PLAYING WITH BINARY FORMATS

TIPS, TRICKS AND STEGANOGRAPHY USES

-

Arnau Gàmez i Montolio | @arnaugamez

AGENDA

- About
- Preliminars
- Basics
- Common formats
- Playing with it
- Useful tools
- To know more
- Questions

ABOUT

WHO AM I

Arnau Gàmez i Montolio | @arnaugamez

- 20yo. Maths & CS student @ UB
- President of Hacking Lliure
- Worked as software dev in research groups @ UB
- Many CONs (mainly infosec)
- Also interested in music (pianist), rubik's cube(s)...

PRELIMINARS

QUICK POLL

-

How many of you know what steganography is?

How many of you have tried stego challenges before?

CONSIDERATIONS

- Introductory (quick) talk
- Steganography motivation
- Hands-on approach
- Few slides. Many demo

SCOPE

- Few common formats visited
- From general concepts to concrete examples
- Manual craft of files to get dirty
- r2 included ;)

BASICS

BINARY FILE

- **Definition:** Computer file that is not a text file
- Sequence of bytes
- Compiled computer programs
- Images, sounds, compressed files

FILE FORMAT

- Standard way that information is encoded
- **Interpretation:** Headers & metadata
- **Identifcation:** Signature or magic number
- ELF, PE, MACH-O
- JFIF, PNG, ZIP, WAV, MP3, PDF

STEGANOGRAPHY

- Concealing a file/message within another file/message
- != Security by obscurity
- Advantage over only cryptography: does not attract attention
- Media files are ideal for stego transmisson due to their large size

COMMON FORMATS

JPG

PNG

ZIP

PLAYING WITH IT

(DEMO)

USEFUL TOOLS

GENERAL

- radare2
- file
- binwalk
- exiftool
- strings/rabin2
- steghide

IMAGE FILES

- Stegsolve
- Steganabara
- Gimp
- compare (ImageMagick)

AUDIO FILES

- Audacity
- Sonic visualizer

TO KNOW MORE

BINARY FORMATS RESOURCES

- https://github.com/corkami/pics (priceless)
- Check the PoC || GTFO articles on binary formats
- Just follow @angealbertini and all his amazing work

STEGO RESOURCES

- https://github.com/apsdehal/awesome-ctf (check stego sections)
- https://hackthebox.eu challenges (really funny)

QUESTIONS?

THANK YOU!

-

Mail: arnau *[at]* hackinglliure *[dot]* org

Twitter: @arnaugamez | @HackingLliure