

0xFF

Flipping bits for fun

#TALK

Subject: CTF

2019-04-11

Speaker: Calle, Head of Security at Kry

Presentation

45min

Discussion

15min

What is CTF?

An introduction to competitive hacking

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

```
Breakpoint 1, main () at scan.c:14
14      printf ("num is: %d\n", num);
(gdb) i r esp
esp      0xffffd070      0xffffd070
(gdb) x/40xw 0xffffd070
0xffffd070:  0x08048600      0xffffd087      0x0804a000      0x08048572
0xffffd080:  0x00000001      0x41fffd144      0x41414141      0x41414141
0xffffd090:  0x41414141      0x41414141      0x41414141      0x41414141
0xffffd0a0:  0x41414141      0x41414141      0x41414141      0x41414141
0xffffd0b0:  0x41414141      0x41414141      0x41414141      0x41414141
0xffffd0c0:  0x41414141      0x41414141      0x41414141      0x41414141
0xffffd0d0:  0x41414141      0x41414141      0x41414141      0x41414141
0xffffd0e0:  0x41414141      0x41414141      0x41414141      0x41414141
0xffffd0f0:  0x41414141      0x41414141      0x41414141      0x41414141
0xffffd100:  0x00000000      0xf7ff0500      0xf7e32979      0xf7ff0000
(gdb) p &string
$1 = (char (*)[21]) 0xffffd087
(gdb) x/s string
0xffffd087:  'A' <repeats 121 times>
(gdb) p &num
$2 = (int *) 0xffffd09c
(gdb) p num
$3 = 1094795585
(gdb) █
```

int num;
char string[21];

Category: Reverse engineering

- Understand

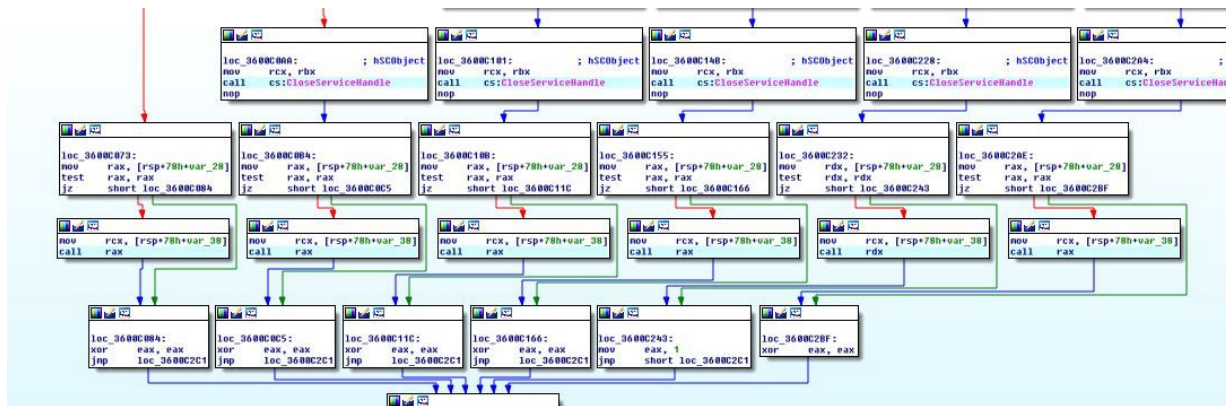
- Software
- Hardware
- Protocols

- Setups

- Crackme
- Packers
- Encryption

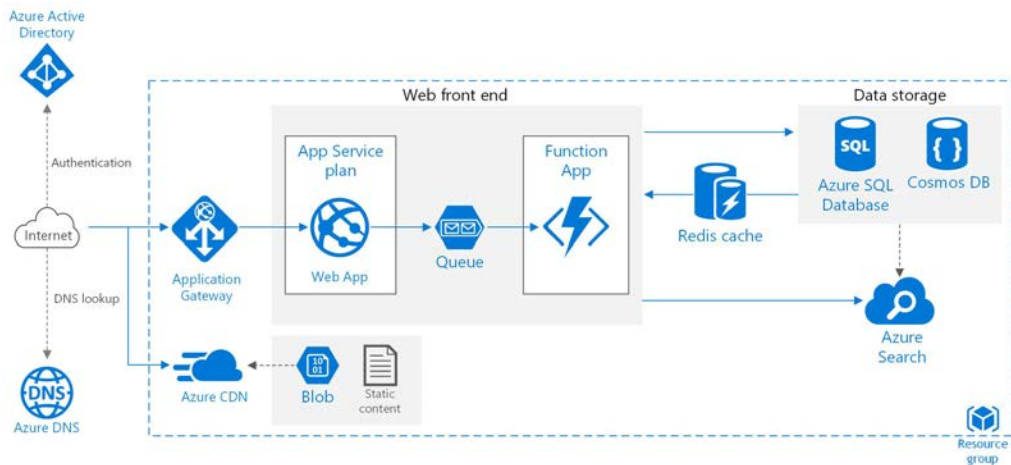
- Tools

- IDA, Binja, Ghidra, radare2
- GDB, pwndbg, windbg, qemu
- Python, lots and lots of Python



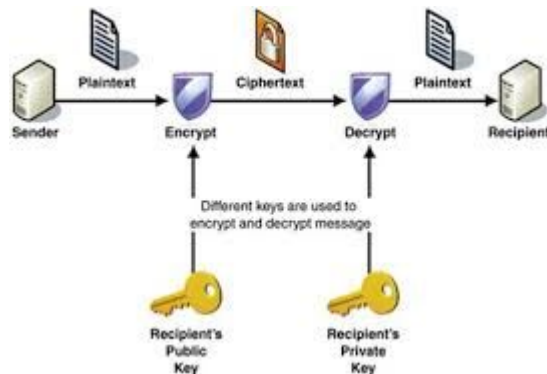
Category: Web

- 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



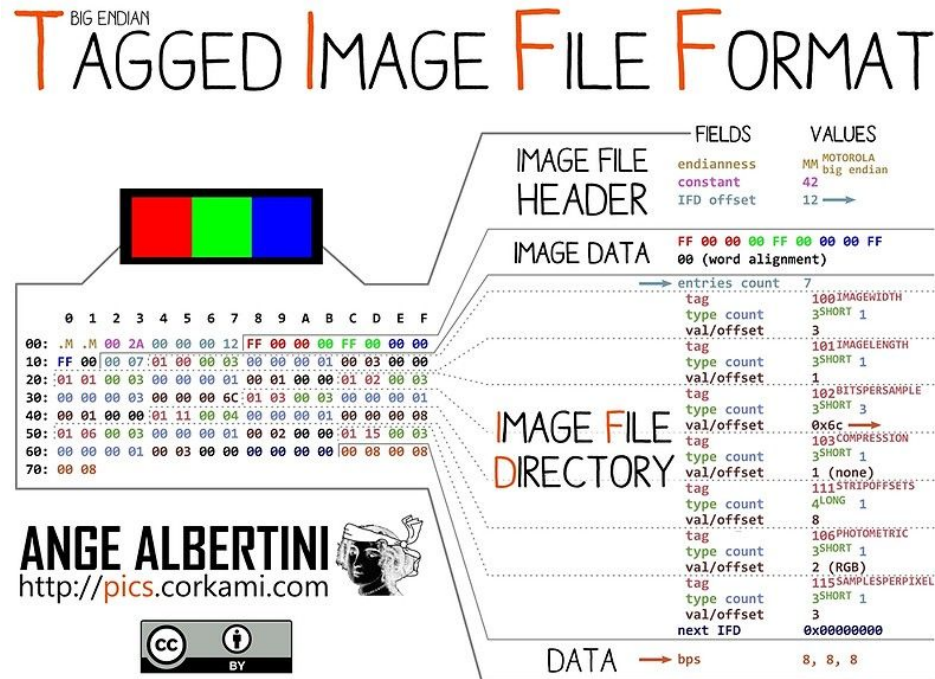
Category: Cryptography

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



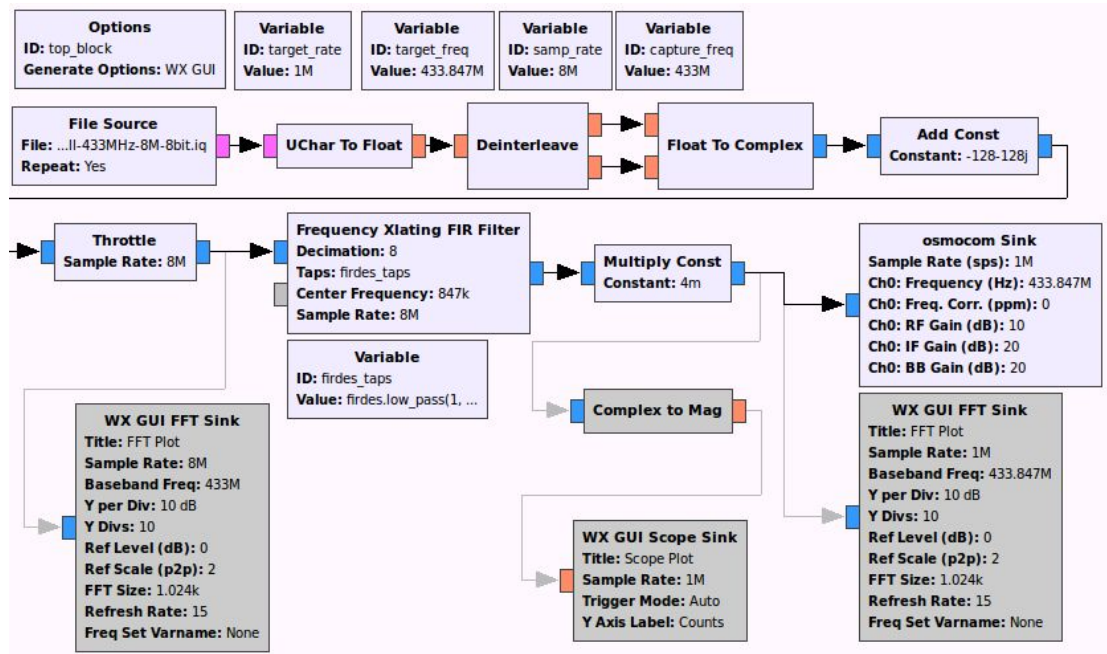
Category: Forensics

- 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



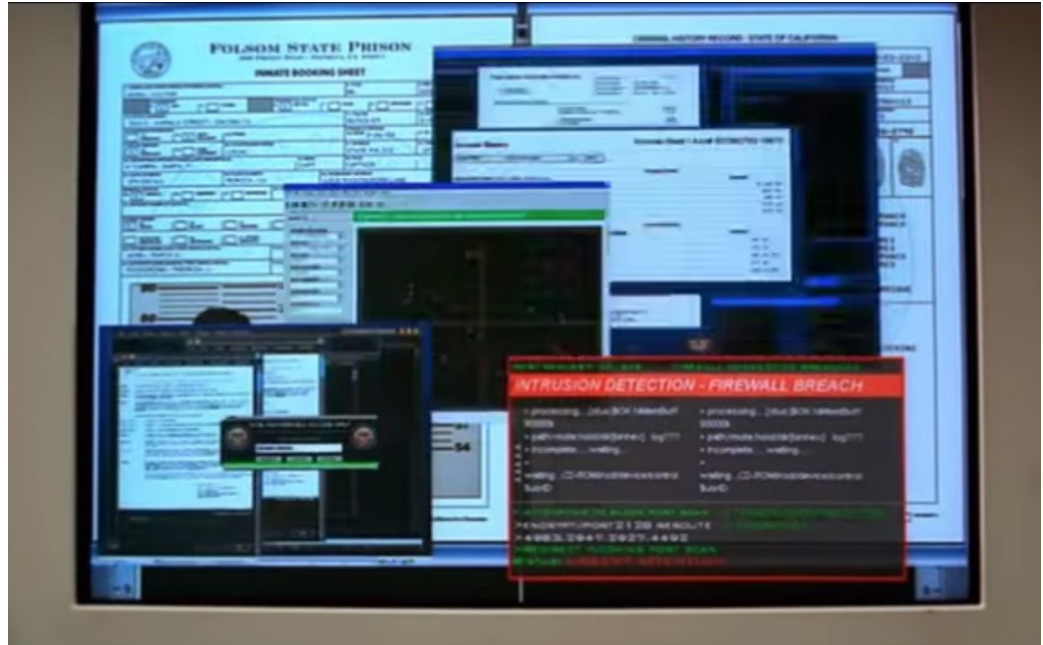
Jeopardy Style - The standard format

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

Web	RE	Pwn	Crypto	Forensics	Misc
\$200	\$200	\$200	\$200	\$200	\$200
\$400	\$400	\$400	\$400	\$400	\$400
\$600	\$600	\$600	\$600	\$600	\$600
\$800	\$800	\$800	\$800	\$800	\$800
\$1000	\$1000	\$1000	\$1000	\$1000	\$1000

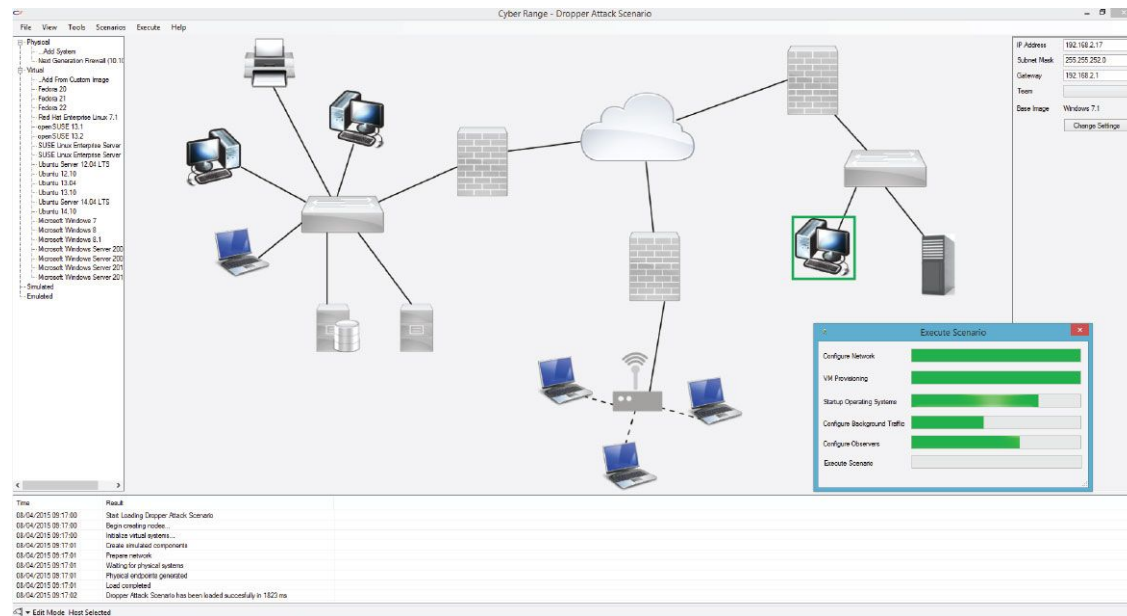
Attack/Defense - The intense classic

- 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](https://picoctf.com) - Beginner friendly
- [CTFTime.org](https://ctftime.org) - Calendar and rankings
- [OWASP Juice shop](https://owasp-juice.shop) - Web CTF in a box
- pwnable.kr - Pwnables
- [OverTheWire.org](https://overthewire.org) - Mix with focus on pwn

Thanks for listening - Now go hack!