Workshop
Introduction to RE and Stego using r2

HackDay UdG

Associació Hacking Lliure

2 de desembre de 2017

About us

Hacking Lliure (@HackingLliure)

- Associació de Hacking Ètic i Seguretat Informàtica
- Started late 2016
- UB & Catalunya
- Official presentation February 2017
- We’ve had workshops and talks in WLAN security, passwords, RE, IoT…

About us

Enric Florit (@enricflorit)

- Maths + Info at UB
- Co-Founder of Hacking Lliure
- Co-CTO at skibeta.com
- enric@hackinglliure.org

Arnau Gàmez (@arnaugamez)

- Maths + Info at UB
- President and Co-Founder of Hacking Lliure
- Former PhD research assistant at Physics UB
- arnau@hackinglliure.org

Reverse Engineering

“Reverse engineering is the processes of extracting knowledge or design information from anything man-made and reproducing it or reproducing anything based on the extracted information. The process often involves disassembling something and analyzing its components and workings in detail.”

Radare2

What is r2?

- Reverse Engineering Framework
- Free and OpenSource
- Perfect for beginners & pro’s

Radare2

We can use r2 to. . .

- Analyze code
- Disassembly
- Low level debugging
- Forensics

Radare2

Radare has A LOT of tools. We will use some of them:

- **radare2**
- **rahash2** Block based hashing utility
- **rabin2** Binary program info extractor
- **rax2** Radare base converter
- **r2pm** Radare2 package manager

Reverse Engineering

What are we going to do?

- Read some assembly code to discover what a program does
- Extract strings and information from a binary file
- Modify binary files to change their behavior

Reverse Engineering

Materials

- IOLI Crackmes: https://dustri.org/b/files/IOLI-crackme.tar.gz
- Assembly cheatsheet: http://www.jegerlehner.ch/intel/
- Radare2: https://github.com/radare/radare2

Demo

Steganography

“Steganography is the practice of concealing a file, message, image, or video within another file, message, image, or video.”

Demo

(Super) Demo

Conclusions

- You don't need to be a radare2 master to do reverse engineering
- There are always FLOSS alternatives

Thank you

Q&A

https://hackinglliure.org

Twitter **@HackingLliure**

info@hackinglliure.org