PES UNIVERSITY

PESU SOC

PESU ISFCR

CYBERCLASH

RULE BOOK

CYBERCLASH
RULE BOOK

This rulebook is designed to ensure fair play, safety, clarity, and fun during CyberClash. The goal is to give teams maximum creative freedom while maintaining ethical, legal, and technical boundaries so the event runs smoothly.

1. EVENT OVERVIEW

CyberClash is a competitive cybersecurity hackathon focused on attack–defend thinking, problemsolving, teamwork, and learning. Teams may be required to analyze systems, identify vulnerabilities, defend assets, or simulate attacks only within defined scopes. This is a controlled, educational environment, not real-world hacking.

2.TEAM COMPOSITION

• Teams must consist of 4 members .
• Team members cannot change after registration closes.
• Cross-team collaboration or sharing of solutions is strictly prohibited.
• Each team must nominate one point-of-contact for official communication.

Phase 1: Environment Setup and System Build

In this phase, both Red Team and Blue Team members are required to design, configure, and prepare their respective systems and tools.

* Blue Teams will focus on setting up monitoring, logging, detection, and response mechanisms.
* Red Teams will prepare their attack strategies, tools, and methodologies.

CYBERCLASH
RULE BOOK

Phase 2: Attack and Defense Simulation
In this phase, the live simulation begins.
* Teams will be assigned by the organizers to attack specific teams based on the selected problem statements and to defend against assigned adversaries.
* Red Teams will execute controlled attacks based on the problem statements provided by the organizers.
* Blue Teams will detect, analyze, respond to, and document incidents in real time.

3.GENERAL CODE OF CONDUCT
All participants are expected to:
• Act professionally and respectfully toward organizers, mentors, judges, and other teams.
• Compete ethically and honestly.
• Follow instructions provided during briefings and updates.
Zero Tolerance
The following will result in immediate disqualification:
• Harassment, intimidation, or discrimination of any kind.
• Cheating, plagiarism, or copying another team's work.
• Tampering with infrastructure outside the allowed scope.
• Attempting to sabotage another team physically or digitally.

CYBERCLASH
RULE BOOK

4.SCOPE OF ATTACK & DEFENSE

Allowed Scope

Participants may:

• Attack only the systems, applications, IPs, files, or environments explicitly provided by organizers.

• Use tools and techniques relevant to the challenge objectives.

• Analyze logs, binaries, traffic, or code provided as part of the challenge.

Out-of-Scope (STRICTLY PROHIBITED)

Participants must NOT:

• Attack any real-world system, website, or network.

Scan or probe:

• Other teams' personal devices

• Organizers' systems

• College/university networks

• Perform DoS/DDoS attacks unless explicitly allowed in a specific challenge.

• Exploit vulnerabilities in the event platform itself (website, scoring system, infrastructure).

• If something is not explicitly allowed, assume it is not allowed.

CYBERCLASH
RULE BOOK

5.TOOL USAGE POLICY

Allowed Tools

• Open-source security tools (e.g., Nmap, Burp Suite Community, Wireshark, Metasploit modules within scope)
• Custom scripts written by your team
• Provided virtual machines, containers, or sandboxes

Restricted / Disallowed Tools

• Automated exploitation frameworks that perform uncontrolled attacks
• Tools requiring paid licenses (unless explicitly permitted)
• AI tools used to auto-generate full solutions without understanding

Organizers reserve the right to ban any tool that threatens fairness or stability.

6.AI & EXTERNAL HELP POLICY

• AI tools (ChatGPT, Copilot, etc.) may be used only for learning, syntax help, or brainstorming.
• Directly copying solutions, exploit code, or write-ups is not allowed.
• Internet access is permitted unless restricted for a specific challenge.
• Asking mentors for hints is allowed; asking for solutions is not

CYBERCLASH
RULE BOOK

7.DATA HANDLING & PRIVACY

Participants must:

• Not upload challenge data to public repositories or forums.
• Not share flags, answers, or hints outside their team.
• Delete provided datasets or credentials after the event if instructed.

Any leakage of sensitive data will be treated seriously.

8.SUBMISSION RULES

• Submissions must be made only through the official submission channel.
• Late submissions will not be considered unless explicitly allowed.
• Each submission must include:
• Solution / exploit / defense explanation
• Tools used
• Clear reasoning or methodology

Incomplete or unclear submissions may receive reduced scores.

CYBERCLASH
RULE BOOK

9.SCORING & JUDGING

Judging will be based on:

- Correctness
- Depth of understanding
- Creativity and innovation
- Clarity of explanation
- Adherence to rules

Judges' decisions are final and binding.

10.WARNINGS, PENALTIES & DISQUALIFICATION

Warning System

- First violation: Verbal or written warning
- Second violation: Score penalty
- Severe violation: Immediate disqualification

Examples of Severe Violations

- Attacking out-of-scope systems
- Sharing flags or answers
- Intentionally disrupting the event
- Ignoring organizer instructions

11. TECHNICAL ISSUES

- Teams are responsible for their own devices and backups.

Organizers are not responsible for:

- Data loss due to local issues
- Misconfigured personal systems
- If a challenge environment fails, notify organizers immediately.

Do not attempt to fix or bypass infrastructure issues yourself.

CYBERCLASH RULE BOOK

12.FAIR PLAY CLAUSE

Any attempt to gain unfair advantage, even if not explicitly mentioned in this rulebook, may result in penalties.
Spirit of the event matters as much as the rules.

13.FLEXIBILITY & CREATIVE FREEDOM

CyberClash encourages:

- Innovative approaches
- Creative thinking
- Learning-by-doing

If you are unsure whether an action is allowed:
Ask before you act.

14.ORGANIZER RIGHTS

Organizers reserve the right to:

• Modify rules during the event (with notice)
• Disqualify teams violating rules
• Resolve disputes at their discretion

15.ACKNOWLEDGEMENT

By participating in CyberClash, all teams acknowledge that they have read, understood, and agreed to abide by this rulebook.
Let’s keep CyberClash challenging, ethical, and fun