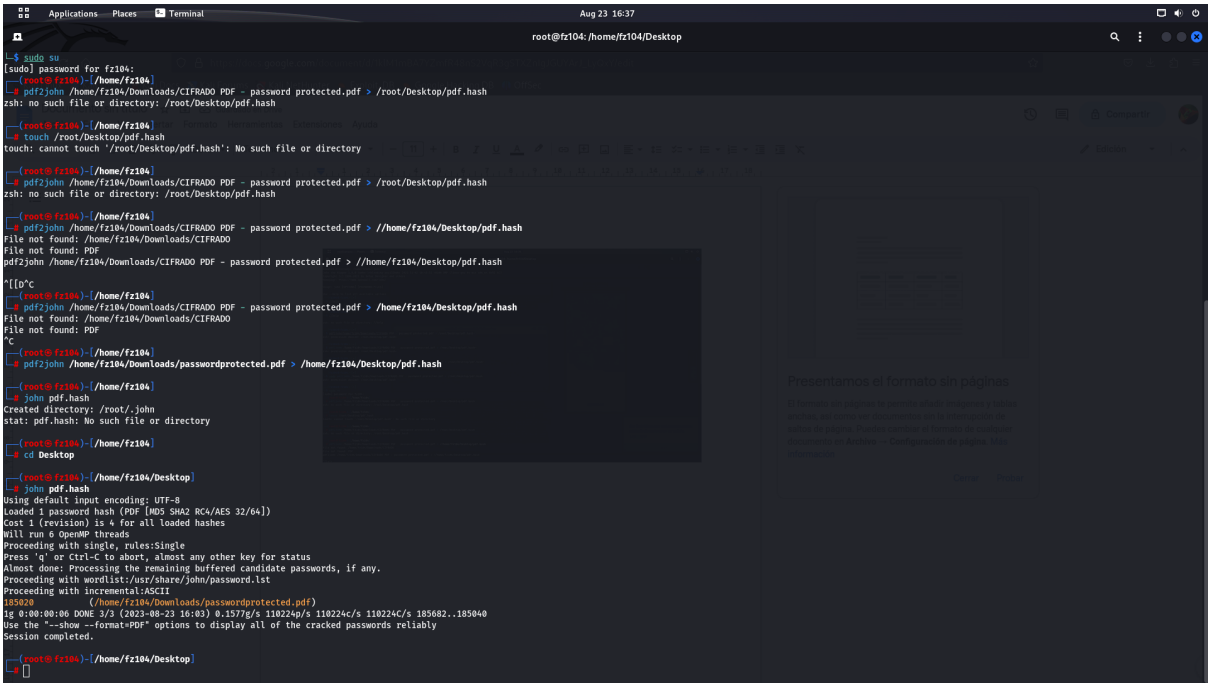
Nombres Ignacio Silva
VItelio Nunez
Grupo 6

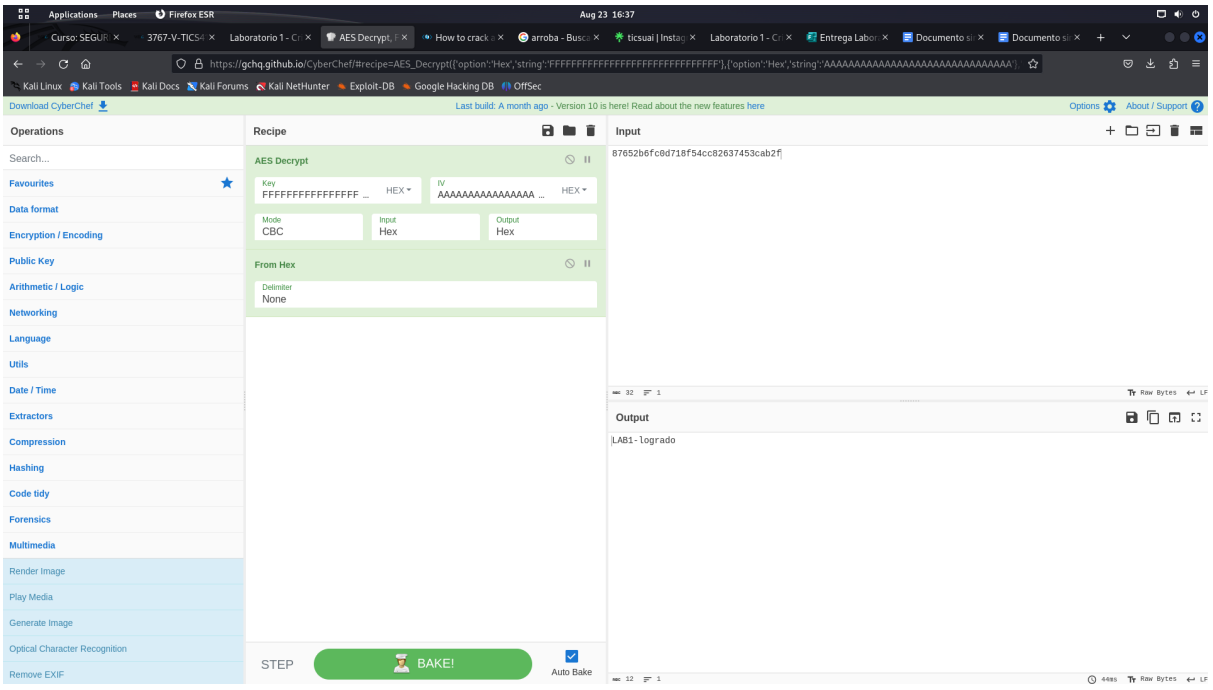
Resumen Experiencia

En la presente experiencia aprendimos a descifrar códigos encriptados mediante hash, para asi poder leer información cifrada. Luego al avanzar en la actividad logramos descifrar el mensaje oculto mediante el cifrado AES/128 arrojando el mensaje LAB1/Logrado.


Applications Places Terminal
Aug 23 16:36
root@fz104: /home/fz104/Desktop
$ john
Created directory: /home/fz104/.john
John the Ripper 1.9.0-jumbo-1+bleeding-aec1328d6c 2021-11-02 10:45:52 +0100 OMP [linux-gnu 64-bit x86_64 AVX2 AC]
Copyright (c) 1996-2021 by Solar Designer and others
Homepage: https://www.openwall.com/john/
Usage: john [OPTIONS] [PASSWORD-FILES]
Use --help to list all available options.
(fz104㉿fz104)-[~]
$ //help
zsh: no such file or directory: //help
(fz104㉿fz104)-[~]
$ //help
zsh: no such file or directory: //help
(fz104㉿fz104)-[~]
$ pdf2john/home/fz104/Downloads/CIFRADO PDF - password protected.pdf > /root/Desktop/pdf.hash~
zsh: permission denied: /root/Desktop/pdf.hash~
(fz104㉿fz104)-[~]
$ pdf2john /home/fz104/Downloads/CIFRADO PDF - password protected.pdf > /root/Desktop/pdf.hash~
zsh: permission denied: /root/Desktop/pdf.hash~
(fz104㉿fz104)-[~]
$ sudo pdf2john /home/fz104/Downloads/CIFRADO PDF - password protected.pdf > /root/Desktop/pdf.hash~
zsh: permission denied: /root/Desktop/pdf.hash~
(fz104㉿fz104)-[~]
$ sudo pdf2john /home/fz104/Downloads/CIFRADO PDF - password protected.pdf > /root/Desktop/pdf.hash
zsh: permission denied: /root/Desktop/pdf.hash
(fz104㉿fz104)-[~]
$ sudo su
[sudo] password for fz104:
(root㉿fz104)-[/home/fz104]
pdf2john /home/fz104/Downloads/CIFRADO PDF - password protected.pdf > /root/Desktop/pdf.hash
zsh: no such file or directory: /root/Desktop/pdf.hash
(root㉿fz104)-[/home/fz104]
touch /root/Desktop/pdf.hash
touch: cannot touch '/root/Desktop/pdf.hash': No such file or directory
(root㉿fz104)-[/home/fz104]
pdf2john /home/fz104/Downloads/CIFRADO PDF - password protected.pdf > /root/Desktop/pdf.hash
zsh: no such file or directory: /root/Desktop/pdf.hash
(root㉿fz104)-[/home/fz104]
pdf2john /home/fz104/Downloads/CIFRADO PDF - password protected.pdf > //home/fz104/Desktop/pdf.hash
File not found: /home/fz104/Downloads/CIFRADO
File not found: PDF
pdf2john /home/fz104/Downloads/CIFRADO PDF - password protected.pdf > //home/fz104/Desktop/pdf.hash
^[[n^c


Applications Places Terminal
Aug 23 16:36
root@fz104: /home/fz104/Desktop
$ john
Created directory: /home/fz104/.john
John the Ripper 1.9.0-jumbo-1+bleeding-aec1328d6c 2021-11-02 10:45:52 +0100 OMP [linux-gnu 64-bit x86_64 AVX2 AC]
Copyright (c) 1996-2021 by Solar Designer and others
Homepage: https://www.openwall.com/john/
Usage: john [OPTIONS] [PASSWORD-FILES]
Use --help to list all available options.
(fz104㉿fz104)-[~]
$ //help
zsh: no such file or directory: //help
(fz104㉿fz104)-[~]
$ //help
zsh: no such file or directory: //help
(fz104㉿fz104)-[~]
$ pdf2john/home/fz104/Downloads/CIFRADO PDF - password protected.pdf > /root/Desktop/pdf.hash~
zsh: permission denied: /root/Desktop/pdf.hash~
(fz104㉿fz104)-[~]
$ pdf2john /home/fz104/Downloads/CIFRADO PDF - password protected.pdf > /root/Desktop/pdf.hash~
zsh: permission denied: /root/Desktop/pdf.hash~
(fz104㉿fz104)-[~]
$ sudo pdf2john /home/fz104/Downloads/CIFRADO PDF - password protected.pdf > /root/Desktop/pdf.hash~
zsh: permission denied: /root/Desktop/pdf.hash~
(fz104㉿fz104)-[~]
$ sudo pdf2john /home/fz104/Downloads/CIFRADO PDF - password protected.pdf > /root/Desktop/pdf.hash
zsh: permission denied: /root/Desktop/pdf.hash
(fz104㉿fz104)-[~]
$ sudo su
[sudo] password for fz104:
(root㉿fz104)-[/home/fz104]
pdf2john /home/fz104/Downloads/CIFRADO PDF - password protected.pdf > /root/Desktop/pdf.hash
zsh: no such file or directory: /root/Desktop/pdf.hash
(root㉿fz104)-[/home/fz104]
touch /root/Desktop/pdf.hash
touch: cannot touch '/root/Desktop/pdf.hash': No such file or directory
(root㉿fz104)-[/home/fz104]
pdf2john /home/fz104/Downloads/CIFRADO PDF - password protected.pdf > /root/Desktop/pdf.hash
zsh: no such file or directory: /root/Desktop/pdf.hash
(root㉿fz104)-[/home/fz104]
pdf2john /home/fz104/Downloads/CIFRADO PDF - password protected.pdf > //home/fz104/Desktop/pdf.hash
File not found: /home/fz104/Downloads/CIFRADO
File not found: PDF
pdf2john /home/fz104/Downloads/CIFRADO PDF - password protected.pdf > //home/fz104/Desktop/pdf.hash
^[[n^c


Applications Places Terminal
Aug 23 16:37
root@fz104: /home/fz104/Desktop
$ sudo su
[sudo] password for fz104:
(root@fz104)-[/home/fz104]
pdf2john /home/fz104/Downloads/CIFRADO PDF - password protected.pdf > /root/Desktop/pdf.hash
zsh: no such file or directory: /root/Desktop/pdf.hash
(root@fz104)-[/home/fz104]
touch /root/Desktop/pdf.hash
touch: cannot touch '/root/Desktop/pdf.hash': No such file or directory
(root@fz104)-[/home/fz104]
pdf2john /home/fz104/Downloads/CIFRADO PDF - password protected.pdf > /root/Desktop/pdf.hash
zsh: no such file or directory: /root/Desktop/pdf.hash
(root@fz104)-[/home/fz104]
pdf2john /home/fz104/Downloads/CIFRADO PDF - password protected.pdf > //home/fz104/Desktop/pdf.hash
File not found: /home/fz104/Downloads/CIFRADO
File not found: PDF
pdf2john /home/fz104/Downloads/CIFRADO PDF - password protected.pdf > //home/fz104/Desktop/pdf.hash
^[[D^C
(root@fz104)-[/home/fz104]
pdf2john /home/fz104/Downloads/CIFRADO PDF - password protected.pdf > /home/fz104/Desktop/pdf.hash
File not found: /home/fz104/Downloads/CIFRADO
File not found: PDF
^C
(root@fz104)-[/home/fz104]
pdf2john /home/fz104/Downloads/passwordprotected.pdf > /home/fz104/Desktop/pdf.hash
(root@fz104)-[/home/fz104]
john pdf.hash
Created directory: /root/.john
stat: pdf.hash: No such file or directory
(root@fz104)-[/home/fz104]
cd Desktop
(root@fz104)-[/home/fz104/Desktop]
john pdf.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 6 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
185020 (/home/fz104/Downloads/passwordprotected.pdf)
1g 0:00:00:06 DONE 3/3 (2023-08-23 16:03) 0.1577g/s 110224p/s 110224c/s 110224C/s 185682..185040
Use the "--show --format=PDF" options to display all of the cracked passwords reliably
Session completed.
(root@fz104)-[/home/fz104/Desktop]
#


Applications Places Firefox ESR
Aug 23 16:37
Curso: SEGUR
3767-V-TICS4
Laboratorio 1 - Cr
AES Decrypt, F
How to crack
arroba - Busca
ticsuai | Instag
Laboratorio 1 - Cr
Entrega Labor
Documento si
Documento si
https://gchq.github.io/CyberChef/#recipe=AES_Decrypt({'option':'Hex','string':'FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF'},{'option':'Hex','string':'AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA'}
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
Search...
Favourites
Data format
Encryption / Encoding
Public Key
Arithmetic / Logic
Networking
Language
Utils
Date / Time
Extractors
Compression
Hashing
Code tidy
Forensics
Multimedia
Render Image
Play Media
Generate Image
Optical Character Recognition
Remove EXIF
Recipe
AES Decrypt
Key
FFFFFFFFFFFFFFFF ...
HEX
IV
AAAAAAAAAAAAAAAA ...
HEX
Mode
CBC
Input
Hex
Output
Hex
From Hex
Delimiter
None
STEP
BAKE!
Auto Bake
Input
87652b6fc0d718f54cc82637453cab2f
32 1
Raw Bytes LF
Output
LAB1-logrado
12 1
46ms
Raw Bytes LF