Yemeni Students
Community

CTF ESSENTIALS: LEARN TO HACK

workshop

Unlock Your Potential in Ethical Hacking: Solve CTF Challenges and Become a Cybersecurity Expert

طور مهاراتك في عالم الاختراق: حل تحديات التقاط العلم وارتق بمهاراتك في الامن السيبراني

APU

Yemeni Students
Community

This version of the slides is designed to serve as a post-workshop reference. It includes additional details, explanations, and step-by-step walkthroughs of the challenges, along with the tools used to solve them

WHAT IS CAPTURE THE FLAG (CTF) ?

APU
Yemeni Students Community

Definition:

- Capture the Flag (CTF) is a cybersecurity competition that challenges participants to solve puzzles and uncover hidden "flags."
- There are three common types of CTFs: Jeopardy-Style, Attack-Defence and mixed.

Purpose:

- Simulates real-world cybersecurity scenarios.
- Aims to teach practical skills through hands-on learning.

How to win:

- Solve challenges to capture as many flags as possible within the competition's time limit.

JEOPARDY-STYLE?

Yemeni Students Community

Challenge Structure:

- Each challenge includes a brief description that outlines the task and hints at the tools or skills needed to solve it.
- May include resources such as files (e.g., logs, images) or URLs for analysis.

Challenge-Based Scoring System:

- Challenges are assigned different point values based on their difficulty.
- Solving harder challenges earns more points.

Flag format:

- Flags typically follow a format such as flag{example_flag} or CTF{example123}.
- submit "flags" as proof of solving the challenge, submitting the correct flag automatically updates the scoreboard.

CTF CHALLENGE CATEGORIES

(JEOPARDY-STYLE)

APU

Yemeni Students Community

FORENSICS

ANALYZING DIGITAL EVIDENCE LIKE LOGS OR FILES.

MISCELLANEOUS

UNIQUE CHALLENGES MIXING VARIOUS SKILLS.

CRYPTOGRAPHY

SOLVING ENCRYPTION AND DECODING PUZZLES.

STEGANOGRAPHY

HIDING AND EXTRACTING DATA FROM IMAGES, AUDIO, ETC.

OSINT (OPEN SOURCE INTELLIGENCE)

USE OF PUBLICLY AVAILABLE INFORMATION FROM WEBSITES, SOCIAL MEDIA, AND PUBLIC RECORDS FOR INVESTIGATIVE PURPOSES.

REVERSE ENGINEERING

ANALYZING AND UNDERSTANDING COMPILED CODE.

WEB SECURITY

EXPLOITING VULNERABILITIES IN WEB APPLICATIONS.

BINARY EXPLOITATION

FINDING AND EXPLOITING VULNERABILITIES IN BINARIES.

IMPORTANCE OF CAPTURE THE FLAG (CTF) ?

APU
Yemeni Students Community

- **Practical Learning:** Provides real-world experience with cybersecurity tools and prepares participants for actual cyberattacks.
- **Find Weaknesses:** Helps identify system vulnerabilities and enhances skills in areas like encryption and hacking.
- **Skill Improvement & Security Awareness:** Improves defense mechanisms and raises awareness about the importance of online security.
- **Networking :** Connects you with professionals in the field and showcases essential skills for cybersecurity jobs.
- **Challenge-Based Learning:** Encourages learning through problem-solving in practical, competitive environments.

APU

Yemeni Students
Community

DEMO

DEMO

Yemeni Students Community

Exif Info

CATEGORY: FORENSICS

I believe there is a password hidden and a file as well.
Can you confirm it?

https://drive.google.com/drive/folders/1aOunVhyIqM1p0FXAFZF94ZZINyHYgANg?usp=sharing

flag format: YSC{flag}

DEMO

Yemeni Students Community

Exif Info

SOLUTION

- the challenge is solved using the “Exiftool” tool, which is used to read, write, edit metadata of different types of files
- when using the tool we can find a description of the file that contains a password
- usually when given a password it means the file might include a hidden file within it, so we use another tool “Steghide” that allows us to extract hidden files, the hidden file is a txt file that includes the flag.

DEMO

Yemeni Students Community

French Secret

CATEGORY: CRYPTOGRAPHY

I encrypted my flag using the 'YSC' key. I bet you know which cipher I used.

WKE{Yf_Ofb_$ITGfi_k34F$_eGhj4P}

flag format: YSC{flag}

DEMO

Yemeni Students Community

French Secret

SOLUTION

- the name of the challenge is a hint of the type of encryption used, when googling it you find out that it is another name for the Vigenère cipher
- “CyberChef” and “dCode” are the biggest websites for cryptography (encrypting and decrypting)
- look for the Vigenère cipher, put “YSC” as the key, and “WKE{Yf_Ofb_$ITGfi_k34F$_eGhj4P}” as the text to find the flag.

DEMO

Yemeni Students Community

Super salty

CATEGORY: OSINT

it's super salty... can you find out where this place is??

flag format: YSC{Name_Of_Place}

DEMO

Yemeni Students Community

Super salty

SOLUTION

- OSINT challenges usually require manual searching to find information on the internet, in this case, at first it might look like a frozen surface, but when using the “Google images” tool, we find out that the location is a salt flat “Uyuni Salt Flat”

DEMO

Yemeni Students Community

inspect

CATEGORY: WEB SECURITY

the following code may need inspection:

~~https://ysc.pythonanywhere.com/inspect~~

flag format: YSC{flag}

DEMO

Yemeni Students Community

inspect

SOLUTION

- hint given is the name of the challenge, “inspect” which is an option when right-clicking on pages in browsers, that allows us to view all loaded files of the website (HTML, CSS, JS)
- in this challenge, when viewing these files we find different parts of the flag, we put them together to get the final flag.

APU

Yemeni Students
Community

Hands-On!

ysc.pythonanywhere.com

CTF WRITEUP

Yemeni Students Community

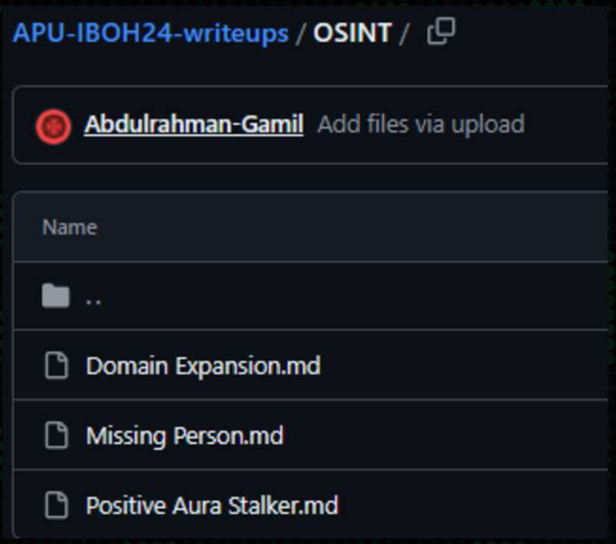
A detailed explanation of how a CTF challenge was solved, usually posted on platforms like Github, Youtube, Bloggers, or Social media.

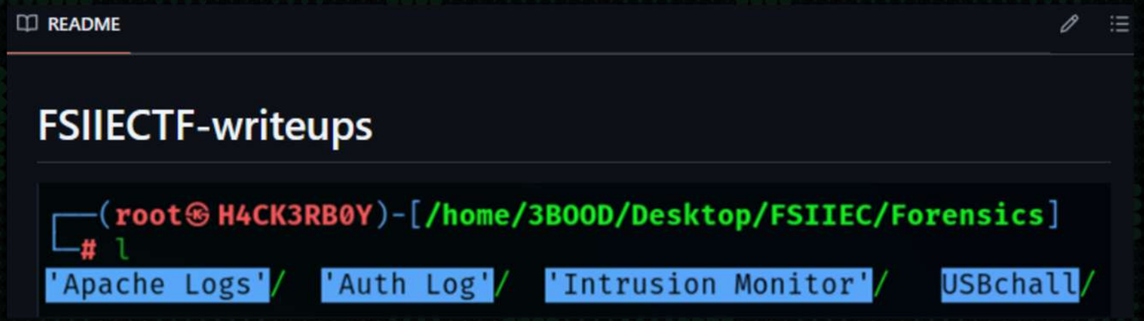
Purpose:

- Share knowledge.
- Document learning.
- Help others understand solutions.

Benefits:

- Improves skills.
- Supports community learning.





Platforms Recommended to Practice more

APU

Yemeni Students Community

SKR CTF

for beginners

CTFlearn

The most beginner-friendly way to learn cyber security.

HTB CTF

picoCTF

Let Us Connect :)

APU

Yemeni Students Community

Yazen

Abdulrahman

APU

Yemeni Students
Community

TOP 1

AGHM

APU

Yemeni Students
Community

TOP 2

a18m

APU

Yemeni Students
Community

TOP 3

MohamedHemdan

APU

Yemeni Students
Community

THANK YOU

YAZEN ABOBAKR AHMED AL-MEHDHAR & ABDULRAHMAN GAMIL MOHAMMED AHMED