

## **Regulation**

### **“ASEAN STUDENTS CONTEST ON INFORMATION SECURITY 2020”**

#### **Article 1. Purpose**

1. To raise and promote awareness of higher-education institutions (colleges, universities, vocational schools and research institutes) of information security to implement Scheme No. 893 (Prime Minister Decision no. 893/QĐ/TTg dated 19/06/2016 *Information Security Awareness and Responsibility by 2020*).

2. To promote research, learning and experience exchange on information security to implement Scheme No. 99 (Prime Ministry Decision no. 99/QĐ-TTg dated 14/01/2015 *Training and Development of Human Resources in Information Security by 2020*).

3. To promote, recognize and nurture talents in cybersecurity in Vietnam and ASEAN; to create favorable environment and lay the foundation for the training and development of professional human resources in the field.

#### **Article 2. Scope and Eligibility**

1. Scope: The contestant teams are from ASEAN member states.

2. Eligibility: Students from higher-education institutions in ASEAN. Up to 04 students from the same institution shall form a team. A member should have not participated more than two (02) times in the Final Round of previous contests.

3. The participation of all members in each team shall be voluntary. All the participating teams shall respect and comply with the rules set by the Organizer and other relevant legal regulations.

4. All members should bring along documents for identification purpose (ID card, student ID, ...)

5. Those contestants and teams who violate the rules shall be treated in accordance with the contest's regulations, ranging from receiving warnings, having scores deducted or being disqualified.

#### **Article 3. Theme, format and timeline of the Contest**

1. Theme: Compete on cybersecurity knowledge and skills following CTF format.

2. Contest format: The contest consists of 03 rounds: Starting Round, Qualifying Round and the Final Round

a) Starting Round: Online CTF (Jeopardy) on October 17, 2020, within the duration of 4 hours.

- The format of this round includes: Pwnable (exploiting software errors, buffer overflow, format string, shellcode...); Reverse engineering (software source code reverse engineering, unpacking the packers, crypters to protect the software); Web (Web application attack techniques); Network/Forensic (Investigate, analyze, trace digital cases); Crypto/ACM (Decode puzzles, attack cryptographic algorithms, use programming/algorithmic skills to solve games, mazes...).

- Each university from ASEAN Member States will choose up to 03 best teams from the Starting Round to compete in the Qualifying Round.

b) The Qualifying Round: Onsite CTF (Jeopardy) for teams from Vietnam and online CTF (Jeopardy) for teams from other ASEAN Member States. Video conferencing tools may be used to surveil remote contestants to ensure fair competition. The expected date of this round is on October 31<sup>st</sup>, 2020 and last for 8 hours.

- The format of this round includes: Pwnable (exploiting software errors, buffer overflow, format string, shellcode...); Reverse engineering (software source code reverse engineering, unpacking the packers, crypters to protect the software); Web (Web application attack techniques); Network/Forensic (Investigate, analyze, trace digital cases); Crypto/ACM (Decode puzzles, attack cryptographic algorithms, use programming/algorithmic skills to solve games, mazes...).

- 10 best teams of Vietnam from the Qualifying Round shall compete in the Final Round, together with the best teams from the Qualifying Round of other ASEAN Member States (01 best team of each country).

c) Final Round: Onsite CTF (Attack & Defense) with teams from Vietnam and online CTF (Attack & Defense) with teams from ASEAN Member States. The expected date of this round is November 28<sup>th</sup>, 2020. In case teams from Vietnam could not able onsite participation (due to COVID-19, etc...), online participation is alternatively possible.

- In the Final Round, the teams shall be tested on their ability to counter-measure cyber-attacks against their opponents and to defend their own computer networks.

Detailed description of the contest and the award-winning criteria shall be communicated to every participating team prior to each stage of the contest.

The Organizer shall reserve the right to change the timings of the contest in each round to meet the actual requirements. Any changes as such shall be informed to the participating teams directly and via the official website of the Organizer.

### 3. Sign-up schedule:

- The team registration is no later than September 30<sup>th</sup>, 2020.

- The online application form can be downloaded from the Organizer's official website and sent to its email address at [ascis@vnisa.org.vn](mailto:ascis@vnisa.org.vn) upon completion.

The list of successfully registered teams and their relevant information shall be made available on VNISA's website so that all the participating teams can review and report any inaccurate information. Requests for correction, if any, need to be sent to the Organizer at least 01 week prior to the commencement of each round.

- Strictly follow the instructions in the test rooms and the contest's rules.

## Article 4. Awards

### 1. Qualifying Round:

a) 01 First Prize, several second, third and consolation prizes. The number of second/third and consolation prizes shall be decided by the Organizer based on the number of competing teams in each contest site.

b) The awards to be presented include:

- Certificates of Merit by VNISA;

- Financial awards (in cash or artifacts).

## 2. Final Round:

a) 01 Grand Prize, 02 Second Prizes, 03 Third Prizes and Consolation Prizes

b) The teams winning Grand Prize and Second Prizes will receive Certificates of Merit from the Minister of Education and Training.

c) The teams winning titles will receive cash awards (whose values will be determined by the Organizer) and certificates from Ministry of Information and Communications .

## **Article 5. Financial Support**

ASEAN teams attending the contest in Viet Nam shall receive financial assistance from the Organizer to cover part of their expenses (including flight tickets, meals and accomodation). Otherwise, expenses shall be covered by own.

## **Article 6. Extra information**

1. All the participants will have to provide proof of identity such as student IDs, personal IDs (or passports, applicable to ASEAN students), bring along their own laptops, which should have RJ45 port.

2. Information about the contest: is available on the Organizer's official website at <http://ascis.vnisa.org.vn>

3. Contact information of the Organizer:

Vietnam Information Security Association (VNISA)

Address: no. 155 An Trach street, Dong Da District, Hanoi;

Tel: (+84) 26290 1028;

Email: [ascis@vnisa.org.vn](mailto:ascis@vnisa.org.vn).