INPT

CIT

OSINT & STEGANOGRAPHY

MADE BY:

FATIMA EZZAHRA ACHAIT

MOHAMMED KHALDOUNE

PLAN

1. WHATIS OSINT
2. SOME OSINT METHODS
3. GOOGLE DORKS
4. GOOGLE HACKING DATABASE
5. GATHERING INFO
6. OHSINT-CHALLENGES
7. WHATIS STEGANOGRAPHY
8. STEGO-IMAGES
9. STEGO-AUDIOS
10. DEMO : EMBEDDING & EXTRACTION
11. STEGO-CHALLENGES

WHAT IS OSINT?

OSINT = Open Source INTelligence

Definition:

methodologies consist of finding, collecting, and analyzing data from publicly available information

SOME OSINT METHODS

- Google Dorking - Google Hacking Database

- Getting info starting from account name, e-mail address, IP address or domain name

- Getting info starting from image

GOOGLE DORKS

advanced search techniques

+

specialized search engine parameters

discover confidential information

GOOGLE DORKS

- filetype/ext	filetype:pdf
- site	site:"www.google.com"
- intext	intext:"keyword"
- intitle	intitle:"keyword"

Google Dorks Cheat Sheet :

GOOGLE HACKING-DATA3ASE

GATHERING INFO

- Search using Google Dorks

- HaveIbeenPwned: https://haveibeenpwned.com/

- theHarvester, recon-ng

- WayBack Machine

- Page Source Code

GATHERING INFO FROM IMAGE

|Reverse Image Search
|---> Google Image Search: 🔗
|---> Yandex Image Search: 🔗

|ExifTool

CHALLENGE-1

From where this shipment is taking off from ?

CHALLENGE-2

What information can you possibly get with just one photo?

- What is this user's avatar?
- What city is this person in?
- What is his personal email address?
- What site did you find his email address on?
- Where has he gone on holiday?
- What is this person's password?

WHAT IS STEGANOGRAPHY?

STEGANOGRAPHY IS THE PRACTICE OF HIDING A SECRET MESSAGE INSIDE OF (OR EVEN ON TOP OF) SOMETHING THAT IS NOT SECRET.

Note : It’s not a form of cryptography

STRINGS

Want to see the text inside a binary or data file? The Linux strings command pulls those bits of text—called “strings”—out for you.

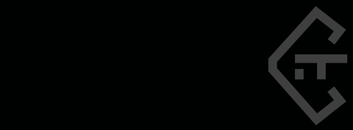
```
--$ strings software.exe

--$ strings -n 2 software.exe                    : use two as the minimum length

--$ strings  download.bin | less
```

BINWALK

binwalk - tool for searching binary images for embedded files and executable code

```
--$ sudo apt install binwalk                    :  install binwalk
--$ binwalk [path/to/binary]                    :  Scan a binary file
--$ binwalk -e software.exe                     : to extract those embedded files
--$ binwalk --dd='.*' [path/to/binary]          : Extract all the files from the binary
```

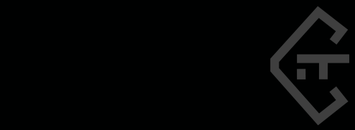
Note : binwalk accepts all file types as arguments



STEGO-IMAGES

Tools to get hidden data in images:

```
--$ exiftool image.png

--$ steghide extract -sf picture.jpg          : [JPEG, BMP, WAV, AU]
--$ steghide info received_file.wav

--$ zsteg image.png                           : [PNG, BMP]

--$ stegcracker  file  [wordlist.txt]

--$ stegoveritas  file
```



STEGO-AUDIOS

Tools to get hidden data in audios:

--$ spectrum analyser https://academo.org/demos/spectrum-analyzer/

--$ Sonic Visualizer

DEMO : EMBEDDING & EXTRACTION

EMBEDDING & EXTRACTION USING :

- EXIFTOOL
- STEGHIDE
- STEGCRACKER

CHALLENG-3

Get The Flag, Maybe you will need glasses for this one !!

CHALLENG-4

Let's do the final Exam and find the three keys !!

ANY QUESTIONS ?