So You Want to Build a Cybersecurity Competition?

12 THINGS TO CONSIDER BEFORE GETTING STARTED

NICE | community coordinating council

This document is a publication of the NICE Community Coordinating Council, Cybersecurity Skills Competitions Community of Interest.

Drafting Committee:
Amelia Phillips (lead and author)
Dan Manson

The Cybersecurity Skills Competitions Community of Interest is a voluntary collaboration of industry, academic, and government representatives formed to provide a forum for anyone who is interested in sharing and learning how to empower a public and private competition ecosystem. The community enables this by promoting a wide spectrum of competitions and effective practices for players, athletes, teams, schools, sponsors, organizers, and others that advance cybersecurity knowledge, skills, and competencies to grow and sustain a diverse national talent pool.

Authored September 2020
Published September 2023

Table of Contents

Introduction

Competitions are a great way to get participants, especially students, excited about cybersecurity. Cybersecurity competitions provide participants with experiential practice and can extend the opportunity for existing personnel to learn new techniques and tackle challenging problems. Competitions can also aid in identifying promising candidates.

This is an introductory guide, offering considerations on how to create your own cybersecurity competition. While several cybersecurity competitions already exist, many schools and organizations continue to build new competitions to meet the needs of the industry and bring in new people. This is intended to be a living document that will be updated as needed.

Key Steps to Create and Run a Cybersecurity Competition

1 Determine Your Target Audience

Think about your audience, the level of difficulty, and experience of players for the competition:

- Middle school, high school, college students, professionals, and transitioning or dislocated workers can enjoy and learn from cybersecurity competitions.
- Content can be tailored for each audience and difficulty level.

2 Determine The Type of Competition

Basic decisions that you will need to make regarding your competition include the style of competition, how the players will participate, and the competition structure.

Competition Style

The three main categories of competitions are capture the flag, cyber defense, and forensics. However, there are also policy, social engineering, and cryptology competitions.

Capture the Flag (CTF) competitions are designed to challenge participants to solve computer security problems by capturing and defending computer systems. The structure is similar to the traditional outdoor sport where several teams have flags and the objective is to capture the other team's flag. Cybersecurity CTF events consist of a series of challenges that vary in their degree of difficulty and require participants to exercise different skillsets to solve. Once an individual challenge is solved, a “flag” is earned with a certain number of points. In the cybersecurity CTF competition, flags are placed in various locations; they might be in a file, in the database, or stuck into source code. The goal is to hunt them all down. If you want to create a Capture the Flag competition, there are three main types:

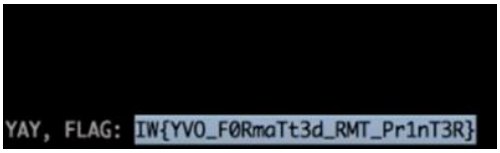

Image 1: Example of Flag participant would find and submit for points.

attack and defense, Jeopardy or quiz, and mixed. Jeopardy or quiz competitions are more appropriate for middle and high school players. Typical tasks are related to networking, programming, applications, mobile, forensics, reverse engineering, and cryptography. Teams are rewarded with points for each challenge they complete. Attack and defense competitions involve more resources and are better for college and professional players. Teams must capture and defend vulnerable computer systems, typically hosted on virtual machines in an isolated network. Teams work to maintain ownership of the systems while denying access to the other competing teams. A mixed CTF, that combines Jeopardy and attack and defense styles is the most challenging for participants. Teams must strategically divide their efforts and play to each of their member's strengths by completing security challenges and maintaining ownership of the systems while simultaneously defending them against their competitors, and hacking into target vulnerable systems. Capture the Flag platforms can include open-source software such as the Facebook CTF platform, CTFd, and OWASP Juice Shop.

Cyber Defense competitions can involve hardening virtual images or a red team/blue team competition. Hardening is the process of applying security configurations to reduce vulnerabilities that could lead to exploitation of the system. Hardening virtual images are more appropriate for middle school and beginning high school players. Red team/blue team competitions involve more resources and are better for advanced high school, college, and professional players. In this style of event the red team attempts to capture flags while the blue team attempts to defend the various flags from being captured. The attackers learn vital techniques while the defenders have a chance to learn how to defend their systems from an active attack.

Red Team is another style that allows participants, whether working alone or on a team, to capture various flags while there is no team defending them. In this format there is one primary target, the CTF host, that holds all the flags. Simple Cyber Defense competitions can be designed by creating virtual images of Windows and Linux operating systems. Advanced Cyber Defense competitions can be created by working with schools and consortiums that build and host Collegiate Cyber Defense Competitions (CCDC).

Forensics competitions can involve a physical crime scene investigation, simple media imaging and analysis, advanced imaging and analysis, and network and memory forensics. Crime scene investigation and simple media imaging and analysis are more appropriate for middle and beginning high school players. Advanced imaging and analysis, and network and memory analysis are more appropriate for advanced high school, college, and professional players. Forensics competitions can be created by working with schools and consortiums that build and host these types of competitions.

Policy competitions provide an opportunity for participants from multiple disciplines to interact and compete to achieve a deeper understanding of the policy challenges associated with cybersecurity crisis and conflict. Using an interactive competitive scenario, teams respond to a realistic, evolving cyber-attack and analyze the threat it poses to national, international, and private sector interests and provide policy analysis and recommendations. Points are gained by

application of substantive knowledge across a range of areas, including any number of policy domains as well as insights from technology, business, law, and written and spoken communication skills.

Social Engineering (SE) competitions demonstrate how much information can be freely obtained either through online sources or via telephone elicitation. SE events have participants attempt to obtain specific pieces of information, or flags, from assigned private sector companies, through legal and creative methods. Competitions are divided into two parts; information gathering, which often takes place prior to the event, and the "live call" phase that occurs during actual competition.

Crypto Challenges are comprised of two independent Internet rounds. The first round (duration 4 hours 30 minutes) is individual and consists of two sections: A and B. Theoretical problems in mathematics of cryptography are offered to participants. The second round (duration 1 week) is devoted to research and programming problems of cryptography solved in teams (up to three members). The North American Computational Linguistics Open Competition (NACLO) is a contest in which high school students solve linguistic problems. In solving these problems, students learn about the diversity and consistency of language, while exercising logic skills. No prior knowledge of linguistics or second languages is necessary. Professionals in linguistics, computational linguistics, and language technologies use dozens of languages to create engaging problems that represent cutting edge issues in their fields. The competition has attracted top students to study and work in those same fields. It is truly an opportunity for young people to experience a taste of natural-language processing in the 21st century.

Participation Mode

The participation mode describes how the participants will compete. Competition participation mode can be face-to-face, online, or a combination of both. For a face-to-face competition, the participants gather in the same physical location, which is a location that has been pre-determined by the competition organizers. For an online competition, the participants compete from any virtual location.

The style of competition you choose will inform the participation mode. All competition styles can involve all participation modes.

Competition Structure

Think about the level of complexity your competition will have. Questions to consider include: Will your competition have qualifying rounds? Will your competition be team-based, designed for individual players, or both? If teams, how many teams will your competition support? Will your competition be local, regional, or national?

3 Determine the Facilities Needed for the Competition

The facilities will vary depending on the type of competition. They can be divided into three main categories: 1) IT infrastructure, 2) game space, and 3) sideline.

IT Infrastructure

This includes the entire digital infrastructure needed to support all aspects of the competition. This will include hardware, software, storage, and networking components.

Competition IT Infrastructure includes the infrastructure needed for game play, game monitoring, and scoring. This may include websites, a cyber range, and a scoring engine.

Administrative IT Infrastructure includes the infrastructure needed to support competition promotion, registration, prizes, swag, and feedback.

Game Room

For face-to-face competitions, this includes the physical location in which the competition game play, competition monitoring, and competition scoring will occur.

Sideline

This includes the additional physical or virtual locations needed during the event, for example, registration area, lodging and dining locations, ceremony locations, or an online chatroom for players to communicate outside of the competition activities. This may involve the development of a website that supports the administrative aspects of the competition.

Facility needs may include rooms, electricity, connectivity, computers, printers, displays, projection, and other audio and visual needs. Questions to consider include: Is the venue provided by a college or consortium? What type of IT infrastructure is needed? Do items need to be purchased or are in-house resources available? Do you need a scoring engine? Who will provide it? Will permissions need to be obtained for use of facilities or resources? Will food be provided? Will it be catered or in-house?

4 Determine Funding Needs for the Competition

Whether you have a small budget or a large one, prepare a detailed list of costs associated with your competition. Costs can include competition design and development, platform development, facilities, transportation, prizes and swag, food, parking, and overall planning and management.

5 Determine Sources of Support for the Competition

Support can come from local military, law enforcement, industry, schools, grants, and sponsors.

- Financial support can be general or targeted for specific budget items. Explore sponsorship at all levels, including local, regional, national, and global.
- Volunteers can also provide support in the form of judges, red team (attackers or pen testers), set-up activities, and administration. Reach out to others who have built and run competitions. Visit the websites of existing competitions to get contact information for experienced competition designers.

6 Design and Develop the Competition

Competition Challenges

Competition game play involves actions that the participants must perform, such as answering questions or performing tasks. Designing and developing the competition actions, or challenges, is a significant part of building a competition. This will include insight into, and potentially inform, the support, facilities, and funding needed for the competition. Volunteers and industry experts will be helpful in designing, developing, and validating the challenges that participants will engage in during the competition.

Linking challenges to industry-recognized frameworks, such as the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF), the NICE Workforce Framework for Cybersecurity (NICE Framework) or the Center for Internet Security Critical Security Controls (CIS) Framework and Benchmarks, help to ensure that the competition provides a relevant and useful cybersecurity experience for the participants.

Competition Roadmap

The competition roadmap describes the structure for how participants will play through the competition to completion and will be included as part of the competition rules. Participants need to know: What do we have to do to win or finish?

Examples of roadmaps include:

- Scoring will be based on keeping required services up, controlling or preventing un-authorized access, and completing business tasks that will be provided throughout the competition. Teams accumulate points by successfully completing injects [tasks] and maintaining services. Teams lose points by violating service level agreements, usage of recovery services, and successful penetrations by the Red Team (CCDC[1]).
- The goal of the competition is to achieve the best rank. A smaller (lower) numerical rank is better than a higher (larger) rank, e.g. a rank of 1 is better than a rank of 2. The three

[1] https://www.nationalccdc.org/index.php/competition/competitors/rules

factors that determine rank are points, accuracy, and time of last correct submission (National Cyber League[2]).

- Winners are determined based on who achieves the highest score in the shortest amount of time. Participants will answer questions about different types of web application attacks, as well as analyze log files, packet captures, and a live target (CyberQuests[3]).
- Players progress through the levels by answering questions and earning points. The next level will unlock after a number of points is obtained (DFIR NetWars[4]).

7 Determine Sources of Players Needed for the Competition

Players can be recruited from schools, organizations, and interested community and government stakeholders. Develop a plan for player recruitment and recurring player participation.

8 Determine Rules and Approvals Needed for the Competition

- Determine and agree upon the rules and procedures that will apply for the competition. This also includes procedures for resolving conflicts and addressing cheating or other forms of player misconduct.
- Consider risk management, technology failure, backup procedures, legal, health, and safety policies.
- Approvals may be needed for facilities, players, coaches, and others involved with the competition.

9 Develop a Project Plan for the Competition

The project plan should be developed well in advance of the competition event date and should address all the steps covered above. It should also include a schedule for obtaining permissions, reserving facilities, ordering swag, sending out invitations, etc. Make sure that all key players are aware of the project plan and the project milestones.

10 Don't Forget the Details

Competitions involve many moving parts. Remember these details for the main event and add your own details to this list:

[2] https://cyberskyline.com/events/ncl/info#brackets
[3] https://uscc.cyberquests.org/
[4] https://www.sans.org/cyber-ranges/

- Test the scoring engine, track items being shipped from sponsors, plan the awards ceremony or distribution, create team packets, develop a structured registration and fee collection process, train volunteers and provide oversight, develop a post-competition survey, pay bills that the competition incurs, and develop a competition archive with artifacts to share with new players.
- Face-to-face considerations: ensure there are tables and chairs for sponsors, coaches, and chaperones, arrange for parking, and consider the impact of poor weather conditions.

11 Do Have Fun with the Competition

Competitions are not a test. They are an opportunity for experiential learning. Competitors should view a competition as a chance to play with their friends and make new friends. All players gain experience. Those who win the competition gain bragging rights, but no one fails a competition.

12 Competition Terminology[5,6]

Black Team
Support team that provides technical and administrative support for the competition.

Blue Team
Defensive security team focused on protection, operational security, damage control, and incident response.

Red Team
Offensive security team focused on ethical hacking to attack targets through penetration testing, physical hacks, social engineering, web app scanning, etc.

Gold Team or White Team
Neutral team that plans and administers the competition, organizes the other teams, and monitors progress.

Orange or Green Team
Neutral team that represents typical end-users or customers.

[5] https://www.blackhat.com/docs/us-17/wednesday/us-17-Wright-Orange-Is-The-New-Purple-wp.pdf
[6] https://www.nationalccdc.org/index.php/competition/competitors/rules

Appendix A: Resources

https://github.com/apsdehal/awesome-ctf

https://github.com/AnarchoTechNYC/meta/wiki/InfoSec#hacking-challenges

https://github.com/zardus/ctf-tools

https://blog.didierstevens.com/

https://github.com/DidierStevens/DidierStevensSuite

https://www.hacker101.com/

https://thehackersmeetup.medium.com/beginners-guide-to-capture-the-flag-ctf-71a1cbd9d27c

https://ctf101.org/

https://ctfd.io/whats-a-ctf/

https://www.social-engineer.org/wp-content/uploads/2018/11/2018-SocialEngineeringCaptureTheFlagReport.pdf

https://competitions.cr.yp.to/

https://www.maths.manchester.ac.uk/cryptography/

https://amp.blog.shops-net.com/5447862/1/cryptography-contests.html

https://simonsingh.net/cryptography/cipher-challenge/

https://cryptopals.com/

https://csrc.nist.gov/projects/hash-functions/sha-3-project

https://www.mysterytwisterc3.org/en/

https://mvngu.wordpress.com/2010/12/25/challenge-your-cryptology-skills/

https://www.cyberlympics.org/about-global-cyberlympics/

https://www.nacloweb.org/

https://ioling.org/

https://onling.org/

https://en.wikipedia.org/wiki/Computational_linguistics

https://www.linguisticsociety.org/content/naclo

https://www.uklo.org/how-it-works#general

https://www.cisecurity.org/cis-benchmarks