It’s just a game

> whoami

-

> whoami

- Lorenzo Demeio (**not** De Meio, Demeglio or De Meglio)

> whoami

- Lorenzo Demeio (**not** De Meio, Demeglio or De Meglio)
- Graduated in Cryptography at the University of Trento

> whoami

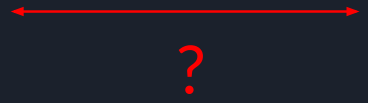
- Lorenzo Demeio (**not** De Meio, Demeglio or De Meglio)
- Graduated in Cryptography at the University of Trento
- CTF organizer with the Cybersecurity National Lab since 2022

> whoami

- Lorenzo Demeio (**not** De Meio, Demeglio or De Meglio)
- Graduated in Cryptography at the University of Trento
- CTF organizer with the Cybersecurity National Lab since 2022
- CTF player with **about:blankets** – **Devrar**

Why are we here?

“CTF & Offensive Security for Risk Management Awareness”

CTF World  Real World

What is a CTF?

Capture The Flag

In computer security, **Capture the Flag (CTF)** is an **exercise** in which participants attempt to find text strings, called "flags", which are secretly hidden in purposefully vulnerable programs or websites.

What is a CTF?

Capture The Flag

In computer security, **Capture the Flag (CTF)** is ~~an **exercise**~~ a game in which participants attempt to find text strings, called "flags", which are secretly hidden in purposefully vulnerable programs or websites.

What is a CTF?

Game

A **game** is a **structured** type of **play**

Why playing?

- Is it useful for your job?
- Is it useful for networking?
- Do you make money with it?

Why playing?

- Is it useful for your job? Yes, it can be
- Is it useful for networking?
- Do you make money with it?

Why playing?

- Is it useful for your job? Yes, it can be
- Is it useful for networking? Sometimes
- Do you make money with it?

Why playing?

- Is it useful for your job? Yes, it can be
- Is it useful for networking? Sometimes
- Do you make money with it? Absolutely not

The first connection

The first connection

Why playing?

To solve a challenge you have to go through the process of **studying**, **understanding** and **applying**

The first connection

Why playing?

By playing you learn **theory**, **techniques** and **skills** that can be used in the **real world**

Gamification

This first connection is the perfect application of the concept of **gamification**

Gamification

Gamification is the process of integrating game design elements and principles into non-game contexts. The goal is to increase user engagement and motivation through the use of game elements such as points, badges, leaderboards, and more.

Gamification

This first connection is the perfect application of the concept of **gamification**

Capture The Flag

A **Capture The Flag (CTF)** is the result of the **gamification** of real-world offensive security

Gamification

This first connection is the perfect application of the concept of **gamification**

Capture The Flag

A **Capture The Flag (CTF)** is the result of the **gamification** of real-world offensive security ?

The game goes on

- Once you've created a **game**, you've created the possibility of **complexity**
- The simpler the rules, the higher the complexity
- Challenges of higher complexity are often not from the real world

An example

Sus (ImaginaryCTF 2023)

```
def sus(sz, d):
    while True:
        p = getPrime(sz)
        pp = sum([p**i for i in range(d)])
        # pp == p**2 + p + 1
        if isPrime(pp):
            return p, pp


p, q = sus(512, 3)
r = getPrime(512 * 3)
n = p * q * r
```

An example

Sus (ImaginaryCTF 2023)

```
while True:
    Gx, Gy = (randint(1, 100), randint(1, 100))
    E = EllipticCurve(Zmod(n), [0, Gy**2 - Gx**3])
    G = E(Gx, Gy)
    n*G
```

Is the connection lost?

- Challenges often are **not related** to the real world anymore
- The theory, techniques and skills you learn are **hardly applicable** to the real world
- The things you learn are very specific and often **don’t generate** a deeper **knowledge**

Is the connection lost?

Are these high-complexity CTFs just a game?

Yes, but that doesn’t mean they don’t have an **impact** on the **real world**

A deeper connection

A deeper connection

- The challenges contain **high-complexity problems**
- The player has to districate between this complexity
- The complexity of the problems is still **connected to the real world**, even though the topic of the challenge may not be. For example (from the crypto world):
  - Understanding the **mathematical structure** behind the problem
  - Understanding where the **information** is leaked
  - Getting a feeling of where there is something "**unusual**"
- The skill of "**navigating**" this kind of complexity is what remains from these challenges
- This skill is then **crucial in the real world**

Why playing?

Why playing?

To deal with the complexity and to learn how to navigate it

Why playing?

Why playing?

And because we love the game

Thank you for the attention!