

PLAYER 1



HIGHSCORE 2500



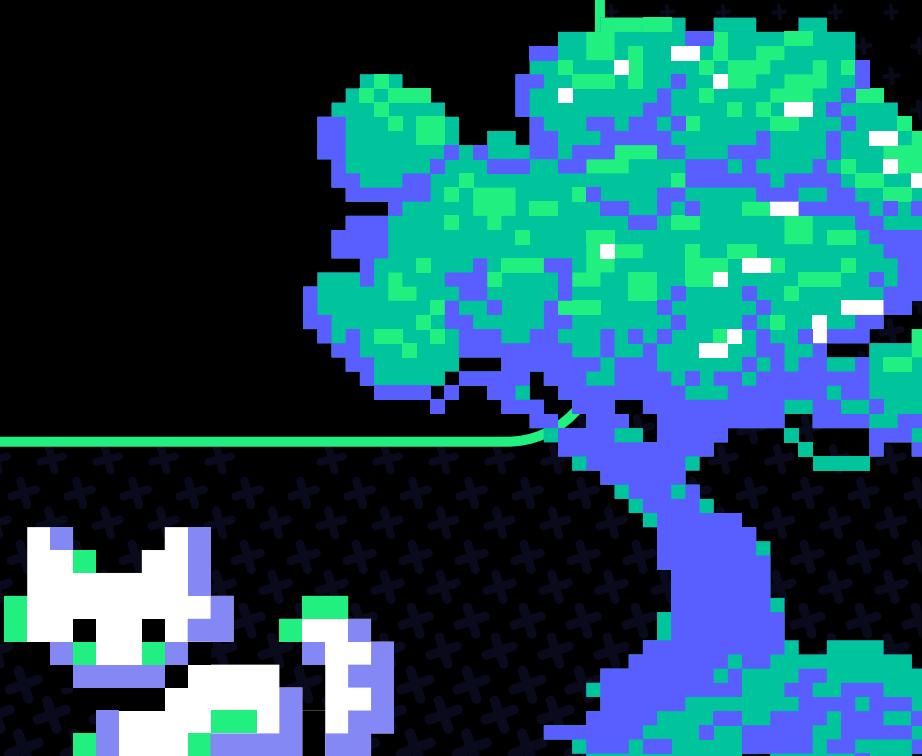
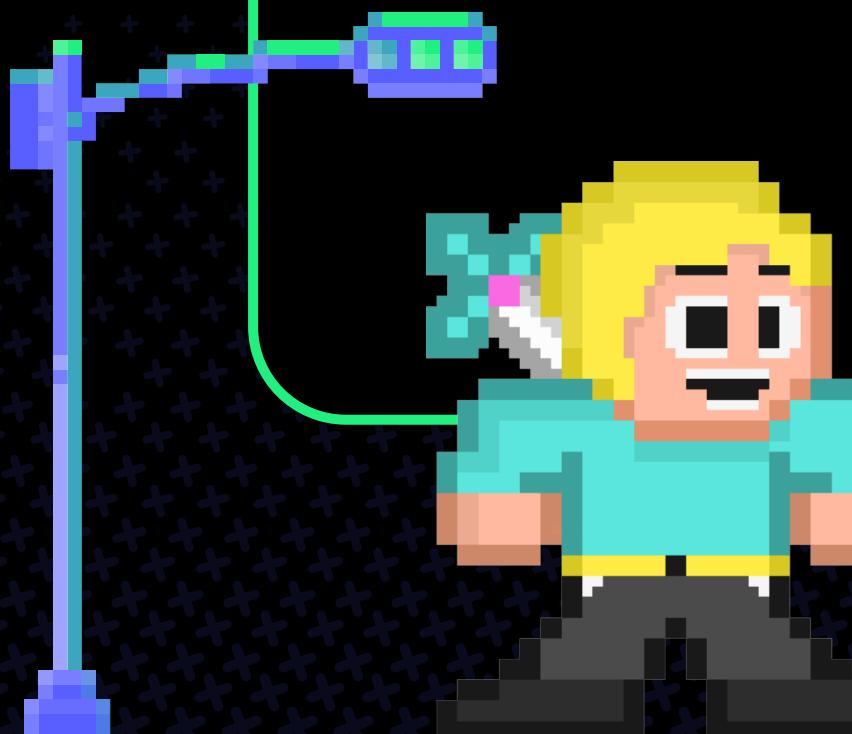
PLAYER 2

FLAG DIVE: INTRO TO CTF

START

MENU

SIGN IN



MENU

01

07

12



A BIT ABOUT ME

- NURUL HANAN - HANAN
- CYBERSECURITY LEARNER, BLOGGER, CTF
PLAYER & CHALLENGE CREATOR, SPEAKER,
ALUMNI MCC 2022, GCC 2023, MCC 2023
CREW
- ASSOCIATE IN MNC



NURUL

BACK TO
AGENDA PAGE

MENU

➡ 01

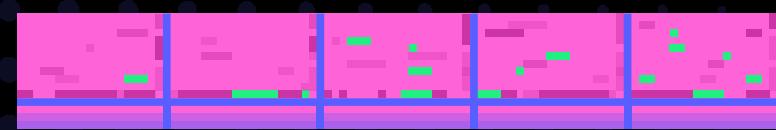
♦ 07

★ 12

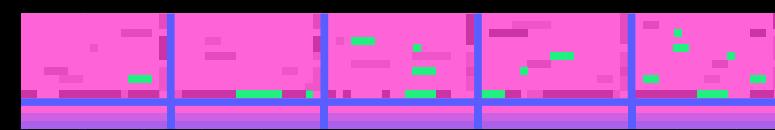


AGENDA

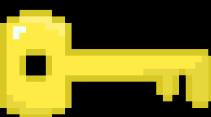
◆ TOPICS COVERED



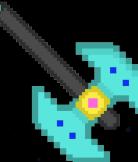
UNDERSTANDING
CYBERSECURITY



WHAT IS CTF?



COMMON CATEGORIES
IN CTF



CTF TRAINING
PLATFORM

SIGN IN

BACK TO AGENDA PAGE

UNDERSTANDING CYBERSECURITY



MENU



WHAT IS CYBERSECURITY?



CYBER + SECURITY

A PRACTICE IN PROTECTING COMPUTER SYSTEM, NETWORKS, DIGITAL ASSETS FROM POSSIBLE RISKS, UNAUTHORIZED THREATS, ACCESS, THEFT AND MALICIOUS ATTACKS.

VARIOUS TECHNIQUES AND APPROACHES ARE IMPLEMENTED TO ENSURE THE CONFIDENTIALITY, INTEGRITY AND AVAILABILITY OF THE DIGITAL ASSETS TO BE REMAINED SECURED.

MAIN GOAL: TO MITIGATE THREATS AND ENSURE THE SECURITY OF INDIVIDUALS AND ORGANIZATIONS

MENU



TEAMS



- ◆ DEFENSIVE SECURITY
DEFEND AND PROTECT SYSTEM NETWORK AGAINST CYBER THREATS AND ATTACKS

- ◆ OFFENSIVE SECURITY
FIND VULNERABILITIES AND BREAKTHROUGH THE DEFENSES OF THE SYSTEM

- ◆ GRC
GOVERNMENT & RISK COMPLIANCE ENSURES SYSTEM SECURITY IS AS ACCORDANCE TO THE STANDARD AND POLICY (ISO270001)



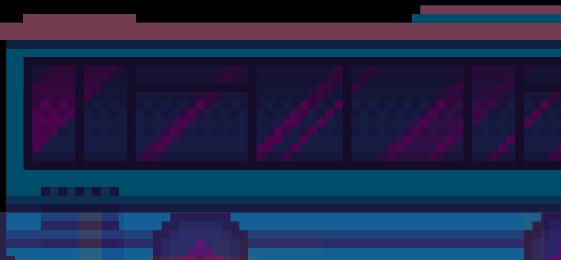
WHAT IS CTF?



C+T+F = CAPTURE + THE + FLAG

- CYBERSECURITY COMPETITION THAT REQUIRES PARTICIPANTS TO SOLVE RELATED SECURITY QUESTIONS AND PUZZLES IN ORDER TO OBTAIN FLAG.
- WINNER OF THE GAME GOES TO THE TEAM/PERSON THAT OBTAINS THE MOST FLAGS WITHIN TIME BEFORE THE END OF THE GAME.

SUBMIT MOST FLAGS -> GAIN HIGHEST SCORE ->
WINNER WINNER CHICKEN DINNER!



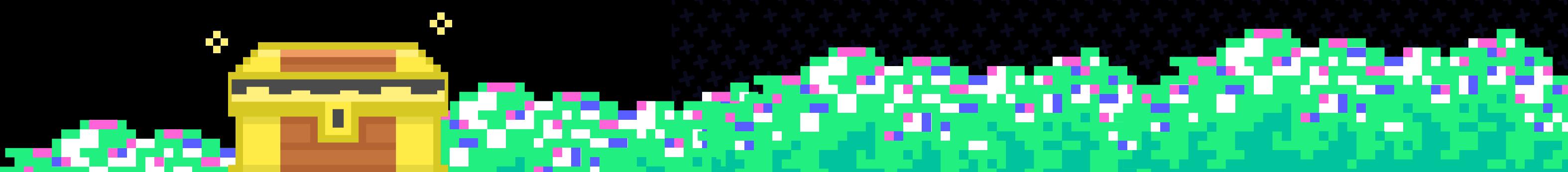
GAME FORMAT

JEOPARDY
STYLE

ATTACK &
DEFENSE

PHYSICAL

TIME ATTACK



JEOPARDY STYLE

- ➔ CHALLENGES AND PUZZLES ARE DIVIDED INTO VARIETIES OF CATEGORIES
- ➔ TEAMS ARE REQUIRED TO SOLVE THE QUESTIONS PROVIDED BY ORGANIZERS WITHIN THE TIME LIMIT
- ➔ THE TEAM WITH MOST SUBMITTED FLAG WINS

ATTACK & DEFENSE

- ❖ EACH PARTICIPATING TEAM HAS THEIR OWN ENVIRONMENT THAT MUST BE PROTECTED FROM BEING ATTACK BY OTHERS WHILE ATTEMPTING TO GAIN ACCESS OVER OTHER TEAMS' NETWORK OR SYSTEM
- ❖ TEAMS WILL BE GIVEN POINTS WHEN THEY SUCCESSFULLY GAIN ACCESS AND BREACH OPPONENT'S DEFENSE

HOWEVER TEAMS WILL BE PENALIZED IF THEIR OWN SYSTEM OR NETWORK ARE BREACHED

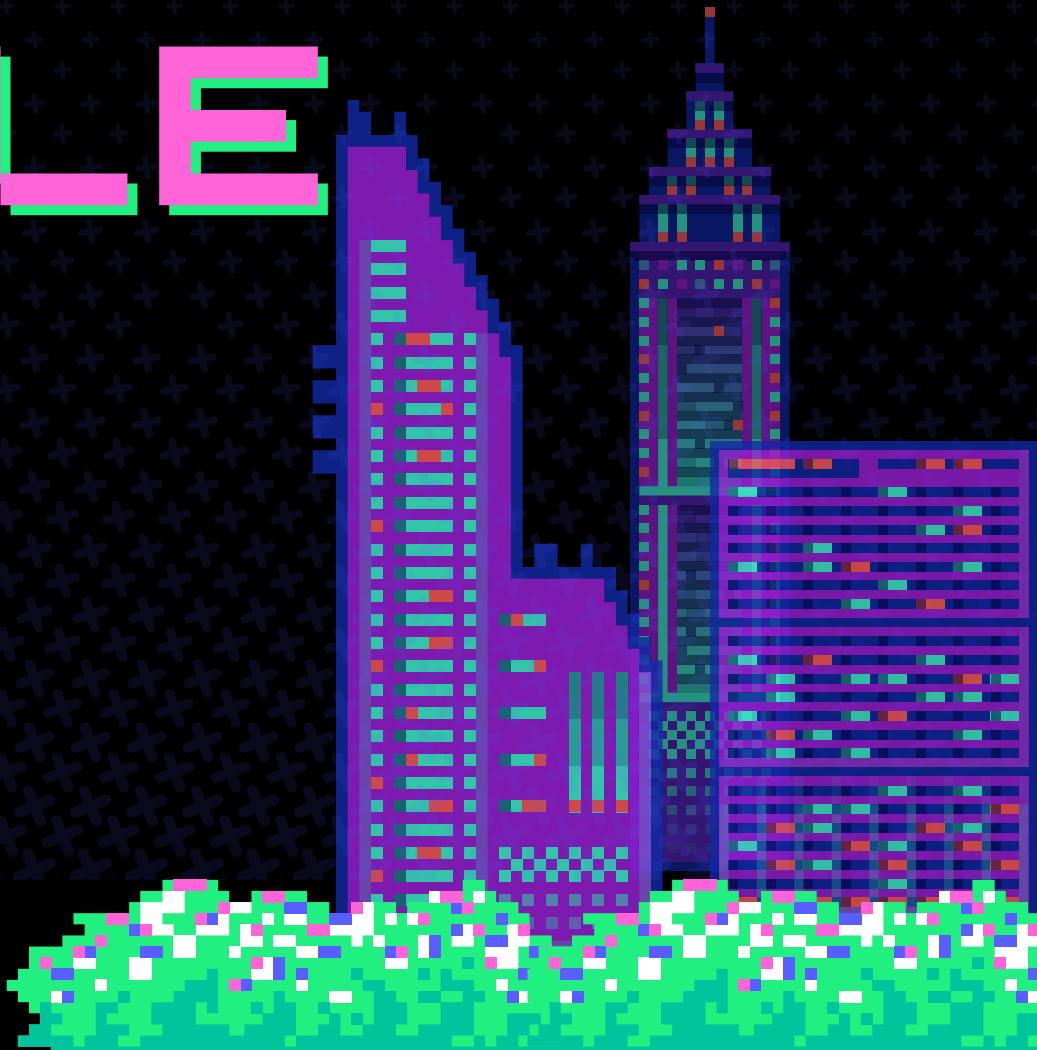
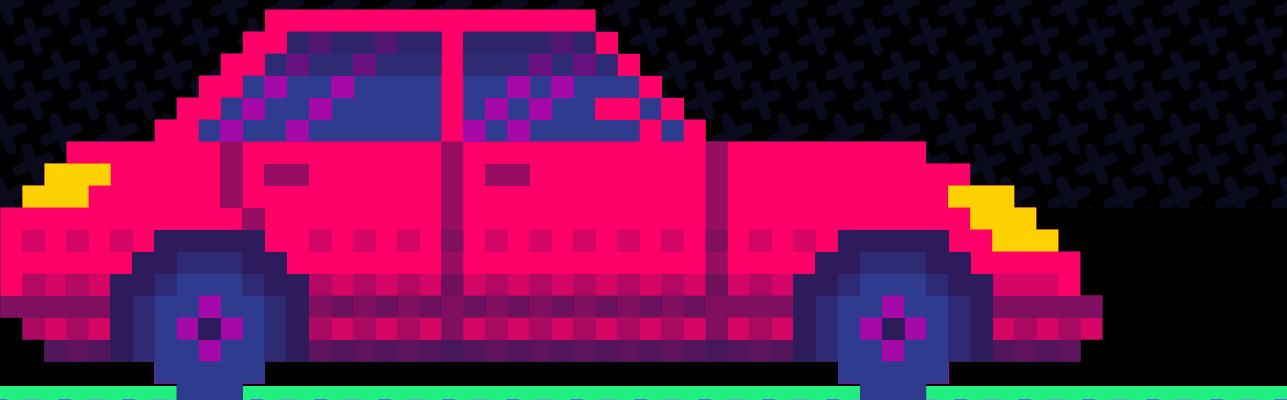
PHYSICAL

- ➔ CHALLENGES ARE MOSTLY RELATED TO PHYSICAL SECURITY (I.E, HARDWARE MANIPULATION)
- ➔ GOAL: TO DEMONSTRATE AN UNDERSTANDING OF PHYSICAL SECURITY CONCEPTS AND TECHNIQUES TO OVERCOME REAL-WORLD SCENARIOS .

TIME-ATTACK

- ◆ INVOLVES SOLVING AS MANY CHALLENGES AS POSSIBLE WITHIN A SET TIME LIMIT
- ◆ GOAL: TO DEMONSTRATE SKILLS UNDER TIME PRESSURE AND THINK QUICKLY TO SOLVE PROBLEMS WITHIN THE GIVEN TIME FRAME

COMMON
CATEGORIES IN
JEOPARDY STYLE
CTF





01



07



★ 12



WEB EXPLOITATION

FORENSICS

BINARY
EXPLOITATION/ PWN

STEGANOGRAPHY

MISCELLANEOUS

CRYPTOGRAPHY

REVERSE
ENGINEERING

BOOT2ROOT

OSINT

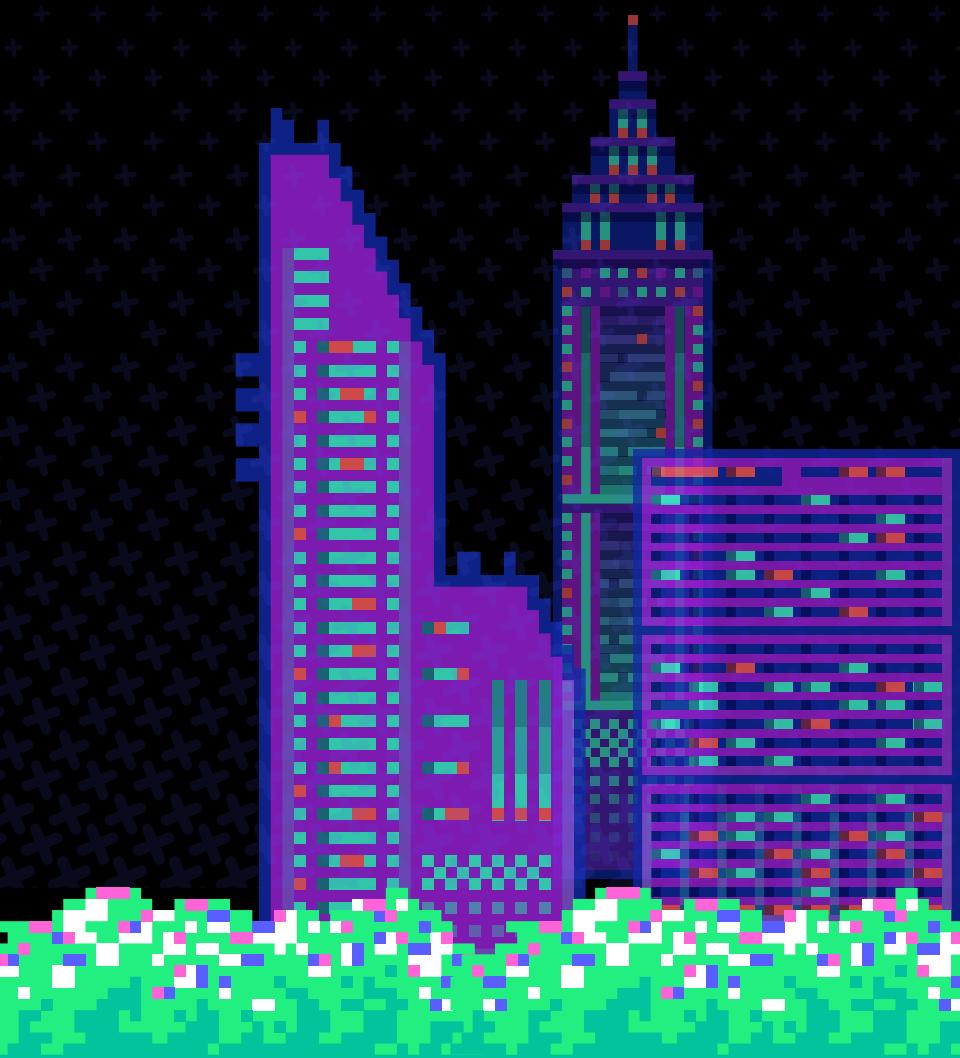
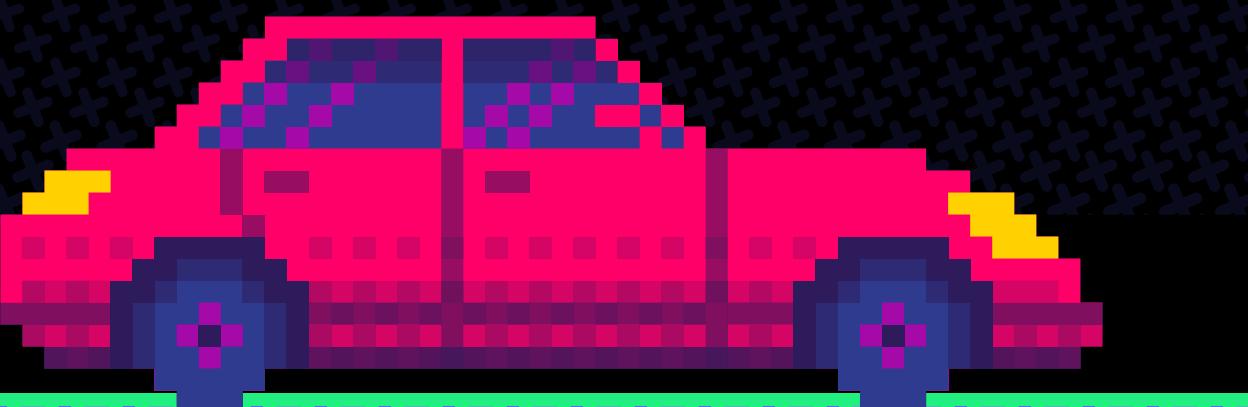
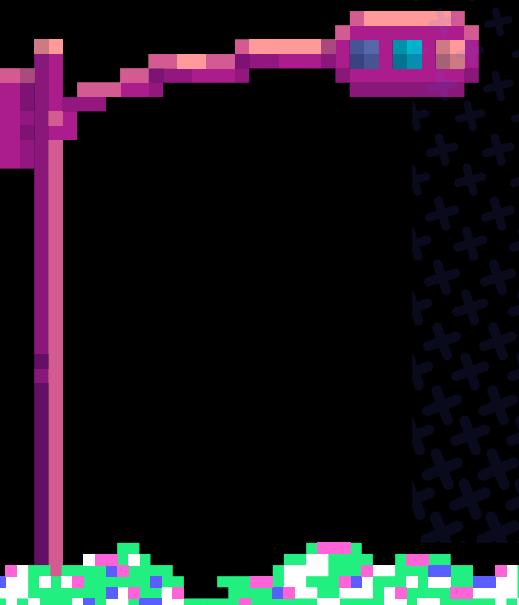
MENU



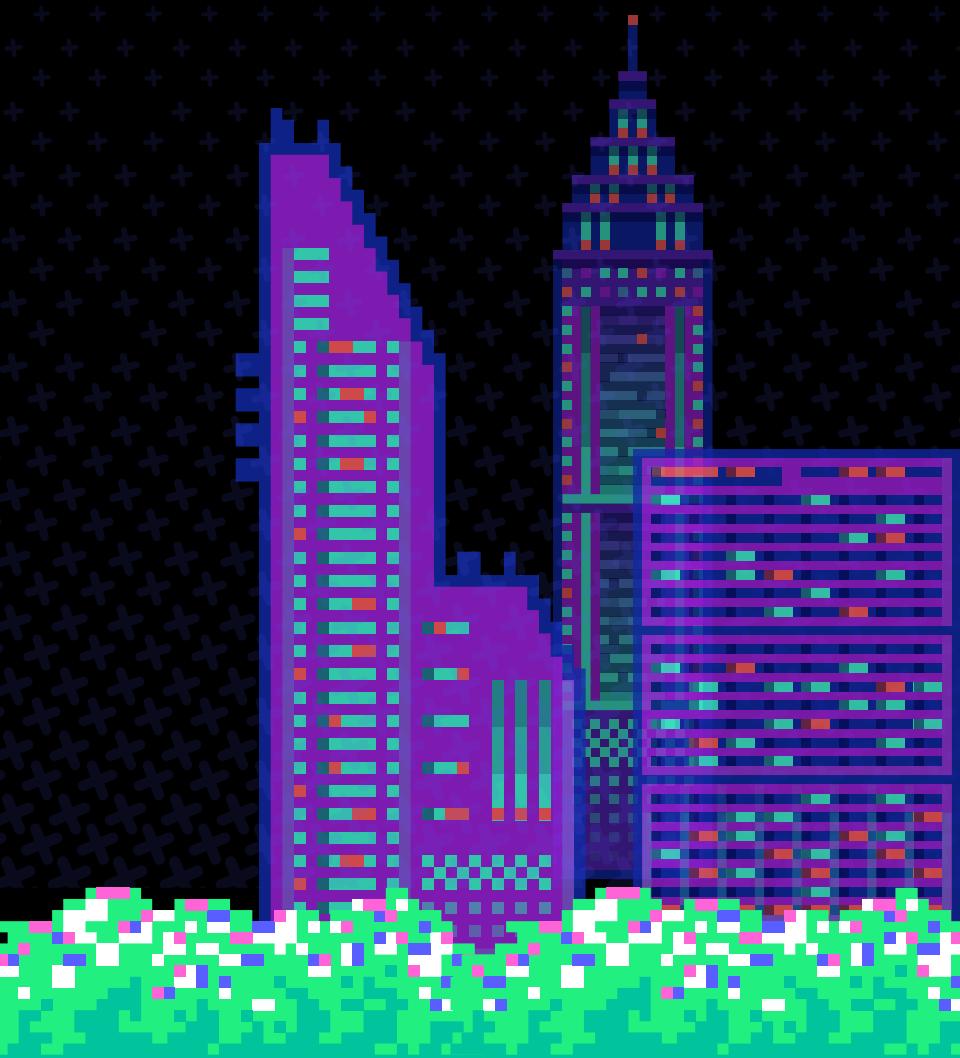
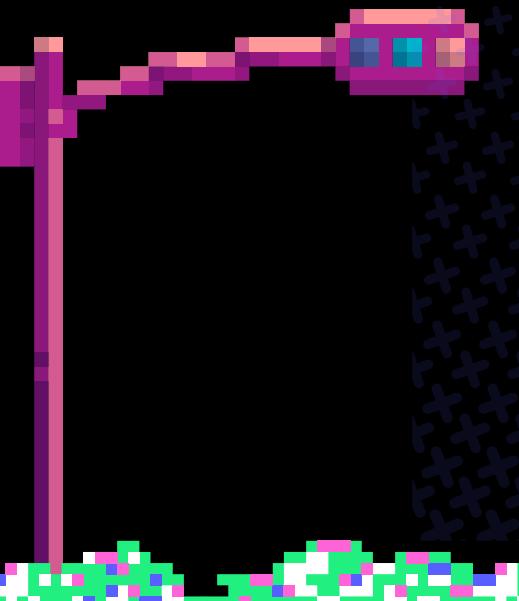
SCORING FORMAT

- ◆ JEOPARDY-STYLE/STATIC FORMAT
EACH QUESTIONS HAS ITS OWN SCORE.
FIRST SOLVER, RANKS TOP FOR THE
QUESTION.
- ◆ DECAYING/DYNAMIC FORMAT
FIRST SUBMISSION OF CORRECT
FORMAT, GETS THE HIGHEST SCORE FOR
THE QUESTION. SCORE DECREASES AS
MORE CORRECT SUBMISSION OF FLAGS
- ◆ ATTACK-AND-DEFENSE FORMAT
YOU GET POINTS WHEN YOU
SUCCESSFULLY ATTACK AND DEFENSE
YOUR SYSTEM & NETWORK. FAILED TO
DO SO, LOSE POINTS.

TIPS & TRICKS



DEMONOWU?



DEMO

CATEGORY: OSINT

CHALLENGE: LITTLE NAVILERRA HIDING

WHILE THE KEY TO UNLOCK HOLDS BY NAVILLERA, SHE WENT HIDDEN FROM THE WORLD...UNTIL ONE DAY...WE FIGURED OUT SHE FORGOT TO ERASE HER TRACE.

HER X WAS LEAKED

FIND THE KEY TO UNLOCK THE FORBIDDEN.

FLAG FORMAT: FLAGD!VE{FLAG}

FLAG

DEMO

CATEGORY: OSINT

CHALLENGE: LITTLE NAVILERRA HIDING

WHILE THE KEY TO UNLOCK HOLDS BY NAVILLERA, SHE WENT HIDDEN FROM THE WORLD...UNTIL ONE DAY...WE FIGURED OUT SHE FORGOT TO ERASE HER TRACE.

HER X WAS LEAKED

FIND THE KEY TO UNLOCK THE FORBIDDEN.

FLAG FORMAT: FLAGD!VE{FLAG}

FLAG

WRONG

DEMO

CATEGORY: OSINT

CHALLENGE: LITTLE NAVILERRA HIDING

WHILE THE KEY TO UNLOCK HOLDS BY NAVILLERA, SHE WENT HIDDEN FROM THE WORLD... UNTIL ONE DAY... WE FIGURED OUT SHE FORGOT TO ERASE HER TRACE.

HER X WAS LEAKED

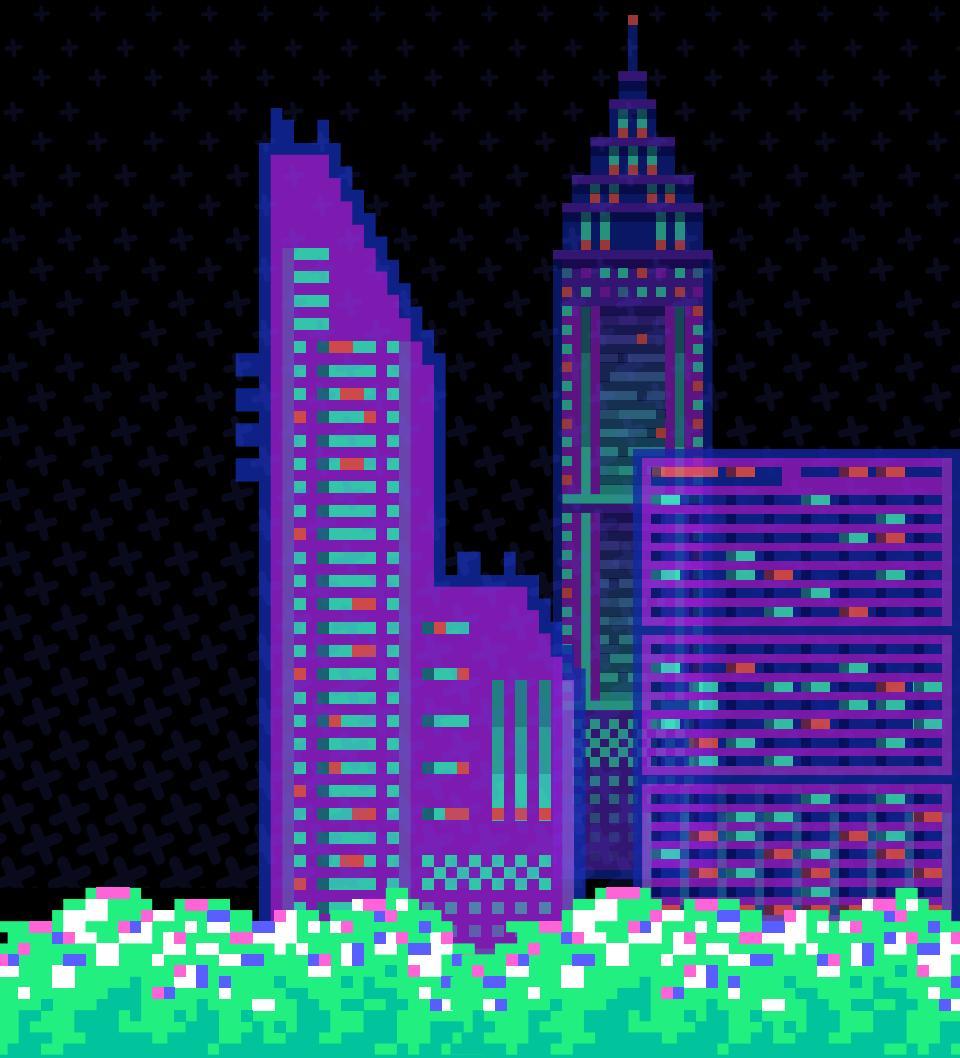
FIND THE KEY TO UNLOCK THE FORBIDDEN.

FLAG FORMAT: FLAGD!VE{FLAG}

FLAGD!VE{OSINT_EAZY_PEAZY}

CORRECT

FAMOUS CTF TRAINING PLATFORMS



FREE PLATFORM

picoCTF

OverTheWire

SKRCTF

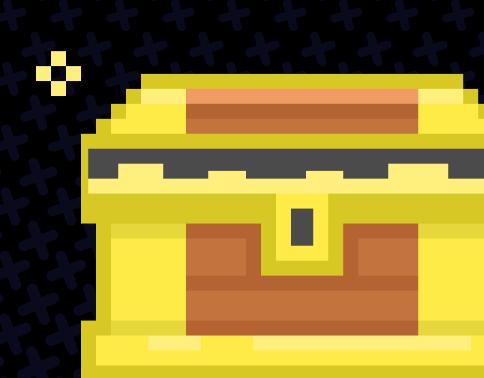
PARTIALY FREE PLATFORM

TryHackMe

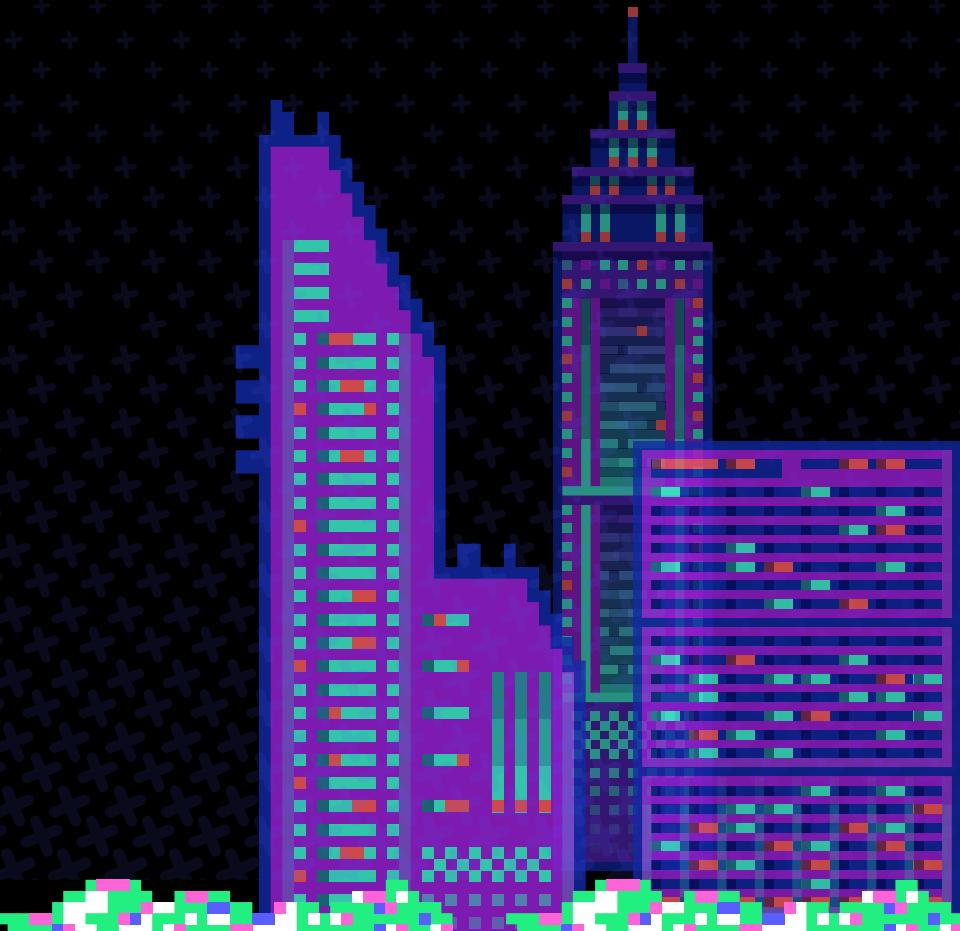
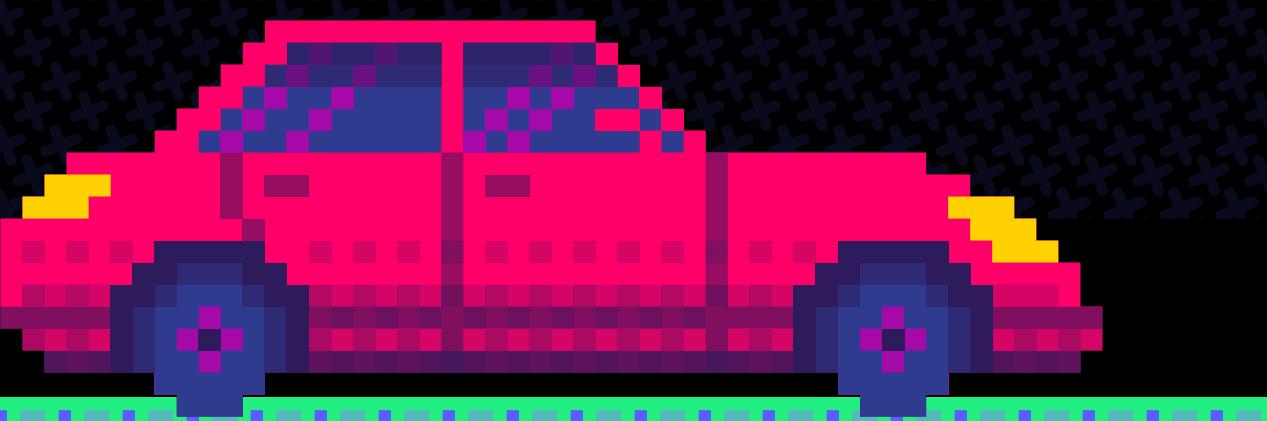
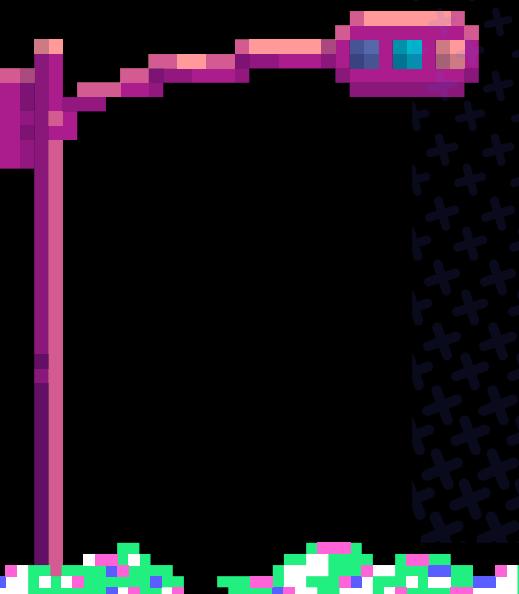
HackTheBox

Let's Defend.io

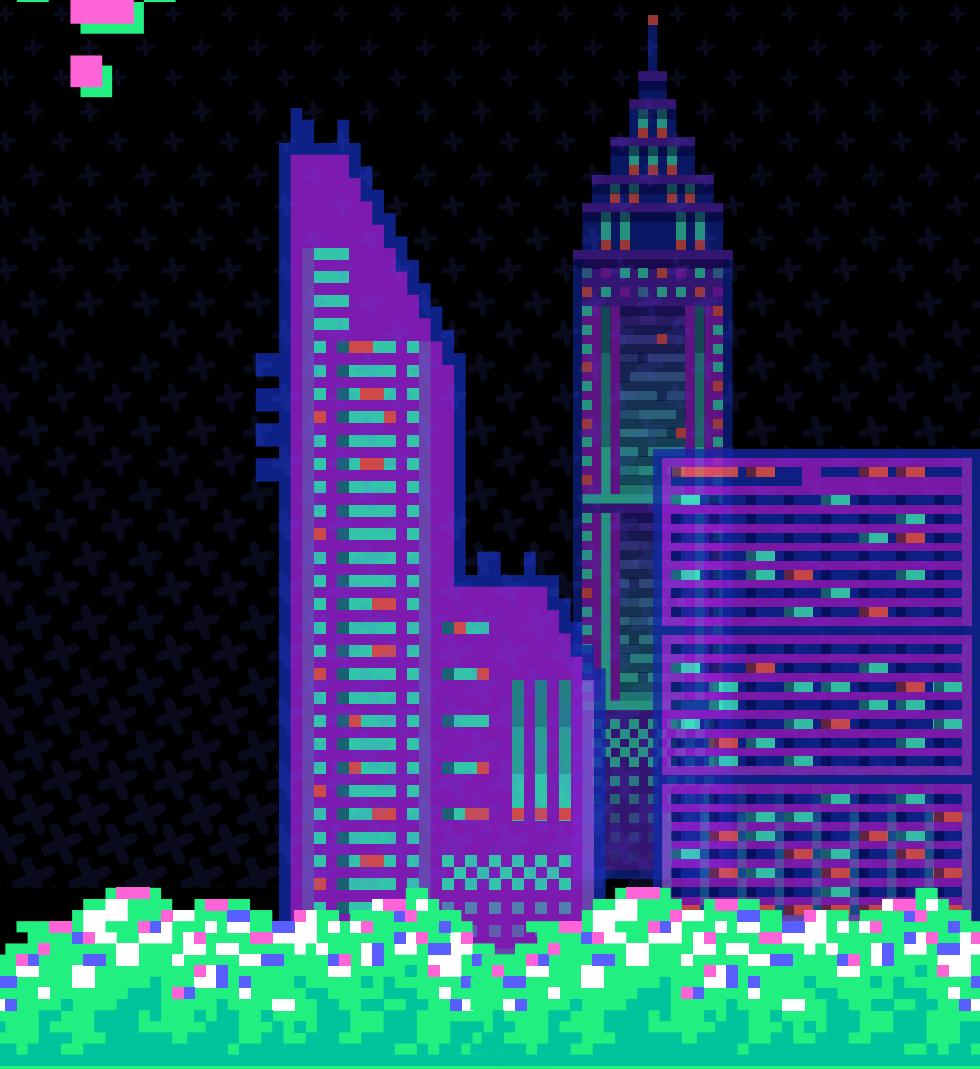
**Feel free to checkout CTFtimes to get more
updates on current and on-going CTF
competition worldwide!**



**COMMON TOOLS
USED FOR CTF**



ANOTHER DEMO?



LET'S CONNECT

Feel free to connect with me:

- www.linkedin.com/in/nurulhanan791

