
CYBERQUEST
CTF 101
CTF TRAINING &STRATEGIES

ABOUT ME

- Hey there! I’m Lentine Khakai, a cybersecurity analyst with a love for hacking things (ethically, of course 😄).
- I'm into offensive security, and when I’m not breaking into vulnerable machines, you’ll probably find me knee-deep in a CTF.
- I'm a proud member of p3rf3ctr00t_ke, where I tackle challenges in OSINT, Web Exploitation, and Prompt Injection.
- Currently interning at CyBlack and working as a cybersecurity trainer, I spend my days teaching, hacking, and helping others grow in the field.

INTRO TO CTFS

WHAT IS A CTF?

CTFs are cybersecurity competitions where security challenges are set up for participants to "hack". Once a challenge is solved, participants get a "flag" which is usually a string, password, filename etc. Flags are then submitted for points. Points for each flag depend on the difficulty of the challenge, the higher the difficulty - the more the points. Platforms such as CTFTime can be used to find any CTFs happening.

TYPES OF CTFS

There are 2 main types of CTF competitions:

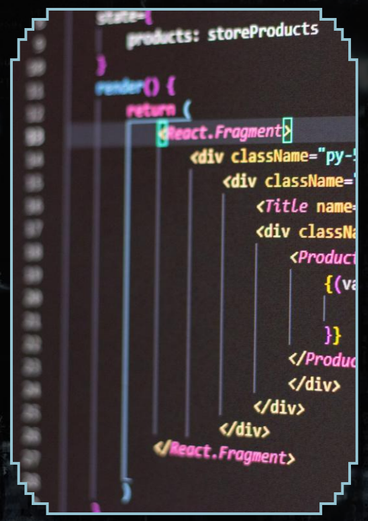
1. **Jeopardy-style CTF:** a collection of “hacking” challenges organised according to different categories such as web, forensics, cryptography, steganography, networking, and binary. The challenges are often sorted by difficulty levels, allowing beginners to also easily participate. E.g PICO CTF, HTB Cyberapocalyse etc

2. **Attack-Defense Style CTF:** a more advanced version of a CTF requiring teams to defend their own servers against attack, and attack opponents’ servers to score. These CTFs require more skills to compete and are almost always done in teams.
   - **King of the Hill (KotH):** a variation of the Attack-Defense style CTF, teams compete to main control over a designated system or resource. The longer a team maintains control, the more points they accumulate. Other teams attempt to take over and defend the hill, leading to a dynamic and competitive environment. e.g THM's KoTH, HTB Battlegrounds

CTF CATEGORIES

CTF challenges span across different areas in cybersecurity. The usual challenges that you will encounter include:

- Web exploitation
- Cryptography
- Reverse Engineering
- Forensics
- Network security
- Binary exploitation (pwn)
- Steganography
- Misc (miscellaneous)
- OSINT
- Hardware
- Machine Learning & AI
- Mobile
- Blockchain
- PPC (Professional programming and coding)
- Boot2root



1. WEB EXPLOITATION

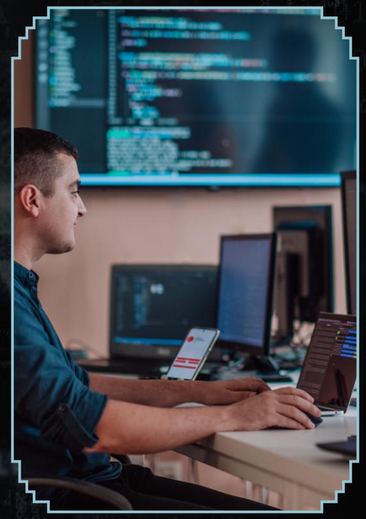
Involves finding and exploiting vulnerabilities in web applications such as SQL injection, XSS, CSRF, LFI, etc.

Tools Used:

- Burp Suite
- Postman
- Browser dev tools

Resources

- Portswigger Web Academy
- HTB Web Challenges
- Wizer CTF
- OWASP Juiceshop



2. CRYPTOGRAPHY

Solving puzzles related to encryption, decryption, ciphers, and encoding.

Tools Used

- Dcode
- CyberChef
- Python scripts
- Hashcat/John The Ripper
- CrypTool

Resources

- CrptoHack
- OverTheWire : Krypton
- CrytoPals

3. REVERSE ENGINEERING

Understanding and manipulating compiled programs to reveal hidden logic or flags.

Tools Used

- Ghidra / IDA Free
- GDB / pwndbg
- X64dbg (for Windows)
- Cutter

Resources

- Malware Unicorn RE101
- Crackmes.one
- Challenges.re

4. BINARY EXPLOITATION (PWN)

Exploiting memory corruption in binaries (e.g., buffer overflows, ROP chains).

Tools Used

- GDB + pwndbg /peda
- Pwntools (Python lib)
- ROPgadget
- Checksec

Recources

- Pwn College
- CTF University: Pwn101
- Pwnable.tw

5. FORENSICS

Analyzing disk images, memory dumps, logs, or network traffic to extract clues or hidden data.

Tools Used

- Wireshark
- Autopsy / Sleuth kit
- Volatility

Resources

- Root Me : Forensics
- DFIR Training
- Cyberdefenders

6. STEGANOGRAPHY

Hiding and finding data in media files (images, audio, video).

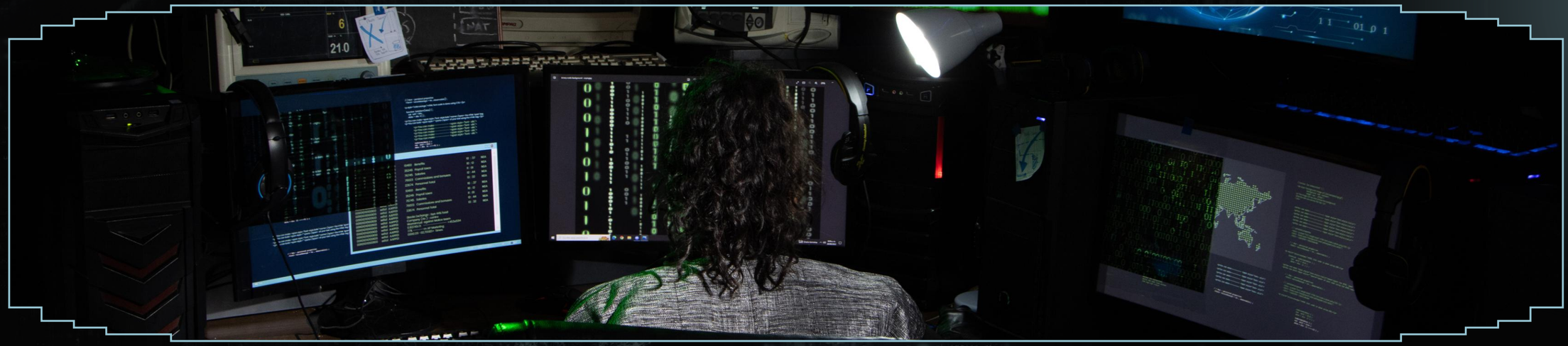
Tools Used

- Steghide
- Zsteg
- Binwalk
- Exiftool
- Audacity

Resources

- Root Me: Steganography
- CTFLearn Stego Challenges

•Frida / Objection
•Android emulator / Genymotion



7. MOBILE

Reverse engineering or exploiting Android/iOS applications.

Tools Used

- Frida /Objection
- Andoid Emulator / Genymotion
- MobSF (Android) / jadx / apktool

Resources

- Crackmes.one Mobile challenges
- TryHackMe – Android Room

8. NETWORK FORENSICS

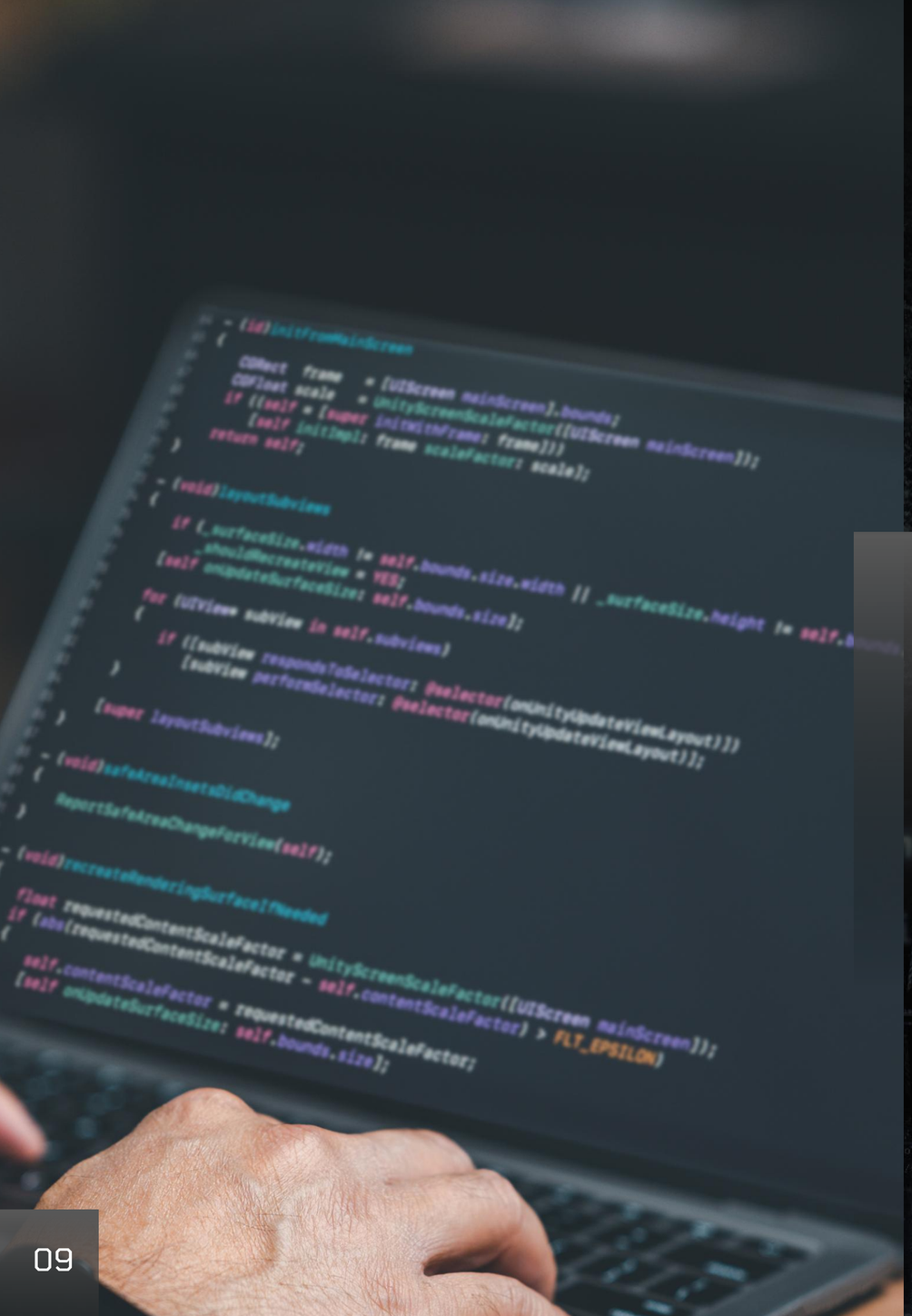
Analyzing network data (e.g., PCAP files) to extract credentials, files, or understand traffic flow.

Tools Used

- Wireshark
- Tcpdump
- Tshark
- NetworkMiner

Resources

- CyberDefenders
- CyberTalents



9. BOOT2ROOT

Simulated vulnerable machines where the goal is to escalate from user to root and capture flags.

Tools Used

- Nmap / Rustsan
- Gobuster / ffuf / Feroxbuster
- Burpsuite
- Linpeas / Winpeas
- Metasploit

Resources

- HackTheBox
- TryHackMe
- VulnHub

10. PPC (Professional Programming and Coding)

Algorithmic problem-solving using programming: sorting, searching, pathfinding, etc.

Tools Used

- Any programming language depending on the challenge
- IDE / Text editors such as Vscode

Resources

- Leetcode
- CodeWars
- HackerRank

10. OSINT (OPEN-SOURCE INTELLIGENCE)

Finding information from public sources like social media, websites, domains, and metadata.

Tools Used

- Google Dorking
- Exiftool
- theHarvester
- Sherlock
- Shodan.io
- Censys.io

Resources

- HackYourMum Osint challenges
- Tracelabs

11. HARDWARE

Interacting with physical devices such as microcontrollers, firmware, serial communication, logic analysis.

Tools Used

- Logic analyzers (Saleae, Sigrok)
- Arduino / Raspberry Pi
- Ghidra (for firmware RE)
- JTAG / UART tools

Resources

- Hackaday projects
- Hardware CTFs at DEFCON

12. BLOCKCHAIN

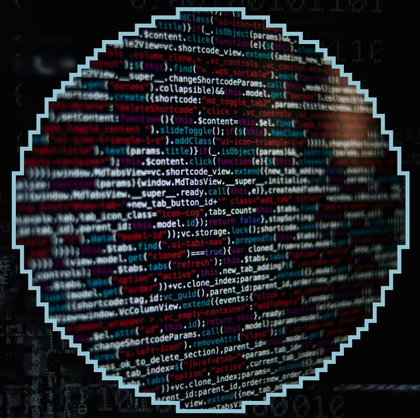
Exploiting smart contracts or misconfigured blockchain logic, mostly Ethereum and Solidity.

Tools Used

- Remix IDE (Solidity IDE)
- Ganache
- MetaMask
- Sepolia

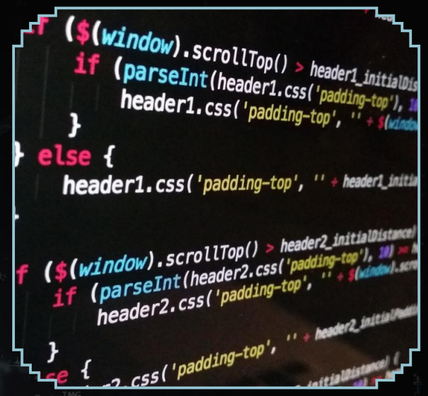
Resources

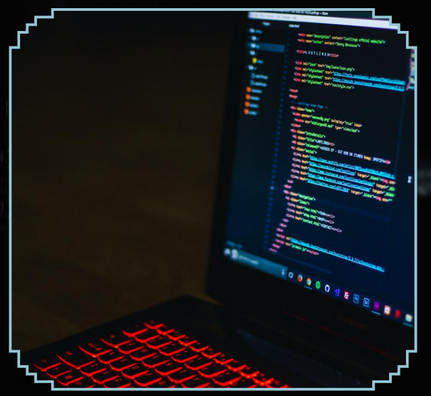
- Ethernaut CTF
- Damn Vulnerable DeFi
- Chainshot



CTF STRATEGIES

1. Make sure you understand the rules of the CTF and the format of flags, this can save a lot of time
2. Form a diverse team. Have a team with players of different skill sets, then divide and conquer challenges based on area of expertise if it is a jeopardy style ctf. If an attack-defense CTF, work on it together while using platforms like discord to be in constant communication
3. Quickly go for the quick wins and then focus on harder challenges. If you get stuck on a challenge for long, move to another and circle back later
4. Document your process as much as possible, including failed techniques. These notes may come in handy in different ctf challenges
5. Have your tools ready and well organized before the CTF. Advisable to have a backup VM with all tools needed installed before the CTF in case of any hiccups. You can also take a snapshot of your VM and roll back in case anything breaks.
6. PRACTICE MAKES PERFECT!! Use platforms like TryHackMe, HackTheBox, CTFLearn, PicoCTF
7. Read writeups of challenges to learn new techniques from others
8. Learn to stay calm under pressure. Do not panic if you do not know where to start, break down problems into small parts
9. COLLABORATE, do not forget to work with your teammates, they can help brainstorm ideas
10. Take breaks.





THANK YOU

GET IN TOUCH WITH ME:

Khakai.github.io

lentinemugalo@gmail.com