
NYP INFOSEC DECEMBER
2024 CTF

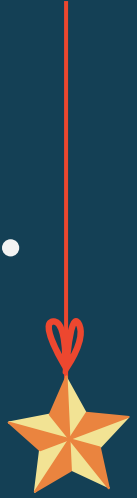

01
INTRO TO CTF
NYP INFOSEC DECEMBER 2024 CTF


01
INTRO TO CTF
BUT WHAT IS A CTF EVEN ABOUT?

BUT WHAT IS A CTF EVEN ABOUT?

CHALLENGE

Solve a variety of cybersecurity-related challenges and capture all the flags you can.



FLAGS

The Flag Format looks Something like this “NYP{I_<3_Th3_Se@s0n}”

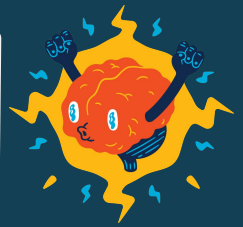
HIDDEN

Flags are usually hidden In vulnerable Program, Website or Cipher

7

CATEGORIES

CRYPTO



DESCRIPTION

- Challenges focus on decoding, decrypting, and analysing secure communications.
- Learn about ciphers, encryption algorithms, and cryptographic keys.
- Good tools: Cyberchef, dcode, hashcat

KEY CONCEPT

- Classical ciphers (Caesar, Vigenère)
- Modern encryption (AES, RSA)
- Hashing and cracking

2. WEB

DESCRIPTION

- Challenges involve discovering vulnerabilities in web applications.
- Exploit weak configurations, improper inputs, and server-side flaws.
- Good tools: BurpSuite

KEY CONCEPT

- Injection attacks
- Broken access controls
- Poor business logic
- Misconfigurations

3. FORENSICS

DESCRIPTION

- Investigate digital artifacts to uncover hidden data.
- Work with file systems, memory dumps, and logs, images.
- Good tools: Wireshark, metadata viewers (stegsolve, zsteg)

KEY CONCEPT

- File/Data Recovery
- Memory Analysis
- Log Analysis

4. REVERSE ENGINEERING

DESCRIPTION

- Analyze and understand compiled programs to find hidden secrets or vulnerabilities.
- Work with assembly code and software binaries.
- Good tools: Ghidra, IDA Pro

KEY CONCEPT

- Debugging
- Disassemblers
- Understanding Assembly Language & C

5. PWN / BINARY EXPLOITS

DESCRIPTION

- Exploit vulnerabilities in binaries to gain control or retrieve flags.
- Learn stack-based attacks, buffer overflows, and ROP chains.
- Goof tools: pwntools, GDB, ghidra

KEY CONCEPT

- Buffer Overflow
- Exploit Development
- Return-Oriented Programming (ROP)

6.

OSINT 

DESCRIPTION

- Use publicly available information to gather insights and data.
- Social media, websites, and public databases are key sources.
- Good tools: google

KEY CONCEPT

- Data mining
- Social media analysis
- Reconnaissance techniques

7

MISC

DESCRIPTION

- A variety of challenges that don't fit traditional categories.
- Test your creativity and problem-solving skills.

KEY CONCEPT

- Think outside the box

02

CTF RULES

I love following the rules

FLAG FORMAT

NYP{Sample_Flag}

DEAR SANTA...

- Do NOT hack or deny access to the CTF Server
- Do not ask for participants' IPs or network configurations.
- Hacking into others' computers is prohibited.
- No flag sharing – earn your own flags.
- Violation of these rules results in immediate disqualification.

CTF GUIDELINES

1. Kali activities are restricted to the CTF platform only (e.g., **no Nmap on public IPs** – it's illegal).
2. Do **not** attempt to scan, enumerate, or hack the CTF platform itself unless explicitly stated as part of a challenge.
3. Complete the feedback form for attendance taking.
4. Follow the **Computer Misuse Act** (CMA 1993).
5. Be mindful – illegal actions have serious consequences.


DISCLAIMER!!
Hacking unauthorized devices is **illegal** and punishable under the **Computer Misuse Act** and **Cybersecurity Act**.
Proceed responsibly –
DON'T SAY WE NEVER WARN YOU

03 EVENT SCHEDULE

25-26 Dec (Virtual)
27 Dec (Physical)

CTF SCHEDULE

WED 25 – DAY 1	THU 26 – DAY 2	FRI 27 – DAY 3
OPENING CEREMONY: 1130 – 1200	CTF CONTINUES	PHYSICAL @ LS32: 0900
CTF START – ALL CHALLENGES RELEASED 1200		PHYSICAL CHALLENGE RELEASE 0920
		END OF DEC CTF 1200
		CLOSING CEREMONY + NETWORKING SESSION 1230 – 1300

CTF THEME

I MEAN ITS PRETTY OBVIOUS

04

SANTA

The mastermind of Christmas, relying on your skills to save the holiday! 🎅

ELVES

Santa's tech-savvy helpers, guiding you through the challenges. 🛠️

GRINCH

The cunning hacker determined to ruin Christmas – stop them at all costs! 🐾

CTF PLATFORM INFORMATION

ACCESS THE CTF PLATFORM AT
HTTPS://CTFD.NYPINFOSEC.NET

LOGIN CREDENTIALS ARE SENT TO YOUR EMAIL - **CHECK YOUR SPAM FOLDER !**

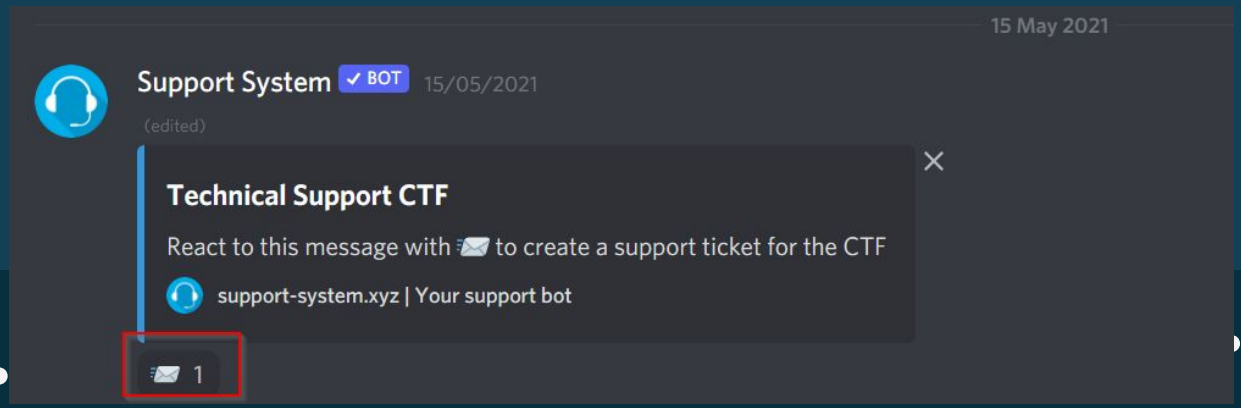
NOTIFY US ON DISCORD IMMEDIATELY IF YOU DIDN'T RECEIVE YOUR CREDENTIALS.

DISCORD:
CHECK YOUR SCHOOL EMAIL

TECHNICAL SUPPORT

For technical support, use the **#tech-support** channel in the Discord server.

Try not to DM EXCOs or subcomm members – the support system ensures faster assistance!



WRITEUPS

PLEASE DO MAKE

We encourage everyone to do a write up on how they solve the different challenges to share after the ctf

MORE WRITEUP!

To learn from one another as there are different ways to solve challenges


SO LETS SAVE
CHRISTMAS