High School On-Site Cybersecurity

OVERVIEW

Participants will complete a cybersecurity exam covering general cybersecurity vocabulary and knowledge needed to execute tasks commonly performed by all levels of cybersecurity professionals. Applying leadership and 21st century skills, participants will prepare a video presentation on-site that would detail how they would complete an actual cybersecurity challenge within a specified, limited amount of time. This presentation should include how they would go about identifying a breach in computer security as if they were competing in "Capture the Flag" type games that will be available at the National TSA Conference. Teams should be well versed in the main areas of the challenge. These areas might include exploit development, digital puzzles, cryptography, reverse engineering, binary analysis, mobile security, etc.

ELIGIBILITY

Two (2) teams per chapter may participate.

ATTIRE

TSA competition attire is required.

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.

PRELIMINARY ROUND

1. The Exam
    a. The use of reference materials or external assistance is not permitted during the exam.
    b. Individuals will only be allowed one (1) opportunity to take the exam.
    c. One (1) hour is allowed to complete the exam.
        i. Timing begins with the first question and ends at the conclusion of one (1) hour.
    d. Breaks are not permitted during testing and time cannot be paused.
    e. (12) teams with the highest averaged scores are selected as semifinalists to complete the presentation portion of the event. A semifinalist list in random order is posted.

SEMIFINAL ROUND

1. The Presentation
    a. The semifinalists are required to attend the orientation meeting prior to receiving access to the challenge topic. Students will be given twenty-four (24) hours to complete and submit their presentation via the online link: PUTONLINE SUBMISSIONLINKHERE (submissions MUST be submitted via the link provided. Teams will paste a web link to their video presentation; a hosted link can be in .mp4/.mov file format or a link to their video presentation on YouTube) Teams MUST include a signed digital/scanned copy of the official TSA Copyright checklist form as well as any consent forms in .pdf format.
2. Participants enter this event with the following scenario in mind:
    a. You are a cybersecurity consultant who is bidding for a contract from a large firm. The company has been notified that there is a security breach (the topic that was selected at the orientation meeting) and your job is to show, via your presentation, how someone can use that breach to gain access to their system and then show/describe how to secure that breach. The goal is to win the "contract" by providing the best presentation / documentation in order to secure the breach and possible future and additional breaches.

3. No identifying information other than the participant's identification number and conference title and year are permitted. Identification information shall be the listed on the title page / opening screen of the presentation.
4. Participants shall focus on the following in their presentation / documentation:
    a. Identify and explain the security problem.
    b. Explain how your team would achieve that security breach.
    c. Explain how your team would secure the breach.
    d. Give examples of other possible security breaches and describe how your team would protect the company from those breaches as well as other potential ones in the future.
    e. The presentation / video, should be at least two (2) minutes in length and no-longer than ten (10) minutes in length.
        i. ***teams MUST submit a link to their video (.mp4/.mov or YouTube is acceptable)*
5. Participants must use fictitious company names for both the consulting firm and the company that is seeking out cybersecurity services. Real names may not be used.
6. Teams must submit their presentation in one of the following formats as a weblink; .mov, .mp4 or YouTube) audio / voice-over may be used.
7. 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.
    a. Highlight your proposal with creative visual elements (e.g., graphics, photos, titles, transitions) to actively engage the audience. Participants may use images "labeled for reuse," but must properly cite the source (refer to the General Rules).
    b. No commercial or copyrighted material may be used. If the entry contains images of people, proof of consent must be provided for each person in the presentation.
    c. Minors require parental consent
    d. Use the Photo /FilmVideo Consent and Release form (see Forms Appendix) for any individuals included in the presentation.
8. Judges score the presentation.
9. The top ten (10) finalists are announced at the TSA conference awards ceremony.

EVALUATION

PRELIMINARY ROUND

1. The exam

SEMIFINAL ROUND

1. The presentation
2. Refer to the official rating form for more information

SAMPLE CHALLENGE TOPICS

This list serves only as an example of challenge categories.

1. **Web Security**
    a. The Web Security category often features custom developed web applications which include some web security flaw that must be identified and exploited. Very often SOL injection, command injection, directory traversal, and XSS vulnerabilities are introduced and exploited in these categories.
    b. Examples:
        i. Exploiting poor security controls in a website as a regular user to gain higher level access.
        ii. Exploiting poor security practices in a website in order to read arbitrary data from the vulnerable server.
        iii. Exploiting a SOL injection vulnerability to extract the content of an intentionally vulnerable server.
2. **Forensics**
    a. The Forensics category often features memory dumps, hidden files, or encrypted data which must be analyzed for information about underlying information.
    b. Examples:
        i. Extracting hidden files from an image of a hard drive.
        ii. Extracting hidden files from a memory dump.
        iii. Determining the flow of data in a packet capture to ascertain the origin or destination of data.
3. **Cryptography**
    a. 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.
    b. Examples:
        i. Securing web traffic (passwords, communication, etc.).
        ii. Securing copyrighted software code.
4. **Reverse Engineering**
    a. 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.
    b. Examples:
        i. Determining what input causes a program to return True.
        ii. Disassembling a game to find a hidden Easter egg not normally accessible or a cheat code to make it easier to win the game.
        iii. Optimizing a program to make it run to completion.
        iv. Exploiting a buffer overflow with some security mitigations in place to gain a command shell and read a file.
        v. Exploiting a format string vulnerability to gain a command shell and read a file.

STEM INTEGRATION

This event has connections to the STEM areas of Science, Technology, Engineering, and Mathematics.

LEADERSHIP AND 21sr 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:

- Information support & services
- Network systems
- Programming & software development
- Web & digital communications
- Technical support specialist Computer software engineer
- Cybersecurity engineer
- Cryptographer
- Cyber Crime Investigator
- Cyber defense incident responder
- Cyber forensics expert Cyber legal advisor
- Cyber operator
- Vulnerability assessor

Participant / Team ID# _____

CYBERSECURITY

2021 & 2022 Official Rating Form

HIGH SCHOOL

Judges: Using minimal (1-4), adequate (5-8), 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 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.

TEST (50 points)	
TEST SUBTOTAL (50 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: _____	

PRELIMINARY SUBTOTAL (50 points)	

SEMIFINAL PRESENTATION (120 points)				Record scores in the column spaces below.
CRITERIA	**Minimal performance**	**Adequate performance**	**Exemplary performance**	
	1 – 4 points	**5 – 8 points**	**9 – 10 points**	
PRESENTATION (130 points)				
Identification and explanation of security breach (X2)	Identification and explanation of the issue is unclear.	Issue is defined and explained appropriately, however, some points need clarification.	A clear and concise definition and explanation of the issue is evident.	
Explanation of how to achieve said security breach (X2)	There is little evidence of research; there is a lack of understanding of the issues cited.	There is some evidence of research; an adequate understanding of the issue(s) are present.	Thorough research is clearly evident with a firm understanding of the issues established.	
Explanation of how to fix and protect against future said security breach (X2)	There is little evidence of research; there is a lack of understanding of the issues cited.	There is some evidence of research; an adequate understanding of the issue(s) are present.	Thorough research is clearly evident with a firm understanding of the issues established.	
Overview of various other possible security breaches	Identification and explanation of the issue is unclear	Issue is defined and explained appropriately,	A clear and concise definition and explanation of the issue is	

(X2)		however, some points need clarification	evident	
Overview of how to protect against various other possible security breaches (X2)	There is little evidence of research; there is a lack of understanding of the issues cited.	There is some evidence of research; an adequate understanding of the issue(s) are present.	Thorough research is clearly evident with a firm understanding of the issues established.	
Creativity, Aesthetics, and Artisanship (X1)	The presentation lacks creativity; the work is unorganized and sloppy.	Some visual elements of creativity exist in the work; presentation is generally organized in its explanation of the issue and the visual elements somewhat enhance the presentation.	The presentation exudes creativity; essential design principles and elements are well integrated; presentation logically communicates an important idea and is engaging.	
Articulation (X1)	Communication of the proposal is unclear, unorganized, and or illogical; leadership and/or 21st century skills are not evident.	Communication of the proposal is somewhat logical and clear; leadership and/or 21st century skills are somewhat evident.	Communication of the proposal is clear, concise, and logical; leadership and/or 21st century skills are clearly evident.	
Overall Impact (X1)	The presentation does not detail or enhance the essential components of the participant's problem identification and proposal.	The presentation somewhat enhances the essential components of the participants problem identification and solution.	The presentation greatly details and enhances the essential components of the participant's problem identification and solution.	
			SEMIFINAL PRESENTATION (130)	

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: _____	

SEMIFINAL SUBTOTAL (Exam plus Semifinal Presentation) (180 points)	
To arrive at the TOTAL score, add any subtotals and subtract rules violation points, as necessary. TOTAL (180)	