CTFs to Cyber Security Careers

Cyber SHE-ield 2025

whoami

- Alias @m0n1x90
- Founder @TamilCTF
- Security Engineer @Zoho
- Red Teaming / Application Security / Malware Dev
- Part time full stack development
- Blog at m0n1x90.dev

What Cybersecurity looks like...

Why cybersecurity matters ?

- Personal, financial, and corporate data must be safeguarded from breaches
- Sectors like healthcare, banking, and energy rely on cybersecurity
- Cyberattacks cost billions globally, affecting economies
- Cybercrime is increasing, affecting individuals, businesses, and governments
- Many more unknown and upcoming attack surface ???

Why CTF for Cybersecurity ?

- Drastic skill enhancement
- Understanding multiple tech stack and frameworks
- Exploring other domains
- Debugging and investigation
- Real world competition
- Adaptability to real world exploits / CVEs

	w/o CTF	w/ CTF
Experience	✓	✓
Theory	✓	✓
Practice		✓
Debugging Skill		✓
Real World Exploits		✓
Versatility		✓

What is CTF ?

Jeopardy-style

- Mixed
- Beginner Friendly

Attack Defense

- Red Team
- Blue Team

Boot2Root

- Pwn

- A cybersecurity competition where participants solve security-related challenges
- CTF Time, Pico CTF
- Try Hack Me, Hack The Box etc.
- VulnHub, VulnLab etc.
- PwnCollege

Exploration in CTFs

- Beginner categories like Web, Cryptography, Reverse Engineering, Forensics, Pwn, OSINT etc.
- One step further – Cloud Attacks, Web3, Hardware Hacking etc.
- Unlocking opportunities in each domain
- Understanding attack vectors / prevention methodologies quicker
- Fuzzing and exploiting real world like applications
- Boosting confidence and skill level

Example CTF Problem ?

Are you confident in your coding skills …

Testing You C/C++ Proficiency 😉

```c
#include <stdio.h>
#include <string.h>

void win() {
    printf("Congrats! You got the flag: %s\n", "TCTF{Buffer_Overflow_Success}");
}

void vulnerable_function() {
    char buffer[32];  // 32-byte buffer
    printf("Enter your input: ");
    gets(buffer);  // Unsafe function - causes buffer overflow
    printf("You entered: %s\n", buffer);
}

int main() {
    printf("Welcome to CTF buffer overflow challenge!\n");
    vulnerable_function();
    return 0;
}
```

What you gain in CTFs ?

- Strong problem solving skills correlating with real world expertise
- Can use it in Bug Hunting, Vulnerability Research, Secure Coding etc.
- Networking with like-minded people
- Research & Continuous Development
- Knowing reality that Cybersecurity world is just more than theory
- Landing careers in your own field of expertise

CTFs to Career - Know your domain

- Forensics = Malware Analyst , Incident Responder, SOC
- Web = App Sec / Bug Hunting
- Pwn = Binary Exploitation / Vulnerability Research
- Reverse Engineering = Malware Analyst / Vulnerability Research
- Cryptography = Mathematic / Complex Algorithms
- Hardware = IoT / ICS / Other hardware

CTFs to Career - Hiring CTFs

- Many cybersecurity companies use CTFs to identify skilled candidates
- Some organizations offer direct job opportunities to top CTF players
- Employers look for strong problem-solving, teamwork, and technical expertise
- Performance in CTFs can replace traditional hiring processes like resumes & interviews (Depends on the company process)*

Start Now

- Participate in CTFs regularly and identify your favorite skill
- Build a portfolio (CTF write-ups, Blogs, Exploits, Vulnerable Apps)
- Obtain industry reputed certifications (Adds preference to your resume)
- Building network with professionals via LinkedIn & conferences
- Contribute to open-source security projects

Start Now

- Follow cybersecurity experts on social media
- Start with beginner-friendly CTFs and gradually move to advanced levels
- Join local cybersecurity clubs or online communities
- Perseverance Never Fails 😎, Hack the planet !!!

Thank You

Follow Me On
@m0n1x90