Effectiveness of CTF education

Measuring the learning outcomes of Jeopardy CTF's

Research Group Network and Systems Engineering Cyber Security

2022

let's change
YOU. US. THE WORLD.

THE HAGUE
UNIVERSITY OF
APPLIED SCIENCES

Effectiveness of CTF education

Measuring the learning outcomes of Jeopardy CTF's

Author
D. Meinsma, S. Barjas, M. Gilhespy, M. Björkqvist

Department
Research Group Network and Systems Engineering Cyber Security

Datum
31-Aug-2022

Type project
Research Project

Version
1.1

The Hague University of Applied Sciences 2022

Summary

Adversarial thinking is essential when dealing with cyber incidents and for finding security vulnerabilities. Capture the Flag (CTF) competitions are used all around the world to stimulate adversarial thinking. Jeopardy-style CTFs, given their challenge-and-answer based nature, are used more and more in cybersecurity education as a fun and engaging way to inspire students.

Just like traditional written exams, Jeopardy-style CTFs can be used as summative assessment. Did a student provide the correct answer, yes or no. Did the participant in the CTF competition solve the challenge, yes or no.

This research project provides a framework for measuring the learning outcomes of a Jeopardy-style CTF and applies this framework to two CTF events as case studies. During these case studies, participants were tested on their knowledge and skills in the field of cybersecurity and queried on their attitude towards CTF education.

Results show that the main difference between a traditional written exam and a Jeopardy-style CTF is the way in which questions are formulated. CTF education is stated to be challenging and fun because questions are formulated as puzzles that need to be solved in a gamified and competitive environment. Just like traditional written exams, no additional insight into why the participant thinks the correct answer is the correct answer has been observed or if the participant really did learn anything new by participating.

Given that the main difference between a traditional written exam and a Jeopardy-style CTF is the way in which questions are formulated, learning outcomes can be measured in the same way. We can ask ourselves how many participants solved which challenge and to which measurable statements about “knowledge, skill and attitude” in the field of cybersecurity each challenge is related.

However, when mapping the descriptions of the quiz-questions and challenges from the two CTF events as case studies to the NICE framework on Knowledge, Skills and Abilities in cybersecurity, the NICE framework did not provide us with detailed measurable statements that could be used in education. Where the descriptions of the quiz-questions and challenges were specific, the learning outcomes of the NICE framework are only formulated in a quite general matter.

Finally, some evidence for Csíkszentmihályi’s theory of Flow has been observed. Following the theory of Flow, a person can become fully immersed in performing a task, also known as “being in the zone” if the “challenge level” of the task is in line with the person’s “skill level”. The persons mental state towards a task will be different depending on the challenge level of the task and required skill level for completing it. Results show that participants state that some challenges were difficult and fun, where other challenges were easy and boring.

As a result of this project, a guide / checklist is provided for those intending to use CTF in education.

Content

Exposition

“This is cybercrime-ology, a podcast about cybercrime, its research, and its researchers. My name is Michael and this time I have something a little special for you. I am sure you have all heard about CTF competitions and how important they are for those in the hacking community and for organizations looking for new cybersecurity talent. … Would there be any advice that you would give to people who were thinking of being a participant, playing these games and learning more about how offensive techniques work?” [1]

“Everybody Google’s, so don’t be afraid to Google. … It’s about learning. If you didn’t learn doing a challenge, you need to move up in the difficulty level of the challenges that you are doing. If you did learn something new during a challenge, it was a good challenge.”

-- Jax, design team for Northsec, designing top-level competitions for white hats and students.

1 https://www.cybercrimeology.com/episodes/capture-the-flag-what-is-how-to-design-and-how-to-compete-in-ctfs-for-hackers

Objective

To encourage young people to enhance their cybersecurity abilities, the ECSC (EU Agency for Cybersecurity) brings together young cyber talent from across Europe in an annual event, the European Cyber Security Challenge (ECSC).[2] [3]

1 Problem Statement

Adversarial thinking is essential when dealing with cyber incidents and for finding security vulnerabilities.[4] Capture the Flag (CTF) competitions are used all around the world to stimulate adversarial thinking.[5] Jeopardy-style CTFs, given their challenge-and-answer based nature, are used more and more in cybersecurity education as a fun and engaging way to inspire students (Vykopal, 2020). However, to date not much research has been done on measuring the learning outcomes of CTFs and their effectiveness for education.

2 Objective

This research project aims to provide a framework for measuring the learning outcomes of a Jeopardy-style CTF and apply this framework to a Jeopardy-style CTF event as a case study. As a result of this project, a guide / checklist will be provided for those intending to use such a CTF in education.

3 Research Questions

To achieve this objective, this research will answer the following research questions:

Main question

How to measure the learning outcomes of a Jeopardy-style CTF?

Sub-questions

1. *Which measurement is most suited for measuring the effectiveness of Jeopardy-style CTFs?*
2. *What are the learning outcomes that are assessed by CTFs?*
3. *Which framework can be used to measure the effectiveness of Jeopardy-style CTFs?*
4. *How effective are Jeopardy-style CTFs in enabling successful learning outcomes?*
5. *Is there a difference in the effectiveness of CTFs for beginners versus more experienced participants?*

4 Report Outline

In the next chapter of this report, a brief introduction will be provided into important terminology used in this study and the related work. After this, an overview will be provided of the methodology used to answer this project's research questions. The remaining chapters of this report will focus on each research question separately, working towards answering this study's main research question. This report will conclude with a discussion on this project's limitations and will provide suggestions for future work. Attached to this report, a Guide / Checklist for CTF Education will be provided and 3 appendixes with datasheets used.

---

2 https://www.enisa.europa.eu/topics/cybersecurity-education/eu-cyber-challenge
3 https://www.enisa.europa.eu/publications/towards-a-common-ecsc-roadmap
4 ECSC 2020 curriculum. Vienna, Austria. December 2019
5 https://www.enisa.europa.eu/publications/ctf-events

Related Work

This chapter will provide a brief introduction into important terminology used in this study and the related work.

1 Learning outcomes

The phenomenon of learning outcomes has been examined by a wide range of studies in education and although findings indicate that there is a dominant established definition, alternative definitions have been identified, asserting that learning outcomes involve more than what can be described in pre-specified and measurable terms (Prøitz, 2010). In this study, learning outcomes are described as a set of explicit and measurable statements about the “knowledge, skill and attitude” the learner should have, which are being assessed by the particular education program (Keshavarz, 2011). It is important to note for the discussion of this study that these measurable statements are about the “knowledge, skill and attitude” the learner *should have* during the assessment and not about the “knowledge, skill and attitude” the learner *has obtained* by participating in the education program.

2 Capture the Flag (CTF)

A Capture the Flag (CTF) is a special kind of information security competition. Jeopardy-style CTFs have challenges (tasks) in a range of categories, such as Web, Forensics, Crypto and Binary and teams can obtain flags (proofs of successful completion) for every solved task.[6] Research shows that incorporating gamified simulations of cybersecurity breach scenarios in the form of challenge-based Jeopardy-style CTFs increases student engagement and leads to more well-developed skills (Leune, 2017). Further, replacing traditional homework assignments with CTF games is generally more favourable for both instructors and students and a Jeopardy-style CTF can be used as summative assessment (Vykopal, 2020).

Another style of CTF is an attack-defence competition, where every team has their own network with vulnerable services and teams can obtain points for successfully attacking the opponents' services and protecting their own. While looking back at the lessons learned from running a worldwide educational CTF event for more than 10 years (Giovanni, 2014) argues that with the added motivation provided by a more competitive interactive environment, only attack-defence CTFs can be properly called CTF competitions. However, the focus on technical knowledge about cryptography and network security, like the focus on attacking and defending network services in attack-defence CTFs, leads to the neglect of more human aspects in cybersecurity, such as social engineering and cybersecurity awareness, which are also part of ACM/IEEE curricular guidelines (Svabensky, 2020).

3 Student engagement

Although it is stated that using CTFs in education increases student engagement, it remains open to discussion if this is in fact the case. The 2017 paper by Leune et al. cited above only showed a direct correlation between the level of understanding and the level of enjoyment that participants reported *after* participation in the CTF post-assessment questionnaire, not that this level of enjoyment had increased by participating. Similarly, research on immersive education already showed that the simulation of systems only led to engagement when the participant’s skill level was already high (Cooper, 2009). Another example of a learning obstacle in CTFs is the difficulty newcomers face in becoming immediately immersed in competition and the phenomenon of participants with “insufficient skill levels” avoiding challenges with high point values (Chung, 2014). Perhaps this phenomenon can be explained using Csíkszentmihályi’s theory of Flow (Csikszentmihalyi, 1990), where a person can become fully immersed in performing a task, also known as “being in the zone” if the “challenge level” of the task is in line with the person’s “skill level”. As shown in the figure 1 and the example on the next page, following the theory of Flow a persons mental state towards a task will be different depending on the challenge level of the task and required skill level for completing it.

6 https://ctftime.org/ctf-wtf/

For example, a participant may become anxious during a CTF competition if the challenge level is too high compared to the participant's skill level or become bored if the challenge levels are too low for their skill level.

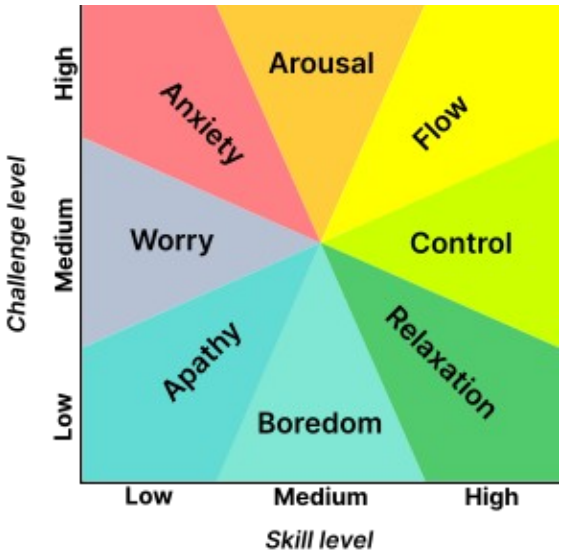

Fig 1: Mental state in terms of challenge level and skill level, according to Csikszentmihalyi's flow model.
Source: https://en.wikipedia.org/wiki/Flow_(psychology)

Research Methodology

This chapter will provide an overview of the methodology used to answer this project's research questions. This project consisted of three main phases, described below:

1 Literature review, expert sessions and choosing the platform

Answering sub-questions 1 and 2 on which measurement is most suited for measuring the effectiveness of Jeopardy-style CTFs and what learning outcomes are being assessed by CTFs, relevant scientific papers have been reviewed. On the topic of which papers may be relevant, suggestions have been provided by contacts at the Masaryk University Institute of Computer Science, known for the development of the KYPO cyber range platform.[7] For the more human aspects of this research, such as measuring "attitude", expert sessions have been organized with colleagues from the research groups on Cybercrime & Cybersecurity and Cyber Security and Safety of the Centre of Expertise Cyber Security at The Hague University of Applied Sciences.

Which learning outcomes can be measured effectively is greatly impacted by the choice of platform used to organize CTF competitions. Given that the Hague University of Applied Sciences is the co-founder of the Dutch Joint Cyber Range[8], this platform has been chosen for the full access in use and development, full insight into monitored data for learning analytics and ownership related to data protection regulation.

2 Organizing two CTF competitions

To generate case studies, for the purpose of answering sub-question 3, on which framework can be used to measure the effectiveness of Jeopardy-style CTFs, this project organized a 3-day national school CTF in the Netherlands (a heterogeneous group of participants), during which students from the Utrecht University of Applied Sciences aided greatly in the deployment of the platform. A rerun of the same CTF competition was carried out for a group of computer science students at Fontys University of Applied Sciences (a more homogeneous group of participants). Organizing a 3-day competition allowed this study

7 https://crp.kypo.muni.cz/
8 https://www.jointcyberrange.nl/

to investigate the possibility of measuring a participants' growth in "knowledge, skill and attitude" over time.

A self-hosted implementation of the Capture The Flag framework CTFd[9] was used to host the challenges on the Dutch Joint Cyber Range and log the results of the competition. CTFd is a popular choice for hosting CTF challenges and has been used in education by the computer science department of The Hague University of Applied Sciences and students from Utrecht University of Applied Sciences.

Importantly for this study, CTFd can be used to log and monitor what participants submit in their attempts to score points. The framework is flexible in how questions and challenges can be formulated and flexible in formulating the criteria for correct answers (flags). However, the framework does not track a participant's behaviour at their computer. This would have provided more insight for the research but would have also dramatically increased the complexity of the technical setup. Due to the ambition of hosting a nationwide competition for many participants, resource limitations resulted in the constraint of not providing all participants with their own virtualized remote working environment.

Using the flexibility of CTFd in formulating questions and answers, this study has been able to incorporate not only challenges to be solved during the competition, but also quiz-questions, feedback-questions, questions for the participants on online sources (blogs, tutorials) used, and questions that could provide insight into their attitude towards CTF education.

Most of the challenges and questions for the competition were developed by the authors of this study and a colleague instructor from Hanze University of Applied Sciences. The learning content of the CTF was inspired by the Dutch Technical Security 101 podcast.[10]

3 Analyzing the data

In order to measure the effectiveness of Jeopardy-style CTFs in transferring learning outcomes and to see if there is a difference in the effectiveness of CTFs for beginners versus more experienced participants, logs files from the self-hosted implementation of the Capture The Flag framework CTFd have been exported to .csv format.

Note on Privacy
- Logs files with personal identifiable information from participants, like IP-adresses and email accounts, linking them to their CTFd user_id have not been exported from the platform and are not part of the dataset used in this research.

These research results have been parsed again using Jupyter Notebook to provided a summary on each participant's performance during the CTF and provided answers. These summaries can be found in Appendix 2 and 3.

Note on Consent
- While parsing the exported .csv files, all data has been removed from the dataset from user_id's which did not give their explicit consent for their data to be used in this research.

Given that in Case Study 1, only 17 of the CTF participants provided their consent to participate in this research and that in Case Study 2, only 19 of the CTF participants were willing to participate, a quantitative research approach in analysing the data would not be adequate. For this reason, a qualitative and explorative research approach has been used in comparing the summaries of each participant and identifying important observations within the set of datapoints.

The .csv files and Jupyter Notebook scripts used for this study can be requested by contacting the Centre of Expertise Cyber Security research group at the Hague University of Applied Sciences, mail: cybersecurity@hhs.nl

9 https://github.com/CTFd/CTFd
10 https://anchor.fm/ts101

Measuring effectiveness

To answer the question on which measurement is most suited for measuring the effectiveness of Jeopardy-style CTFs, the term “effectiveness” needs to first be elaborated. At the end of this chapter, a section will be provided on “measuring attitude”.

4 Effectiveness in learning

In the context of “learning” one point of view on the effectiveness of CTF competitions is the view presented in the Exposition of this report, with the quote from the cybercrime-ology podcast episode on designing CTFs:

“Everybody Google’s, so don’t be afraid to Google. … It’s about learning. If you didn’t learn doing a challenge, you need to move up in the difficulty level of the challenges that you are doing. If you did learn something new during a challenge, it was a good challenge.”

This first statement can be interpreted as the point of view that a CTF is effective if participants have learned something new during the competition.

In contrast to this point of view, in the Related Work section of this report, learning outcomes are described as a set of explicit and measurable statements about the “knowledge, skill and attitude” the learner should have, and which are being assessed by the particular education program.

This second statement can be interpreted as the point of view that a CTF is effective if it can be used for assessment in education, such as been done in the cited work by (Vykopal, 2020).

The difference between these two statements is that in the second statement a participant can demonstrate all learning outcomes of an education track during the final CTF assessment, while having learned nothing new in the education program, indicating that the participant should in fact have “moved up in the difficulty level”. Just like in traditional written exams, being able to provide all the right answers does not mean that you have learned something new during the education program.

How does one measure the effectiveness of traditional written exams? As instructors, working in the field of education, we have been taught to consider how many students solved which question on the exam and to which measurable statements about “knowledge, skill and attitude”, in the related field of study, are the questions related (van Berkel, 2017).

5 Assess, learning something new

To merge both points of view, this study proposes to use CTFs to assess if participants have learned something new, where “learning something new” could be defined as a change or growth in the participant’s “knowledge, skill and attitude” by competing in the CTF.

To now answer the question on which measurement is most suited for measuring the change or growth in a participant’s “knowledge, skill and attitude”, several choices have been made in the design of the setup for the second phase (the two case studies) of this project:

1. **More measurements are better than a single measurement**

Measuring changes in growth can be done more effectively by doing multiple measurements instead of a single measurement. The national school CTF[11] in the Netherlands is a yearly 3-day event, which allows for more opportunities for measurement than for example the 1-day Challenge the Cyber event[12], the Dutch preliminary CTF for the European Cyber Security Challenge.

11 https://scholencompetitie.jointcyberrange.nl/
12 https://challengethecyber.nl/

2. **Focus on immersion**
Instead of providing participants with a questionnaire before and after the CTF-event, which could have a negative effect on engagement, this study proposes, given the question-answer based nature of Jeopardy-style CTFs, to merge skill challenges with quiz-questions on knowledge and questions related to a participant's attitude to the competition as part of the competition.

3. **Questions and challenges should be linked**
To measure a change or growth for a participant, questions and challenges should be linked to each other. A link between a question and a challenge could be defined as that they share the same topic from the field of study and that they are approximately the same complexity for the student to solve. With these links, potential correlations can be uncovered, such as that participants that are able to solve the skill challenges and knowledge questions for a particular topic, also state that they have a positive attitude towards the topic. If these links are preserved over the course of several days, perhaps changes and growth in these correlations could be visualized.

6 Measuring attitude

As stated in this report's Research Methodology, for the more human aspects of this study, such as measuring "attitude", expert sessions have been organized with colleagues from the Centre of Expertise Cyber Security at The Hague University of Applied Sciences.

Given the complex and widely debated term "attitude" (Tanur 1992), this study does not aim to provide a fixed definition to be used. To limit the scope, this study proposes to focus on asking participants directly how they think and feel about the topics from the field of study, such as Web, Forensics, Crypto or Binary and to focus on asking participants how they think and feel about themselves as CTF players and pose open questions on why they think CTF competitions might be fun and useful in education.

Learning Outcomes

Although frameworks exist that specify which knowledge, skill and attitude young cybersecurity talent should have, such as the 2020 NICE Framework for Cybersecurity[13], CTFs are not mapped onto these frameworks at a detailed level. As shown by a survey on national cyber security competitions by EU member states in the 2021 ENISA document "Towards a common ECSC Roadmap" cited in the Objective section of this report, there is a great variety of cyber security topics and skills that competitions use. Very few competitions seem to be teaching non-computer science topics such as cyber security law, policy and ethics. Work by (Svabensky, 2020), cited in the Related Work section of this report, showed similar results in the neglect of the more human aspects in cybersecurity, such as social engineering and cybersecurity awareness.

1 Categories

A key observation from this study, in answering the question of which learning outcomes are being assessed by CTFs, is that currently, learning outcomes assessed by using CTFs are at "Category" level and have a main focus on adversarial thinking, with categories such as finding vulnerabilities in cryptography, cracking, reversing and the exploitation of binaries and finding vulnerabilities in web-applications and mobile applications. Although present, less focus in spent on the response to adversaries, with topics such as forensics, incident response and defence tactics.

2 Foundational knowledge, skill and attitude

Given that CTFs are assumed to be a fun and engaging way to inspire students as mentioned in the objective of this report, it is no surprise to the authors of this study that organizations looking for new cybersecurity talent use CTF-events as well. It is our belief that a foundational attitude for solving challenges at CTFs is the attitude of "not giving up", similar to the well-known phrase in the hacker-community "try harder" from the popular Offensive Security Certificate, OSCP [14]

A second foundational attitude which we think might be interesting for organizations looking for new cybersecurity talent is that CTF competitions challenge participants to proactively "do research". As mentioned by Jax in the cybercrime-ology podcast episode on designing CTFs, referred to in the Exposition of this report:

"Everybody Google's, so don't be afraid to Google. … It's about learning."

Although currently CTFs focus mainly on adversarial thinking, the question-answer-based nature of Jeopardy-style CTFs would allow these CTFs to also assess other foundational knowledge and skill in cybersecurity curricula. In the next chapter, as a proof of concept, the challenges and questions developed for the Dutch national school CTF, used as case study for this research, have been mapped to the 2020 NICE Framework for Cybersecurity.

13 https://www.nist.gov/system/files/documents/2020/11/17/supplement_nice_specialty_areas_and_work_role_ksas_and_tasks.xlsx
14 https://www.offensive-security.com/offsec/say-try-harder/

A Framework

This section will provide insight into the setup of the two case studies used in this project to answer question 3 on which framework can be used to measure the effectiveness of Jeopardy-style CTFs.

Based on the learnings from answering questions 1 and 2 (which measurement is most suited for measuring the effectiveness of Jeopardy-style CTFs, which learning outcomes are being assessed by CTFs), a set of questions and challenges have been developed for a 3-day Jeopardy-style CTF competition.

1 The quiz-questions and challenges

As mentioned in the previous chapter on Research Methodology, the learning content of the CTF was inspired by the Dutch Technical Security 101 podcast. For each day of the 3-day CTF competition a quiz-question and challenge has been developed for the following 5 categories: Botnets, Digital Forensics, Cloud and Linux, Internet of Things, Secure by Design and Ethical Hacking (of a Web application). Short descriptions of each quiz-question and challenge can be found in Appendix 1, as well as a mapping of each quiz-question and challenge to the learning outcomes of the NICE framework on Knowledge, Skills and Abilities in the field of Cyber Security. It is noteworthy that the learning outcomes in the NICE framework are formulated in a quite general matter, where the short descriptions of the quiz-questions and challenges are more specific. In the effort of mapping these descriptions on the framework, a lot of times the following two general learning outcomes needed to be picked due to the absence of a better match in the NICE framework:

K0435: Knowledge of fundamental cyber concepts, principles, limitations, and effects.
S0264: Skill in recognizing technical information that may be used for leads to enable remote operations.

As mentioned in the previous chapter on Research Methodology, the .csv files, containing more detailed information on the formulation of questions and challenges used during the two case studies, can be requested by contacting the Centre of Expertise Cyber Security research group at the Hague University of Applied Sciences, mail: cybersecurity@hhs.nl

All questions and challenges are developed with the aim to be easy and act as an introduction to the field.

2 Attitude-questions

As can be seen in the ‘how to read’ instructions in Appendix 2 and 3 on answers provided by the participants in Case Study 1 and 2, participants have also been asked to provide insight into:

- if the competition was the participant’s first CTF or if the participant states the be a beginner, average, experienced or expert CTF player.
- the participant’s opinion on if and why CTFs are useful in education.
- the participant’s opinion on if the participant has learned nothing, not so much, a little or a lot from the 1st day of the CTF.
- the participant’s opinion on when a person has a security mindset.
- if the participant aims to participate in the Dutch preliminary CTF for the European Cyber Security Challenge after this event.

3 Sources used and Feedback questions

Finally, each day of each category, participants could score extra points for listing links to websites / sources used in solving the quiz-question and challenge, and participants could score extra points for providing feedback on the quiz-question and challenge by listing 3 words.

How well the participants performed, and which answers have been provided in both case studies, can be reviewed in Appendix 2 and 3.

The Effectiveness of CTFs for Education

As stated in the previous chapter on Measuring Effectiveness, the objective is to use CTFs to assess if participants have learned something new, where “learning something new” could be defined as a change or growth in the participant’s “knowledge, skill and attitude” by competing in the CTF. And, as stated in the chapter on Research Methodology, a qualitative and explorative research approach has been used in comparing the summaries of each participant and identifying important observations within the set of datapoints.

1 The willingess to participate in this research and the willingess to answer questions

Not all participants during the two case studies were willing to participate in this research and not all participants that were, were willing to provide answers to all the questions. Two clear differences in this respect are visible in Appendix 2 and 3.

(1) Only in Case Study 1, some of the participant summaries show that they have completed all quiz-questions and challenges, such as user_18 and user_31. In Case Study 2, none of the participant’s summaries show that a participant had solved all quiz-questions and challenges, however the instructor of the group of students in Case Study 2 informed us that some of the students had been able to solve all quiz-question and challenges during the competition.

(2) Although participants had the opportunity to state in the feedback-questions that quiz-questions and challenges were too difficult or boring, some participants, such as user_69 and user_73, did not answer the feedback questions when they were not able to solve the quiz-question and challenges of a given day and category. Other users showed, such as user_87 and user_92, that feedback was provided only when the participant had solved both the quiz-question and challenge of a given day and category. Some users, such as user_82 and user_107 did provide some answers to the feedback-questions without having solved both the quiz-question and the challenge.

These observations show that being able to provide an answer to a question, does not mean that the participant is willing to do so. Appendix 2 and 3 together show that participants in both case studies that were able to solve a lot of quiz-questions and challenges, (such as user_81 and user_99), answered more questions and provided more feedback than their groupmates.

2 A positive opinion on CTF education does not directly result in high performance

Almost all participants that did answer the attitude-question on if and why CTFs are useful in education, were positive about the use of CTFs, but this did not reflect in high performance for these users. For example, user_65 states to really like the use of CTFs, but was not able to solve a lot of quiz-question and challenges. And where users 23, 47, 61, 88 and 93 all made a statement about enjoying being challenged, user_23 and user_47 were able to solve more quiz-questions and challenges than the other three users.

3 A high performance does not directly result in increased interest

When looking at the attitude-question on whether the participant aims to participate in the Dutch preliminary CTF for the European Cyber Security Challenge after this event, not all participants with high performance in the case study state that they will do so. User_31 and user_53 are positive about the participation in the Dutch preliminaries, where user_18, user_54 and user_81 are doubtful about it and user_99 states to be not interested.

4 No clear evidence for growth over time

When looking at Appendix 2 and 3, no clear evidence is presented on growth over time. Some participants were able to solve a lot of quiz-questions and challenges, some participants a few and some participants even fewer. Comparing day 1, 2 and 3, more quiz-question and challenges have been solved on 1 day than on day 3 and for some participants, such as user_25, user_33 and user_47, a clear drop in the amount of solves is visible in comparing day 1 and day 2 and comparing day 2 and day 3. Only user_92 and user_109 showed improvement in solving quiz-question and challenges in comparing day 2 and day 3, but not when comparing day 2 and day 1.

5 Some evidence for the theory of Flow

In the previous chapter on Related Work, the theory of Flow has been mentioned as a potential explanation for the phenomenon where a participant could become fully immersed in solving a challenge, if the “challenge level” is in line with the person’s “skill level”, and that a participant may be become anxious if the challenge level is too high compared to the participant’s skill level or become bored if the challenge levels are too low for their skill level.

While looking at the list of unique words used by the participants as answers on the feedback-questions, some evidence in favour of the theory of Flow can be observed.

Most of the participants described the category Botnets with words in line with ‘easy’, ‘not too difficult’, but ‘fun’, where user_25 and user_54 stated that the category Botnets was ‘easy’ and ‘boring’. And in the other categories, words like ‘difficult’ and ‘challenging’ were used when words like ‘fun’ and statements like ‘learned a lot’ were also used. Although user_81 stated that Internet_of_Things was ‘too difficult’, for which user_81 did not solve both the quiz-question and challenge, and user_99 used the word ‘stupid’ and ‘difficult’ for the same category. Neither participant dropped out of the competition. However, as stated above, although the feedback-questions were embedded in the competition and participants would receive points for answering the questions, not all participants were willing to answer them.

6 Investment in sources

As mentioned in the previous chapter on the Framework used to formulate questions and challenges and setup the CTF competition for Case Study 1 and 2, participants were asked to provide links to websites used to solve the quiz-questions and challenges. Doing this would speak in favour of the participant’s willingness to invest in their own learning process. In total the participants had the opportunity to provide 18 unique links to websites used (6 categories x 3 days). As can be seen in Case Study 1 and 2, all three cases can be found in both case studies where the ‘Investment in sources’ number is around the same number, below or above the amount ‘yes’ that have been listed when the participant had solved both the quiz-question and the challenge of a given category and day.

7 Adversarial thinking and having a Security Mindset

As stated in the previous chapter on the Objective of this research project, Capture the Flag competitions are used all around the world to stimulate adversarial thinking. As can be seen in Appendix 2 and 3 participants state that a person has a security mindset when containing the elements described below. It is important to note that this is not a definition, just a summary of answers provided:

“If the person is aware of the consequences of actions and aim for improvement. When the person has insight into threats, puts security first, applies security by design principles, and proactively looks for vulnerabilities from the perspective from a hacker, informs the right person, so they can be fixed.”

This summary shows that the ability to do adversarial thinking is part of having a Security Mindset, but having a Security Mindset also means having the goal to fix things and aiming for improvements in security.

Beginner and expert players

In this chapter we will present our findings related to the question on the effectiveness of CTFs for beginner players versus more experienced players.

We have previously made some statements concerning the effectiveness of CTFs for beginners versus more experienced players. (1) A positive opinion on CTF education does not directly result in high performance. (2) A high performance does not directly result in increased interest, and (3) some evidence for the theory of Flow, where a participant may be become anxious if the challenge level is too high compared to their skill level or become bored if the challenge levels are too low for their skill level.

1 Perceived level and perceived learnings

Additional observations can be found in Appendix 2 and 3 when reviewing the answers provided to the question on whether the competition was the participant's first CTF or if the participant states the be a beginner, average, experienced or expert CTF player. As can be seen, the participant's opinion on their own skill level did not match with the performance during the competition, where "beginners", such as user_23 performed as good as "average" players, and "average" players, such as user_18 and user_31 outperformed more "experienced" players such as user_54 and user_81. Additionally, user_19 and user_99 solved a lot of quiz-question and challenges, while stating that this was their first CTF. Terminology like beginner, average, experienced and expert seem to be fluid and depends on the user's own perception. Further questioning on "compared to whom" do you think you are a beginner, average, experienced or expert CTF player would further clarify the provided answer.

The participants were also asked on their opinion as to whether they had learned nothing, not so much, a little or a lot from the 1st day of the CTF. These answers also did not match with the participant's performance, such as user_18 and user_69. Participants could of course have stated that they did not learn a lot from day 1, in both cases, if day 1 was too difficult or if day 1 was too easy for the participant.

As stated in the previous chapter on the Framework used for the CTF competition for both Case Study 1 and 2, the quiz-questions and challenges were designed with the aim to be achievable and to act as an introduction to the field of study. Plotting the participants' answers on their perceived level and perceived learnings in a two-factor diagram, table 1, showing a wide distribution, but with a clear peak in 'beginner' players positively stating to have learned something new from this CTF.

Table 1: Two-factor diagram on participant's preceived level and perceived learnings.

Learnings / Level	**1st CTF**	**beginner**	**average**	**experienced**
No, nothing	69, 73		18	
No, not much	26	47	33	54
Yes, a little	99	23, 25, 65, 88, 89, 95	31, 53	81
Yes, a lot		51	61	

Where, number N refers to the answer from partipant 'user_N'

Learning outcomes of Jeopardy-style CTFs

In this research, we have take the first steps to answer the main research question on how to measure the learning outcomes of a Jeopardy-style Capture the Flag (CTF) competition. Given that the sub-questions leading towards answering this main question did not provide us with solid answers, we offer our observations as argumentation for our final answer.

Just like traditional written exams, Jeopardy-style CTFs can be used as summative assessment. Did a student provide the correct answer, yes or no. Did the participant solve the challenge, yes or no. When we asked students directly if, and why, they think CTFs are useful in education, they answered that CTFs are challenging and fun. Students stated that CTFs are a different way of learning, in which you actively learn many different skills by doing and learn to apply many different methods. It's a gamified, competitive environment, where you are tasked to solve puzzles, in which you can challenge yourself with difficult tasks and need to do investigation and learn how to think like a cyber attacker.

We have stated that the main difference between a traditional written exam and a Jeopardy-style CTF is the way in which we formulate the questions (Vykopal, 2020). Where traditional written exams questions are about the ability to recite knowledge from books and articles, being able to apply certain methods to solve equations or pick the right path forward, in CTFs these questions are formulated differently, as puzzles in a gamified and competitive environment, which according to feedback from participants is fun.

During our research we did not see any clear evidence that participants who state to be positive about CTFs performed better than other students, or that students who solved a lot of challenges will definitely take on the next step and participate in the Dutch preliminary CTF for the European Cyber Security Challenge. Additionally, the student's opinion of their own skill level did not match with their performance during the competition, where "beginners" performed as well as "average" players and "average" players outperformed more "experienced" players.

Just like traditional written exams, we did not obtain any more insight into why the student thinks the correct answer is the correct answer. Did the student already know the answer or did the student learn something new during the competition? When a student states that he or she did not learn anything new from a challenge, is this because the student already knew the solution to the challenge or that the challenge was too difficult? Also, if a student did not solve a challenge, was this because the challenge was too difficult or because the student was not motivated enough to fill in an answer? Just like traditional written exams, Jeopardy-style CTFs will show us if a student solved the challenge, yes or no.

The difficulty in creating challenges for a CTF is that they need to be just challenging enough. Using Csíkszentmihályi's theory of Flow, where a person can become fully immersed in performing a task, a task is challenging if the "challenge level" of the task is in line with the person's "skill level". A student may become anxious if the challenge level is too high compared to the student's skill level or become bored if the challenge level is too low.

How then, shall we measure the effectiveness of a Jeopardy-style Capture the Flag (CTF) competition in enabling successful learning outcomes? The same way as we measure the effectiveness of a traditional written exam. How many students solved which challenge and to which measurable statements about "knowledge, skill and attitude" in the field is this challenge related. Difficult questions remain on who the groups of students are? What they can already do and what do they already know? And what do you want them to learn?

Sadly frameworks, like the NICE framework on Knowledge, Skills and Abilities in Cyber Security, do not provide us with much insight. K0435: Knowledge of fundamental cyber concepts, principles, limitations, and effects. Which fundamental cyber concepts are being referred to? S0264: Skill in recognizing technical information that may be used for leads to enable remote operations. What type of technical information? Which methods for remote operations?

If done right, Jeopardy-style CTFs are challenging and fun. Education should be challenging and fun.

Discussion

This chapter will conclude this research project with a discussion on this project's limitations and will provide suggestions for future work.

As stated in the previous chapter, given that the sub-questions leading towards answering the main question of this research did not provide us with solid answers, we could offer only our observations as argumentation for the final answer.

Reviewing Appendix 2 and 3 shows, in the incremental count of assigned user_id numbers, that in both case studies combined, over 100 users participated. However, only 36 of the participants were willing to participate in this research and as stated in the previous chapter on The Effectiveness of CTFs for Education, not all participants were willing to answer all questions. Also, it is unclear if each user_id represents an unique person. Participants or whole groups of students could have worked together behind one user_id, meaning that some user_id's would represent a larger population than other user_id's. Involving a colleague instructor to participate in this research with a large group of students as part of their education also did not help, given the similar presence of empty answers in Case Study 2 as in Case Study 1. Making the feedback and attitude-questions part of the competition and providing participants points for providing an answer did not solve the problem. Due to this low response-rate, no statistical statements on correlations and no statistically significant outcomes could be provided.

The framework used for this research did not track a participant's behaviour at their own computer. This would provide more insight into the steps a participant took when trying to solve a challenge, but unless it can be confirmed that only one student uses a particular computer, the problem of collaboration among participants will not be controlled for. Aiming to control for this issue would have limited the scalability of our experimental setup.

The framework used for this research did provide data on invalid submissions by participants, but this was not further investigated. Reviewing what participants guess is the correct answer would provide more insight into the participants reasoning, but only for the participants who submit their guesses and not for participants who reason internally. Furthermore, a series of invalid submissions does not mean that a participant does not know the theory behind the challenge but could mean that the challenge is formulated unclearly. If a participant is able, with some luck, to guess the correct answer, solving the challenge will also not show if the participant knew the correct answer. Individual conversations with participants, or review of write-ups after the CTF competition remain a necessity in order to check if learning happened. Other techniques like asking the same question multiple times in a slightly different way, could have a negative effect on immersion and a negative effect on CTF education begin perceived as challenging and fun.

Organizing a 3-day competition allowed this study to investigate the possibility of measuring a participant's growth in "knowledge, skill and attitude" over time. No evidence for this has been observed. We believe that a significantly longer period will be required for this observation and to investigate the retention of knowledge and skill after participating in a CTF competition.

Lastly, frameworks, like the NICE framework on Knowledge, Skills and Abilities in cybersecurity, do not provide us, working in education, with measurable statements on knowledge, skill and attitude, that can be used to measure learning outcomes.

Literature list

van Berkel, H., Bax, A., & Joosten-ten Brinke, D. (2017). Toetsen in het hoger onderwijs. (4 ed.) Bohn Stafleu van Loghum. https://doi.org/10.1007/978-90-368-1679-3

Csikszentmihályi M (1990). FLOW: The Psychology of Optimal Experience (PDF). Harper and Row. ISBN 978-0-06-016253-5.

Cooper, Karen. (2009). Go With the Flow: Engagement and Learning in Second Life.

Kevin Chung, & Julian Cohen (2014). Learning Obstacles in the Capture The Flag Model . In *2014 USENIX Summit on Gaming, Games, and Gamification in Security Education (3GSE 14)*. USENIX Association.

Vigna, Giovanni & Borgolte, Kevin & Corbetta, Jacopo & Doupé, Adam & Fratantonio, Yanick & Invernizzi, Luca & Kirat, Dhilung & Shoshitaishvili, Yan. (2014). Ten Years of iCTF: The Good, The Bad, and The Ugly.

Keshavarz M. (2011). Measuring course learning outcomes. Journal of Learning Design, [S.l.], v. 4, n. 4, p. 1-9, feb. 2011. ISSN 1832-8342. Available at: <https://www.jld.edu.au/article/view/84>. doi:http://dx.doi.org/10.5204/jld.v4i4.84.

Kees Leune, K. and Salvatore P.J. (2017). Using Capture-the-Flag to Enhance the Effectiveness of Cybersecurity Education. In Proceedings of the 18th Annual Conference on Information Technology Education (SIGITE '17). Association for Computing Machinery, New York, NY, USA, 47–52. https://doi.org/10.1145/3125659.3125686

Prøitz, T.S. (2010). Learning outcomes: What are they? Who defines them? When and where are they defined?. Educ Asse Eval Acc 22, 119–137 (2010). https://doi.org/10.1007/s11092-010-9097-8

Jan Vykopal, Valdemar Švábenský, and Ee-Chien Chang. (2020). Benefits and Pitfalls of Using Capture the Flag Games in University Courses. Proceedings of the 51st ACM Technical Symposium on Computer Science Education. Association for Computing Machinery, New York, NY, USA, 752–758. https://doi.org/10.1145/3328778.3366893

V. Švábenský, P. Čeleda, J. Vykopal, and S. Brišáková, (2020). Cybersecurity Knowledge and Skills Taught in Capture the Flag Challenges, Elsevier Computers & Security, 2020, ISSN 0167-4048, DOI:10.1016/j.cose.2020.102154, URL:https://www.sciencedirect.com/science/article/pii/S0167404820304272

Tanur, J. M. (Ed.). (1992). Questions About Questions: Inquiries into the Cognitive Bases of Surveys. Russell Sage Foundation. http://www.jstor.org/stable/10.7758/9781610445269

Guide / Checklist for CTF Education

In this chapter we will provide our guide and checklist for setting up a CTF to be used in education. This approach is based on a didactic approach that is been used in the higher education in the Netherlands (described in chapter 6). The first step is selecting the categories (forensics, web, reverse engineering, crypto etc.) you want the (student) group to engage with. Inspiration for selecting categories could be based on past CTF challenges, infosec blogs, research and trend reports. After selecting the categories, it is necessary to write down the learning outcomes. The learning outcomes describes the situation by the end of a CTF. It is a description of the knowledge and skills the group will have at the end of the CTF. The next step is to start creating the challenges. A good practice is to write the build instructions into a README file. The README file contains the configuration of the challenge, the problem description, the difficulty of the challenge and the flag. Also, it is important to think about a realistic problem description (scenario) for the CTF. To create some structure, the challenges will follow the logical order of the phases of a pentest or cyber kill chain. The difficulty of the challenges can be categorized in the following three levels:

- Easy – This level of difficulty requires the use of known tools and general field related knowledge.
- Medium – This level of difficulty requires configuration and the use of tools or simple scripting to perform a exploit and specific field related knowledge.
- Hard – This level of difficulty requires the creation of complex scripts and in-depth sector specific knowledge.

Below you will find a short example of selecting a category, describing the learning outcomes, building a realistic scenario and selecting the difficulty level.

Category: Web

Learning outcomes: Students are able to perform a SQL-Injection on a web application.

Problem description (Scenario): PH is a upcoming professional photographer with his own blog. Nowadays everybody wants to work with him and post their pictures on his blog. PH asked one of his contacts to build a mechanism, which he can use to select the users that can send in their pictures. He heard some stories from other people. That their blogs are being held hostage with ransomware. Can you help PH identify his vulnerabilities? You need to find out what is hidden in flag.txt through blackbox pentesting!

Difficulty level: Easy

Configuration:
- Networking: DHCP
- Recent PHP Vulnerability

Quiz: Which OWASP Top 10 vulnerability was number one in 2017 and is now number three of the OWASP Top 10:2021?

Hints: Start with reviewing source code or use nikto :)

Flag: JCR(8asdNq23e9)

Appendix 1: Challenges descriptions and learning outcomes, 3-day Jeopary-style CTF

Short descriptions of each quiz-question and challenge, as well as a mapping of each quiz-question and challenge to the learning outcomes of the NICE framework on Knowledge, Skills and Abilities in the field of Cyber Security.

Table 2: Case study, 3-day Jeopardy-style CTF, Challenge descriptions and learning outcomes, part 1

Category	Day	Short description	NICE Framework, Learning outcomes
Botnets	1	Challenge: Install Kali Linux in a virtual machine.	S0073: Skill in using virtual machines.
Botnets	1	Quiz: What type of file extension can you import into VirtualBox to preload a virtual machine?	K0097: Knowledge of the characteristics of physical and virtual data storage media.
Botnets	2	Challenge: Setup a host-only network.	S0073: Skill in using virtual machines.
Botnets	2	Quiz: Description of a host-only network.	K0001: Knowledge of computer networking concepts and protocols, and network security methodologies.
Botnets	3	Challenge: Check if both machines are on the same network and can communicate with eath other.	S0004: Skill in analyzing network traffic capacity and performance characteristics.
Botnets	3	Quiz: What is the file extension of a digital CD image?	K0097: Knowledge of the characteristics of physical and virtual data storage media.
Digital Forensics	1	Challenge: Identifying files by their file signature	S0215: Skill in evaluating and interpreting metadata.
Digital Forensics	1	Quiz: What is the name of the information at the beginning of a file which a computer would use to determine the type of the file?	K0449: Knowledge of how to extract, analyze, and use metadata.
Digital Forensics	2	Challenge: Identify the filesystem with which a disk image has been formatted.	S0065: Skill in identifying and extracting data of forensic interest in diverse media (i.e., media forensics).
Digital Forensics	2	Quiz: What is the signature of a filesytem formatted with NTFS (in hex).	K0117: Knowledge of file system implementations
Digital Forensics	3	Challenge: Using knowledge of file and filesystem signatures, extract files from a corrupt disk image.	S0065: see above
Digital Forensics	3	Quiz: What is the name of the process used in digital forensics, to extract files from a filesystem, where normal methods of reading files are not possible?	K0017: Knowledge of concepts and practices of processing digital forensic data.

Table 3: Case study, 3-day Jeopardy-style CTF, Challenge descriptions and learning outcomes, part 2

Category	Day	Short description	NICE Framework, Learning outcomes
Cloud and Linux	1	Challenge: inspired by runc vulnerability, break out of docker container.	S0293: Skill in using tools, techniques, and procedures to remotely exploit and establish persistence on a target.
Cloud and Linux	1	Quiz: question on describe a defense-in-depth approach. Guess the analogy.	K0112: Knowledge of defense-in-depth principles and network security architecture.
Cloud and Linux	2	Challenge: escaping a chroot jail.	S0293: Skill in using tools, techniques, and procedures to remotely exploit and establish persistence on a target.
Cloud and Linux	2	Quiz: 2nd question on describe a defense-in-depth approach. Guess the analogy.	K0112: Knowledge of defense-in-depth principles and network security architecture.
Cloud and Linux	3	Challenge: exploiting privileged container permissions.	S0293: Skill in using tools, techniques, and procedures to remotely exploit and establish persistence on a target.
Cloud and Linux	3	Quiz: Which CWE definition is used for failures in changing working directories in chroot jails?	K0634: Knowledge of exploitation techniques.
Internet of Things	1	Challenge: Cracking a WPS key on a remote server.	S0264: Skill in recognizing technical information that may be used for leads to enable remote operations.
Internet of Things	1	Quiz: What essential element of cybersecurity is most affected by this lack of computational power?	K0435: Knowledge of fundamental cyber concepts, principles, limitations, and effects.
Internet of Things	2	Challenge: Cracking a weak password in a PCAP file from a WPA-2 handshake.	A0100: Ability to perform wireless collection procedures to include decryption capabilities/tools.
Internet of Things	2	Quiz: What is the name of the metric used to measure how secure a password is?	K0435: Knowledge of fundamental cyber concepts, principles, limitations, and effects.
Internet of Things	3	Challenge: Play back the captured RTSP stream inside a PCAP file.	S0182: Skill in analyzing target communications internals and externals collected from wireless LANs.
Internet of Things	3	Quiz: What tool is commonly used to search and index vulnerable web services?	K0013: Knowledge of cyber defense and vulnerability assessment tools and their capabilities.

Table 4: Case study, 3-day Jeopardy-style CTF, Challenge descriptions and learning outcomes, part 3

Category	Day	Short description	NICE Framework, Learning outcomes
Secure by Design	1	Challenge: Find default password based on telnet banner.	S0264: Skill in recognizing technical information that may be used for leads to enable remote operations.
Secure by Design	1	Quiz: Is it a good or a bad idea to use the same password on many different websites? Why?	K0158: Knowledge of organizational information technology (IT) user security policies (e.g., account creation, password rules, access control).
Secure by Design	2	Challenge: Find the poorly protected password for another user.	S0264: Skill in recognizing technical information that may be used for leads to enable remote operations.
Secure by Design	2	Quiz: What is a technique to thwart a rainbow table attack on stored, hashed passwords?	K0403: Knowledge of cryptologic capabilities, limitations, and contributions to cyber operations.
Secure by Design	3	Challenge: Brute-force a weak password.	S0264: Skill in recognizing technical information that may be used for leads to enable remote operations.
Secure by Design	3	Quiz: What is a good way to come up with a strong password?	K0158: Knowledge of organizational information technology (IT) user security policies (e.g., account creation, password rules, access control).
Ethical Hacking	1	Challenge: Perform a vulnerability scan on a web application.	S0001: Skill in conducting vulnerability scans and recognizing vulnerabilities in security systems.
Ethical Hacking	1	Quiz: Which OWASP Top 10 vulnerability was number 1 in 2017 and is now number 3 of the OWASP Top 10:2021?	K0624: Knowledge of Application Security Risks (e.g. Open Web Application Security Project Top 10 list)
Ethical Hacking	2	Challenge: Use bruteforcing techniques to find difficult to find directories/files.	S0001: Skill in conducting vulnerability scans and recognizing vulnerabilities in security systems.
Ethical Hacking	2	Quiz: This vulnerability allows user to submit input into files or upload files to the server. What is this type of vulnerability called?	K0624: Knowledge of Application Security Risks (e.g. Open Web Application Security Project Top 10 list)
Ethical Hacking	3	Challenge: find a existing exploit PoC and upload a malicious file.	S0293: Skill in using tools, techniques, and procedures to remotely exploit and establish persistence on a target.
Ethical Hacking	3	Quiz: How many ports are scanned with a default nmap scan?	S0264: Skill in recognizing technical information that may be used for leads to enable remote operations.

Appendix 2: Participants results Case Study 1

How to read:

Stated level:	In Dutch, if the participants stated that this was the participant's first CTF or if the participant states the be a beginner, average, experienced or expert CTF player.
Opinion on CTF education:	In Dutch, the participant's opinion on if and why CTFs are useful in education.
Stated learnings from day 1:	In Dutch, the participant's opinion on if the participant has learned nothing, not so much, a little or a lot from the 1st day of the CTF.
Security Mindset?:	In Dutch, the participant's opinion on when a person has a security mindset.
Challenge the Cyber?:	In Dutch, if the participant aims to participate in the Dutch preliminary CTF for the European Cyber Security Challenge after this event.
Investment in sources:	How many unique links to websites the participant has provided during the 3-day CTF as anwser to the question on which sources were used to solve the the challenges and quiz-questions. Max score is 18.

[Category, 3 times a yes/No, for day 1, day 2 and day 3. A 'yes' will be listed if the participant was able to solve both the quiz-question and the challenge of the category on the given day. A 'NO' will be listed if the participant did only solve the quiz-question or the challenge or none of the two for the category on the given day.]
[In Dutch, a list of unique words used by the participant to describe the quiz-questions and challenges from the category as answer on the feedback-questions.]

user_18

Stated level:	gemiddeld
Opinion on CTF education:	Ik hou gewoon van puzzelen en ik ben vast niet de enige. Dat is denk ik een zekere manier om de aandacht van de studenten er bij te houden
Stated learnings from day 1:	Nee, niets
Security Mindset?:	Als deze persoon zich bewust is van de mogelijke implicaties van zijn acties, de gevolgen er van en hoe deze persoon dat kan en wil verbeteren
Challenge the Cyber?:	Ik heb nog geen idee. Ik zie het wel, of ik er ben of niet. Dat hangt er een beetje er van af of de rest van de groep mij er bij wil hebben of niet
Investment in sources:	15

['Botnets', 'yes', 'yes', 'yes']
['sorry', 'goedvoorbeginners', 'waarom_perse_virtualbox', 'wel_entertaining', 'leuk', 'simpel', 'veels_te_easy', 'easy']

['Digital_Forensics', 'yes', 'yes', 'yes']
['niet_zo_moeilijk', 'uitdagender', 'notbad', 'interessant', 'interesting', 'beginnerfriendly', 'veel_van_geleerd', 'xxd_helps', 'uitdagend']

['Cloud_and_Linux', 'yes', 'yes', 'yes']
['amusing', 'find_/_-perm_/4000', 'relatief_voor_de_hand_liggend', 'reallife_applicable_ish', 'basic_enumeration', 'suidperms', 'grappig', 'easy']

['Internet_of_Things', 'yes', 'yes', 'yes']
['Goede_vlag_op_de_achtergrond_smileyface', 'complex', 'voordehandliggend', 'clever', 'Interessant', 'interessant', 'echt_oprecht_super_leuk', 'niet_te_easy', 'easy']

['Secure_by_Design', 'yes', 'yes', 'yes']
['but', 'simple', 'google', 'rootpasswd_weak_lol', 'leuk', 'cuda_helps', 'easy', 'entertaining']

user_19
Stated level: dit_is_mijn_eerste_ctf
Opinion on CTF education:
Stated learnings from day 1:
Security Mindset?:
Challenge the Cyber?:
Investment in sources: 13

['Botnets', 'yes', 'yes', 'yes']
[' leerzaam', 'leerzaam', ' interessant', 'makkelijk', 'leuk', ' leuk', ' snel', ' makkelijk', ' niet al te lastig']

['Digital_Forensics', 'NO', 'yes', 'yes']
[' leerzaam', ' interessant', 'leerzaam', 'leuk', ' leuk', ' niet moeilijk']

['Cloud_and_Linux', 'NO', 'yes', 'yes']
[' leerzaam', 'leerzaam', 'leuk', ' apart', ' leuk', ' goed te doen']

['Internet_of_Things', 'yes', 'NO', 'yes']
[' leerzaam', ' uitdagend', 'Leuk', 'leuk', ' lastig']

['Secure_by_Design', 'yes', 'yes', 'yes']
[' leerzaam', ' uitdagend', 'leuk', ' leuk', ' snel', ' lastig', 'uitdagend']

user_23
Stated level: beginner
Opinion on CTF education: uitdagend en leuke manier om belangrijke skills te leren
Stated learnings from day 1: Ja, een beetje
Security Mindset?: wanneer iemand inzicht heeft in de dreigingen
Challenge the Cyber?: nee helaas te oud
Investment in sources: 14

['Botnets', 'yes', 'yes', 'yes']
['snel', 'quizvraag', 'leuk', 'simpel', ' bekend', ' snel', 'eerder']

['Digital_Forensics', 'yes', 'yes', 'NO']
['niettemoeilijk', 'leerzaam', ' veelzijdig', 'leuk', 'interessant', ' snel']

['Cloud_and_Linux', 'yes', 'yes', 'yes']
[' misleidend', 'zeer', 'leerzaam', ' interessant', 'niettemoeilijk', 'leuk', 'moeilijk']

['Internet_of_Things', 'yes', 'NO', 'NO']
['onduidelijk', 'leerzaam', 'interessant', 'dachten', 'veelte', 'moeilijk']

['Secure_by_Design', 'yes', 'yes', 'yes']
['temakkelijk', ' interessant', 'leerzaam', 'leuk', 'interessant', 'optelossen', 'woord3', ' snel']

user_25

Stated level:	beginner
Opinion on CTF education:	Actief leren door het te doen. En de competitie
Stated learnings from day 1:	Ja, een beetje
Security Mindset?:	
Challenge the Cyber?:	
Investment in sources:	9

['Botnets', 'yes', 'yes', 'NO']
['incorrect', ' saai', 'simpel', 'Makkelijk', ' makkelijk', 'saai']

['Digital_Forensics', 'yes', 'yes', 'NO']
['temakkelijk', ' simpel', ' interesant', 'makkelijk', ' leuk', ' slim']

['Cloud_and_Linux', 'yes', 'yes', 'NO']
[' leerzaam', ' interessant', 'makkelijk', ' leuk', 'Makkelijk', ' makkelijkerdanverwacht']

['Internet_of_Things', 'yes', 'NO', 'NO']
['moeilijk', 'leerzaam', 'leuk']

['Secure_by_Design', 'yes', 'yes', 'NO']
[' simpel', ' sneaky', 'leuk', 'makkelijk', ' leuk', ' makkelijk']

user_26

Stated level:	dit_is_mijn_eerste_ctf
Opinion on CTF education:	jouw_antwoord
Stated learnings from day 1:	Nee, maar weinig
Security Mindset?:	
Challenge the Cyber?:	
Investment in sources:	2

['Botnets', 'yes', 'yes', 'NO']
[' woord3', 'woord1', ' woord2']

['Digital_Forensics', 'yes', 'NO', 'NO']
[' woord3', 'woord1', ' woord2']

['Cloud_and_Linux', 'yes', 'NO', 'NO']
[' woord3', 'woord1', ' woord2']

['Internet_of_Things', 'yes', 'NO', 'NO']
[' woord3', 'woord1', ' woord2']

['Secure_by_Design', 'yes', 'NO', 'NO']
[' woord3', 'woord1', ' woord2']

user_30
Stated level:
Opinion on CTF education:
Stated learnings from day 1:
Security Mindset?:
Challenge the Cyber?:
Investment in sources 12

['Botnets', 'yes', 'yes', 'yes']
[' leerzaam', ' prima', 'leuk', 'makkelijk', ' goed', ' leuk']

['Digital_Forensics', 'NO', 'yes', 'yes']
[' leerzaam', 'geinig', ' leuk', ' makkelijk', ' en', 'goed']

['Cloud_and_Linux', 'NO', 'yes', 'yes']
[' leerzaam', 'nice', 'makkelijk', ' grappig', ' leuk']

['Internet_of_Things', 'yes', 'NO', 'yes']
[' uitdagend', ' lastig', 'leuk']

['Secure_by_Design', 'yes', 'yes', 'yes']
[' JOHN', ' leerzaam', 'omweg', 'geinig', ' eerst', ' leuk', ' makkelijk', ' googlen', 'uitdagend']

user_31
Stated level: gemiddeld
Opinion on CTF education: eigen georganiseerde CTF events
Stated learnings from day 1: Ja, een beetje
Security Mindset?: security first en willen verbeteren in zijn vak
Challenge the Cyber?: zeker!
Investment in sources 15

['Botnets', 'yes', 'yes', 'yes']
[' #kali', ' 2', ' 3', ' wel_interessant', ' meer een quiz vraag', 'de challenge was vandaag ook meer een quiz vraag', 'makkelijk', 'simpel', ' ']

['Digital_Forensics', 'yes', 'yes', 'yes']
[' 3', ' woord3', ' goede tool zoeken', 'leuk', 'leuke challenge', 'opgelost met strings', ' goedlezen', ' en om te doen', ' wel leuk om te zien']

['Cloud_and_Linux', 'yes', 'yes', 'yes']
[' en leerzaam ', 'gedacht', 'Leuke opdracht', ' om te doen', ' was leuk om uit te zoeken hoe dit precies zat', 'Deze wist ik nog niet', 'makkelijker', 'dan', '2', '3)']

['Internet_of_Things', 'yes', 'yes', 'yes']
[' 3', ' wireshark', 'Lekker moeilijk zeg', ' pin', 'sister?', 'Leuk om een custom wordlist te maken', ' dacht eerst reaver', ' maar bleek toch default ', ' d']

['Secure_by_Design', 'yes', 'yes', 'yes']
['goed te doen', 'Ik ging de hash kraken van Alice kraken met hashcat', 'Leuk', ' bleek het gewoon admin te zijn :P', ' cracking!', ' wel leuk om te doen', ' leuk', ' makkelijk', ' d', ' defaultpassword']

user_33

Stated level:	gemiddeld
Opinion on CTF education:	CTF's_zijn_een_goede_leermethode
Stated learnings from day 1:	Nee, maar weinig
Security Mindset?:	
Challenge the Cyber?:	
Investment in sources	9

['Botnets', 'yes', 'yes', 'NO']
[' saai', 'makkelijk', ' wel_leuk', ' ...', ' makkelijk', 'botnets?!']

['Digital_Forensics', 'yes', 'NO', 'NO']
[' geleerd', ' leerzaam', 'leuk']

['Cloud_and_Linux', 'yes', 'yes', 'NO']
[' gemakkelijk', 'leerzaam', 'leuk', ' leuk', 'challenge_was_uitdagend', ' ..']

['Internet_of_Things', 'yes', 'NO', 'NO']
[' uitdagend', 'moeilijk', ' leerzaam', 'leuk']

['Secure_by_Design', 'yes', 'yes', 'NO']
[' saai', 'leerzaam', ' geen_uitdaging', ' leuk', ' ...', 'eenvouding']

user_47

Stated level:	beginner
Opinion on CTF education:	de uitdaging om op zoek te gaan naar de vlaggen
Stated learnings from day 1:	Nee, maar weinig
Security Mindset?:	wanneer iemand op zoek gaat naar kwetsbaarheden en dit meld aan de juiste instanties
Challenge the Cyber?:	Nee, ik ben te oud om mee te doen
Investment in sources	8

['Botnets', 'yes', 'yes', 'yes']
[' ...', ' saai', 'makkelijk']

['Digital_Forensics', 'yes', 'NO', 'NO']
[' beginnend', ' leerzaam', 'leuk']

['Cloud_and_Linux', 'yes', 'NO', 'NO']
[' ...', ' ongerelateerd', 'makkelijk']

['Internet_of_Things', 'yes', 'yes', 'NO']
[' leerzaam', ' uitdagend', 'leerzaam', ' leuk', 'moeilijk']

['Secure_by_Design', 'yes', 'yes', 'yes']
[' leerzaam', 'leuk', 'makkelijk', ' ...']

user_51

Stated level:	beginner
Opinion on CTF education:	je leert door spelletjes te spelen hoe hackers te werk gaan
Stated learnings from day 1:	Ja, heel veel
Security Mindset?:	wanneer je niet alleen denkt vanuit het perspectief van jezelf, maar ok dat van de hacker
Challenge the Cyber?:	
Investment in sources	10

['Botnets', 'yes', 'yes', 'yes']
[' leerzaam', 'verassend', ' interessant', 'leuk', 'makkelijk', ' goed', ' leuk', ' te doen', ' googelen']

['Digital_Forensics', 'yes', 'yes', 'NO']
[' leerzaam', ' uitdagend', ' verwarrend', 'leuk', ' fantastisch']

['Cloud_and_Linux', 'NO', 'NO', 'NO']
[]

['Internet_of_Things', 'NO', 'NO', 'NO']
[]

['Secure_by_Design', 'NO', 'NO', 'NO']
[]

user_53

Stated level:	gemiddeld
Opinion on CTF education:	competitief voor de lol en het aanleren van het gedachtegoed van echte cyberaanvallers
Stated learnings from day 1:	Ja, een beetje
Security Mindset?:	als_iemand_security_by_design_hanteert
Challenge the Cyber?:	maar_natuurlijk_:)
Investment in sources	15

['Botnets', 'yes', 'yes', 'yes']
[' incorrect', 'nadenken', ' saai', ' brainfart', ' snel', 'makkelijk', ' bijzonder', ' lastig']

['Digital_Forensics', 'yes', 'yes', 'yes']
[' uitdagend', ' interessant', ' osint', 'complex', 'simpel', ' forensisch', 'makkelijker', ' zoeken']

['Cloud_and_Linux', 'yes', 'yes', 'yes']
[' boeiend', 'makkelijk', 'interessant', ' kort', ' geluk', ' snel', ' red-teamingachtig']

['Internet_of_Things', 'yes', 'yes', 'yes']
['moeite', ' uitdaging', ' uitdagend', ' lastiger', ' boeiend', 'complexer', 'interessant', ' lastig', ' kraken']

['Secure_by_Design', 'yes', 'yes', 'yes']
[' saai', ' osint', 'makkelijk', ' beginner', ' snel']

user_54

Stated level:	gevorderd
Opinion on CTF education:	creëren van een CTF
Stated learnings from day 1:	Nee, maar weinig
Security Mindset?:	Wanneer iemand naar een normaal apparaat kijkt en nadenkt over hoe je dat eventueel kan aanvallen of juist verdedigen
Challenge the Cyber?:	misschien
Investment in sources	10

['Botnets', 'yes', 'yes', 'yes']
['beginner', ' saai', 'makkelijk', ' botnets?', 'botnet?', 'saai']

['Digital_Forensics', 'yes', 'NO', 'yes']
['cheated', 'beginner', ' cronjob', 'prima', 'leuk', ' makkelijk', 'saai']

['Cloud_and_Linux', 'yes', 'yes', 'yes']
['opniveau', 'leerzaam', 'makkelijk', 'leuk', 'top', 'auto-exploit', 'cronjob']

['Internet_of_Things', 'NO', 'yes', 'yes']
[' leerzaam', 'prima', ' uitdagend', 'pittig', 'leerzaam', 'mentalist', 'top', 'uitdagend']

['Secure_by_Design', 'yes', 'yes', 'yes']
['beginner', ' saai', 'prima', 'makkelijk', 'hetzelfde', ' beginner', 'saai']

user_60

Stated level:	dit_is_mijn_eerste_ctf
Opinion on CTF education:	
Stated learnings from day 1:	
Security Mindset?:	
Challenge the Cyber?:	
Investment in sources	3

['Botnets', 'NO', 'yes', 'NO']
['Tedoen', 'Leuk', 'Leerzaam']

['Digital_Forensics', 'NO', 'yes', 'NO']
[' Uitdagend', ' Leuk', 'Lastig']

['Cloud_and_Linux', 'NO', 'NO', 'NO']
[]

['Internet_of_Things', 'NO', 'NO', 'NO']
[]

['Secure_by_Design', 'NO', 'NO', 'NO']
[]

user_61

Stated level:	gemiddeld
Opinion on CTF education:	Leuke uitdaging en leerzaam voor zowel docent als student
Stated learnings from day 1:	Ja, heel veel
Security Mindset?:	
Challenge the Cyber?:	
Investment in sources	2

['Botnets', 'NO', 'NO', 'NO']
[]

['Digital_Forensics', 'NO', 'NO', 'NO']
[]

['Cloud_and_Linux', 'NO', 'yes', 'NO']
['nieuw', 'leerzaam', 'leuk']

['Internet_of_Things', 'NO', 'NO', 'NO']
[]

['Secure_by_Design', 'NO', 'NO', 'NO']
[]

user_65

Stated level:	beginner
Opinion on CTF education:	I really like it
Stated learnings from day 1:	Ja, een beetje
Security Mindset?:	als je denkt in hoever het systeem veilig is en dit kan proberen te breken
Challenge the Cyber?:	Hell yeah
Investment in sources	2

['Botnets', 'NO', 'NO', 'NO']
[]

['Digital_Forensics', 'NO', 'NO', 'NO']
[]

['Cloud_and_Linux', 'NO', 'NO', 'NO']
[]

['Internet_of_Things', 'NO', 'NO', 'NO']
[]

['Secure_by_Design', 'NO', 'NO', 'NO']
[' uitdagend', ' leerzaam', 'leuk']

user_69

Stated level:	dit_is_mijn_eerste_ctf
Opinion on CTF education:	ik weet niet
Stated learnings from day 1:	Nee, niets
Security Mindset?:	wat?
Challenge the Cyber?:	nee ik heb geen zin
Investment in sources	2

['Botnets', 'NO', 'NO', 'NO']
['normaal']

['Digital_Forensics', 'NO', 'NO', 'NO']
['normaal']

['Cloud_and_Linux', 'NO', 'NO', 'NO']
['normaal']

['Internet_of_Things', 'NO', 'NO', 'NO']
['normaal']

['Secure_by_Design', 'NO', 'NO', 'NO']
['normaal']

user_73

Stated level:	dit_is_mijn_eerste_ctf
Opinion on CTF education:	
Stated learnings from day 1:	Nee, niets
Security Mindset?:	
Challenge the Cyber?:	
Investment in sources	1

['Botnets', 'NO', 'NO', 'NO']
[]

['Digital_Forensics', 'NO', 'NO', 'NO']
[]

['Cloud_and_Linux', 'NO', 'NO', 'NO']
[]

['Internet_of_Things', 'NO', 'NO', 'NO']
[]

['Secure_by_Design', 'NO', 'NO', 'NO']
[]

Appendix 3: Participants results Case Study 2

See Appendix 2 for instructions on how to read.

user_80

Stated level:	beginner
Opinion on CTF education:	
Stated learnings from day 1:	
Security Mindset?:	
Challenge the Cyber?:	
Investment in sources	5

['Botnets', 'yes', 'NO', 'NO']
[' Zip?', 'Erg Groot Bestand', ' Leuk Idee']

['Digital_Forensics', 'yes', 'NO', 'NO']
[' Leerzaam', '', 'Leuke Opdracht']

['Cloud_and_Linux', 'NO', 'NO', 'NO']
[' verder is de opdracht leuk', ' leerzaam', 'Groote File Download niet erg leuk']

['Internet_of_Things', 'NO', 'NO', 'NO']
['Leerzaam', 'Nice', 'Lastig']

['Secure_by_Design', 'yes', 'NO', 'NO']
[' leerzaam', 'interresant', 'Makkelijke Quiz']

user_81

Stated level:	gevorderd
Opinion on CTF education:	Je leert veel verschillende methodes toe te passen
Stated learnings from day 1:	Ja, een beetje
Security Mindset?:	leuk
Challenge the Cyber?:	misschien
Investment in sources	12

['Botnets', 'yes', 'yes', 'yes']
[' gokken', ' te', 'veel', 'Makkelijk', ' makkelijk', ' simpel', ' geen vm nodig', 'super makkelijk', ' snel']

['Digital_Forensics', 'yes', 'yes', 'yes']
[' verschillende tools', ' redelijk te doen', ' eerdere opdracht', 'Leuk', 'nieuw', ' moeilijk', ' filesystem', ' anders', 'super makkelijk']

['Cloud_and_Linux', 'yes', 'yes', 'NO']
['Leuk', 'moeilijk', ' ', ' simpel', 'makkelijk', ' docker', ' snel']

['Internet_of_Things', 'yes', 'NO', 'yes']
['nieuw', 'eel moeilijk', ' makkelijk', ' ', 'extreem moeilijk', ' niet gelukt', ' snel', ' snap het niet']

['Secure_by_Design', 'yes', 'yes', 'yes']
[' gokken', 'Leuk', ' linux', 'makkelijk', ' bekend', ' john', ' snel']

user_82
Stated level: beginner
Opinion on CTF education:
Stated learnings from day 1:
Security Mindset?:
Challenge the Cyber?:
Investment in sources 2

['Botnets', 'NO', 'NO', 'NO']
[]

['Digital_Forensics', 'NO', 'NO', 'NO']
['irretant', 'parts', 'intressant']

['Cloud_and_Linux', 'NO', 'NO', 'NO']
[]

['Internet_of_Things', 'NO', 'NO', 'NO']
[]

['Secure_by_Design', 'NO', 'NO', 'NO']
[]

user_83
Stated level: dit_is_mijn_eerste_ctf
Opinion on CTF education:
Stated learnings from day 1:
Security Mindset?:
Challenge the Cyber?:
Investment in sources 11

['Botnets', 'NO', 'NO', 'NO']
[]

['Digital_Forensics', 'NO', 'NO', 'NO']
[]

['Cloud_and_Linux', 'NO', 'NO', 'NO']
[]

['Internet_of_Things', 'NO', 'NO', 'NO']
['leuk', ' leerzaam', ' uitdagend']

['Secure_by_Design', 'NO', 'NO', 'NO']
[]

user_86
Stated level: dit_is_mijn_eerste_ctf
Opinion on CTF education:
Stated learnings from day 1:
Security Mindset?:
Challenge the Cyber?:
Investment in sources 12

['Botnets', 'NO', 'NO', 'NO']
[]

['Digital_Forensics', 'yes', 'NO', 'NO']
[]

['Cloud_and_Linux', 'NO', 'NO', 'NO']
[]

['Internet_of_Things', 'yes', 'NO', 'NO']
[]

['Secure_by_Design', 'yes', 'NO', 'NO']
[]

user_87
Stated level:
Opinion on CTF education:
Stated learnings from day 1:
Security Mindset?: als_ze_nadenken_over_vulnerabilities
Challenge the Cyber?: ja
Investment in sources 2

['Botnets', 'yes', 'NO', 'NO']
['leerzaam', 'interessant', 'makkelijk']

['Digital_Forensics', 'yes', 'NO', 'NO']
['gemiddeld', '', 'interessant']

['Cloud_and_Linux', 'NO', 'NO', 'NO']
[]

['Internet_of_Things', 'NO', 'NO', 'NO']
[]

['Secure_by_Design', 'NO', 'NO', 'NO']
[]

user_88

Stated level:	beginner
Opinion on CTF education:	De_uitdaging_en_de_moeilijkheidsgraad
Stated learnings from day 1:	ja, een beetje
Security Mindset?:	Als_je_over_zelf_gemaakte_dingen_na_gaat_denken_of_ze_veilig_zijn
Challenge the Cyber?:	ja
Investment in sources	7

['Botnets', 'yes', 'yes', 'yes']
['eentonig', 'saai', 'makkelijk', 'leerzaam', 'leuk']

['Digital_Forensics', 'yes', 'NO', 'NO']
['leuk', 'logisch', 'uitdagend']

['Cloud_and_Linux', 'NO', 'NO', 'NO']
['leerzaam', 'moeilijk', 'onoverzichtelijk']

['Internet_of_Things', 'NO', 'NO', 'NO']
['leerzaam', 'moeilijk', 'uitdagend']

['Secure_by_Design', 'yes', 'NO', 'NO']
['leuk', 'makkelijk', 'uitdagend']

user_89

Stated level:	beginner
Opinion on CTF education:	leuk_uitdagend_leerzaam
Stated learnings from day 1:	Ja, een beetje
Security Mindset?:	leuk, leerzaam, uitdagend
Challenge the Cyber?:	wie_weet
Investment in sources	4

['Botnets', 'NO', 'NO', 'NO']
['leuk', ' leerzaam', ' uitdagend']

['Digital_Forensics', 'NO', 'NO', 'NO']
['leuk', ' leerzaam', ' uitdagend']

['Cloud_and_Linux', 'NO', 'NO', 'NO']
['leuk', ' leerzaam', ' uitdagend']

['Internet_of_Things', 'NO', 'NO', 'NO']
['leuk', ' leerzaam', ' uitdagend']

['Secure_by_Design', 'NO', 'NO', 'NO']
['leuk', ' leerzaam', ' uitdagend']

user_92

Stated level:	beginner
Opinion on CTF education:	
Stated learnings from day 1:	
Security Mindset?:	Wanneer iemand constant zoekt naar kwetsbaarheden
Challenge the Cyber?:	Ja
Investment in sources	5

['Botnets', 'NO', 'NO', 'yes']
[' leuk', ' interressant', 'Beetje makkelijk']

['Digital_Forensics', 'NO', 'NO', 'NO']
[]

['Cloud_and_Linux', 'NO', 'NO', 'yes']
[' leuk', ' leerzaam', 'makkelijk']

['Internet_of_Things', 'NO', 'NO', 'NO']
[]

['Secure_by_Design', 'NO', 'NO', 'yes']
[' interresant', ' leuk', 'uitdagend']

user_93

Stated level:	
Opinion on CTF education:	je leert op een leuke manier, je kunt met moeilijkere challenges ook jezelf uitdagen om wat lastigere opdrachten te maken
Stated learnings from day 1:	Ja, een beetje
Security Mindset?:	
Challenge the Cyber?:	
Investment in sources	9

['Botnets', 'NO', 'NO', 'NO']
[' leuk', ' Handig', ' Interresant', ' makkelijk', 'snel', 'Nieuw']

['Digital_Forensics', 'yes', 'NO', 'NO']
[' Handig', 'Leuk', 'Lastig', ' moeilijk', ' uitdagend', ' Nieuw']

['Cloud_and_Linux', 'NO', 'NO', 'NO']
[' leuk', ' makkelijk', 'snel', ' handig', ' interresant', 'leuk']

['Internet_of_Things', 'yes', 'NO', 'NO']
[' nieuw', ' leuk', ' makkelijk', 'snel', ' interresant', 'leuk']

['Secure_by_Design', 'yes', 'NO', 'NO']
[' leuk', ' makkelijk', 'snel', 'makkelijk', ' niet nieuw', ' snel']

user_94
Stated level:
Opinion on CTF education: nietaltijdmaarsomswelleuk
Stated learnings from day 1: Ja, een beetje
Security Mindset?:
Challenge the Cyber?:
Investment in sources 9

['Botnets', 'NO', 'NO', 'NO']
[' leuk', ' lastig', ' handig', 'interessant']

['Digital_Forensics', 'yes', 'NO', 'NO']
[' leuk', ' lastig', ' handig', 'interessant']

['Cloud_and_Linux', 'NO', 'NO', 'NO']
[' leuk', ' lastig', ' handig', 'interessant']

['Internet_of_Things', 'yes', 'NO', 'NO']
[' goedequiz', ' leuk', 'Prima', 'interessant', ' lastig']

['Secure_by_Design', 'yes', 'NO', 'NO']
[' leuk', ' lastig', ' handig', 'interessant']

user_95
Stated level: beginner
Opinion on CTF education: Het is een totaal andere leervorm, ook is toch een kleine wedstrijd wat het ook wel leuk maakt
Stated learnings from day 1: Ja, een beetje
Security Mindset?: Een fout of kwetsbaarheid te indentificeren, en deze koste wat het kost proberen op te lossen
Challenge the Cyber?: Misschien
Investment in sources 15

['Botnets', 'NO', 'NO', 'NO']
[' leerzaam', 'interessant', 'Leuk', ' tof']

['Digital_Forensics', 'yes', 'NO', 'NO']
[' leuk', ' leerzaam', 'interessant', 'Leuk']

['Cloud_and_Linux', 'NO', 'NO', 'NO']
[' hendig', ' leerzaam', 'interessant', 'Leuk']

['Internet_of_Things', 'yes', 'NO', 'NO']
[' gaaf', ' leerzaam', 'interessant', 'Leuk']

['Secure_by_Design', 'yes', 'NO', 'NO']
[' hendig', ' leerzaam', 'interessant', 'Leuk']

user_99

Stated level:	dit_is_mijn_eerste_ctf
Opinion on CTF education:	VEELNIEUWEOPTIESENSPEURWERK
Stated learnings from day 1:	Ja, een beetje
Security Mindset?:	wanneer iemand goed is in een bepaald onderwerp en niet zozeer alles, het onderwerp is dan wel cyber security
Challenge the Cyber?:	<script>alert("Nee, ik heb helaas geen interesse")</script>
Investment in sources	12

['Botnets', 'yes', 'yes', 'yes']
['', 'Spannend', 'Uitdagend', 'Leuk']

['Digital_Forensics', 'yes', 'yes', 'yes']
['', 'leuk', 'makkelijk', 'teverwachten']

['Cloud_and_Linux', 'yes', 'yes', 'NO']
['onlogischeflagnotatie', 'zoekend', 'gemakkelijk', 'easy', 'onduidelijk', 'makkelijk', 'goedvorobeginners', 'leuk', 'google']

['Internet_of_Things', 'yes', 'NO', 'NO']
['', 'moeilijk', 'stom', 'voordehandliggenen', 'lastig', 'leuk', 'google']

['Secure_by_Design', 'yes', 'yes', 'yes']
['Leerzaam', 'gemakkelijk', ' Prettig', ' Begrijpelijk', 'vanzelfsprekend', 'leuk', 'google']

user_101

Stated level:	
Opinion on CTF education:	
Stated learnings from day 1:	
Security Mindset?:	Ja, je leert zwakheden om jezelf daarvoor te beschermen.Als hij/zij probeert veilig te werken en backups maakt.
Challenge the Cyber?:	Ja, maar ik beloof niks!
Investment in sources	5

['Botnets', 'NO', 'yes', 'NO']
[' onmogelijk', ' null', 'ARM64', ' refreshing', 'makkelijk', ' snel']

['Digital_Forensics', 'NO', 'NO', 'NO']
[]

['Cloud_and_Linux', 'NO', 'yes', 'NO']
['leuk', ' leerzaam', ' uitdagend']

['Internet_of_Things', 'NO', 'NO', 'NO']
['t_challeng']

['Secure_by_Design', 'yes', 'NO', 'yes']
['Leuk', ' leerzaam', ' su-root', 'EASY', ' 3-minuten', 'Makkelijk']

user_103
Stated level:
Opinion on CTF education: lijkt me wel handig, maar dan moet het wel bij het onderwerp passen wat die week word gegeven
Stated learnings from day 1: Nee, niets
Security Mindset?:
Challenge the Cyber?:
Investment in sources 1

['Botnets', 'NO', 'NO', 'NO']
[]

['Digital_Forensics', 'NO', 'NO', 'NO']
[]

['Cloud_and_Linux', 'NO', 'NO', 'NO']
[' leerzaam', 'moeilijk', ' uitdagend']

['Internet_of_Things', 'NO', 'NO', 'NO']
[]

['Secure_by_Design', 'NO', 'NO', 'NO']
[]

user_106
Stated level:
Opinion on CTF education:
Stated learnings from day 1: een beetj
Security Mindset?:
Challenge the Cyber?:
Investment in sources 3

['Botnets', 'NO', 'NO', 'NO']
[]

['Digital_Forensics', 'NO', 'NO', 'NO']
[]

['Cloud_and_Linux', 'NO', 'yes', 'NO']
[' moeilijk', 'raar', ' uitdagend']

['Internet_of_Things', 'NO', 'NO', 'NO']
[]

['Secure_by_Design', 'NO', 'NO', 'NO']
[]

user_107
Stated level:
Opinion on CTF education:
Stated learnings from day 1:
Security Mindset?: als ze niet achterlopen
Challenge the Cyber?: had heel graag meegdaan, heb er geen tijd voor
Investment in sources 2

['Botnets', 'NO', 'NO', 'NO']
[]

['Digital_Forensics', 'NO', 'NO', 'NO']
[]

['Cloud_and_Linux', 'NO', 'NO', 'NO']
[' prima', ' moeilijk', 'langdradig']

['Internet_of_Things', 'NO', 'NO', 'NO']
[]

['Secure_by_Design', 'NO', 'NO', 'NO']
['oke', 'moeilijk', 'uitdagend']

user_109
Stated level:
Opinion on CTF education:
Stated learnings from day 1:
Security Mindset?: Als een persoon zowel kijkt naar de beveiliging als het pentesten.
Challenge the Cyber?: Nee
Investment in sources 3

['Botnets', 'NO', 'NO', 'NO']
[]

['Digital_Forensics', 'NO', 'NO', 'NO']
[]

['Cloud_and_Linux', 'NO', 'NO', 'yes']
[' onduidelijk', 'moeilijk', ' uitdagend']

['Internet_of_Things', 'NO', 'NO', 'NO']
[]

['Secure_by_Design', 'NO', 'NO', 'yes']
[' onduidelijk', 'moeilijk', ' uitdagend']

user_113
Stated level:
Opinion on CTF education:
Stated learnings from day 1:
Security Mindset?:
Challenge the Cyber?:
Investment in sources 2

['Botnets', 'NO', 'NO', 'NO']
[]

['Digital_Forensics', 'NO', 'NO', 'NO']
[]

['Cloud_and_Linux', 'NO', 'NO', 'NO']
[]

['Internet_of_Things', 'NO', 'NO', 'NO']
[]

['Secure_by_Design', 'NO', 'NO', 'yes']
['leerzaam', 'moeilijk', 'uitdagend']