GUIDE TO CYBERSECURITY COMPETITIONS FOR COMPETITORS

NICE | community coordinating council

This guide is a publication of the NICE Community Coordinating Council Community of Interest on Cybersecurity Skills Competitions.

Guidebook Drafting Committee:
Marcelle Lee (lead and author)
Gina Sharp (contributor)
Mari Galloway (contributor)
Nik Roby (contributor)
Shelley Morris (contributor)
Jai Vetter (contributor)
Robin Burkett (contributor)
Mariah Kenney (contributor)
Tracy Bruhn (contributor)
Amanda Joyce
Brian Markus

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 2022
Published September 2023

Table of Contents

Introduction

The Guide to Cybersecurity Competitions for Competitors (Guide) was designed to help those interested in playing in cybersecurity competitions and gaining more knowledge about the types of competitions and the necessary knowledge and skills associated with each. Further, the Guide provides information about how to develop those knowledge and skills as well as how to find venues in which to compete.

Intended Audience

Anyone interested in learning more about the different types of cybersecurity competitions from grade school students to industry professionals looking to hone their skills, will fine value in this Cybersecurity Competitions Guide. Trainers, educators, and coaches can also make use of this document in providing guidance to their students. A background in science, technology, engineering, and mathematics (STEM) is not a requirement.

Value of Competing

The skills and experience gained from participating in cybersecurity competitions cannot be overstated. In addition to being able to demonstrate hands-on-keys with a variety of tools, participants can speak to their experiences competing in interviews. New hires without job experience can leverage competition experience in the place of formal on-the-job training or experience. Listing competitions on their resume can make a job candidate stand out from otherwise equally qualified candidates. Additionally, competitors gain confidence in their abilities and learn valuable “core skills” such as time management, problem-solving, and teamwork.

Quite a few organizations are using cybersecurity competitions for recruiting purposes, because they recognize that the intellectual curiosity combined with technical aptitude demonstrated by competitors can be a good indication of employability. Competitions such as the Collegiate Cyber Defense Competition (CCDC) feature recruiting stations and job fairs. Most cybersecurity conferences have sponsors running a variety of competitions.

Additionally, participating in competitions is fun and great for building relationships!

Image 1: US flag at the top of a hill.

Types of Competitions

Capture the Flag (CTF)

The term CTF is used broadly to refer to all types of cybersecurity competitions, though it actually refers to the capture of virtual or digital flags that generally present in the form of a text file or hash, or via access gained into restricted areas. Like other cybersecurity terminology, the meaning of CTF stems from the military. According to the US Army Center of Military History, “the term, in common usage, refers to the capture of a unit's colors (flags) by the enemy in battle, or the taking away of a unit's colors as a punishment or disciplinary measure.”

Challenge and Puzzle

The challenge and puzzle type of competition involves a series of questions that need to be answered by the participant and is sometimes referred to as “Jeopardy-style” competitions. Generally, these are timed events and can be both individual or team oriented. Topics vary, ranging from hash cracking, to “hacker” trivia, to network traffic analysis. Often artifacts, such as log files, packet captures, or sample code are provided for analysis. Examples of this type of CTF include National Cyber League, USCC Cyberquests, Department of Energy CyberForce® Conquer the Hill, and Global Cyberlympics.

Offense and Defense

In offense and defense, also known as red team and blue team, there are defenders (blue team) and attackers (red team). This terminology stems from the Cold War during which America identified the Soviets as “red” and the Allied forces as “blue” (see Figure 1). The defenders are required to harden provided resources and keep critical services running while defending against attackers. These are typically team-based competitions with a finite duration. Examples include CyberPatriot, Collegiate Cyber Defense Competition, and the Department of Energy CyberForce Competition®.

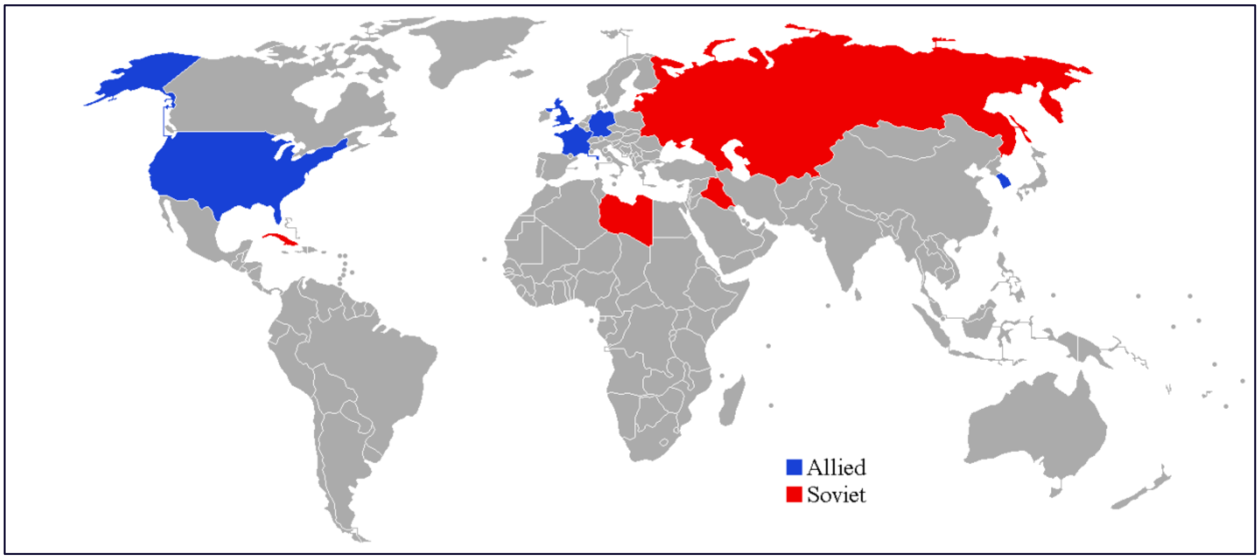


Figure 1: Red and blue nations during the Cold War.

Offense vs. Offense

In an offense vs. offense competition, also known as “red vs. red” and “force-on-force”, teams are provided services for which they find associated vulnerabilities via reverse engineering. The teams then write exploits that they can use against the other teams’ services to score points in what is typically a rounds-based setting. Services are continuously monitored and teams lose points if their services go offline. This style of game was made famous at DEF CON and is what is played in the main CTF at the conference.

Specialty

Specialty competitions involve niche areas of cybersecurity. Format and duration vary widely. One example is a Social Engineering CTF. Featured at security conferences such as DEF CON, social engineering competitions involve discovering information about a target organization prior to a live competition where the participant attempts to reach the target by phone and have them perform some sort of activity, disclosing information that could be used to gain access to a company. This is often done by sending phishing emails and an employee clicks a malicious link. Another example is Trace Labs' Search Party CTF, which has participants, typically working in teams, find information online about missing people. Points are awarded for the most useful information. The information is then provided to local authorities to help locate the missing persons.

Image 2:Conference attendees participating in a competition.

Commercial and Vendor

Commercially there are two types of offerings, those that specialize in offering cyber ranges, training, and exercises as a core product such as Aries Security's Capture The Packet or Metova's CyberCENTS, and those that create competitions used for marketing or recruiting purposes to raise awareness of their products such as Corelight's Hunt From Home and Splunk's Boss of the SOC.

Live Action

Live action cybersecurity competitions are typically held in an Esports arena and feature teams playing against each other in both hands-on-keys technical and policy-oriented competitions. An example of this type of competition is the Wicked6 Cyber Games, during which spectators have the opportunity to view the competitors in action, with a running live commentary by

THE WOMEN'S SOCIETY OF CYBERJUTSU PRESENTS
WICKED6 CYBER GAMES
CONGRATULATIONS!
rFlows
BuffOvrFlows
Technology, Cybersecurity and Policy Program
UNIVERSITY OF COLORADO BOULDER
2019 WICKED6 CHAMPIONS

Image 3: Winners of the 2019 Wicked6 Cyber Games.

cybersecurity celebrities and visits by local dignitaries. This type of competition has also been used in military training exercises.

Hackathon

Hackathons, also known as codefests or hackfests, typically refer to coding events where the competitors attempt to solve a problem by developing software. These are often associated with universities, such as the HackHarvard hackathon. Participation in these events can be either team or individual and are generally timed events.

Image 4:US Army personnel participating in a cyber training exercise.

Hybrid

Most competitions fall into the hybrid category, since it is not unusual to have elements of the different varieties make an appearance. Topics, format, and duration can all vary widely. An example of a hybrid competition is SANS NetWars, which features a multi-level environment with the lower levels consisting of solving challenges and the upper levels involving offense and defense activity between competitors.

Real World Application

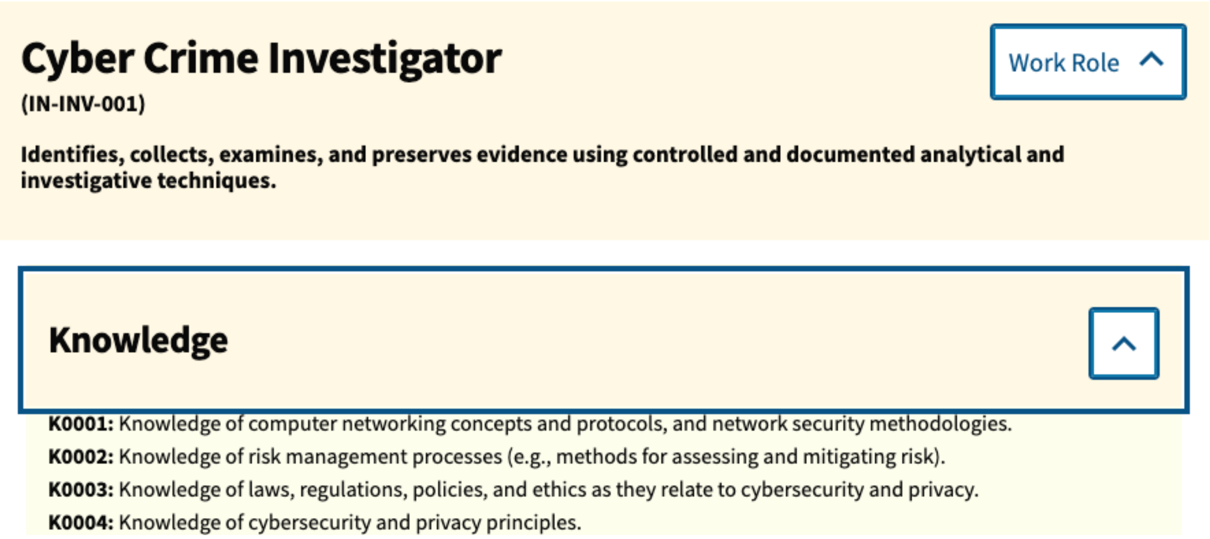
The various knowledge and skills associated with participating in cybersecurity competitions can be tied back to industry guides and frameworks. Having a correlation between known resources helps substantiate the value of what is learned.

Workforce Framework for Cybersecurity (NICE Framework)

Developed by the National Institute of Standards and Technology (NIST), the NICE Framework breaks cybersecurity work roles into seven different categories, as follows:

- Analyze;
- Collect & Operate;
- Investigate;
- Operate & Maintain;
- Oversee & Govern;
- Protect & Defend; and
- Securely Provision.

Details on the categories are listed on the NICE Framework website, including work roles and descriptions of common tasks and the associated knowledge and skills. An example is shown in Figure 2.



Cyber Crime Investigator

(IN-INV-001)

Identifies, collects, examines, and preserves evidence using controlled and documented analytical and investigative techniques.

Knowledge

K0001: Knowledge of computer networking concepts and protocols, and network security methodologies.

K0002: Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).

K0003: Knowledge of laws, regulations, policies, and ethics as they relate to cybersecurity and privacy.

K0004: Knowledge of cybersecurity and privacy principles.

Figure 2: Example from the Workforce Framework for Cybersecurity.

MITRE ATT&CK Framework

The MITRE ATT&CK framework features a knowledge base of adversary tactics and techniques based on real-world observations and correlates to red team/blue team activity. Many organizations use this framework in their research and analysis, and this is a useful resource in learning about threat actor methodology. Topics in the framework include:

- Initial Access;
- Execution;
- Persistence;
- Privilege Escalation;
- Defense Evasion;
- Credential Access;
- Discovery;
- Lateral Movement;
- Collection;
- Exfiltration;
- Command and Control; and
- Impact.

Center for Internet Security Critical Controls

The Center for Internet Security promulgates a list of twenty critical security controls, originally developed by the US Department of Defense. These are broken down into basic, foundational, and organizational controls. The controls also correlate to red team and blue team activity.

Getting Involved

Cybersecurity competition opportunities abound and can be online or in-person, team-based or individual, and topic-specific or general interest. An excellent source of information about upcoming cyber competitions is the CTF Time website. Social media platforms such as Twitter can also provide leads on upcoming events. Community organizations are also a good source of information. The Women's Society of Cyberjutsu, for example, has an extremely active group of competitors with a dedicated Slack site. Local Meet-up events can be a resource for finding like-minded individuals to practice with.

As mentioned earlier, most cybersecurity conferences offer cybersecurity competitions to attendees. The BSides security conferences are smaller in size in terms of attendees and are often low-cost or even free. In addition, BSides events occur all around the globe. Larger conferences such as DEF CON offer many types and levels of competitions.

Preparation

While most competitions do not require advance preparation, it makes sense to build out a cybersecurity toolkit. Doing so will also help with development of technical knowledge and skills. We recommend starting by building a virtual lab environment, using VirtualBox or one of the VMWare products. These are the platforms that allow you to run virtual machines (VMs). A good virtual machine to start with is the Kali Linux penetration testing distribution, which comes with many built-in hacking tools. In addition to those tools, it is useful to have an advanced text editor, a debugger, and a hex editor. To practice, take a look at Vulnhub for other VMs that you can install in your hypervisor and practice or other sites that offer cloud-based virtual machines on which to practice your skills.

Image 5: Meeting participants sitting around a large conference table.

Platforms such as TryHackMe, Hack the Box, PicoCTF, and Over the Wire are examples of self-paced learning opportunities presented in a competition-style environment.

Cheat sheets are also useful and are available for myriad topics. A curated repository can be found online. Additionally, there are cybersecurity professionals on YouTube such as John Hammond who share content, as well as numerous websites that are helpful in solving challenges.

Finally, there are many competition walk-throughs available online. Remember never to practice hacking on a system that you need for other important operations. Also do not hack anything that you do not own or have not been given explicit permission by the owner to do so. Hacking systems when you have not been provided explicit permission could result in legal or financial ramifications.

Conclusion

The security industry desperately needs additional people to join the ranks. As much as they need new people, it is rare to find positions that will train someone with minimal hands-on skills. That's where competitions come in. They give inexperienced people the experience they need to understand and talk about security concepts in a way that they really understand. In competitions, the experience is real. It may be a game, but the learning is often immediately applicable in a cybersecurity role. In addition to gaining knowledge and skills, one of the most valuable outcomes of participating in competitions is confidence. When someone masters a concept in a competition and then they find the concept in the real world, they approach it not as something they have never seen, but as something in which they have already been exposed. Participating in competitions makes you a winner regardless of the outcome.

The members of the NICE Cybersecurity Skills Competitions Community of Interest encourage you to get out there and try a competition.
You have nothing to lose and everything to gain!

Appendix A: Resources

https://www.nationalcyberleague.org/
https://uscc.cyberquests.org/
https://www.cyberlympics.org/
https://www.uscyberpatriot.org/
https://www.nationalccdc.org/
https://cyberforce.energy.gov
https://www.defcon.org/
https://www.social-engineer.org/social-engineering-ctf-battle-of-the-sexes/
https://www.tracelabs.org/initiatives/search-party
https://www.ariessecurity.com/
https://cybercents.com/

https://www3.corelight.com/ctf/hunt-from-home
https://events.splunk.com/Defense-and-Intelligence-Community-Boss-of-the-SOC
https://wicked6.com/
http://hackharvard.io/

https://www.sans.org/cyber-ranges/netwars-tournaments/
https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center
https://niccs.us-cert.gov/workforce-development/cyber-security-workforce-framework
https://attack.mitre.org/
https://www.cisecurity.org/controls/
https://ctftime.org/
http://wsccompetitions.slack.com

https://www.meetup.com/
http://www.securitybsides.com/
https://www.virtualbox.org/
https://www.vmware.com/
https://tools.kali.org/tools-listing
https://www.vulnhub.com/
https://drive.google.com/drive/u/1/folders/1cfwjm_VqXwAFpFdBnUXkUi0-qT4_cpiJ
https://www.youtube.com/user/RootOfTheNull
https://docs.google.com/spreadsheets/d/1AkczyGQbtabSMbxq1P-c7u3NSXlmXqqv3cDoVpTlSoM