CYBERSECURITY

OVERVIEW

Applying leadership and 21st century skills, participants respond to a cybersecurity challenge by identifying a breach in computer security via "Capture the Flag" games. Areas of challenge might include exploit development, digital puzzles, cryptography, reverse engineering, binary analysis, mobile security, etc. Participants must accurately address a series of on-site problems within a specified, limited amount of time.

ELIGIBILITY

Two (2) teams per chapter may participate.

TIME LIMITS

A. Participants are required to attend the orientation meeting prior to receiving access to the challenges.

B. Forty-eight (48) hours, beginning at the event orientation meeting, are allowed to complete the online preliminary challenge.

PROCEDURE

PRE-CONFERENCE

A. Prior to registration, chapter advisors collect an executed TSA Student and Parent Consent Release Form for all participants participating in Internet-based competitions and will verify having done so upon affiliation. A link to the form can be found on the TSA website.

B. The release form must be completed for every participant in order for the participant to compete in this event. Chapter advisors keep copies of the executed forms and may be asked to produce them if needed.

C. Once registered and Student/Parent Consent forms are in possession of the chapter advisor, instructions to create teams on the Cybersecurity platform will be communicated to the chapter advisor.

ON-SITE CHALLENGE

A. Participants report to the event area at the time and place stated in the conference program to attend the mandatory orientation session.

B. Participants receive information pertaining to the event specifics.

C. Participants provide their own computer hardware, including applicable software to solve challenges (e.g. NetCat or Putty).

D. Teams have forty-eight (48) hours from the designated start time announced during the informational session to complete the online challenge.

E. Teams that do not attend the informational session will not receive additional time and will need to meet with the CRC Manager of the event in order to participate.

F. For website support, teams shall contact the CRC coordinator or manager.

G. Solutions are scored in real-time and results are posted on an online scoreboard. The URL is provided on-site.

H. The top ten (10) finalists are announced at the awards ceremony.

REGULATIONS AND REQUIREMENTS

Students will work to develop their leadership and 21st century skills in the process of preparing for and participating in this TSA competitive event. The development and application of those skills must be evident in their submission, demonstration, and/or communication pertaining to the entry.

A. Participants who have not properly set-up their teams on the cybersecurity platform online prior to conference are NOT permitted to participate at the National Conference. Teams are not permitted to set-up their teams on-site.

B. Participants should concentrate their efforts prior to the competition on researching, understanding, and practicing all aspects of cybersecurity. Please refer to the sample challenge topics listed below and the resources on the TSA website.

C. Materials:

1. Teams are responsible for providing:

   a. computer(s), including applicable software to solve challenges

   b. one (1) or two (2) auxiliary monitors, optional

   c. one (1) Power strip, optional

   d. Internet access

D. Teams may receive online hints on the platform throughout the competition but are not given the solution by organizers.

E. Teams are not to share solutions between teams, but they may communicate with their own team members. The sharing of information between teams will result in automatic disqualification.

SAMPLE CHALLENGE TOPICS

This list serves only as an *example* of challenge categories.

A. Web Security

1. The Web Security category often features custom developed web applications which include some web security flaw that must be identified and exploited. Very often SQL injection, command injection, directory traversal, and XSS vulnerabilities are introduced and exploited in these categories.

2. Examples:

   a. Exploiting poor security controls in a website as a regular user to gain higher level access.

   b. Exploiting poor security practices in a website in order to read arbitrary data from the vulnerable server.

   c. Exploiting a SQL injection vulnerability to extract the content of an intentionally vulnerable server.

B. Forensics

1. The Forensics category often features memory dumps, hidden files, or encrypted data which must be analyzed for information about underlying information.

2. Examples:

   a. Extracting hidden files from an image of a hard drive.

   b. Extracting hidden files from a memory dump.

   c. Determining the flow of data in a packet capture to ascertain the origin or destination of data.

C. Cryptography

1. Cryptography is the reason we can use banking apps, transmit sensitive information over the web, and in general protect our privacy. However, a large part of CTFs is breaking widely used encryption schemes that are improperly implemented.

2. Examples:

   a. Securing web traffic (passwords, communication, etc.).

   b. Securing copyrighted software code.

D. Reverse Engineering

1. The Reverse Engineering category often features programs from all operating systems which must be reverse engineered to determine how the program operates. Typically, the goal is to get the application to reach a certain point or perform some action in order to achieve a solution.

2. Examples:

   a. Determining what input causes a program to return True.

   b. Disassembling a game to find a hidden Easter egg not normally accessible or a cheat code to make it easier to win the game.

   c. Optimizing a program to make it run to completion.

   d. Exploiting a buffer overflow with some security mitigations in place to gain a command shell and read a file.

   e. Exploiting a format string vulnerability to gain a command shell and read a file.

ADVANCED SAMPLE TOPICS

This list serves only as an *example* of challenge categories.

A. Binary Exploitation

1. The Binary Exploitation category often features compiled programs that have a vulnerability allowing a competitor to gain a command shell on the server running the vulnerable program. This often requires reverse engineering skills.
2. Examples:
   a. Exploiting a buffer overflow to gain a command shell and read a file.
   b. Exploiting a buffer overflow with some security mitigations in place to gain a command shell and read a file.
   c. Exploiting a format string vulnerability to gain a command shell and read a file.

EVALUATION

A. The successful completion of the problems, including the time in which it takes teams to complete each challenge.

Refer to the official rating form for more information.

STEM INTEGRATION

Depending upon the subject of the problem, this event may align with the STEM (Science, Technology, Engineering, and Mathematics) educational standards.

LEADERSHIP AND 21ST CENTURY SKILLS DEVELOPMENT

This event provides opportunity for students to build and develop leadership and 21st century skills including but not limited to:

- Communication
- Collaboration/Social Skills
- Initiative
- Problem Solving/Risk Taking
- Critical Thinking
- Perseverance/Grit
- Creativity
- Relationship Building/Teamwork
- Dependability/Integrity
- Flexibility/Adaptability

CAREERS RELATED TO THIS EVENT

This competition has connections to one (1) or more of the careers below:

- Vulnerability Assessor
- Chief Information Security Officer
- Forensic Expert
- Security Architect
- Security Director
- Incident Responder
- Security Manager
- Security Auditor
- Cryptographer
- Security Engineer
- Security Analyst

Participant/Team ID# ____

CYBERSECURITY

2021 & 2022 OFFICIAL RATING FORM

HIGH SCHOOL

Judges: Using minimal (1-4 points), adequate (5-8 points), or exemplary (9-10 points) performance levels as a guideline in the rating form, record the scores earned for the event criteria in the column spaces to the right. The X1 or X2 notation in the criteria column is a multiplier factor for determining the points earned. (Example: an "adequate" score of 7 for an X1 criterion = 7 points; an "adequate" score of 7 for an X2 criterion = 14 points.) A score of zero (0) is acceptable if the minimal performance for any criterion is not met.

Go/No Go Specifications

- Before judging the entry, ensure that the items below are present; indicate presence with a check mark in the box.
- If an item is missing, leave the box next to the item blank and place a check mark in the box labeled ENTRY NOT EVALUATED.
- If a check mark is placed in the ENTRY NOT EVALUATED box, the entry is not to be judged.

□ Computer hardware is present

□ ENTRY NOT EVALUATED

CYBERSECURITY CHALLENGE (100 points)				
Record the completed score and time for the online preliminary problem.				
Team A Score:		**Team B Score:**		
Time (Needed for tie breaker):		**Time (Needed for tie breaker):**		
			SUBTOTAL (100 points)	

Rules violations (a deduction of 20% of the total possible points for the above sections) must be initialed by the judge, coordinator, and manager of the event. Record the deduction in the space to the right. Indicate the rule violated: _______________	

To arrive at the TOTAL score, add any subtotals and subtract rules violation points, as necessary.	**TOTAL (100 points)**	

Comments:

____

I certify these results to be true and accurate to the best of my knowledge.

JUDGE

Printed name: ______________________________ Signature: ______________________________

CYBERSECURITY EVENT COORDINATOR INSTRUCTIONS

PERSONNEL

A. Event coordinator

B. Assistants for set-up and clean-up, two (2) or more

MATERIALS

A. Coordinator's packet, containing:

1. Event guidelines, one (1) copy for the coordinator
2. TSA Event Coordinator Report
3. List of assistants

B. Tables and chairs for participant orientation session

C. A copy protocol for the online management materials/ on-site equipment as needed

D. Adequate conditions, tools, materials, monitoring, and testing devices for the problem

RESPONSIBILITIES

AT THE CONFERENCE

A. Attend the mandatory coordinator's meeting at the designated time and location.

B. Report to the CRC room and check the contents of the coordinator's packet.

C. Review the event guidelines and check to see that enough evaluators and assistants have been scheduled.

D. Inspect the area(s) in which the event is being held for appropriate set-up, including room size, chairs, tables, outlets, etc. Notify the event manager of any potential problems.

E. One (1) hour before the semifinal event is to begin, meet with evaluators to review time limits, procedures, regulations, evaluation, and any other details pertaining to the event. If questions arise that cannot be answered, speak to the event manager before the event begins.

ON-SITE CHALLENGE

A. Begin the event at the scheduled time by closing the doors and checking the entry list.

B. All participants and evaluators should be in the room at this time.

C. Participants not present for the orientation must have approval of the CRC in order to participate.

D. Once teams are seated and general announcements have been given, distribute and review the procedure.

E. Check and post the online progress throughout the preliminary event via the scoreboard.

F. After the designated time of forty-eight (48) hours has elapsed, the challenge site becomes unavailable.

G. Submit the finalist results and all related forms in the results envelope to the CRC room.

SUPPORT

For competition support, organizers shall contact the CRC competitions manager.