0xFF

Flipping bits for fun

#TALK

Subject: CTF

2019-04-11

Speaker: Calle, Head of Security at Kry

What is CTF?

An introduction to competitive hacking

Carl Svensson @ 0xFF April 2019

Agenda - What are we going to talk about?

- Biography
- Capture the Flag - Basics
  - Categories
- Jeopardy style
- Attack/Defense
- Demo - Examples
- Resources

Biography - Who am I? What am I doing here?

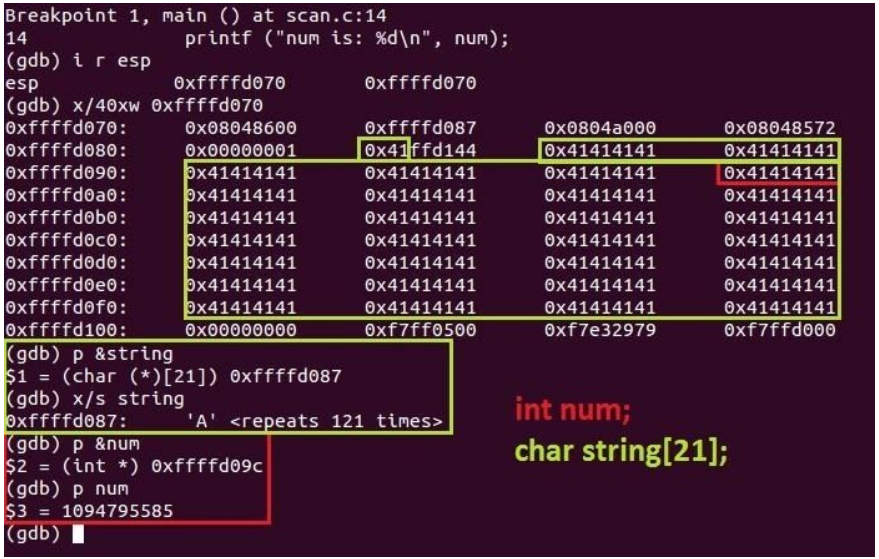
- Carl Svensson, 27
- MSc in Computer Science, KTH
- Previously: Consultant @ Bitsec
- Currently: Head of Security @ KRY/LIVI
- CTF team: HackingForSoju (world #12)
- Contact:
  - E-mail: calle.svensson@zeta-two.com
  - Twitter: @zetatwo
  - Website: https://zeta-two.com
  - YouTube: https://youtube.com/ZetaTwo

Capture the Flag - Competitive hacking

- Security challenges
- Categories
  - Pwn
  - RE
  - Web
  - Crypto
  - Forensics
  - Misc
- Individual or in teams
- Online or offline
- Time constrained (CTF) or long running (Wargame)

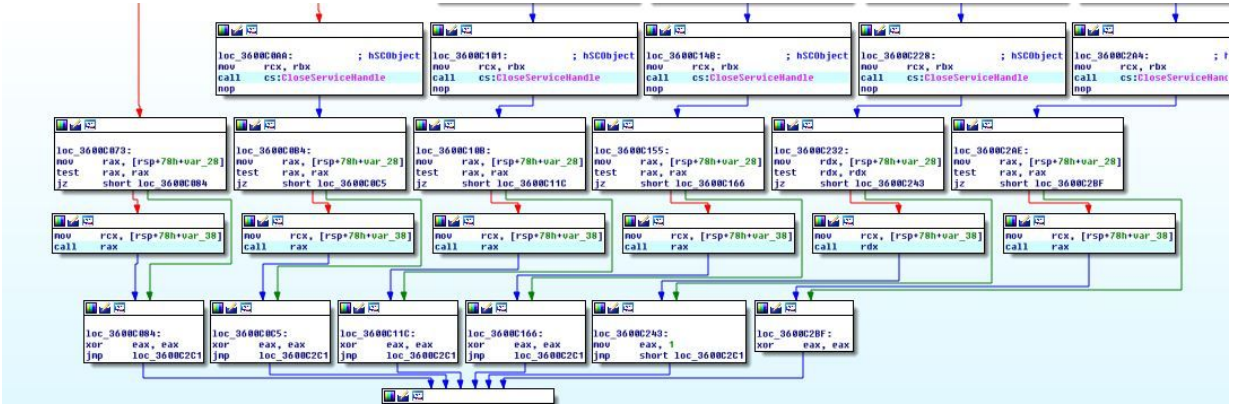
Category: Pwnable

- Exploit programs
- Set-up
  - Remote
  - Local
- Contexts
  - Machine code: x86, ARM, MIPS, etc.
  - Userland vs Kernel
  - Higher level: Java, Python, etc.
- Tools
  - IDA, Binja, Ghidra, radare2
  - GDB, pwndbg, windbg, qemu
  - Python, lots and lots of Python



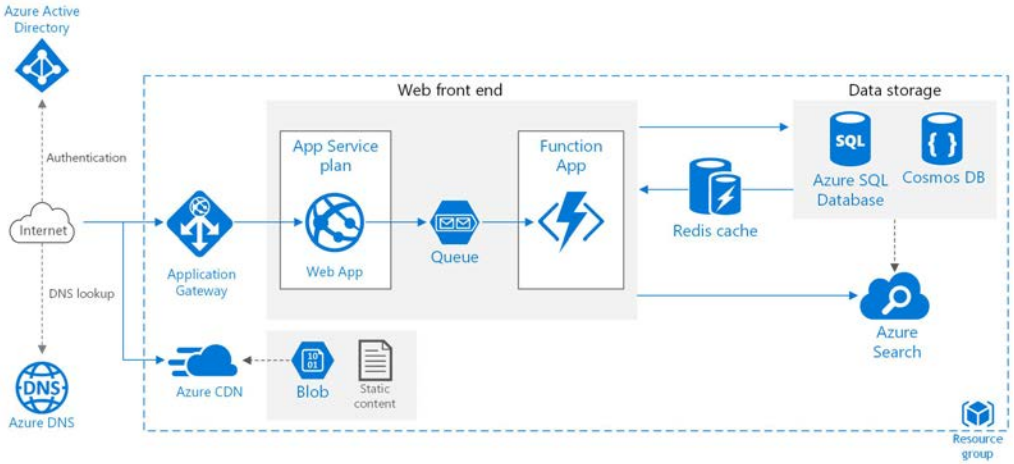
Category: Reverse engineering

- Understand
  - Software
  - Hardware
  - Protocols
- Setups
  - Crackme
  - Packers
  - Encryption
- Tools
  - IDA, Binja, Ghidra, radare2
  - GDB, pwndbg, windbg, qemu
  - Python, lots and lots of Python



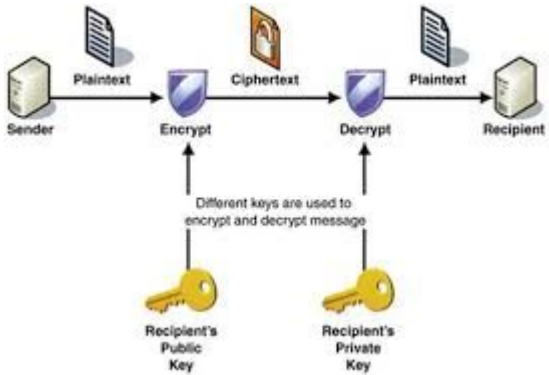
Category: Web

- Server side
  - PHP, Python, Java
  - Injections - SQL, CMD, Template
  - Deserialization, XXE
  - SSRF
- Client side
  - XSS
  - CSRF
- Context
  - Flag in file, DB, other
- Tools
  - Burp Suite, sqlmap
  - Python, lots and lots of Python



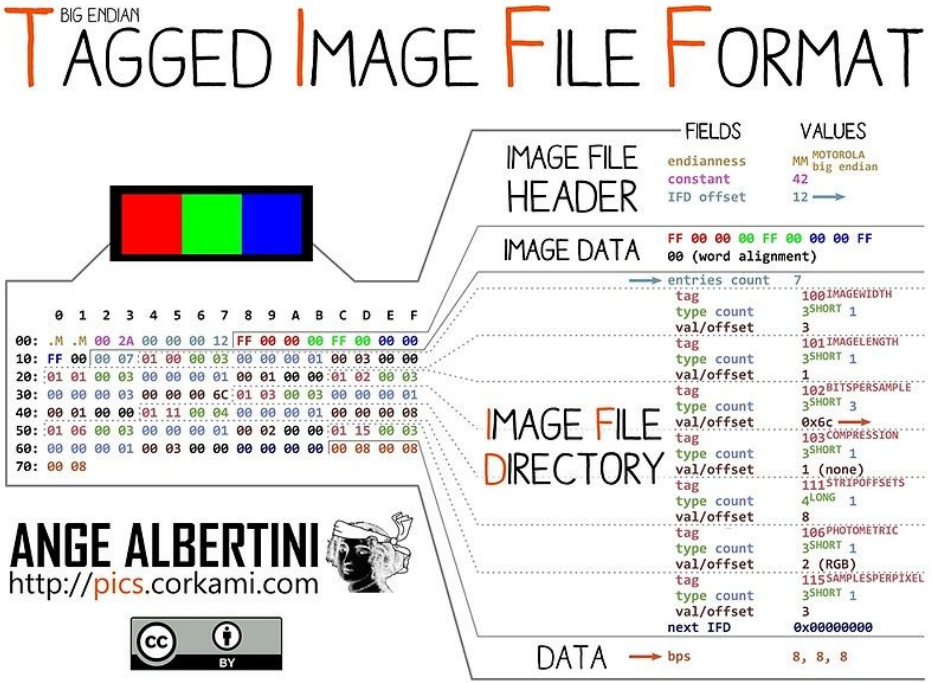
Category: Cryptography

- Break encryption
  - Recover key
  - Recover message
  - Forge signature
- Scenarios
  - Custom schemes
  - Academic attacks
- Tools
  - Academic papers, blogs
  - SageMath
  - Python, lots and lots of Python



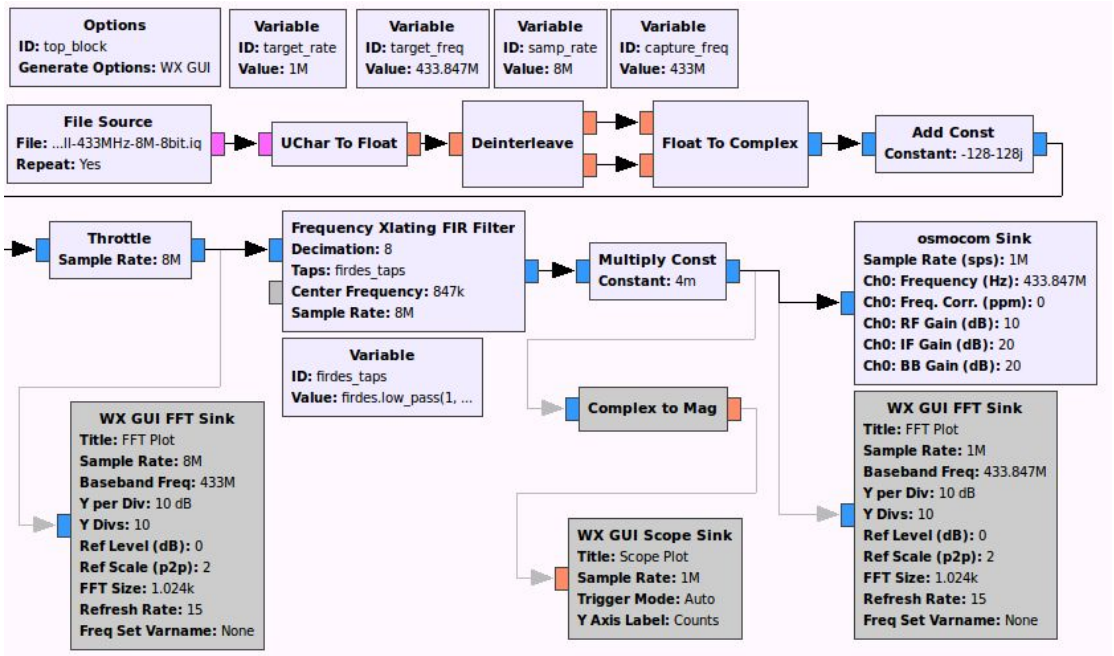
Category: Forensics

- Recover lost/hidden data
  - File systems
  - Network traffic
  - File formats
- Tools
  - Foremost, Sleuth Kit
  - Wireshark
  - binwalk, 010 Editor



Category: Miscellaneous

- DSP
- Machine learning
- Smart contracts
- Programming



Category: Zajebiste

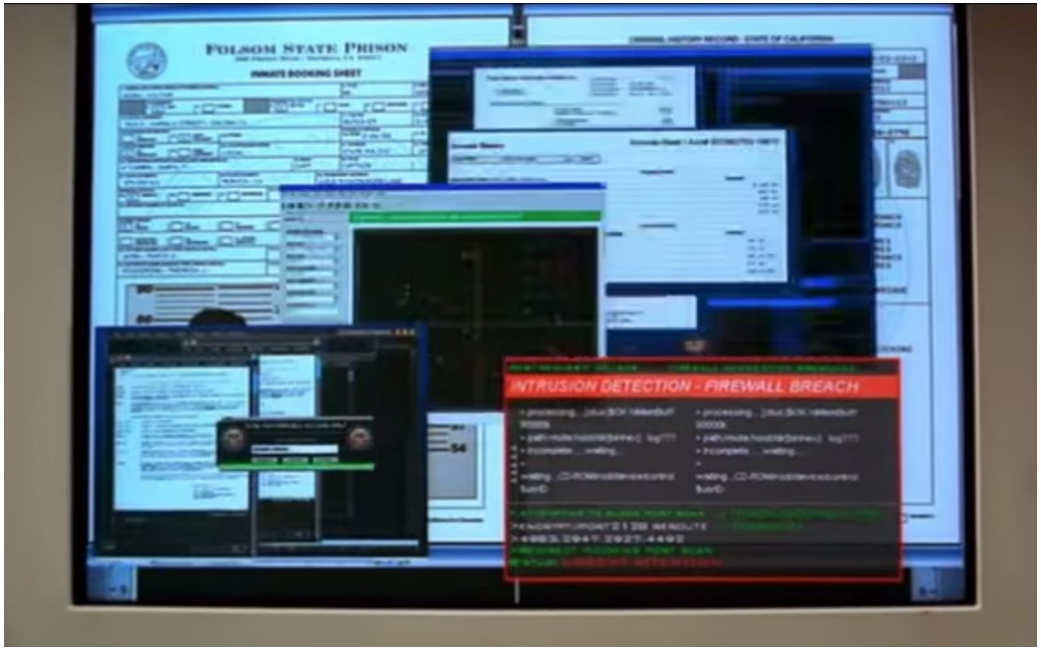
- Polish: “Awesome”
- CTF: 0-day
- Previously unknown
- Typically difficult

Jeopardy Style - The standard format

- Pick a challenge
- Solve it
- Submit flag
- Get score
- Repeat
- Most points win

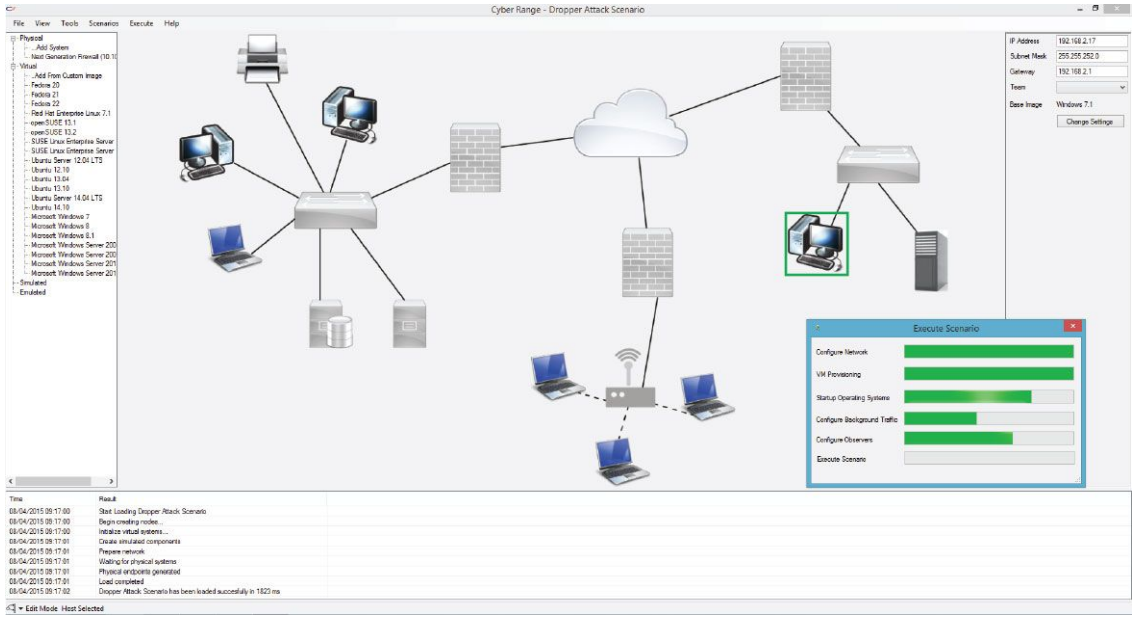
Attack/Defense - The intense classic

- One setup per team
- Find vulnerabilities
  - Patch your own
  - Exploit the others
- Keep services running
  - Checker
- Deflect attacks
- Tools, tools, tools
- Movie like



Other formats - Quests/scenarios

- Simulated attacks
- Whole networks
- Not challenge based
- Emulating “real world”
- Very rare



So what’s the purpose of all this?

- Educational
  - Improve within your area
  - Discovers completely new areas
- Competitive
- Fun
- Social

Example 1 - PicoCTF 2018
Irish Name Repo

Example 2 - Säkerhets-SM - BiffCrypt

Example 3 - Midnight Sun CTF HFS-VM2

Convinced? Great! Where do you start?

- PicoCTF.com - Beginner friendly
- CTFTime.org - Calendar and rankings
- OWASP Juice shop - Web CTF in a box
- pwnable.kr - Pwnables
- OverTheWire.org - Mix with focus on pwn

Thanks for listening - Now go hack!