Preparing for Success in CCDC: Observations by a Competitor Turned Coach

Cody Welu
Cody.Welu@dsu.edu
The Beacom College of Computer and Cyber Sciences
Dakota State University
Madison, SD, USA

Abstract

Collegiate cybersecurity competitions were created to build and test students' cybersecurity knowledge in a secure yet challenging environment. One such competition, the Collegiate Cyber Defense Competition, focuses on defending a computer system from attackers while maintaining critical services. Creating successful teams takes plenty of preparation. Selecting a team of competitors is just the first step, then teams divide themselves into specific roles based on their expertise. Successful teams work on learning to defend common operating systems and server services on a weekly or more frequent basis. Additionally, holding monthly mock competitions that closely mimic the real event can provide significant benefit to the team. While competitors must have technical skills, there are many skills and considerations to form a winning team that are not as obvious on the surface. Building technical and soft skills are just a portion of the benefits competitions of this style bring to competitors, sponsors, and universities alike.

Keywords: CCDC, Cybersecurity Competitions, Networking, Team Building, Cybersecurity Education

1. INTRODUCTION

A goal of cybersecurity education is to prepare students to enter the workforce ready to secure and defend today's information networks. While this often starts as a theoretical discussion in the classroom, hands-on activities are effective tools in helping students practice and retain the concepts presented in the classroom (Bei et al., 2011). Learning-by-doing can enhance student learning and mastery of cybersecurity topics. Many cybersecurity competitions have been created over the years in part as a fun way to apply and test cybersecurity knowledge in a secure yet challenging environment. One such competition is the Collegiate Cyber Defense Competition (CCDC) which was first hosted by the University of Texas at San Antonio in 2005 (Conklin, 2005). This competition is a blue team competition in which teams are charged with defending a computer network from active attackers.

There are many steps and considerations in preparing for CCDC that will be discussed in this paper. I have had the opportunity to be a competitor on a national second place team, and coach a national second place team nine years later. To assist other teams in preparing for CCDC, this paper reflects on CCDC experiences and lessons learned by myself, a student-turned-coach. The following sections will discuss the structure of the competition, followed by tips on putting together a successful team. Technical skills may be an obvious aspect, but over the years our competition teams have found team dynamics to be a critical component to building a successful team. Preparing the teams for the competition will also be discussed, concluding with observations of the many benefits the competition allows.

2. COMPETITION STRUCTURE

The core of the Collegiate Cyber Defense Competition (CCDC) is the same today as it was in 2005. As a defensive focused competition, competitors are given a network of computers,

servers, and in some cases networking hardware that they must secure. This competition is much different than wider-known cybersecurity capture-the-flag (CTF) competitions. In those contests, competitors are often charged with solving several small challenges in areas such as exploitation, reverse engineering, vulnerability analysis, and more. For this defensive-focused competition, the CCDC development team creates a new fictional business each year which is used at the national competition. This includes computer systems configured for the fictional organization. These will traditionally include both Windows and Linux-based systems. Often, security best practices are not used when creating the environment, leaving the competition teams plenty of opportunities to improve the security of the network. While teams are improving the security of the environment, they must also defend the network from active attacks. A very stressful aspect of the competition for blue teams are the active attackers. This group, dubbed the red team, is not a competition team but rather is a team of security professionals attempting to hack into the competitors' networks during the entirety of the competition time (Conklin, 2005). Teams are charged with keeping critical network services functional, totaling approximately half of the available points in the competition.

The other half of the available points in the competition are through performing injects. In CCDC, injects are tasks that teams must carry out separate from fending off the red team. Some examples include writing a new cybersecurity policy for the business, performing research on the latest significant vulnerability and checking to see if the environment is affected, and adding new user accounts to the network. In general, injects may include any other task that an IT team may be charged with completing in a real business environment.

3. THE COMPETITION TEAM

Current National Collegiate Cyber Defense Competition (NCCDC) rules permit up to 12 students on a roster, but only eight can participate in each event. The other four students are listed as alternates and typically practice with the team in the case they'll need to sub in for one of the eight students selected for the competition team. Of the eight students participating in any CCDC event, up to two may be graduate students. As a part of the official CCDC rules, teams must also select a team captain for each competition from the roster. Separate from official CCDC rules, most successful teams place specific roles on the eight competitors, though methods have traditionally varied. Some teams give competitors role assignments specific to individual server technologies, such as FTP and SSH services as a specific role (Sroufe et al., 2010). Other teams simply assign roles based upon the core operating system: Linux or Windows. While actual team composition varies a bit year-to-year, our general structure when forming a team is to choose three students who are strong in securing Linux systems, three students who are strong in securing Windows systems, one student who is strong in operating network-based firewalls like Palo Alto and Cisco, and finally one person who is strong in some combination of policy writing, organizational skills, and team management. Table 1 shows an example of team roles along with the skills and technologies each role may work with.

Role	Skills/Technologies
Firewall Admin	Networking, VLANs, Firewall, Palo Alto, Cisco
Linux Admin	Mail Servers, SSH Servers, Linux Firewall/Services, User Management
Linux Admin	Web Servers, SQL Servers, Web Applications, Linux Firewall/Services
Linux Admin	Web Servers, SQL Servers, Linux Firewall/Services
Windows Admin	Active Directory, DNS, Windows Firewall, Windows Services, User Management
Windows Admin	Active Directory,
Windows Admin	IIS, MS SQL, Web Applications
Inject Handler	Policy writing, communication skills, task management, organization skills

Table 1: Example Team Roles

Within those general groupings, competitors typically train on broad security techniques for their designated operating system. For example, all competitors must know how to configure a firewall on either Linux or Windows, whichever they are assigned. When machines have had a basic hardening applied to the operating system, it is then that competitors can specialize a bit more, typically by service. Some common services within each operating system team are web applications, file sharing services, mail servers, and database servers. While teams do not know what specific technologies will be in play at a competition, they can be sure there will likely

Topic	Level
Command Line Interfaces	Basic
Windows Basics	Basic
Firewall Basics	Basic
Defending SSH Servers	Intermediate
Windows OS Hardening	Intermediate
Firewalls: pfSense	Intermediate
Scripting on Windows: PowerShell	Intermediate
Scripting on Linux: Bash	Intermediate
Web Servers: Windows (IIS)	Advanced
Web Servers: Linux (Apache, nginx, etc)	Advanced
SQL Servers: MS SQL, mySQL, and more	Advanced
Logging with Splunk and Elastic	Advanced
Firewalls: Palo Alto and Layer 2 vs. Layer 3	Advanced
Firewalls: Cisco	Advanced
Dealing with Service Dependencies	Advanced
Common Web Apps	Advanced
Inject and Report Writing	Intermediate
Windows: Active Directory	Advanced
User Management	Intermediate

Table 2: Sample Training Topic List

be at least one of each of these services. Table 2 provides a sample training topic list. Each topic would be covered in one or two team meetings.

We typically reserve at least one role almost exclusively to handling injects that come forward during the competition. Often an inject will require a specific task to be carried out on one or multiple servers, so it is the responsibility of the inject handler to determine which other team members must complete an inject. Therefore, this team member must be extremely organized to manage the numerous injects that the team must complete during the competition. Additionally, this person must host qualities of a leader on the team. In fact, for many years, the inject handler team member also served as the team captain. While our collegiate teams have typically found this to be a good fit, there is a potential downside. The team captain could be called into meetings with competition officials, and if they are the only member dedicated to injects, no one is left to handle them in the captain's absence.

4. TEAM DYNAMICS

One of the most significant non-technical takeaways from the past six years of coaching CCDC teams is the concept of team dynamics. Gathering a group of highly technical students to compete in this challenging competition is important, but equally important to the success of the team is how well they work together. Prior studies have shown there is a relationship between team dynamics, effective teamwork, and successful outcomes (Wei & Ohland, 2021). It was found that teams that address conflict and come to consensus are more productive than teams who do not manage conflict well. These results have held true in practice in our collegiate teams over the years. The less conflict among the team members, the better members perform in the competition.

As an example of common conflict on our teams, there are frequently differing opinions on training goals and outcomes during each weekly practice. An effective way to flesh out differences of opinions is to simply communicate. We encourage all members of our teams to write their goals and priorities down so the team captain can compile them together into a single list. Next, students can vote on the goals they find to be most important to cover first, helping the team prioritize as a whole.

A core aspect of effective conflict resolution is good communication. In fact, bad communication was a source of conflict in one of our competition teams. One team member, while technically proficient, was not communicating effectively during the regional competition. This person was not updating the team about which tasks he was working on and ended up duplicating effort with other team members. This, coupled with the fact that he didn't seem to take the competition seriously led a few team members to recommend his removal from the team. This was a source of significant conflict, as yet other members saw him as a valuable member of the team. Resolution came in the form of the entire team effectively communicating their concerns with everyone, and the team captain and faculty advisor agreeing that the issue was in fact due to poor communication rather than a lack of technical ability during the competition. Improved communication from the individual and among the entire team led to a more successful team in the next competition. The lesson learned here is to promote effective communication in teams. Encourage team members to frequently share what they're working on and what problems they're struggling with.

Successful teams will participate in team building activities to boost morale, comradery, and ideally increase competition performance. These activities should not just be fun get-togethers, however. Research shows that team building activities have the potential to boost short-term

morale or performance, but the effect is not lasting (Land, 2019). To have lasting impact, it was found that team building activities should be deliberately added to existing training on the concepts required to perform well at a technical level in the competition. Simply holding team building exercises that only contain lectures on teamwork does not show lasting positive effects (Klein et al., 2009).

Every CCDC team needs a leader at its core. This team member often naturally takes on this role or is voted to this role by fellow team members as the team captain. This person takes charge to develop team meetings and trainings and acts as a moderator within the team. A leadership quality our collegiate team has found to be important is collaboration. It is imperative that the team captain encourages a collaborative climate which is known to improve the effectiveness of a team (Larson & LaFasto, 1989). Collaboration encourages more of a bottom-up approach to team management. This is a healthy leadership style which lends itself well to competition teams. Rather than having one leader dictate everything for the entire team, each member on the team should assume some sort of collaborative leadership role with the ability to take charge in some way. This could be in their own area of technical expertise, or simply the ability to direct and lead when a difficult task is presented to the team. In fact, research shows that students who prefer collaborative leadership roles experience more team cohesion and less conflict (Beigpourian et al., 2019).

5. PREPARING FOR CCDC

As with any competition, the most successful teams practice regularly. Some CCDC teams practice weekly, some even more frequently. Our collegiate teams typically meet 1-2 times each week for approximately 2 hours. It becomes difficult for most students to dedicate an extreme amount of time to cybersecurity competitions as they're balancing classwork, other clubs and activities, and in many cases jobs as well.

At the start of the academic year, the 12-person CCDC roster has not yet been set. Therefore, all interested students are involved in the weekly meetings. Most meetings are spent working on technical skills. Early in the year the team will focus on the basics that apply to every major system: firewall configuration, bulk password change scripts, and other general system hardening topics. Next, the group will move to more specific technologies that are likely to be seen in CCDC environments such as Microsoft Active Directory and cross-platform SQL servers. Later in the season, typically after the core competition team has been selected, students will dig even deeper into their area of expertise. As an example, at least one member on the team should be familiar with common open-source Human Resource Management (HRM) web applications, like Orange HRM. This practice often will include setting up the specific server or service from scratch and learning how to configure and secure it.

Learning specific services is important, but teams will find a significant benefit in holding a practice competition modeled as closely to CCDC as possible. Every month or two, a subset of students will build out an entire network similar to that which would be found at an NCCDC event. This will include a mix of Windows and Linux systems with common critical scored services such as email, multiple web applications, file servers, and SSH servers. There also is a core network firewall that starts in an unconfigured state. The status of these critical services is checked frequently during the competition by a custom scoring engine that is created and maintained by students and alumni.

Building a practice environment that closely mimics the local regional CCDC event can be difficult, especially for teams new to the competition. General guidance when building a practice environment would be to include a mix of operating systems and services along with a network firewall. Some regions have very large competition networks with upwards of 60 scored services that competitors must keep online, while other regions may only have ten such services. Teams and coaches can look for inspiration when setting up practice networks by utilizing network diagrams from past regional and national competitions. Some of these diagrams are cataloged on a public Github page found here: https://github.com/mubix/howtowinccdc/tree/master/documents

Other than the time required, a major common hindrance to setting up a practice CCDC environment is the availability of computing resources. Some universities have plenty of resources available to students to create environments such as a virtual computing lab or physical hardware. Other teams will search for sponsorship from local businesses to obtain resources. A practice CCDC environment could be setup on as small as a single server using virtualization technology, if required. In fact, some regional events will utilize cloud hosting infrastructure, though that can be cost prohibitive

Operating System	Scored Service	Other Service
pfSense	None	Network Firewall
Windows Server (2019)	Active Directory (LDAP), DNS	DHCP
Windows Server (2022)	SMB	
Windows Client (10)	Remote Desktop Protocol	
Linux Server (CentOS)	Web (Application like Orange HRM)	SQL
Linux Server (Debian)	NFS	
Linux Client (Ubuntu Desktop)	SSH	

Table 3: Sample Basic Practice Environment

for teams to practice with. A sample list of systems in a small practice environment is provided in Table 3. While the services listed in the other service column might not be directly scored by the scoring engine, they must still be kept functional by competition teams. As teams mature and have resources available, they should increase the number of computers and services in future practices. Traditionally, the national CCDC has broken systems into at least two separate networks and IP spaces. An example of a more complex practice environment is provided in Appendix A.

As the second major point-earning portion of the competition is injects, students will prepare these for a practice competition as well. In CCDC, an inject is a prescribed task that is "injected" into the competition that teams must complete within a certain timeframe. These injects include both technical injects and research/policy injects. As an example of a technical inject, teams are directed to consolidate web applications on multiple servers to a single server using the LAMP technology. As an example of a research/policy inject, teams are directed to provide a writeup explaining the Log4j vulnerability and its potential impacts, as well as identifying if any competition systems are vulnerable. All injects must have a due date assigned to them. Most injects would require teams to complete them in 30-120 minutes depending on the complexity of the task. For practice, it is often best to bombard the team with more injects than they can reasonably complete to help simulate the fast-paced stressful environment they will experience in CCDC events.

Preparing a CCDC practice event is extremely time consuming. The preparation team must create the systems that make up the computer network, as well as create injects and test automated scoring mechanisms. It takes a large team to pull off frequent practices of scale. There also is a significant hardware requirement depending on how many systems and teams are supported. There also need to be volunteers ready to participate during the practice as a red team. In many cases students and alumni are excited to volunteer their time to help CCDC teams practice by hacking into their systems as a red team member. It is also noted that previous competition experience does help guide the creation of the environment and pacing of inject delivery.

6. COMPETITION BENEFITS

There are many benefits to cybersecurity competitions at the collegiate level. As previously mentioned, the opportunity students have to practice the skills they learn in the classroom is invaluable. These competitions also expose students to new technologies and help them build new skills. Previous studies have already documented some of the technical skills gained by competitors of cyber competitions at the collegiate level (Pike et al., 2022).

The nontechnical benefits of these competitions are to be mentioned. One of the most obvious benefits to students is the experience working as a team in a fast-paced, high-stress environment. With frequent taskings arriving via inject and constant pressure from the red team hackers, students gain experience and skills that are very difficult to teach in a classroom environment – skills vital for the workforce of today.

The networking opportunities provided in these competitions cannot be overstated. Especially at NCCDC, student teams enjoy the opportunity to meet, talk with, and learn from fellow competitors. Building a community of peers in the industry is a major benefit to these types of competitions. As a former competitor and now coach, I still find myself reaching out to CCDC alumni and coaches to collaborate and seek advice. One method CCDC alumni stay connected is through a LinkedIn group where opportunities and ideas are shared.

Competition sponsors also provide important networking opportunities by hosting a specific networking event during the national

competition. Competitors can meet prospective employers in the vast array of opportunities the cybersecurity field has to offer. In turn, sponsors are excited to hire students who participate in CCDC. It is encouraging to see various sponsors return each year to support students in the competition. Networking is not only for active competitors, but alumni of CCDC can benefit as well. There are many CCDC alumni who bring in their organizations as new sponsors of CCDC.

At another level, the competition also benefits the participating universities. Professors are encouraged to support students through clubs and updated applied curriculum. CCDC also provides a marketing and recruiting opportunity for universities. Some students have chosen a university or transferred to another university due to their involvement and success in cybersecurity competition teams.

7. CONCLUSION

Preparing for success in CCDC can seem like a daunting task. Teams and coaches should spend time training the team on technical skills, learning how to better secure and defend Windows and Linux operating systems as well as common server services. Hosting team-building activities is a fun and essential addition to regular meetings as well. While competing in events like CCDC may be challenging, there are many benefits to encouraging student participation in these cybersecurity competitions. Students can hone their technical cybersecurity skills learned in the classroom, gain experience working with others on a team, work on the ability to work under pressure, and experience numerous networking opportunities. Studies have shown an applied hands-on approach to teaching cybersecurity is beneficial to comprehension, and making those hands-on opportunities more engaging and fun for students is always preferred. Winning competitions like these takes plenty of technical skill, but also takes leadership, teamwork, and collaboration. However, winning is not the only goal. The experience, skill development, and vast networking opportunities these competitions provide are invaluable to all competitors.

The National Collegiate Cyber Defense Competition might be one of the oldest defensive competitions still active today. Due to the impact these events can have on the future workforce, many new competitions are being created and expanded such as the International Cybersecurity Championship & Conference. Continuing to provide the aforementioned opportunities at a local, national, and international level is beneficial for the cybersecurity community.

8. REFERENCES

Bei, Y., Kesterson, R., Gwinnup, K., & Taylor, C. (2011). *CYBER DEFENSE COMPETITION: A TALE OF TWO TEAMS* *.

Beigpourian, B., EbrahimiNejad, H., Ohland, M. W., & Ferguson, D. M. (2019). The Effect of Preferred Leadership Role and Preferred Team Leadership Structure on Students' Perception of Team Processes and Outcome. *2019 IEEE Frontiers in Education Conference (FIE)*, 1–6. https://doi.org/10.1109/FIE43999.2019.9028453

Conklin, A. (2005). *The Use of a Collegiate Cyber Defense Competition in Information Security Education*.

Klein, C., DiazGranados, D., Salas, E., Le, H., Burke, C. S., Lyons, R., & Goodwin, G. F. (2009). Does Team Building Work? *Small Group Research*, *40*(2), 181–222. https://doi.org/10.1177/1046496408328821

Land, S. K. (2019). The Importance of Deliberate Team Building: A Project-Focused Competence-Based Approach. *IEEE Engineering Management Review*, *47*(2), 18–22. https://doi.org/10.1109/EMR.2019.2915600

Larson, C. E., & LaFasto, F. M. J. (1989). *Teamwork: What Must Go Right/What Can Go Wrong*. SAGE.

Pike, R., Weddell, J., & Duong, S. (2022). A Case Study in Identifying and Measuring Skills Honed from a Cybersecurity Competition. *Proceedings of the EDSIG Conference*. https://iscap.info;https://proc.iscap.info

Sroufe, P., Tate, S., Dantu, R., & Cankaya, E. C. (2010). Experiences during a collegiate cyber defense competition. *Journal of Applied Security Research*, *5*(3), 382–396. https://doi.org/10.1080/19361611003601280

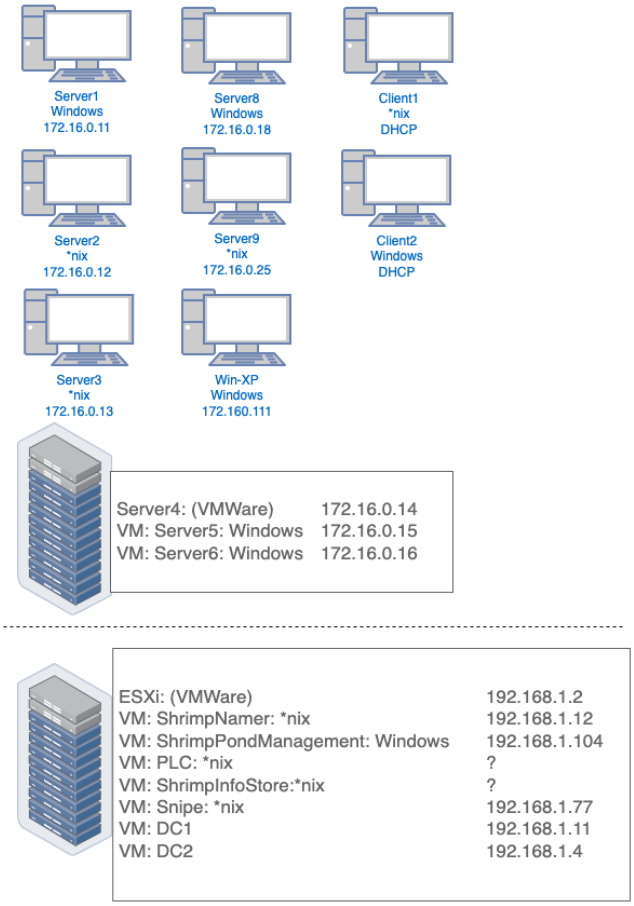
Wei, S., & Ohland, M. W. (2021). The Relative Importance of Team Dynamics in Predicting Effective Teamwork Behaviors. *Proceedings - Frontiers in Education Conference, FIE*, *2021-October*. https://doi.org/10.1109/FIE49875.2021.9637128

ISSN: 2473-4901
v9 n6012

Appendix A

Intermediate Practice Environment

This appendix shows a graphic of the network architecture given to the team during a practice competition. This is typically provided as a part of a team packet that also includes competition structure, rules, and schedule. This appendix also includes a listing of the services that the team must keep online and functional. This sample environment was created for a fictional shrimp manufacturing facility.



Critical Services

For our network to function effectively and efficiently, the following services must always be available and open to **any** external IP address. The critical service **must** remain accessible on the IP address specified and must provide the content and functionality from its original configuration (unless you are directed to or required to make modifications by an inject). Replace the x in the IP shown below with your team number.

- Server1: You must maintain the DNS service on 10.102.1x0.11
- Server1: You must maintain the LDAP service on 10.102.1x0.11
- Win-XP: You must maintain the RDP service on 10.102.1x0.111
- Server2: You must maintain the HTTP service on 10.102.1x0.12
- Server2: You must maintain the SSH service on 10.102.1x0.12
- Server3: You must maintain the HTTP service on 10.102.1x0.13
- Server3: You must maintain the SSH service on 10.102.1x0.13
- Server5: You must maintain the DNS service on 10.102.1x0.15
- Server5: You must maintain the LDAP service on 10.102.1x0.15

- Server6: You must maintain the HTTP service on 10.102.1x0.16
- Server8: You must maintain the FTP service on 10.102.1x0.18
- Server8: You must maintain the RDP service on 10.102.1x0.18
- Server9: You must maintain the HTTP service on 10.102.1x0.25
- Server9: You must maintain the SSH service on 10.102.1x0.25
- ShrimpPondManagement: You must maintain the HTTP service on 10.102.21x.104
- PLC: You must maintain the DNP service on 10.102.21x.105
- PLC: You must maintain the HTTP service on 10.102.21x.105
- DC1: You must maintain the SMB service on 10.102.21x.11
- ShrimpInfoStore: You must maintain the SMB service on 10.102.21x.12
- ShrimpInfoStore: You must maintain the SSH service on 10.102.21x.12
- DC2: You must maintain the LDAP service on 10.102.21x.4
- Snipe: You must maintain the HTTP service on 10.102.21x.77

Additional Network Services

In addition to the critical services, you are scored on, your team must also abide by the following directives concerning network traffic.

Internally you will need to maintain:

File Servers
Client Workstations
Active Directory
Access to critical services
Internet access for workstations

Outbound Services:

Your user base will need outbound access to common protocols such as HTTP, HTTPS, SSH, FTP, SFTP, POP3, DNS, and update services. If a team is not allowing these services outbound from client workstations at a minimum, there may be significant point penalties assessed.