ECSC RULES

SEPTEMBER

TABLE OF CONTENTS

1. INTRODUCTION

The European Cyber Security Challenge is an event that allows top European cyber talent to compete against each other. The following rules are crucial to meet the quality expectations with regards to fair play and respect. The rules are kept as short as possible to avoid complexity and are agreed upon by the Steering Committee a year prior to each Final.

Each member of the Steering Committee can propose amendments to these rules, which will be voted by the Committee according to the principles defined in the ECSC Charter

2. CODE OF CONDUCT

Both players and the jury are expected to fully embrace principles of good sportsmanship to compete fairly, to judge by merit, try not to exploit the game system or the rules in unintended ways. Please consider fair play, even if something is not listed in the rules below. Wherever the latter is not obvious, jury should be consulted before any action taken.

3. RULES

Teams	
Composition	A maximum of 10 people per team and a minimum of 5 per team.
Age	Each team is formed of a maximum of 5 seniors (ages between 21–25), with no limitations in the number of juniors (ages between 14- 20) with a maximum of 10 teammates. The cut-off date for both categories is the 31th December of the competition year..
Nationality	The contestants are from the nationality of the country they represent.
Technical Lead (Captain)	Each team should nominate a technical lead. This person will be the one allowed to discuss team issues with the organization during the competition. The jury will only accept one person per team as technical lead. Questions from other teammates will not be answered.
Respect	Participants shall respect the teamwork of the other teams.
Coach	The coach is responsible for the well-being and behaviour of the contestants and making sure that essential information reaches its recipients and is understood and acted upon. During the competition, the coach will be physically separated from the team players. Communication between coach and team is always on open channel, i.e., within clear earshot of other coaches and limited to non-technical, general level, e.g.: ● Suggesting priorities ● Reporting challenge status (but not technical details or hints) ● General logistics assistance More information about the coach role can be found in the document “Roles definition and limitations”
Physical Attacks	Physical violence and attacks are strictly prohibited.
Presentation PC	Contestants must use the provided presentation computer (Microsoft Windows, PowerPoint, and PDF) for the public presentation. Slides and animations should be tested in advance.
Cheating	
Teamwork	Any kind of communication with people who are not part of the team is not permitted; the only exceptions are communication between the team captain with the organization and communication between coaches and their team. Sharing flags, exploits or any other information among other teams is strictly prohibited, except when explicitly permitted by the challenge description.
Platform	
DoS/DDoS	Participants shall not perform denial of service attacks. We all depend on one working network and therefore just bringing services down is not what we want here.
Network Interruption	Participants shall not pollute/poison/jam the provided wired of Wi-Fi networks. The network is required for running the challenge.
Network Devices	Participants may only connect their devices to the ports enabled by the organization; they will be communicated at the beginning of the competition.
Layer 2 Attacks	Participants shall not use Layer 2 attacks in the wired or wireless network.

Credentials	Each participant can only use the access credentials provided. Credentials cannot be exchanged or reused.
Scoring System	Participants shall not interfere with the scoring system.
Monitoring System	Participants shall not interfere with the monitoring system.
Platform Infrastructure	Participants shall not interfere with the platform infrastructure.
Allowed Hardware/Software	The software and hardware allowed during the competition should be approved by the Steering Committee no less than two months prior to the Final.
Scoring	The scoring system should be approved by the Steering Committee no less than two months prior to the Final.
Lockout	If a participant is locked out from a server/service, the team Captain should ask the designated challenge staff for help.
Public write-ups	No write-ups about the tasks may be published by participants during the challenge.

ENISA
European Union Agency for Cybersecurity

Athens Office
1 Vasilissis Sofias Str.
151 24 Marousi, Attiki, Greece

Heraklion Office
95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Greece

enisa.europa.eu