CTF Workshop
Crim2018 – 31.10.2018
CTF (Capture the Flag)

- Capture the Flag (CTF) is a computer security competition.
- CTF are usually designed test and teach computer security skills.
- Consists of a series of small challenges that vary in their degree of difficulty
- The very first CTF competition was held in 1996 at DEFCON

https://upload.wikimedia.org/wikipedia/commons/4/47/DEF_CON_17_CTF_competition.jpg
CTF (Capture the Flag)

- Competitions can be team-based or individual-based.
- Most of the cyber security conferences today host a CTF competition.
- Different types of CTF competitions include: Jeopardy & Attack/Defend.

![Jeopardy Game Board](https://upload.wikimedia.org/wikipedia/commons/d/d8/Jeopardy_game_board.png)
Jeopardy

• Most common kind of CTF
• Set of challenges which are provided by organizers to competitors
• Each challenge is designed so, that when it is solved, a small piece of text or "flag" is revealed.
• The flag is then submitted to website for points.
• Amount of points rewarded is typically based on the difficulty of the challenge.
• Bonus points might be awarded for first solve.
• Can be held online

https://ox002147.gitlab.io/posts.html
Attack/Defend

• Teams are each given same set of vulnerable server software
• Teams are to setup & audit this software before the competition
• Teams will connect their servers to an isolated network to join the CTF
• Teams will launch attacks against each other servers
• Likewise teams need defend their own servers and keep them functioning normally
• Points are given based on extracting flags and defending own flags, as well keeping their servers operational
• Less common kind and rarely done for general public because of their complexity
CTF Challenge Categories

- Cryptography
- Reverse-engineering
- Forensics
- Web apps
- Misc
Cryptography

• Players are often given a encrypted data, and the goal is usually to crack it to reach the flag.

• Tools:
  – Often scripting or programming is needed
  – Password crackers like (HashCat or John The Ripper) with rockyou dictionary
  – Online hash databases based on rainbow tables

https://alternativeto.net/software/hashcat/
Reverse Engineering

- Often executable (or bytecode) given, which you can run locally
- Can be also obfuscated python or javascript.
- Mostly implements some algorithm and checks the input password. If you get the password right, you get the flag

*Tools:
- GDB or other debugger to debug the executable
- Objdump for disassembly (or free version of IDA PRO)
- Java decompiler

```
gdb-peda start
(c) 2018 Synopsys, Inc.
```

```c
0x0040a3 <frame_dummy+35>:   .sym
0x0040a4 <main>   push esp
0x0040a5 <main+1>:   mov esp,esp
0x0040a7 <main+2>:   and esp,0xffffffff
0x0040a9 <main+4>:   sub esp,0x10
0x0040b0 <main+5>:   mov eax,DMORD FTA [esp+0x8]
0x0040b3 <main+8>:   add eax,0x4
0x0040b5 <main+9>:   mov eax,0x80D FTA [eax]
```

```c
[--- stack ---]
0000 | 0x0040a990 0x0040a9c0 0x0040a9d0 0x0040a9e0 0x0040a9f0 0x0040a000 0x0040a010
0008 | 0x0040a020 0x0040a030 0x0040a040 0x0040a050 0x0040a060 0x0040a070 0x0040a080
0012 | 0x0040b3c0 0x0040b3f0 0x0040b430 0x0040b460 0x0040b490 0x0040b4c0 0x0040b4f0
001c | 0x0040b5a0 0x0040b5d0 0x0040b600 0x0040b630 0x0040b660 0x0040b690 0x0040b6c0
```

Legend: code, data, rodata, value

Temporary breakpoint 1, 0x0040a39e7 in main ()
gdb-peda

https://github.com/longld/peda
Forensics

• Forensics can include any challenge to examine and process a hidden piece of information out of static data file (as opposed to executable programs or remote servers).

• Includes topics like:
  – Steganography
  – File analysis
  – Filesystem analysis
  – Network traffic capture
  – Etc.
Steganography

• File or message hidden in "plain sight".
• Message can be hidden in image, video, audio etc.
• Many techniques available, but the most common is the LSB (Least Significant Bit).
• In LSB for example the last bits of each color of pixel is used to hide data.

Steganography

• Tools:
  – StegHide is able to hide data in various kinds of image- and audio-files.
  – StegSolve is a Analysis tool for several image formats
  – zSteg is a Analysis tool for PNG & BMP files
  – Binwalk is used to identify files embedded in another file
  – Gimp is raster graphics editor
File analysis

- Files can sometimes come without an extension, or with incorrect one.
- File extension is not the only way to identify a type of a file. Format identification can be done also by looking for first few bytes of the files (called Magic bytes).
- Examples of magic bytes:
  - JPG starts with "FF D8" and ends with "FF D9"
  - PNG starts with "89 50 4E 47 0D 0A 1A 0A" and ends with "49 45 4E 44 AE 42 60 82"
  - GIF starts with "47 49 46 38 39 61" and ends with "00 3B"
- Tool for identifying files using magic bytes in Linux is called “file”.

```
root@Machine:~ # file DSC_0064.JPG
DSC_0064.JPG: JPEG image data, Exif standard: [TIFF image data, little-endian, direntries=11, manufacturer=Sony, model=F8131, orientation=upper-right, xresolution=158, yresolution=166, resolutionunit=2, software=41.2.A.7.76_0 f700, datetime=2018:10:25 15:12:17, GPS-Data], baseline, precision 8, 3840x2160, frames 3
```
File analysis

• Other tools for file analysis:
  – strings: Look for "hidden" strings in files
  – binwalk: Identify and extract a file embedded in another file
  – xxd: Create a hex dump of a given binary file.
  – Ghex: Binary file editor
Filesystem analysis

- File given can sometimes be actually a full disk image.
- Image can be mounted to access files inside.
- Flag can be inside the visible file system, but sometimes it can also be in hidden volume, in unallocated space or a deleted file etc.

Tools:
- mount: Attach the file system to existing directory structure
- tree: Quick look of the directory structure
- TestDisk: Recover missing partition tables, fix corrupted ones, undelete files etc.
- extundelete: recover deleted files on ext3 & ext4
- binwalk: Identify and extract a file embedded in another file
- Sleuth Kit: library and collection of tools that allow investigation of disk images
Packet capture (PCAP files)

- Network traffic captured to a file
- Common challenge is to provide a PCAP file and the challenge is to recover transferred file or secret. To make things harder there can be a lot of unrelated traffic included.
- Wireshark is the most common tool for analysing the packet captures
- In Wireshark you can use the "Export objects" functionality to extract files from the capture (e.g. File -> Export objects -> HTTP -> Save all)
- Wireshark can also decrypt encrypted traffic like SSL, WEP, WPA2 etc., if the keys are available

https://upload.wikimedia.org/wikipedia/commons/0/03/Wireshark_screenshot.png
Web apps

• Common goal is to exploit some server, which has some file that includes the flag.
• Applications mostly written in: PHP, Python, Ruby, Javascript
• Vulnerability to exploit could be for example: SQL Injection, XSS, CSRF, deserialization etc.
• Tools:
  – Web browser (dev tools)
  – Burp Suite
  – ZAP
  – Sometimes also automatic scanners such as sqlmap, dirbuster.
Encodings

- Encoding is a technique to represent data using a different format.
- Encoding is needed for example when sending a binary file over a text-based messaging system like email.
- Process is reversible and no key is needed.
- Common encodings for "Hello World":
  - Base64: SGVsbG8gV29ybGQ=
  - Base32: JBSWY3DPEBLW64TMMQ======
  - Base85: 87cURDji,"Ebo7
  - Ascii code: 48 65 6c 6c 6f 20 57 6f 72 6c 64
  - Rot-13: Uryyb Jbeyq
  - Rot-47: w6==@ H@C=5
  - Morse: .. - . - - - - - - - - - - - - - - - -
Capture The Flags are one of, if not **THE** best way to get started in security.

They can be a little hard.

You definitely won't be spoonfed.

You'll probably get stuck at some point.

But if you stick with it, you'll learn more about computers than you ever thought possible. There's no better way to learn something than to experience it for yourself. And in the computer security world, Capture The Flag is the best way to learn by doing.

https://ctfd.io/whats-a-ctf/
CONQUER THE WORLD

Welcome to the CTF Capture the Flag Competition. By clicking "Play," you will be entered into the official CTF challenge. Good luck in your conquest.
• https://188.166.29.140/