



CTF (Capture the flag)

By Team Matrix Elite Hackers

1.0 CTF

- ☐ CTF stands for Capture The Flag.
- ☐ Capture the Flag (CTF) is a special kind of information security competitions.
- ☐ A CTF is an event during which students, teachers, and professionals come together to compete against one another in an effort to test and expand cyber-security skills and awareness.

1.1 Class Requirements for CTF

- ☐ Cryptography
- ☐ Steganography
- ☐ OSINT
- ☐ LFI/RFI
- ☐ XSS
- ☐ SQLI
- ☐ Burp Suite
- ☐ Scanning and Networking
- ☐ Digital Forensic
- ☐ Kali Linux

1.2 There are three common types of CTFs

- ☐ Jeopardy
- ☐ Attack-Defence
- ☐ Mixed Style

1.3 CTF Categories

- Cryptography
- Steganography

- Web Exploitation
- Forensics
- PWN Or Binary Exploitation
- Reverse Engineering
- Miscellaneous
- OSINT

2.0 Cryptography

2.1 Hash Tools

☐ Hash Analyzer -Kali Linux Tool

Hashid, Hash-identifier

☐ Hash Analyzer - Online Tools:

- <https://www.tunnelsup.com/hash-analyzer/>
- https://hashes.com/en/tools/hash_identifier
- <https://www.dcode.fr/hash-identifier>

☐ Hash Encoder/Decoder

- Offline Tools - Hashcat, hash generator, BCTextEncoder, BlueCode
- <https://gchq.github.io/CyberChef>
- <https://md5hashing.net/>
- <https://www.dcode.fr/hash-function>

2.2 Cipher (or Cypher) Tools

☐ Cipher Identifier

- <https://www.dcode.fr/cipher-identifier>

☐ Shift Cipher

- <https://www.dcode.fr/shift-cipher>

☐ Symbol Cipher

- <https://www.dcode.fr/symbols-ciphers>

❑ Encode/Decode

- <https://cryptii.com>
- <https://gchq.github.io/CyberChef>
- <https://www.boxentriq.com/code-breaking/atbash-cipher>
- <https://morsecode.world>
- <https://www.dcode.fr/langage-brainfuck>
- <https://cryptii.com/pipes/binary-decoder>
- <https://github.com/hellman/xortool/>

3.0 Steganography

3.1 Steganography Resource (Tools)

❑ Web Tools (Online Tools)

Steganography - A list of useful tools and resources

- <https://0xrick.github.io/lists/stego/>

Ultimate steganography solver website

- <https://www.aperisolve.com/>

Steganographic Encoder/Decoder

- <https://futureboy.us/stegano/decinput.html>

Steganography Online - Image

- <https://stylesuxx.github.io/steganography/>

❑ Text

Unicode Text - A web tool for unicode steganography , it can encode and decode text.

- <https://www.irongeek.com/i.php?page=security/unicode-steganography-homoglyph-encoder>

❑ Audio Analyzer

Sonic Visualiser

- <https://www.sonicvisualiser.org/>

Audacity - Multi-track audio editor

- <https://www.audacityteam.org/>

❑ Image Kali Linux Tools

Steghide — is a steganography program that hides data in various kinds of image and audio files.

- <http://steghide.sourceforge.net/>

Kali Linux >> sudo apt-get update, sudo apt install steghide

Binwalk - Binwalk is a tool for searching binary files like images and audio files for embedded files and data.

- <https://github.com/ReFirmLabs/binwalk>

Exiftool — Read and write meta information in files

- <https://linux.die.net/man/1/exiftool>

Pngtools — For various analysis related to PNGs

- <https://www.madebymikal.com/category/pngtools/>

Zsteg — PNG/BMP analysis

- <https://github.com/zed-0xff/zsteg/>

StegCracker — Steganography brute-force utility to uncover hidden data inside files.

- <https://github.com/Paradoxix/StegCracker>

❑ Image Windows Tools

OpenStego

- <https://www.openstego.com>

Stegsolve — Apply various steganography techniques to images

- <https://github.com/eugenekolo/sec-tools/tree/master/stego/stegsolve/stegsolve>
- <https://github.com/zardus/ctf-tools/blob/master/stegsolve/install>

HxD - Freeware Hex Editor and Disk Editor

- <https://mh-nexus.de/en/hxd/>

ExifTool - Read, Write and Edit Meta Information!

- <https://exiftool.org/>

QR Code Scanner

- <https://qrcodescan.in/>

Cryptography & Steganography Problem Solving

❑ Tryhackme – CTF collection Vol.1

- <https://tryhackme.com/room/ctfcollectionvol1>

✓ Task: 2,3,4,6,7,8,9,11,13,14,15,16,17,19,20

4.0 Web Exploitation

❑ picoCTF

- <https://picoctf.org/>

❑ Tryhackme

- <https://tryhackme.com/room/learncyberin25days>
- <https://tryhackme.com/room/adventofcyber2>
- <https://tryhackme.com/room/adventofcyber3>

5. Reverse Engineering

❑ Tools

- IDA Pro, CFF Explorer, Ghidra, OllyDbg, Itrace, radare2, apktool, and many more

❑ Learn

- <https://ctf101.org/reverse-engineering/overview/>
- <https://0xinfection.github.io/reversing/>

Problem Solving

❑ picoCTF

- <https://picoctf.org/>

❑ Tryhackme

- <https://tryhackme.com/room/reverselfiles>
- <https://tryhackme.com/room/windowsreversingintro>
- <https://tryhackme.com/room/reloaded>
- <https://tryhackme.com/room/brainstorm>

6. PWN Or Binary Exploitation

☐ Details

- <https://ctf101.org/binary-exploitation/overview/>

☐ Tools

- pwntools, ltrace , strings , gdb , radare 2, Ghidra and many more

Problem Solving

☐ Tryhackme

- <https://tryhackme.com/room/pwn101>
- <https://tryhackme.com/room/introtopwntools>
- <https://tryhackme.com/room/binaryheaven>

☐ picoCTF

- <https://picoctf.org/>

☐ Reference

- <https://ctf101.org/binary-exploitation/what-is-a-format-string-vulnerability/>
- https://owasp.org/www-community/attacks/Format_string_attack
- <https://www.rapidtables.com/convert/number/hex-to-ascii.html>

7. Forensics or Digital Forensics

☐ Details

- <https://ctf101.org/forensics/overview/>

☐ Tools

- Autopsy, hexeditor, foremost, binwalk, Wireshark, and many more

Problem Solving

☐ Tryhackme

- <https://tryhackme.com/room/btautopsy0>
- <https://tryhackme.com/room/wireshark>

☐ picoCTF

- <https://picoctf.org/>

8. OSINT Open-Source Intelligence

☐ Tryhackme

- ☐ <https://tryhackme.com/room/ohsint>

☐ CTF Academy

- ☐ <https://ctfacademy.github.io/osint/challenge1/index.htm>

9. Miscellaneous | Misc

- ☐ Many challenges in CTFs will be completely random and unprecedented, requiring simply logic, knowledge, and patience to be solved. There is no sure-fire way to prepare for these, but as you complete more CTFs you will be able to recognize and hopefully have more clues on how to solve them.

☐ Example

- <https://github.com/ctfs/write-ups-2014/tree/master/ructf-2014-quals/misc-100>
- <https://github.com/ctfs/write-ups-2014/tree/master/olympic-ctf-2014/crypting>

10. CTF Events

☐ DEF CON CTF - CTF World Cup

- Details: <https://defcon.org/html/links/dc-ctf.html>

☐ CSAW CTF

- Details: <https://ctf.csaw.io/>

☐ iCTF: the International Capture The Flag Competition

- Details: <https://shellphish.net/ictf/>

11. Bangladesh CTF Events

☐ Details

- <https://www.cirt.gov.bd/>
- <https://cyberdrill.cirt.gov.bd>

12. CTF Events Tracker

☐ Worldwide security CTF tracking site

- <https://ctftime.org/ctfs/>
- <https://ctftime.org/event/list/upcoming>
- <https://ctf.hackthebox.com/>

13. CTF Ranking

☐ Global Ranking

- <https://ctftime.org/stats/>

14. CTF Resources

☐ Learning Platform

- ☐ <https://ctflearn.com/>
- ☐ <https://tryhackme.com/>
- ☐ <https://ctf101.org/>

☐ Practice Platform

- ☐ <https://ctflearn.com/>
- ☐ <https://ctf.hackthebox.com/>
- ☐ <https://picoc.tf/>
- ☐ <http://pwnable.kr/>
- ☐ <https://ctf.hackme.quest/>
- ☐ <https://ringzer0ctf.com/>
- ☐ <http://reversing.kr/>

☐ GitHub

- ☐ <https://github.com/JohnHammond/ctf-katana>
- ☐ <https://github.com/ctfs/>
- ☐ <https://github.com/p4-team/ctf/>

☐ YouTube Channel

- ☐ John Hammond
- ☐ Hacker Joe
- ☐ LiveOverflow
- ☐ ShmooCon
- ☐ IppSec
- ☐ OWASP

☐ Writeup

- ☐ <https://ctftime.org/writeups>



Team Matrix Elite Hacker

- Facebook: <https://www.facebook.com/teammatriix>
- Google Site: <https://sites.google.com/view/teammatrix>
- Telegram Channel: <https://t.me/teammatrixs>
- YouTube Channel: <https://www.youtube.com/c/TeamMatrixEliteHackers>
- Phone: +8801303818319