Introduction
Operating System
Basic
Cryptography
Steganography
Digital Forensics
Reverse Engineering
Binary Exploit / Pwn
Web
PCAP analysis
Misc
A few tips
Other cheatsheet

Steganography

A method to hiding something in something.

General

1. Usually when organizer gave us Image, Music, Video, Zip, EXE, File System, PDF and other files, it a *steganography* or *forensics* challenge. Run `file` command first.
2. Metadata is important. Checkout the EXIF data of the file by using `exiftool [filename]` command.
3. Try issuing `binwalk [filename]` on the file. They may hide another file in the file.
   - To extract, use `binwalk -e`.
   - To extract one specific signature type, use `binwalk -D 'png image:png' [filename]`.
   - To extract all files, run `binwalk --dd='.*' [filename]`.
4. Try file carve using `foremost -v [filename]` command. Foremost support all files.

Images

1. View the image first
2. Use `strings` command to that file.
   - Try `grep -i [any strings you want to filter]` from the `strings` command output.
   - Example `grep -i "flag{"` to filtering the flag format only. `-i` option to unable case sensitive.
3. Google the images, differentiate the `md5hash`. If you found same image but have a different md5 hash, it may probably have been altered.
4. Analyse the header and the content of the file using any **hex editor**.
5. Know the **file signature**. Maybe they gave us corrupt header! So fix it!
6. Maybe **zoom-in** and **zoom-out** method can get the flag.
7. Use https://www.tineye.com/ to reverse search the image in the internet.
8. Use `imagemagick` command tool to do image manipulation.
9. Use **Stegsolve.jar** tools. There are so many CTF I've participated that I used this tool to unhide flag from an image.
10. File carve using `steghide --extract -sf <filename>`. Try find the password with your own-self. Maybe, the organizer will give hints or the password may in another file.
11. Check for any corruption on PNG file by using `pngcheck <filename.png>` command.
12. Detect stegano-hidden data in PNG & BMP s by `issuing zsteg -a <filename.png>`.
13. Use **SmartDeblur** software to fix blurry on image.
14. Use `stegcracker <filename> <wordlist>` tools Steganography brute-force password utility to uncover hidden data inside files.
15. Use `tesseract` to scan text in image and convert it to .txt file.
16. Another powerfool tool is called `zsteg`.
17. Steganosuite
    - Extract data from image (-x)
18. Some of online stegano decoder :-
    - https://futureboy.us/stegano/decinput.html
    - http://stylesuxx.github.io/steganography/
    - https://www.mobilefish.com/services/steganography/steganography.php
    - https://manytools.org/hacker-tools/steganography-encode-text-into-image/
    - https://steganosaur.us/dissertation/tools/image
    - https://georgeom.net/StegOnline
    - http://magiceye.ecksdee.co.uk/

Compressed file

1. Unzip it.
   1. Use `zipdetails -v` command to display details about the internal structure of a Zip file.
   2. Use `zipinfo` command to know details info about Zip file.
   3. Use `zip -FF input.zip --out output.zip` attempt to repair a corrupted zip file.
   4. Brute-force the zip password using `fcrackzip -D -u -p rockyou.txt  filename.zip`
2. To crack 7z run `7z2hashcat32-1.3.exe filename.7z`. Then `john --wordlist=/usr/share/wordlists/rockyou.txt hash`

Music file

1. Use `binwalk` first. They may embedded something in the file.
2. Use **Audacity**.
3. Use **Sonic Visualizer**. Look at spectogram and other few Pane.
4. Use **Deepsound**.
5. Use **SilentEye**.
6. Some of online stegano decoder for music:-
   - https://steganosaur.us/dissertation/tools/audio

Text

1. Use http://www.spammimic.com/ that can decode hide message in spam text.

PDF

1. qpdf
2. PDFStreamdumper
3. pdfinfo
4. pdfcrack
5. pdfimages
6. pdfdetach
7. pdf-parser.py -v <file>
8. pdftotext
9. peepdf -if <filename>
   - object <value>
10. pdfid