The teacher's training kit

Jugersa Smaja | Fabian Brackhane – Institute for Security and Safety GmbH

Co-funded by the
Erasmus+ Programme
of the European Union

The Cyber4Schools project offers a game-based approach to the topic of digital security. This training kit is aimed and will be made available to the teachers which are participating in the course developed at the beginning of the project. The materials, as previously determined on the O2 deliverables, will be offered during the three training phases for which the Insitute for Security and Safety is responsible for.

The three training stages will include:

1. First Training Stage:
- A list of documents about digital security selected by the partnership among the available online materials produced at EU level and national level (Germany, Estonia and Poland)
- A guide on digital security aspects

2. Second Training Stage:
- A handbook on the implementation, operation and correct distribution of the game on digital security for secondary school pupils with a detailed description of the task of the trainer, facilitator or teacher

3. Third Training Stage:
- Game Playbook: A handbook for the general organisation of the game which will include a set of rules, strategies and payoffs (consequences) for the players and instructions for the educators (teachers) running the game where applicable

NB: Every term in this text marked with an □ *arrow* will be explained in the separate document **"Guide to Cyber Security"**.

1 First Training Stage

1.1 Documents on the topics of digital security

- The ethics of cybersecurity (2020): Https://Library.Oapen.Org/Bitstream/Handle/20.500.12657/47324/9783030290535.Pdf?Sequence=1#Page=111
- The influences of the digital revolution on the educational system of the EU Countries (2019): https://essuir.sumdu.edu.ua/bitstream-download/123456789/74845/1/Cosmulese_mmi_3_2019.pdf
- Digital policies: Comparison between EU, EEU and their member-states (2020): https://www.researchgate.net/profile/Maksim-Vilisov/publication/342765808_DIGITAL_POLICIES_COMPARISONS_BETWEEN_EU_EEU_AND_THEIR_MEMDER-STATES/links/5f059B144585155050948377/DIGITAL-POLICIES-COMPARISONS-BETWEEN-EU-EEU-AND-THEIR-MEMDER-STATES.pdf
- The new EU cybersecurity framework – The NIS directive, ENISA's role and the general data protection regulation (2019): https://reader.elsevier.com/reader/sd/pii/S0267364919300512?tOKEN=516F2DD70B147ECB2E95F5E0556E26E2493D464856C0CEA19C3313E08805412EA51724E764DA371A7027437249272497&originRegion=eu-west-1&ORiginCREATION=20220218155323
- The EU digital education action plan: Opportunities for European universities (2020): https://www.fundacioncyd.org/wp-content/uploads/2021/09/ICYD2020_D_MONOGRAFIA.pdf
- Analysis of disparities in the use of information and communication technology (ICT) in the EU countries (2021): https://jssidoi.org/jesi/uploads/articles/34/Aleksejeva_Analysis_of_disparities_in_the_use_of_information_and_communication_technology_ICT_in_the_EU_countries.pdf
- Cybersecurity in Poland (2022): https://library.oapen.org/bitstream/handlE/20.500.12657/51461/9783030785512.pdf?sequence=1#PAge=436
- Annual cyber security assessment (2019): https://www.ria.ee/sites/default/files/content-editors/kuberturve/ktt_aastaraport_eng_web.pdf

1.2 A short guide on digital security aimed at teachers and facilitators

It is important to distinguish the differences between the aspects of *Digital Security* and *Cyber Security*. While Cyber Security covers a broader range of aspects including the security of the infrastructure, the networks, the systems or the information, Digital Security on the other hand is limited to the security of digital stored information.

As the platform itself tends to dive deeper into the Cyber Security aspects, we recommend following the below structure as a guide to what is needed to know before playing the game from the teacher's perspective. This guide is developed in the separate file **"Guide to Cyber Security".**

Content of the "Guide on Cyber Security"

1. Introduction to Cyber Security: Threats, Vulnerabilities and Attacks
2. Common Terminology
3. Attack Types
4. System Overview: Windows vs. Linux
5. Attack Mechanisms
6. Security Measures

Additionally, we would recommend something less technical, leaning more towards the Digital Security aspects:

- https://bootcamp.berkeley.edu/blog/cybersecurity-in-education-what-teachers-parents- and-students-should-know/
- https://www.security.org/digital-safety/

Co-funded by the Erasmus+ Programme of the European Union

2 Second Training Stage

The following section will serve as a handbook on the implementation, operation and the correct distribution of the game on digital security for pupils with a detailed description of the tasks for the trainer.

2.1 Implementations of the Game (O3 draft)

THE MACHINES: The game itself consists of a number of *virtual machines* that will be available for the pupils. The purpose of this, is to give the pupils a suitable and realistic environment to test their skills and knowledge regarding cyber security. The first machine will be a Windows 10 system, not only representing a machine for normal and everyday use (and most probable to be a target for attacks), but also a machine that the defense team ("Blue team") will find very suitable. "Windows 10 machine specials" including the features that could be used to fortify and protect from attacks, will be a main part of the pupil's material kit at a later stage. This will introduce the pupils to the potentials of the Windows machine from a security perspective.

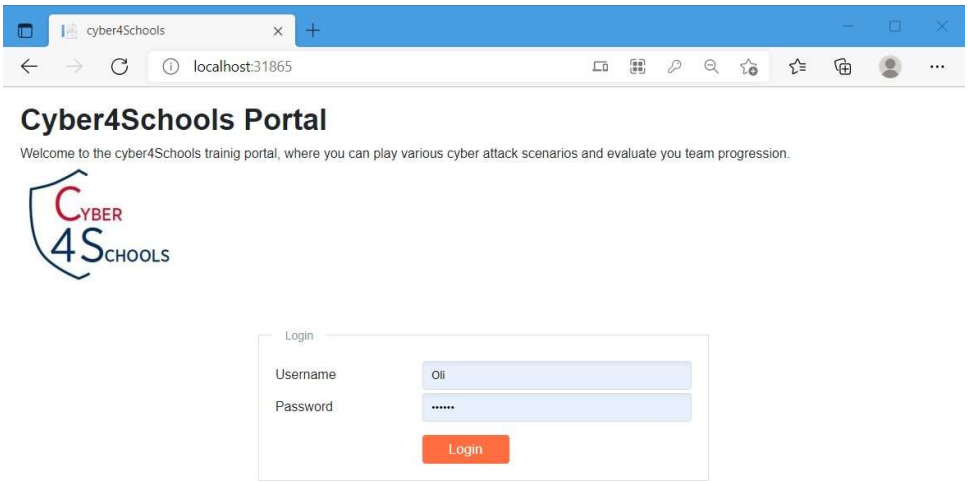
The second machine will be a Linux System. Just as in the real life, Linux has been the most preferred machine for attackers as well as ethical hackers. For this reason, this machine will be provided to the "red team", whose aim will be to surpass the security in front of the Windows Machine and further attack using the built-in attack tools of Linux.

THE SCENARIOS: The game will be played through the guidance and instructions of the Scenarios prepared by the Institute for Security and Safety GmbH, each of them simulating real life examples of attack. There will be tasks for each of the teams regarding these scenarios: some of them have to create and deliver the attacks (the REDs), while others have to put the right measures to protect/stop the attack from happening or escalating (the BLUEs).

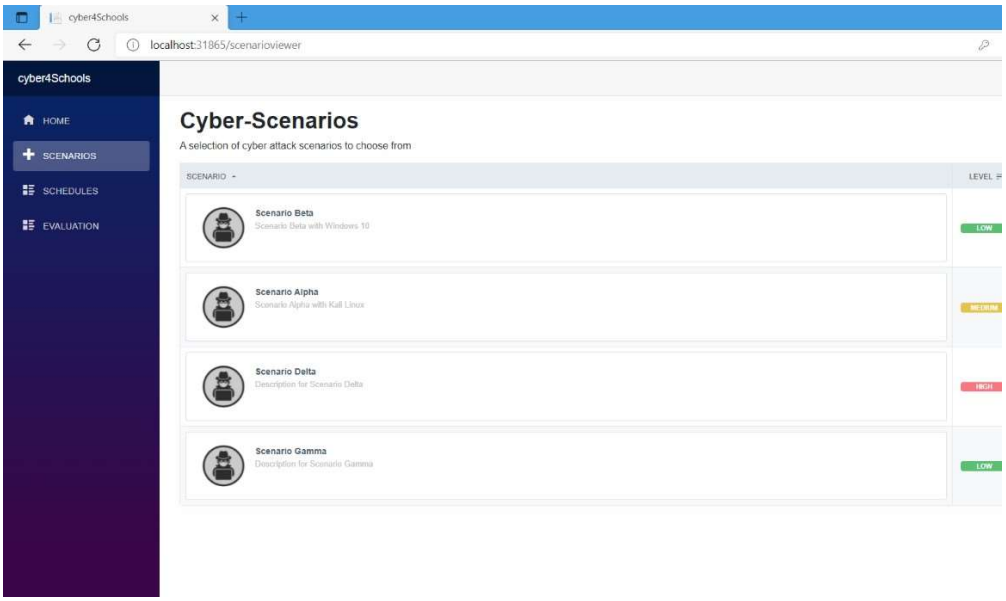
Some of the already prepared scenarios are described on the O3 draft and they cover some of the main concepts of Cyber Security, such as *Social Engineering*, Network Security, Web Application Security, Password Security or *Malware*.

THE WEBSITE: There will be a website available for the game, where most of the platform's features will be observable. These features will include the interfaces for the ranking system, the awards, the scheduling of the game, the team creation, scenario booking options, etc.

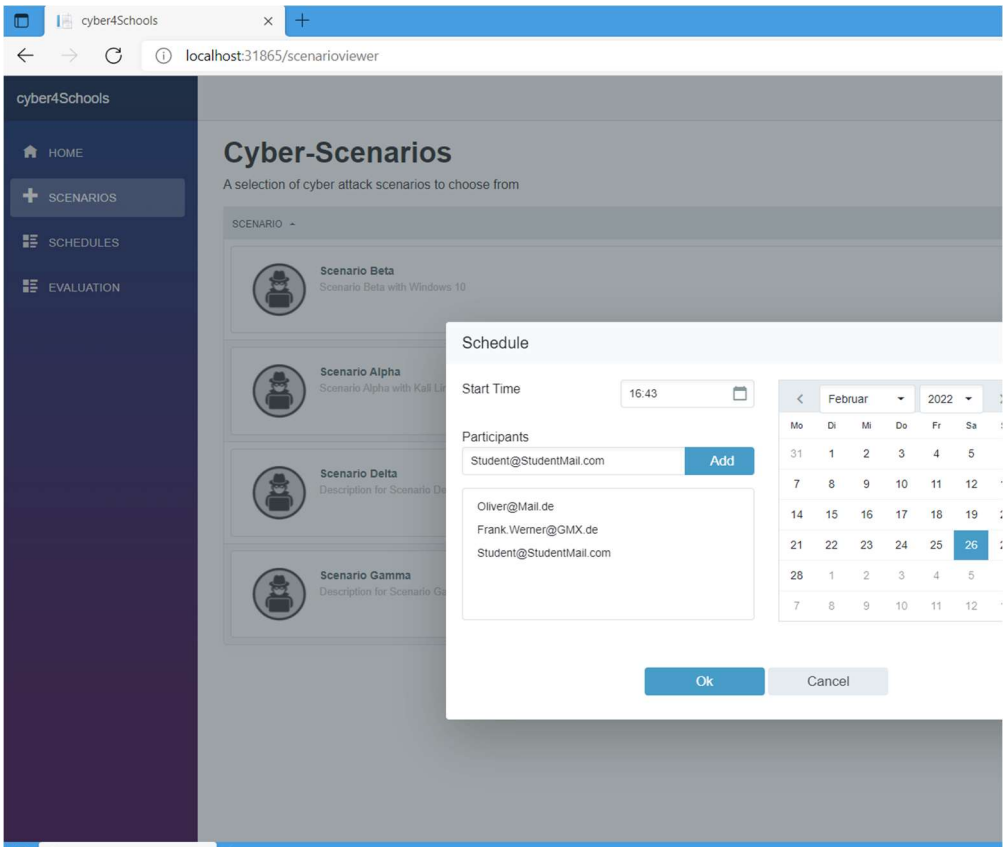
The below screenshoots respresent a demo look of the C4S portal:



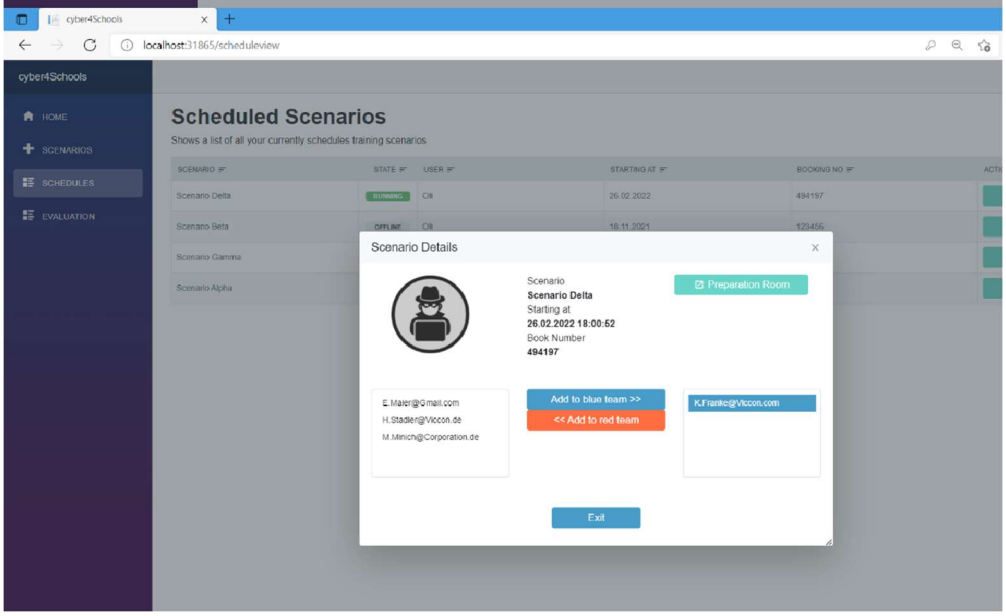
1. **User Login Page**



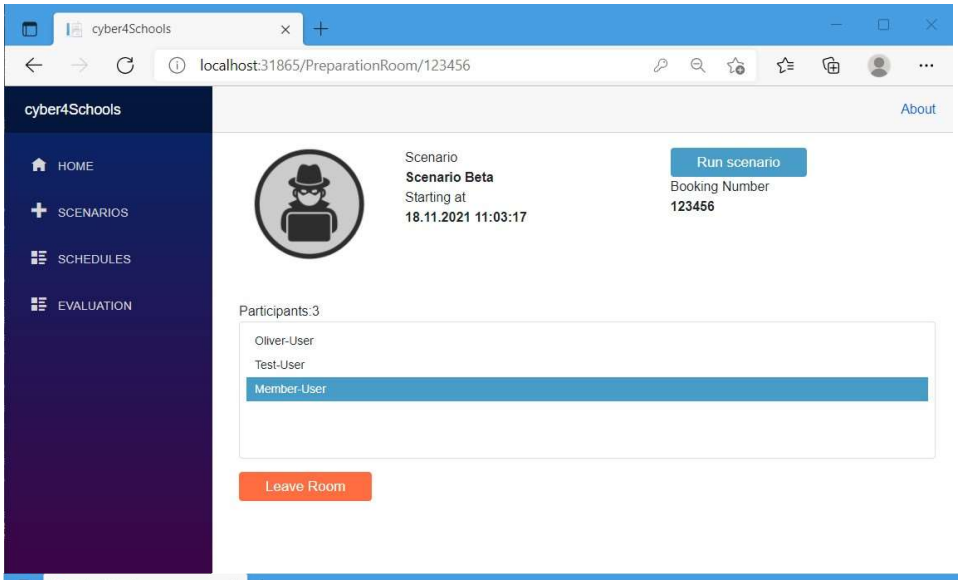
2. **Scenarios**



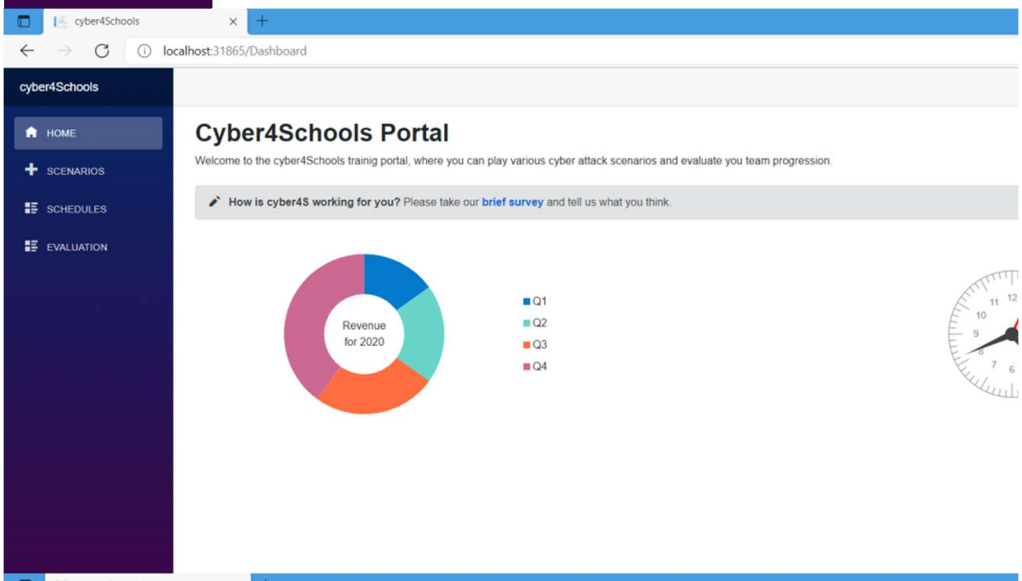
3. Scenario Scheduling



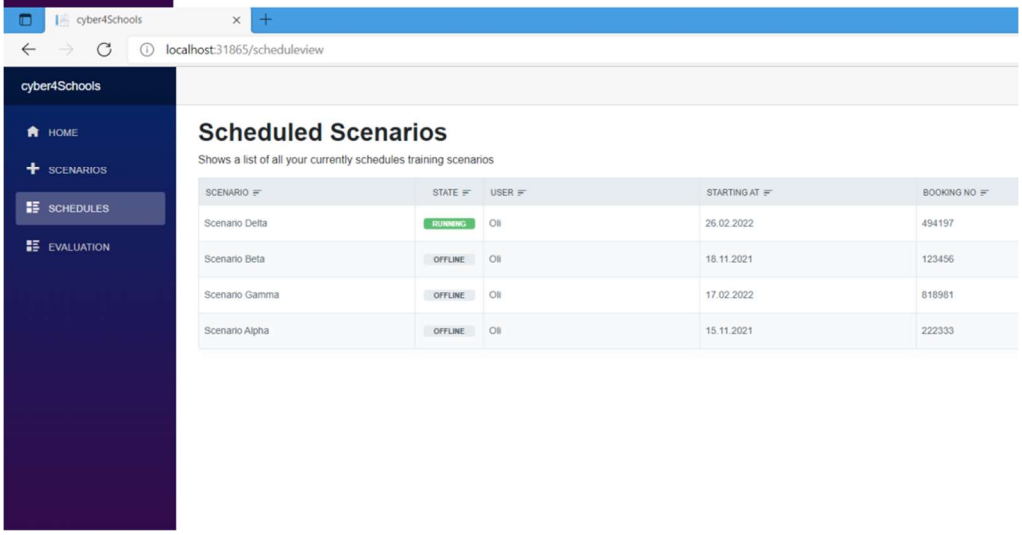
4. Scenario Booking and Team Creation



5. Room Preparation



6. Dashboard View



7. Cyber4 Schools Booking

Co-funded by the Erasmus+ Programme of the European Union

2.2 Operation and Distribution of the Game (O3 draft)

The path that teachers/facilitators/trainers should follow has similarities to the pupils' path. It is understandable that responsibilities for each will be completely different. For example:

Task 1: Cyber Security – Theoretical Material

Teachers will be provided their own material kits regarding cyber and digital security. They will also receive training on the matter to reach a deeper familiarization and understanding of Cyber Secutity terms that will be used during the game.

Later they will have to explain the learning outcomes and the theoretical contents to pupils using the pupils material kit that will also be provided at a later stage.

Task 2: Pre-game

During this stage the teachers will have to explain the gamer types as well as the game mechanics to the pupils. They will also book a scenario and assign the pupils to a team.

Task 3: On Game

The teacher's responsiblities during this stage will be linked to the raised issues during the execution of the game by the pupils. Teachers will have to stay attentive and deal with the issues to make the game less challenging to the pupils facing difficulties.

Task 4: After Game

Here, it is the teachers' responsibility to summarize and recap the most key lessons pupils need to focus on as the game is finished. It is very important to emphasize that these lessons should satisfy whole purpose of the Cyber4Schools game.

2.3 Tasks for the Teacher / Facilitator / Trainer

As the game is executed, the teachers should stay attentive and provide their support if any technical/non-technical issue arises (white team). Therefore, they need to have a clear understanding of the Blue/Red team capabilities for each of the Easy/Advanced levels. Also, they should be able to distinguish the tasks and responsibilities for each of the teams.

The teachers also need to track the pupils' progress in real-time. They can provide their support by also giving hints and disclosing further details of the scenario events to the pupils facing challenges.

In addition, it is their task to give the students enough time to work on the individual subtasks:

- Beginner mode - 15 mins per exercise
- Advanced mode - 30 mins per exercise

Teachers should have a clear understanding of the purpose of the game (as there are attacks involved, pupils might get confused what is considered ethical or not).

Co-funded by the Erasmus+ Programme of the European Union

At the end of each exercise, teachers may point out the main lessons learnt and make sure the right message is delivered. To facilitate this process, there will be follow-up questions regarding each exercise that will also open topics for discussion.

3 Third Training Stage

The third deliverable includes the game playbook including the rules, the strategies, the players payoffs as well as instructions aimed at the trainers/teachers.

THE RULES	THE STRATEGIES	PLAYER PAYOFFS	TEACHER'S INSTRUCTIONS
a. Game competences: - Each of the pupils should read the material kits before playing the game to familiarize themselves with the game mechanics and Cyber Security terms. b. Teams and Groups: - Pupils need to have clear understanding of the Blue and Red team responsibilities. - Pupils can choose between the Blue and Red team before playing the game. - Pupils also need to decide on the player mode between Easy/Advanced. - Team size is limited to 6. c. Timing: - The game is usually scheduled at a fixed time. - Pupils need to observe the time	The pupils need to read and follow the scenario description behind the exercises. Each of the scenarios comes with questions in form of a quiz that need to be solved. Questions will serve as a guidance for the whole solving of the exercises for both the Blue and the Red team. Follow-Up Questions will also help the pupils focus on the most important lessons learnt as well as open new topics for discussion.	a. Ranking: - The ranking feature will list the most successful teams, considering the scenario chosen as well as the difficulty mode. b. Awards: - There will be multiple awards handed to the pupils with the highest ranks. c. Points, hints and tasks: - This will be developed at a later stage as the game is currently under development.	Teachers should make sure all the bullet-points of the second stage training are met. There will be detailed descriptions of the teacher's tasks as soon as the game is fully developed.

limit set for Easy and Advanced levels.

d. Aim:
- Pupils need to choose between multiple scenarios.
- Each of the scenarios represent a simulation of a real life attack.
- Pupils need to solve the set tasks within a given time for the selected event/scenario.
- Team work should be effective in order to solve the exercises.