THE RULES OF GAMES FOR THE FINAL ROUND OF ASCIS 2023

1. **Timeline:**
   From 7:00 – 18:30 (UTC+7) October 28th 2023.

TT	Time	Content
1	7:00 – 7:20	Preparation time: - Join Zoom Meeting https://zoom.us/j/97244749354?pwd=TTk5bExSNzlZNzZYaXpIOHJIOHFEUT09 Meeting ID: 972 4474 9354 Passcode: 281023 - Connect to the exam website https://quals.ascis.vn/ (use the accounts provided in the Starting round)
	7:20 – 7:30	Opening speech
2	7:30 – 11:30	All teams begin to perform the contest (phase 1: jeopardy)
3	11:30 – 12:00	Close the exam system. All teams take a break for 30 minutes. The organizers announced the list of 20 best teams of phase 1
4	12:00 – 17:00	The 20 best teams of phase 1 will advance to attack – defense round https://final.ascis.vn The remaining teams continue to compete in jeopardy (phase 2)
5	17:00 – 17:30	Close the exam system The Judges summarizes the exam results
6	17:30 – 19:30	The Organizers announced the results and awarded the contest prizes

2. **Instructions for competition**

The Final round include 2 phases:

- Phase 1: Jeopardy in 4 hours (from 7:30 -11:30).

End of phase 1, the Organizers close submit, all teams take a break.

The organizers announced the list of 20 best teams of phase 1

- Phase 2: in 5 hours (from 12:00 – 17:00)

The 20 best teams of phase 1 will advance to attack – defense round. The remaining teams continue to compete in jeopardy

Scores for phase 1 will be transferred to phase 2

- End of phase 2, the Organizers close submit, all teams take a break for final notification

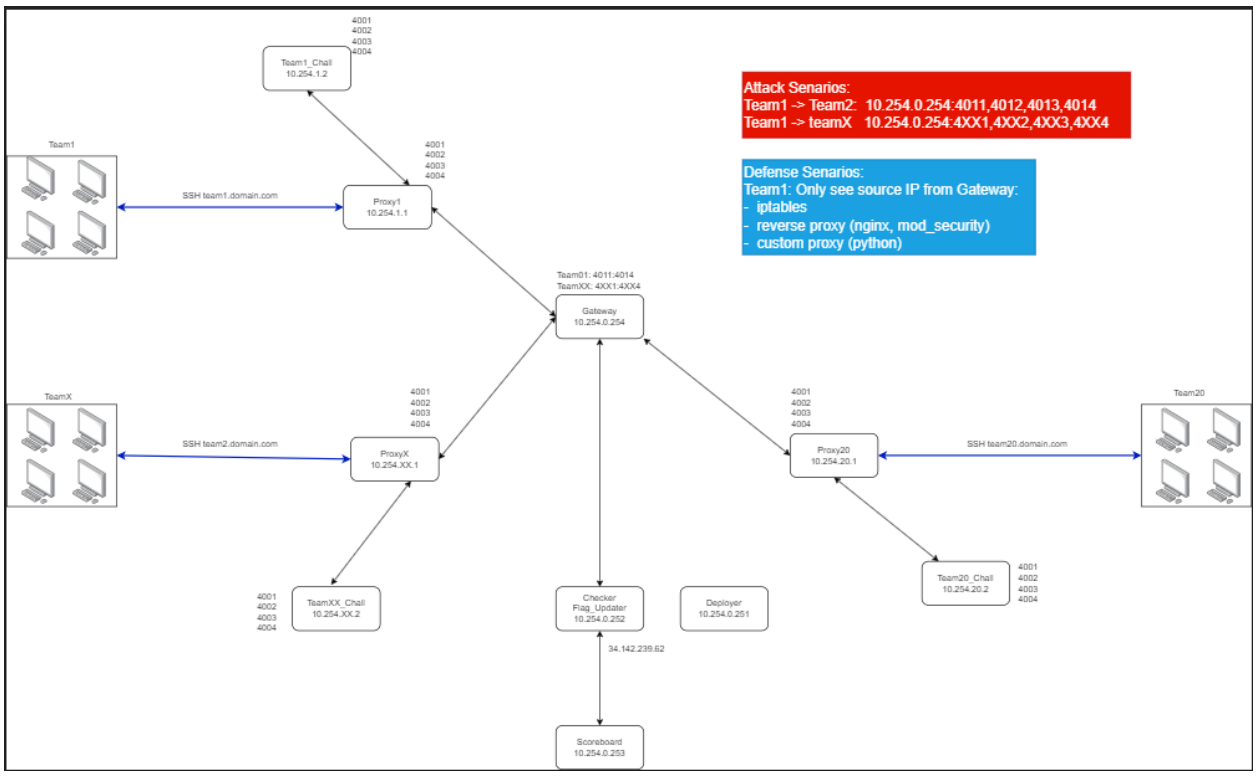
2.1. Jeopardy

- Teams have to tackle the requirements of the game successfully to win the flag.. After finding the flag, the teams need to submit immediately their own flag to get the earliest points, the teams that get the points first have a ranking advantage when they equal to the points of other teams. Format of the flag: ASCIS{*}
- Website: https://quals.ascis.vn/
- Account: Contestants use the accounts provided in the Starting round.
- Challenges: (similar to Starting round).
    - **Reverse Engineering:** Decompile software source code, unpack source code protection packers.
    - **Exploit/PWN:** Find bugs, exploit vulnerabilities in server applications, software, or code (e.g. buffer overflow, write shellcode, format string ...).
    - **WEB:** Exploiting web application vulnerabilities (SQL injection, XSS, Session Hijacking ...).
    - **Crypto:** String decoding, algorithm, algorithm analysis, algorithm programming....
    - **MISC:** Forensics, Programming, Steganography…

  - If you have any questions, please contact the Organizing Committee via chat on the web telegram (https://t.me/+vFsY_PYESL85OWE1) in English.

2.2. Attack-defense

- Competing teams try to protect their systems from attacks from other teams while also trying to attack and earn points from their opponents' systems.
- Website: https://final.ascis.vn
- Account: Will be sent at the start of this phase
- Service table: Will be sent at the start of this phase
- Network model:



- **Gateway**: a computer as a co-server, receiving requests from all teams and forwarding data to the corresponding server
- **Proxy**: the computer on which the teams play is entitled to set the rules of blocking and filtering data. Teams are fully managed for a proxy.
- **Challenge**: teams can't manage this server. Teams can keep 1 sample server to find errors on it.

- Attack: Teams send requests to opponent team's respective services. Cổng dịch vụ của đội bạn tương ứng như sau:
  - The rules is as follow:
    service portal 4{id_of_the_team}{id_of_the_challenge}
  - Example: to attack the No.1 service of team 01, send a request to: 10.254.0.254:4011. Request will come from gateway to proxy of the attacked team, corresponding to port 4001 on the proxy. If no filtering or blocking, the data from proxy continue go to port 4001 of team 1 application.
  - Portal information for each service of the teams is in the appendix table (when entering the competition, the teams will know the specific services and the order of the teams)
  - Flag will change each 15 minutes
- Defense:
  - Teams hold proxy and perform filter on the corresponding port to block and filter dangerous data. If the bot of Organizing committee fails to check the status of the team, the team will lose defense points.

- Teams must protect their services. Organizing committee's system will check regularly and without notice

3. Prizes

There are 2 prize categories for Attack-defense teams and the remaining teams (jeopardy competition only). Each category includes 20 awards. Specifically:

- Prizes for Attack-defense: 01 Grand prize (600$); 03 Second prizes (200$); 05 Third prize (120$); 11 Consolation (80$)
- Prizes for Jeopardy: 01 First prize (200$); 03 Second prizes (80$); 05 Third prizes (50$); 11 Consolation prizes (25$)

ASEAN teams will watch the Closing ceremony and Awarding ceremony live via zoom. Winning teams will receive rewards from the organizers via their paypal accounts and certificate via email.