Maximizing the Educational Benefits of the Palmetto Cyber Defense Competition (PCDC) Experience

Brennon Treadwell
bjt1798@uncw.edu

Geoff Stoker
stokerg@uncw.edu

Congdon School
University of North Carolina Wilmington
Wilmington, NC 28403, USA

Abstract

On April 10, 2022, six students from the University of North Carolina Wilmington (UNCW) attended the Palmetto Cyber Defense Competition (PCDC). For five of these students, this was their first foray into the world of cybersecurity competitions. In this paper, we reflect on that experience from a metacognition perspective, suggest a preparation plan suitable for other novice cybersecurity competitors preparing for their first competition, and suggest that a need exists for more cybersecurity competition experience reports to be created and shared among the academic community to demystify competitions and encourage broader student participation.

Keywords: Cybersecurity, Competition, PCDC, Metacognition

1. INTRODUCTION

The University of North Carolina Wilmington (UNCW) Cyber Defense Club (CDC) is a student-run organization with the goal of engendering and supporting student interest in cybersecurity. The club, open to students of all skill levels and majors, provides members/attendees with opportunities to meet and work with like-minded individuals. The level of participation varies, but students are welcome to join regular meetings, training activities, and outside events like workshops, competitions, and webinars.

As demand for cybersecurity professionals continues to rise ("Cybersecurity Supply/Demand Heat Map," 2022), the purpose of UNCW's CDC, and organizations like it, is becoming increasingly important. Preparing students with relevant and practical skills is key for rapid assimilation into and active participation in the cybersecurity workforce. Cybersecurity competitions are a valuable way to provide that skill development to CDC members. Competition prep takes up a sizable portion of meetings and many students recognize the benefit of the hands-on experience that competitions provide.

Various UNCW CDC members have participated in a variety of competitions over the past few years including:

- Department of Energy's (DoE) CyberForce Competition® (https://cyberforce.energy.gov/cyberforce-competition/)
- Hivestorm© (https://www.hivestorm.org/)
- TracerFIRE (https://youtu.be/1ppotM9d1yA)
- Wicked6 Cyber Games® (https://www.wicked6.com)

The club had sent a team to the Palmetto Cyber Defense Competition (PCDC – https://pcdc-sc.com/) in 2019 and after a two-year hiatus were

ISSN: 2473-4901
v8 n5755

excited to be invited back for the 2022 event. PCDC follows a format somewhat similar to the Collegiate Cyber Defense Competition (CCDC) that provides students an opportunity to further develop their cybersecurity-related technical and managerial skills. The CDC organized and sent a team of six members to compete at PCDC, five of whom had no previous cybersecurity competition experience.

Our goals in writing this paper include:

1. providing future PCDC competitors with a clearer picture of how to prepare for and what to expect at PCDC,
2. suggesting an initial training plan for competition prep based on the recent PCDC experience of our first-time competition participants,
3. developing an understanding of how competitions educationally benefit participants, and
4. encouraging more wide-spread formal sharing of cybersecurity competition experiences in the interest of generating a robust and continually updating knowledge base for new student competitors.

In section 2 of this paper, we provide an overview of PCDC; section 3 evaluates our team's performance before, during, and after the competition; section 4 is a brief literature review of relevant previous work; section 5 provides a discussion of the benefits of PCDC including an application of metacognition; in section 6 we outline an example training plan that can be used when preparing for a competition; in section 7 we discuss plans for future research; and in section 8 we provide a brief recap and conclude.

2. PCDC

Brief Background

The Palmetto Cyber Defense Competition (PCDC) is run by the Naval Information Warfare Center (NIWC) Atlantic and the South Carolina Low Country Chapter of the Armed Forces Communications Electronics Association (AFCEA) ("Event Brochure," 2022). Started in 2013, the competition has been held each year except for 2020 when it was cancelled out of an abundance of caution for and in consideration of the dangers posed by COVID 19. The event provides a venue with different tracks for teams made up of high school students, college students, and professionals to display and further develop their technical skills relating to cybersecurity as well as key soft skills needed to function effectively in a team. This paper is specific to the collegiate portion of the competition, but some of the information may be similar for the high school and professional portions.

PCDC Overview

The most recent collegiate portion of PCDC was held April 10, 2022, at Exchange Park in North Charleston and included 10 teams of up to 6 competitors each from Charleston Southern University, The Citadel, Clemson University, College of Charleston, East Coast Polytechnic Institute (ECPI), Horry-Georgetown Technical College, Trident Technical College, University of North Carolina Wilmington (UNCW), University of South Carolina, and the U.S. Naval Academy.

The competition provides a realistic IT scenario where participating teams (Blue Team) are tasked with defending from threat actor (Red Team) attacks a network that was created to simulate what might be found in a small- or medium-sized business (SMB) environment. The competition network in play was entirely virtual and similar to what is shown in Figure 1. Blue Team members brought personal devices to the competition and used these to log into virtualized desktops hosted in AWS WorkSpaces (https://aws.amazon.com/workspaces/) from which they then accessed the competition network.

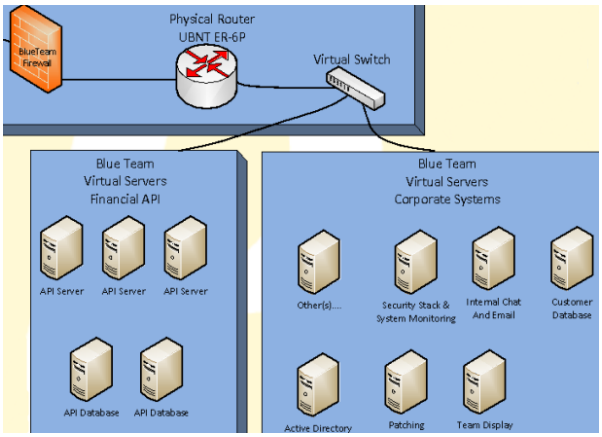

Figure 1. portion of the provided network diagram ("Blue Team Packet," 2022)

Teams were responsible for a variety of tasks including network configuration, service management, threat response, and business task (injects) completion. Injects is a term used to describe tasks assigned to teams that mimic what might be asked of IT professionals during daily operations. For example, the first inject we received asked us to enumerate our network and provide for each discovered machine the IP address, OS, and running services.

The 2022 PCDC scenario specifically tasked teams with defending the network of a fictional cryptocurrency exchange ("Blue Team Packet," 2022). The organizers released this scenario to teams about two weeks before the event. Along with the scenario, the packet contained information that would be critical to understanding the network and how to operate within the competition bounds. For example, the packet included the IP address of the email server, instructions for submitting tickets to the competition officials/administrators (Gold Team), and information related to scoring.

Our PCDC Experience

The six CDC students who originally volunteered and prepared to attend PCDC had no previous competition experience, with demographics that broke out as follows:

- All undergraduates
- 3 females; 3 males
- 1 Hispanic; 2 black/African American; 3 white/Caucasian
- 3 IT majors; 2 CS majors; 1 Business

Unfortunately, two days before the competition, the team captain (male, black, IT) came down with COVID and a substitute (male, white, CS) had to be brought in. The last-minute sub did have some previous cybersecurity competition experience, but not as a team captain.

We found out on the day of the competition that the Blue Team firewall would be out of play and that instead, emphasis would be placed on the hardening of systems. This was somewhat unexpected, but the organizers had decided that too much focus on the firewall might overshadow the importance of individual system security. Given the limited competition time, it appears they wanted to ensure that Blue Teams were able to secure their network at a system level. It is difficult to say what changes will occur for future competitions, but teams should take this into consideration and ensure that they are comfortable working with or without control over a network firewall.

Schedule

In table 1 is the schedule ("Schedule," 2022) provided for the collegiate competition. Upon arrival at the venue, teams signed in, had their laptop chargers checked to ensure they would be compatible with the venue's power constraints, received nametags and complimentary giftbags, and then assembled in an auditorium for the opening activities. Students were welcomed to PCDC, given an overview of the event's history and purpose, and briefed on the process for starting the competition.

To begin the competition, teams were led into a separate room that was divided into 10 sections, one for each team. Although there was a delay due to a misunderstanding/error with the provided AWS WorkSpaces passwords, the event largely unfolded according to the original plan.

Sunday, April 10 2022	
0745-0815	Connectivity Checks
0815-0830	Blue Team Briefing
0830-0900	Competition Begins/Initial Injects/Secure the Network
0900-1545	Operate PCDC Network Under Attack
1545-1550	Break
1550-1605	Red Team Q&A w/ Blue Teams
1605-1620	Break-upload Blue Team Briefs
1620-1645	Blue Team Presentations
1645-1655	Gold Team Debrief: Common Mistakes
1655-1710	Guest Speaker
1710-1730	Awards/Closing Ceremony

Table 1 – PCDC College Day Schedule

Teams were allowed 30 minutes to access and work within their network before the Red Team began their attacks. The Gold Team provided instructions on how to access the default passwords for network accounts, the IP address of a Security Onion server (https://securityonionsolutions.com/software/), and guidance on accessing and responding to business injects.

After the initial 30 minutes passed, the Red Team began their attacks using a variety of methods to access and compromise network systems. For the rest of the competition, the competitors' efforts revolved around continual hardening of machines and responding to injects while detecting and responding to Red Team attacks. Once the competition reaches this point, it can become fast paced, so it is important that teams make the most of the preliminary network access to get a solid head start.

In addition to the technical and business aspects of the competition, PCDC also included social engineering threats. Members of the Red Team would attempt to come into competitor areas and take pictures of workstations or talk to team members to gain information. Teams were rewarded for identifying these security threats and could resolve them by having the team captain ask the social engineers to leave the area.

After the competition portion of the event ended, teams had a chance to meet with Red Team members to ask questions to learn what went wrong and how to improve. This was a brief, but valuable meeting that helped competitors get an outside perspective on their actions and what they could have done differently.

Teams were then assembled into the auditorium to take part in the debrief ceremony. Every Blue Team prepared a presentation to go over various aspects of the competition including what the teams liked, what they disliked, and what they thought could be improved. After competitor presentations, a Red Team representative and then a Gold Team representative spoke about their experiences and what they noticed throughout the competition. This portion of the event is just as valuable as the actual competition itself and gives all participants the opportunity to learn from each other.

Lastly, the awards ceremony took place. The top three teams overall and the top three teams for each scoring subcategory were recognized. The scoring subcategories included service uptime, controlling/preventing unauthorized access, and inject completion.

Rules

The PCDC organizers provided a fairly extensive Preparation Guide (2022) in which 9 rules with 81 subparts are enumerated to govern things like conduct, eligibility, scoring, etc. We will highlight just a couple of specific rules that proved to be especially important to the competition or which may cause confusion among future participants.

Rule 4 and 4.1 cover internet usage during the competition and state that only requested and approved sites may be accessed during the competition ("Preparation Guide," 2022). It seems worth clarifying that this restriction is specific to the internet connection within the virtualized desktops hosted on Amazon WorkSpaces. Outside that environment, competitors can browse the internet freely on their personal machines. Internet activity is monitored, however, and inappropriate usage is not permitted during the competition. This includes viewing explicit material, contacting outside resources, or accessing pirated material.

Rule 8 (7 subparts) covers issues related to questions and disputes, while rule 9 (18 subparts) covers scoring. It is important and extremely beneficial for teams to take extra care in reviewing these sections as they are likely the most critical to competition success.

3. PERFORMANCE

The competition documents provided were a useful starting point in understanding PCDC and the general technical expectations. However, the documents essentially assume that competitors are familiar with or have previous experience with cybersecurity Red Team/Blue Team competitions. Competitors without prior knowledge or experience will likely have difficulty understanding competition expectations.

The primary benefit of the provided materials was to understand the competition background, key roles, scenario, and certain aspects of the working environment. The preparation guide also enumerated a list, provided in Table 2, of suggested networking and security-related study topics that covered what knowledge would be generally applicable to the competition.

PCDC Enumerated Study Topics
1. Perimeter Security. Network and host-based firewalls, intrusion detection systems (IDS), virtual private networks, and DMZs.
2. Patching. Software Patching
3. Networking. Traffic flow, switching, routing, drafting and/or reading a network diagram.
4. UNIX. Flavors of UNIX/Linux, BSD, CentOS, Ubuntu.
5. Windows. Versions 8, 8.1, 10, Server 2008 (both R1 & R2), Server 2012 (both R1 & R2), and Server 2016.
6. User/Account Management.
7. Services and Applications. Email, domain name system (DNS), Active Directory, file transfer protocol (FTP), etc.
8. Tools. Port Scanners, Vulnerability Scanners (OpenVAS), and software-based firewalls (pfSense) and IDS.
9. Database. MySQL, Orange HRM, SQL.
10. Security Onion.
11. Docker Containers.
12. Email Server. Zimbra, Sendmail, Microsoft Exchange.
13. Authentication.
14. General. Admin duties like installing, securing, updating, troubleshooting, etc.

Table 2 – PCDC recommended study topics ("Preparation Guide," 2022)

Specific Preparation Steps

Our team met one week before the competition to go over as a group the documents provided by the organizers and to attempt to establish a plan. We assigned roles to team members based on everyone's experience and comfort level. After that, we went through the list of expected topics

and assigned 2-3 topics per team member based on their role. For example, the Linux administrator was assigned topics 4, 7, and 12. These topics do not cover everything that might be expected of a Linux administrator, but they provided a starting point and gave specific objectives for students to complete.

The team spent the following week preparing separately until the night before the competition when we were able to get together to prepare. At this point, we were able to share information we had researched individually and help each other fill in any gaps. This study session proved immensely helpful to team members, and we would recommend that teams meet as often as possible to prepare as a group.

Each member created a plan of action for the first 30 minutes of the competition. This was essentially a checklist of tasks to perform at the start of the competition based on each individual's role. As an example, the Linux administrator planned to change the default and root passwords, enable a local firewall, and examine active accounts on each machine.

Given constraints due to demands on our team's time and general lack of previous experience, it was challenging to find educational resources that met the needs of our novice team. We found that many of the resources relating to various cybersecurity topics were either too abstracted or too detailed and broad in scope to be useful for preparation. It was difficult to easily find resources that provided details for a small scope that would be easy enough for beginners to understand with clear steps for applying that information in a technical environment.

For instance, point 12 from Table 2 lists Sendmail as a suggested study topic. Without further clarification, it is unclear what that means in terms of required knowledge. Without a clear idea of what to search for, our team's preparation results proved minimally helpful in getting ready for the competition. The vendor documentation (Allman et al., 2001) contains comprehensive instructions for compiling, configuring, installing, and operating Sendmail, but is overwhelming to unpracticed users. On the other hand, many third-party resources were light on details or only offered a small overview of the topic. Without a clear idea of what knowledge is necessary and access to helpful resources, preparing for PCDC can be a challenge.

The CyberPatriot resources recommended in the PCDC prep guide (CyberPatriot, n.d.) further demonstrate the difficulty in finding training resources that meet the need of collegiate teams. The information in the linked training modules is remarkably simple compared to what was expected during the competition, containing primarily introductory information and almost no technical tutorials. The information is too introductory to have any practical use without following up with more in-depth training.

During the Competition

As the competition started, we realized our plan of action was made with incorrect assumptions. The PCDC preparation guides indicated that our team would have access to a network firewall and portions of our plan were contingent upon that expectation. We quickly discovered that being able to adapt and overcome unexpected changes and unforeseen circumstances would be a critical aspect of success.

Given our team's lack of experience and the difficulty in obtaining the necessary training, it is not a surprise that we had the most difficulty relating to the technical aspect of the competition. However, our ability to communicate with each other and work cohesively as a team allowed us to make up for technical deficiencies. Rather than becoming overwhelmed with unknowns, we focused on the tasks we could perform and began to reorganize ourselves to take advantage of each team member's strengths.

Another important aspect of our process during the competition was communicating with the White Team (judges) and the Gold Team. By communicating with them we were able to clarify certain tasks and components of the competition. While our team was not able to place in the top three overall, we did tie for second in the server uptime category and were unofficially told by one of the judges that we ended up in fourth place.

4. LITERATURE REVIEW

According to Beznosov and Beznosova (2007), much of the earlier research into the "computer security attacker-defender game" (p. 427) focused primarily on technical aspects with limited investigation into non-technical facets. In an attempt to guide cyber defense competition development, Woszczynski and Green (2017) expanded on Beznosov's and Beznosova's work identifying a set of learning outcomes for competitions that relate to technological, human, and social factors. Learning outcomes were selected based on survey results which asked competition coordinators and competitors to rank

ISSN: 2473-4901
v8 n5755

which skills were the most important for certain tasks.

To further understand the educational importance of competitions, it is important to understand how hands-on learning experiences fit in to cybersecurity. With an increased demand for cybersecurity professionals, it is important that students are given hands-on learning opportunities to adequately prepare for the workforce (Phelan et al., 2021). Phelan has identified a lack of hands-on learning opportunities as a common barrier to entry in the field and cites quality, cost, and usability as potential reasons for that.

Past research has further demonstrated the positive impact that hands-on experiences offer. It is understood that having the opportunity to test skills as they are learned helps learners recognize knowledge gaps and gain more from educational efforts (Loibl & Rummel, 2014).

5. PCDC AS A LEARNING TOOL

Metacognition Overview

Metacognition is a broad and intricate term that at its simplest is used by educational psychologists to describe "thinking about thinking" (Lai, 2011). Lai provides a solid review of the topic that discusses the foundations of and the current understanding of metacognition. We will use metacognition to describe the educational benefits that competitions provide. For the sake of clarity, we are specifically referring to metacognition as "awareness of the content of one's conceptions" (Hennessey, 1999). In other words, we are referring to how one understands what they know and do not know about a particular subject – in this case, cybersecurity.

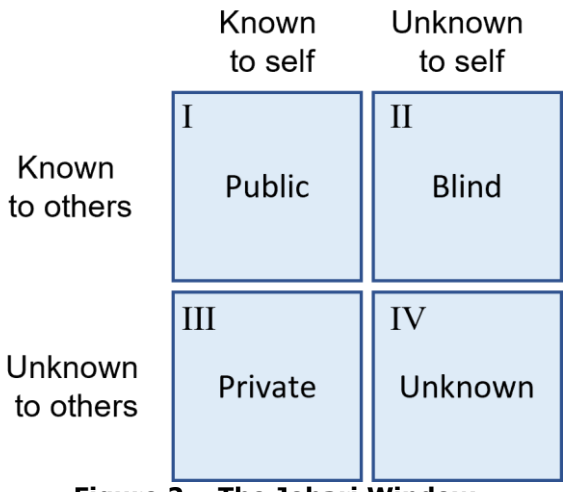

Figure 2 – The Johari Window

The Johari Window (Luft & Ingram 1955) is a 2x2 grid that provides a graphical representation of 4 possible states of self-awareness (Figure 2). Each of the two axes differentiates between the two states "known" and "unknown." The vertical axis indicates the state for others while the horizontal axis reflects the state of the individual or self.

Applying this model to metacognition (awareness of own knowledge), we can represent four distinct categories of information as depicted in Figure 3. We keep the horizontal axis as a measurement of what one knows but modify the vertical axis to reflect one's awareness of what they know.

Using similar terminology, former secretary of defense Donald Rumsfeld spoke about the danger of unknown unknowns in a 2002 press conference.

> …there are known knowns; there are things we know we know. We also know there are known unknowns; that is to say we know there are some things we do not know. But there are also unknown unknowns – the ones we don't know we don't know (Department of Defense, 2002).

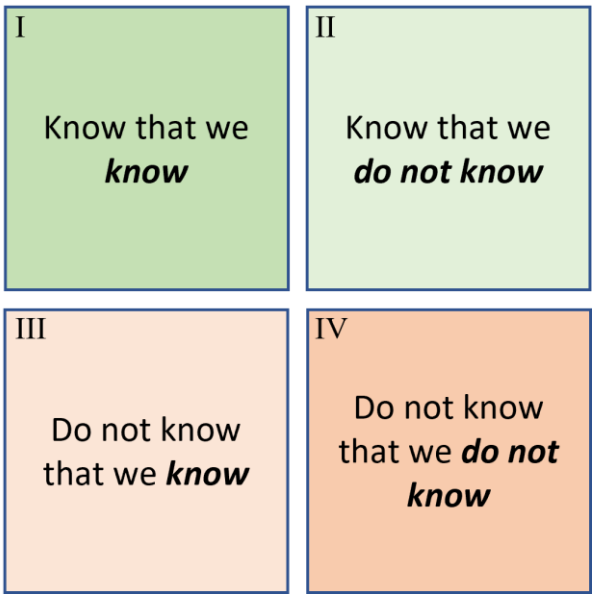

Figure 3 – Graphical depiction of metacognitive information categories.

From our PCDC experience, we found that preparing for competitions is most difficult when you are unaware of your own knowledge gaps. However, we also found that PCDC proved very beneficial in highlighting those knowledge gaps and moving what we "do not know that we do not know" (quadrant IV) to what we "know that we do not know" (quadrant II).

Having the ability to test skills in a practical business-like environment gives students the opportunity to evaluate their capabilities. At PCDC, students were tasked with defending a network. Without clear and definitive outlines regarding the competition bounds and expectations, students may have difficulty accurately gauging their ability to be successful in this setting. However, after actively performing the tasks of network defense, students can more easily recognize what information is needed and of that information, what they already know and what they still need to learn.

Maximizing the Benefit

Our team's experience points towards the benefit of competitions as a tool to highlight knowledge gaps and supports the observations made by Loibl & Rummel (2014) relating to hands-on learning. However, we believe that competitions are not primarily focused on showcasing what one does not know but are perhaps more strongly focused on applying what one does know.

If we revisit figure 3, this observation can be described as moving from Quadrant III, "what we do not know we know," to Quadrant I, "what we know that we know." It is by applying the skills competitors have learned during school, work, and on their own time that the competitors gain a deeper understanding of those skills and the ability to use them in an operational setting.

In order to take full advantage of this benefit, teams must be able to develop the necessary technical skills at a proficient level so they can then apply those skills during the competition. By writing this paper and supplying a sample plan, we hope that this task of preparation is made easier and more effective so that future competitors can take full advantage of the learning opportunities competitions offer.

Importance of Non-Technical (Soft) Skills

It is worth noting that communication and organization are just as important as technical skills when it comes to competitions. While our team was less proficient with technical skills, we were most likely able to contend due to our communication and organization during the competition. In order to facilitate organization, teams should develop a clear plan for competition prep. This plan should be used to guide teams through the preparation process and help communicate expectations to team members. It is important that this plan include opportunities to develop both soft skills and technical skills in order to maximize its benefit.

More Experience Reports

There appears to be somewhat of a strange gap in the information/shared knowledge related to cybersecurity competitions that is readily available online. For many competitions like PCDC (e.g., TracerFIRE, Hivestorm, the national Collegiate Cyber Defense Competition [CCDC] and associated regional competitions), it is relatively easy to find general abstract event descriptions, lists of participating organizations, rules, results, etc. But it can be hard to find the kind of detailed narrative descriptions of what it is actually like to participate in a competition from which hesitant cybersecurity novices might derive some confidence to take that leap.

Seeking greater insight into the details of how cybersecurity competitions unfold for participants, we sought out and examined several academic papers that address cybersecurity competitions (Mirkovic et al., 2015; Pusey et al., 2016; Wee et al., 2016; Bashir et al., 2017; Dunn et al., 2018; Oliver & Elwell, 2018; Straub, 2020). The papers that showed up in our Google Scholar searches unsurprisingly had a research-oriented focus that led them to investigate and report on various aspects of the competitions and/or the participating competitors that were academically interesting, but they were of minimal use to a novice competitor getting ready for their first competition.

In light of this current state of affairs, it seems it would be useful to see a greater focus on the creation and acceptance of cybersecurity competition experience reports in more venues so that they could be shared among the academic community to help demystify competitions, encourage broader competition participation, and accelerate the quality of participants' performances.

6. SAMPLE PLAN

A primary purpose in undertaking this paper was to develop a competition training plan that could be used locally at the UNCW CDC. We have included a sample plan below that will serve that purpose and that can be adjusted by other competitors to possibly meet their needs.

1. ***Establish effective communication***. Communication will be critical when preparing for and participating in competitions so teams should prioritize establishing a channel for communication. Start by setting up a Discord channel, text group, etc. among the team to communicate and organize on a daily basis about mundane things. Teamwork and

cooperation are essential and not likely to exist without effective communication. So, to foster the growth of the collaborative communication skills needed, consider getting together to play a cooperative board game like Pandemic (https://www.zmangames.com/en/games/pandemic/).

2. ***Assign primary roles within the team***. Include positions that cover critical aspects such as Linux administration, Windows administration, database use, web services, business injects, etc. The team captain should be comfortable taking initiative and directing efforts while not necessarily needing to be the most technically savvy.

3. ***Plan regular meetings***, both in-person and virtual. At these meetings, address questions and concerns of members, review information that has been released by the venue, and establish expectations/goals for training for the next meeting.

4. ***Ask competition organizers questions early***. Don't bombard them with simple questions that can be answered by reading the provided materials, but polite, respectful, correspondence is encouraged when teams are unsure of competition information.

5. ***Practice working together***. In addition to weekly meetings, team members should work together, as a group or in smaller pairs, to complete technical training exercises. Create mock networks and practice enumerating and securing them. If there are more experienced team members, consider running short simulations with half the team as red and half as blue.

6. ***Build your own smart book***. As you engage in more competitions, save any helpful training resources or guides to develop a list of resources for specific areas. By having a club or organization wide repository, future teams will be able to benefit from the research and learning that previous teams have done. Teams will also be able to retrospectively identify which resources helped the most and focus on using those for future competitions.

7. FUTURE RESEARCH

To evaluate the effectiveness of our training plan and continue understanding how PCDC and other similar hands-on learning benefits students, we include considerations for future research.

Our primary concern is with evaluating how PCDC and competitions in general impact student learning. We plan to analyze factors that include a team's background, experience, and training process and compare those to the team's self-evaluation of learning. This information will be used to identify what aspects of preparation seem to have the largest impact on how much students learn during PCDC. The most feasible way to go about this is to provide teams with optional surveys to fill out pre/post competition.

We hope to use our results to provide less experienced teams with a set of guidelines to follow when preparing for competitions. In addition, students will receive a greater benefit when taking part in preparation when that preparation considers how to maximize learning. The information will also be used to update and improve upon the sample training plan we have included by applying the insight gained from our research.

As an additional component of our research, we expect to implement the training plan for the coming year and perform a team-wide evaluation of its benefits and areas of possible improvement. While the primary focus is student learning, it will also be helpful to analyze our teams performance next year compared to our performance this year. If our team shows marked improvement, it will indicate the success of the training plan in addition to the benefit of experience.

8. CONCLUSION

The PCDC event offers a great hands-on learning experience for students interested in cybersecurity. Specifically, it prepares students for roles in defending SMB networks through scenarios meant to emulate professional environments. Through this competition, students can expect to develop their technical skills and gain a better understanding of what skills are relevant in the workforce. In addition, PCDC provides a great venue for allowing students to develop their managerial and non-technical cybersecurity skills.

We hope to extend the educational benefits of PCDC by providing future teams an idea of what to expect and how to prepare. We encourage teams to implement and revise our sample training plan to supplement their current preparation process. The plan will be implemented locally at the UNCW CDC and guide future competition prep. We hope to continue using our experiences to further develop our preparation process.

9. REFERENCES

Allman, E., Shapiro, G., & Assmann, C. (2001, October 10). Installation and Operation Guide. https://www.sendmail.org/~ca/email/doc8.12/op.html

Bashir, M., Wee, C., Memon, N., & Guo, B. (2017). Profiling cybersecurity competition participants: Self-efficacy, decision-making and interests predict effectiveness of competitions as a recruitment tool. Computers & Security, 65, 153-165.

Blue Team Packet. (2022, March 31). Palmetto Cyber Defense Competition. https://pcdc-sc.com/documents/PCDC2022_BlueTeamPacket.pdf

Beznosov, K., & Beznosova, O. (2007). On the imbalance of the security problem space and its expected consequences. Information Management & Computer Security. https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.429.4055&rep=rep1&type=pdf

CyberPatriot. (n.d.). Archived Training Modules. https://www.uscyberpatriot.org/competition/training-materials/training-modules

Cybersecurity Supply/Demand Heat Map. (2022, June). CyberSeek Project Web site. https://www.cyberseek.org/heatmap.html

Department of Defense. (2002, February 12). Press conference.

Dunn, M. H., & Merkle, L. D. (2018, February). Assessing the impact of a national cybersecurity competition on students' career interests. In Proceedings of the 49th ACM Technical Symposium on Computer Science Education (pp. 62-67).

Event Brochure. (2022). Palmetto Cyber Defense Competition. https://pcdc-sc.com/documents/PCDC2022_Event_Brochure.pdf

Hennessey, M. G. (1999). Probing the dimensions of metacognition: Implications for conceptual change teaching-learning. Paper presented at the annual meeting of the National Association for Research in Science Teaching, Boston, MA. https://files.eric.ed.gov/fulltext/ED446921.pdf

Lai, E. (2011, April). (rep.). *Metacognition: A Literature Review Research Report*. Pearson. http://images.pearsonassessments.com/images/tmrs/Metacognition_Literature_Review_Final.pdf

Loibl, K., & Rummel, N. (2014). Knowing what you don't know makes failure productive. Learning and Instruction, 34, 74-85. https://www.sciencedirect.com/science/article/pii/S0959475214000656

Luft, J., & Ingram, H. (1955). The Johari Window, a Graphic Model of Interpersonal Awareness. *Proceedings of the Western Training Laboratory in Group Development*.

Mirkovic, J., Tabor, A., Woo, S., & Pusey, P. (2015). Engaging novices in cybersecurity competitions: A vision and lessons learned at ACM Tapia 2015. In 2015 USENIX Summit on Gaming, Games, and Gamification in Security Education (3GSE 15).

Oliver, J. Y., & Elwell, C. (2018, March). Effective Competitions for Broadening Participation in Cybersecurity. In 2018 ASEE Zone IV Conference.

Phelan, M., Devine, S., Aiken, M., & Orban, J. (2021, August). Evaluation of Hands-On Cybersecurity Skill Development. Idaho National Laboratory. https://inl.gov/wp-content/uploads/2021/09/4-Beason-Whitepaper-Final-20210903.pdf

Preparation Guide. (2022). Palmetto Cyber Defense Competition. https://pcdc-sc.com/documents/PCDC2022_Prep_Guide.pdf

Pusey, P., Gondree, M., & Peterson, Z. (2016). The outcomes of cybersecurity competitions and implications for underrepresented populations. IEEE Security & Privacy, 14(6), 90-95.

Schedule. (2022). Palmetto Cyber Defense Competition. http://pcdc-sc.com/documents/PCDC2022_Schedule.pdf

Straub, J. (2020, June). Assessment of cybersecurity competition teams as experiential education exercises. In 2020 ASEE Virtual Annual Conference Content Access.

Wee, C., Bashir, M., & Memon, N. (2016). The cybersecurity competition experience: Perceptions from cybersecurity workers. In Twelfth Symposium on Usable Privacy and Security (SOUPS 2016).

Woszczynski, A. B. & Green, A. (2017). Learning Outcomes for Cyber Defense Competitions. Journal of Information Systems Education, 28(1), 21-42. http://jise.org/Volume28/n1/JISEv28n1p21.pdf