< How to Capture the Flag [CTF] />

Beginning your CTF Journey

1011 011 01 1011001 10 11011 011 01 110110 110111 1101

< Table of contents />

{1: ‘Introduction’,
2: ‘How to Start’,
3: ‘Categories in CTFs’,
4: ‘Demos’,
5: ‘Tips for CTFs’,
6: ‘Questions/Thank you’}

1 0 1 1 0 1 1 0 1 1 0 1 1 0 0 1 1 0 1 1 0 1 1 0 1 1 0 1 1 1 0 1 1 0 1 1 0 1 1 1 1 1 0 1

Resources

https://bit.ly/HTCTF26

1 0 1 1 0 1 1 0 1 1 0 1 1 0 0 1 1 0 1 1 0 1 1 0 1 1 0 1 1 1 0 1 1 0 1 1 0 1 1 1 1 1 0 1

< About ME />

- Teacher at Red Bank Regional HS since 2007
  - CTE - Academy of Information Technology
- Started teaching Cybersecurity in 2018
- Garden State Cyber - CTF Question Writer
- Adjunct - Brookdale CC and Rutgers University
- CyberPatriot 14 Coach of the year
- CyberTeams Coach for 10+ years
- Baseball Coach for 11 years(retired)
- Obtained 5 industry level certifications(expired)
- Advanced Graduate Certificate in Cybersecurity at RIT
- Father of two(Most Important!)

1 0 1 1 0 1 1 0 1 1 0 1 1 0 0 1 1 0 1 1 0 1 1 0 1 1 0 1 1 1 0 1 1 0 1 1 0 1 1 1 1 1 0 1

< What is a CTF? />

1. Cybersecurity Learning Game
2. Gain points by solving Cybersecurity related challenges

1 0 1 1 0 1 1 0 1 1 0 1 1 0 0 1 1 0 1 1 0 1 1 0 1 1 0 1 1 1 0 1 1 0 1 1 0 1 1 1 1 1 0 1

Why CTFs?

Creates Competition

Learn new topics

Fun learning environment

Get kids excited

Resume Builder

1011 011 01 1011001 10 11011 011 01 110110 110111 1101

< Types of CTFs />

Jeopardy Style

1. Focused on solving puzzles and testing computer knowledge

2. Individual and/or small teams

3. Solving questions to show Cybersecurity knowledge.

Attack/Defense

1. Real-world scenarios

2. Team Play

3. Attacking and Defending systems from real world adversaries

Additional Types: Escape Rooms, Scavenger Hunts

1 0 1 1 0 1 1 0 1 1 0 1 1 0 0 1 1 0 1 1 0 1 1 0 1 1 0 1 1 1 0 1 1 0 1 1 0 1 1 1 1 1 0 1

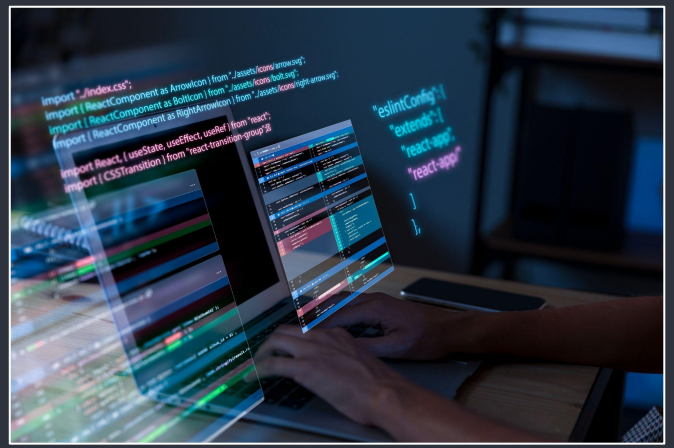
< CTF Topics />

1. General Skills - Linux/Windows Skills
2. OSINT
3. Cryptography CyberChef/Steganography
4. Web
    a. Chrome Dev Tools
    b. Command Injection
    c. XSS
5. Forensics
    a. Network Forensics - Wireshark
    b. Disk Image - Memory(Volatility)
    c. File System - Autopsy
6. Reverse Engineering
7. Programming

1 0 1 1 0 1 1 0 1 1 0 1 1 0 0 1 1 0 1 1 0 1 1 0 1 1 0 1 1 1 0 1 1 0 1 1 0 1 1 1 1 1 0 1

< How to Get Started />

Crypto
Web Exploit
General Skills
OSINT



1011 011 01 1011001 10 11011 011 01 110110 110111 1101

< Cryptography/ Steganography />

Using CyberChef alongside other tools Cryptography/ Steganography Challenges

1 0 1 1 0 1 1 0 1 1 0 1 1 0 0 1 1 0 1 1 0 1 1 0 1 1 0 1 1 1 0 1 1 0 1 1 0 1 1 1 1 1 0 1

< Network Forensics />

With Wireshark & tshark

Someone accessed the server and stole the flag. Use the network packet capture to find it.

1 0 1 1 0 1 1 0 1 1 0 1 1 0 0 1 1 0 1 1 0 1 1 0 1 1 0 1 1 1 0 1 1 0 1 1 0 1 1 1 1 1 0 1

< File Forensics - Fixing a Corrupt File />

1011 011 01 1011001 10 11011 011 01 110110 110111 1101

< Tips for CTFs />

1. Read the question
    a. Glean hints from the question
2. DOCUMENT DOCUMENT DOCUMENT
3. Check out previous versions of the CTF
4. Don’t always start with the easy ones
5. DOCUMENT DOCUMENT DOCUMENT
6. Use CTF flag to your advantage
    a. IE picoCTF

1011 011 01 1011001 10 11011 011 01 110110 110111 1101

< Thanks! />

Do you have any questions?

CREDITS: This presentation template was created by **Slidesgo**, and includes icons by **Flaticon**, and infographics & images by **Freepik**

1 0 1 1 0 1 1 0 1 1 0 1 1 0 0 1 1 0 1 1 0 1 1 0 1 1 0 1 1 1 0 1 1 0 1 1 0 1 1 1 1 1 0 1