

Empowering Cybersecurity Outreach and Learning through Collaborative Challenge Building, Sharing, and Execution

Alexandre Dulaunoy, David Durvaux and Renato Otranto Jr.

CIRCL, European Commission, CERT.br

2024

In a few word explain why a ctf is important



A Capture the Flag (CTF) competition is important because it promotes hands-on learning in cybersecurity, enhances problem-solving skills, fosters teamwork, and helps identify and develop talent in the field.

does it contribute to outreach and building communities?



Yes, CTF competitions contribute to outreach and community building by attracting a diverse group of participants, encouraging collaboration and knowledge sharing, and fostering a sense of camaraderie among cybersecurity enthusiasts.



Agenda

Why a CTF at FIRST?

Gamification as a Vehicle for Sharing Knowledge

Does Gamification Mean CTF?

Pitfalls and points of attentions

Statistics and figures

Conclusion

Who we are?

We are all FIRST SIG SecLounge members and long time CTF contributors.

Table of Contents

Why a CTF at FIRST?

Gamification as a Vehicle for Sharing Knowledge

Does Gamification Mean CTF?

Pitfalls and points of attentions

Statistics and figures

Conclusion

Goals and Objectives of the FIRST CTF

The CTF at FIRST.org is designed to support the objectives and goals of our community, specifically to:

- ▶ Reinforce the FIRST.org community
- ▶ Spread and share knowledge
- ▶ Foster trust and collaboration
- ▶ Reach out to new communities

Additionally, it aims to offer a **fun experience** for everyone involved, including the organisation team!

How Does the CTF Differ?

The CTF¹ is unique because it is designed to:

- ▶ Reach a large audience, including both technical and non-technical participants
- ▶ Cover many aspects, including non-technical ones
- ▶ **Promote constructive behaviours** instead of destructive ones, showing that DFIR can be fun
- ▶ Serve as an entry point to motivate and engage new audiences (outreach)
- ▶ **Promote diversity and encourage teams** with complementary profiles.

¹In the scope of the FIRST CTF objectives

Why the Competitive Aspect?

- ▶ Humans usually love games, challenges, or just enjoy satisfying their curiosity
- ▶ Humans tend to **be competitive while also valuing collaboration**
- ▶ Competition creates an environment with a certain pressure that pushes players to surpass themselves.

And from all of this, what do people get? They learn new skills, make new friends, and learn to work in teams.

Why the Competition or Scoring Aspects?

- ▶ While **competition** (with winners and scoring tables) could be seen as negative,
- ▶ We observe that teams compete in a friendly and respectful manner (even sometimes helping competitors)
- ▶ And usually with **great respect** for both fellow competitors and the organisation² team.

²The organization team can be considered as players too

How Can a CTF Be a Learning Process?

- ▶ CTF³ can be an improved learning model due to multiple factors:
 - ▶ **Active learning**: Applying theoretical knowledge, **group motivation**
 - ▶ Immediate feedback⁴ via scoring
 - ▶ Focusing on **problem-solving** and creative solutions, which are important strategies in day-to-day cybersecurity activities.

³Will you remember this talk?

⁴Did you ever receive immediate feedback on a DFIR report?

Table of Contents

Why a CTF at FIRST?

Gamification as a Vehicle for Sharing Knowledge

Does Gamification Mean CTF?

Pitfalls and points of attentions

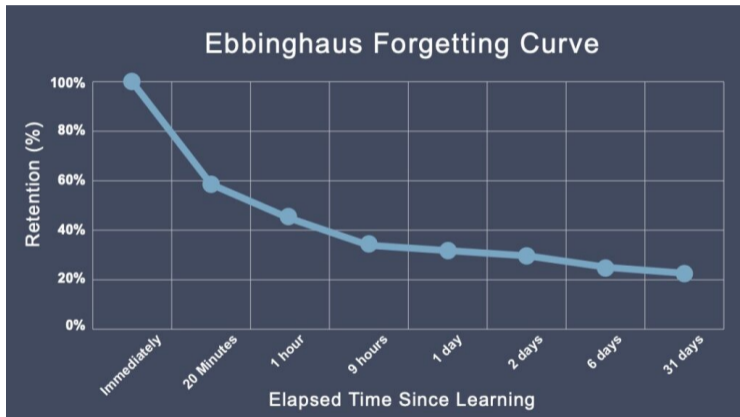
Statistics and figures

Conclusion

How long does it take to forget 90% of what you learn?

- ▶ 1 day
- ▶ 1 week
- ▶ 1 month
- ▶ 1 year
- ▶ 10 years?

The Forgetting Curve: Research⁵ shows that people forget about 90% of what they learn within a month if there is no reinforcement.



⁵Memory: A Contribution to Experimental Psychology, Hermann Ebbinghaus

How CTFs Help and Become an Educational Strategy

- ▶ **Active Learning:** Engages participants, making learning memorable.
- ▶ **Immediate Feedback:** Helps reinforce knowledge through instant correction.
- ▶ **Repetition and Practice:** Reinforces memory by regularly engaging with material.

Lifelong Learning: If you learn how to find the answer, the content itself matters less. You gain confidence and experience in finding answers on your own, which can last a lifetime.

A little bonus...

Playing the CTF this week?

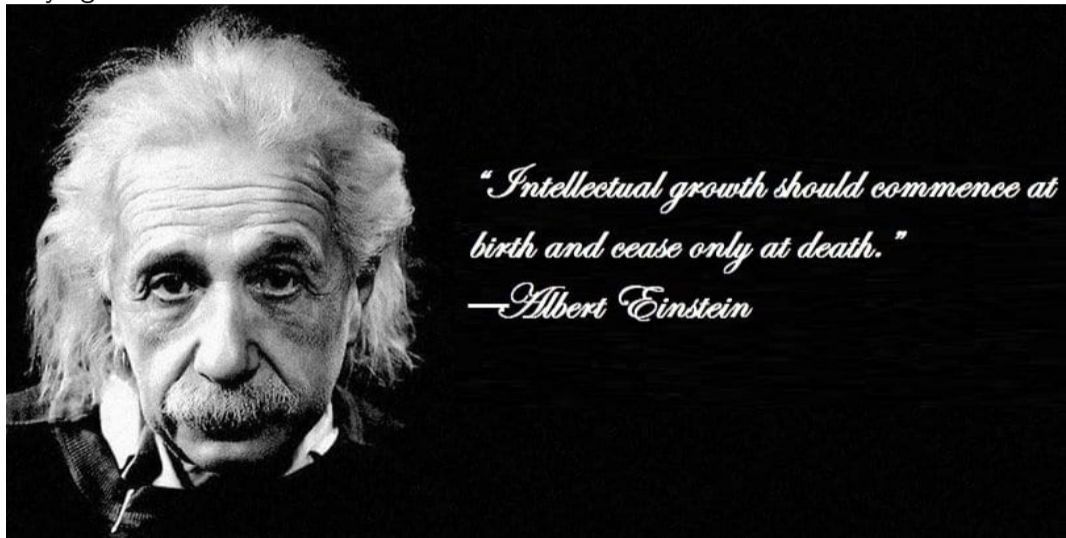


Table of Contents

Why a CTF at FIRST?

Gamification as a Vehicle for Sharing Knowledge

Does Gamification Mean CTF?

Pitfalls and points of attentions

Statistics and figures

Conclusion

What is Gamification in CTF?

- ▶ **Gamification** is the application of game-design elements and game principles in non-game contexts to engage and motivate people to achieve their goals. It leverages elements like points, levels, badges, leaderboards, and challenges to make tasks more engaging and enjoyable.
- ▶ **Capture The Flag (CTF)** is a specific type of gamified competition commonly used in the field of cybersecurity. Participants solve security-related challenges to capture "flags," which are typically pieces of code or information hidden within the challenges.

Risks of Gamification in CTFs

- ▶ **Captive Attention:** The gaming model can sometimes overshadow the educational aspect, reducing the focus on learning.
- ▶ **Balance Between Fun and Learning:** It is critical to maintain a balance between the game elements, fun, and educational objectives while designing challenges.
- ▶ **Design Strategy:** The design strategy of a CTF should embrace playfulness without forgetting the original goals of the FIRST CTF, ensuring it remains a valuable educational tool.

Gamification in CTFs

- ▶ Gamification **blurs the lines** between cybersecurity activities⁶ and play.
- ▶ The gamification of the CTF at FIRST benefits the community at large, rather than just the CTF owners⁷.

⁶Do you prefer to participate in a workshop or play with friends?

⁷For other hackathons/CTF, this is not always the case

Table of Contents

Why a CTF at FIRST?

Gamification as a Vehicle for Sharing Knowledge

Does Gamification Mean CTF?

Pitfalls and points of attentions

Statistics and figures

Conclusion

Does Playing and Organising a CTF Look Like This?



Unfortunately not...

Common Issues in CTFs

- ▶ **Challenge Misalignment:** Challenges may not match the skill levels or interests of the audience.
- ▶ **Competition with Conference Content:** CTFs can sometimes distract from or compete with the main conference sessions.
- ▶ **Lack of Engagement:** Participants might lose interest if the CTF is not engaging or rewarding enough.
- ▶ **Cultural and Gender Inclusivity:** Ensuring the CTF is inclusive and respectful of diverse cultures and genders.
- ▶ **Cheating:** Maintaining the integrity of the competition by preventing and addressing cheating.

Challenge Misalignment

- ▶ **Skill Level Mismatch:**

- ▶ If challenges are too difficult, beginner participants might feel overwhelmed and discouraged, leading to frustration and disengagement.
- ▶ If challenges are too easy, advanced participants might find the competition uninteresting and not stimulating enough.

- ▶ **Irrelevant Content:** Challenges that are not relevant⁸ to the participants' field or current industry trends may fail to engage them. For example, a challenge focused on outdated technology or techniques may not be as engaging.

⁸Crazy CTF content creator who forgot about the audience...

Lack of Engagement and Risks

- ▶ **Low Participation Rates:** Participants dropping out early, lack of attention, or being distracted by other activities.
- ▶ **Minimal Collaboration:** Challenges lacking collaboration between participants⁹ and limited interaction among participants.

⁹Collaboration is key to maintaining engagement

Cultural Sensitivity and Gender Inclusivity

- ▶ **Diverse Content:** Ensure challenges are relevant and respectful¹⁰ to a global audience.
- ▶ **Challenge Design:** Have a diverse team¹¹ to create and test challenges, ensuring fairness.
- ▶ **Inclusive Challenges:** Provide non-technical challenges and mix audiences to promote inclusivity and engagement.

¹⁰Humor can be very different between countries

¹¹Please join us!

Cheating

Every year we face cheating and sometimes aggressive behaviours:

- ▶ Fake accounts/teams created to test flags and retrieve hints
- ▶ Attempts to pressure or blame the CTF team
- ▶ Oversized teams with unreasonable off-site support
- ▶ Other forms of rule violations.

Since there is an incentive (prizes/recognition) to win, it also reveals the unpleasant side of human nature. In the end, **a CTF is just a game.**

How to Detect Cheating?

1. Keep logs (we are in cybersecurity, after all!)
2. Many hints requested with a very low submission ratio
3. Two teams submitting flags in a short time window.
4. Many flags submitted in a very short time span (when the CTF is not paused)
5. Generate rotating flags (unique values)
6. ...

This is not an exhaustive list! Keep in mind, **CTF and cheating will coexist.**

Key for success: preparation...

The FIRST CTF takes about **1 year to prepare**.

1. Establish a **team** of motivated volunteers (they are all super motivated!)
2. Identify what you want to achieve (goals)
3. Identify the topics you want to cover and ensure you have the skills you need
4. Ensure you have the appropriate logistics (you can't imagine the effort put in by the FIRST staff)
5. Establish a work plan and ensure you stay on track (we have a hard deadline)
6. Build, update & maintain supporting infrastructure (5 servers)
7. Review and test challenges
8. Ensure proper players support on-site or remotely.

This is proper **project management**. Don't underestimate.

Replays are also time consuming.

Table of Contents

Why a CTF at FIRST?

Gamification as a Vehicle for Sharing Knowledge

Does Gamification Mean CTF?

Pitfalls and points of attentions

Statistics and figures

Conclusion

Some statistics

On average, the CTF record active participation from

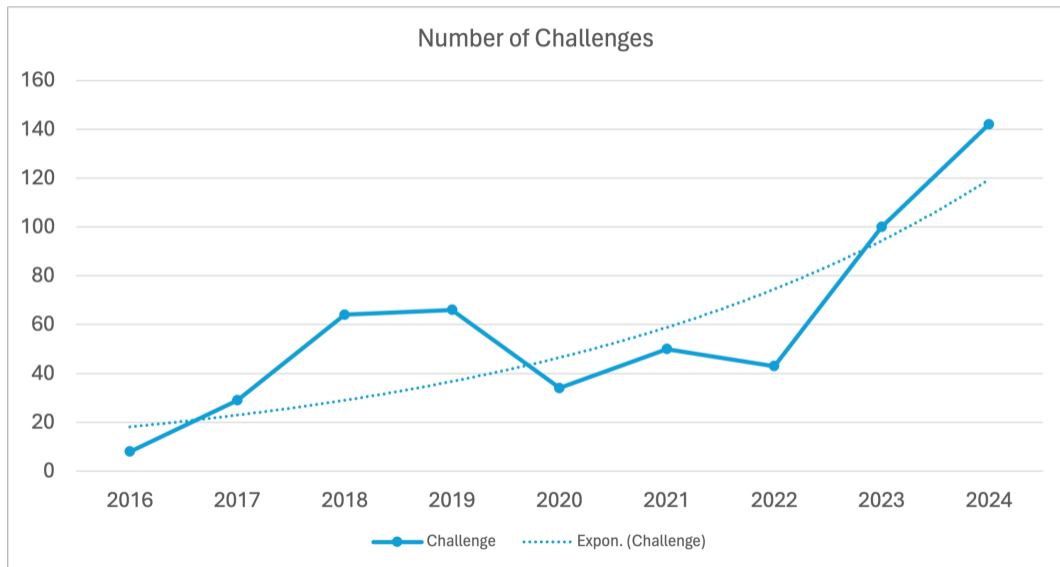
- ▶ 189 players
- ▶ 92 teams

The 2 virtual edition (COVID) in 2020 and 2021 registered record participation with

- ▶ up to 699 active players
- ▶ up to 160 teams

The 2020 event was open to all at no cost demonstrating the outreach it can produce. The 2021 was linked to the virtual edition of the FIRST Annual Conference (participation was lower).

Evolution of the Number of Challenges



Replays

Since 2023, we have introduced replays to expand the outreach of FIRST and promote knowledge sharing. The CTF has been replayed:

- ▶ in October 2023 for a joint LACNIC / FIRST event in Brazil
- ▶ in October 2023 for hack.lu (CIRCL) in Luxembourg
- ▶ in December 2023 for the Norwegian CERTs

More replays are planned for 2024:

- ▶ for Laos and Cambodia
- ▶ for the Association of Southeast Asian Nations (ASEAN) in July 2024
- ▶ ...

Permanent CTF

Since 2012, we have built a database of **over 600 challenges** and **have introduced a permanent learning platform** at <https://ctf.first.org>.

Our goals are to:

- ▶ Share the knowledge of the FIRST community with anyone willing to learn (it's free and open without restriction)
- ▶ Train individuals interested in learning and joining the field (outreach)
- ▶ Provide a channel to attract new talents (diversity and inclusion)

We need support from the FIRST community!

Special thanks to CERT-MC and SWITCH for covering the costs!

Table of Contents

Why a CTF at FIRST?

Gamification as a Vehicle for Sharing Knowledge

Does Gamification Mean CTF?

Pitfalls and points of attentions


Statistics and figures

Conclusion

Conclusion

Hosting a CTF at FIRST is an enjoyable experience, but it offers **much more than just fun...**

- ▶ It complements the FIRST training catalog¹²
- ▶ It serves as a valuable outreach opportunity
- ▶ It promotes diversity and inclusion
- ▶ It represents a significant contribution from the FIRST.org community to the broader cybersecurity field
- ▶ ...

¹²CTFs are an inherent part of the Services/Exercises (9.3) in the FIRST CSIRT Services Framework 

Thanks!

The CTF could not exist without the long-term support of the following organization and many volunteers! This year's CTF team:

- ▶ Ioannis Agrafiotis (ENISA)
- ▶ Aaron Allen
- ▶ Olivier Caleff
- ▶ Andrzej Dereszowski (European Commission)
- ▶ Alexandre Dulaunoy (CIRCL / MISP Project)
- ▶ David Durvaux (European Commission)
- ▶ Tobias Dussa (DFN-CERT)
- ▶ Robert Floodeen (New Anderton)
- ▶ Dan Gioca (European Commission)
- ▶ Jan Gocnik (Team Europe)
- ▶ Pedram Hayati (SecDim)
- ▶ Cristine Hoepers (CERT.br)
- ▶ Aaron Kaplan (European Commission)
- ▶ Alexia Konstantinidi (Team Europe)
- ▶ John Kristoff (Dataplane.org)
- ▶ Sanne Maasackers (Team Europe)
- ▶ Renato Otranto Jr. (CERT.br)
- ▶ Bart Parys (NVISO)
- ▶ Vasiliki Politopoulou (European Commission)
- ▶ Timo Porjamo (CSC.fi)
- ▶ Luciano Righetti (CIRCL / MISP Project)
- ▶ Jessica Schumacher (SWITCH)
- ▶ Efstratios Skleparis (European Commission)
- ▶ Klaus Steding-Jessen (CERT.br)
- ▶ Christina Skouloudi (ENISA)
- ▶ Richard Weiss (Team Europe)
- ▶ DHS CISA
- ▶ Idaho National Labs (INL)

Final Thank You

The CTF would not exist without your support!

A heartfelt thank you to all the players! We deeply appreciate your enthusiasm, valuable feedback, and the tremendous effort you put in!

Thanks!