

PREPARATION GUIDE



It is my pleasure to congratulate you as you have accepted the challenge to prepare for the annual Palmetto Cyber Defense Competition (PCDC) in collaboration with the Lowcountry Chapter of the Armed Forces Communications and Electronics Association (AFCEA), to be held April 12-14, 2025.

This year we are again offering our separate but affiliated Hack Warz®@ PCDC Competition on 13 April for Colleges and Universities in the Southeast Region. We are also continuing the Professional day that we added in 2015 and, new this year. Finally, to get you started we have developed this preparation guide to prepare you for the challenge that is PCDC.

As you are well aware, there is an ever-expanding proliferation in the use of information technology. Technology is everywhere; it's in our pockets, living rooms, offices, refrigerators, microwaves, workplaces, doctor's offices, and grocery stores. With this huge growth in the use of connected technology, criminals are continually finding ways to exploit and exfiltrate personal, business and government information. Recent attacks such as those at the Red Cross (data breach), Bitfinex (thousands of bitcoin stolen), Change Healthcare and Colonial pipeline (Ransomware) SolarWinds (Supply Chain attack), the 'log4j' vulnerability have highlighted the importance of ensuring information technology is secured. According to a study by a firm that studies jobs trends, cybersecurity jobs are growing at a rate of 12 times the overall job market. The field is calling for a new breed of cyber security experts to defend our information systems as well as to research and engineer innovative cyber technologies that offer new and exciting capabilities in a secure manner.

Every year this competition grows and evolves. We hope that the continuation of professional day will do even more to prepare students, as some will be given the opportunity to work along-side trained cybersecurity professionals. The continued growth of this event is the direct result of providing unique and valuable training to students in South Carolina. This could not be done without all of the sponsors and the cyber security professionals who have dedicated numerous hours of volunteer time. They have all done a wonderful job each year putting this together. But the ultimate reason we are successful is because the students competing work very hard to prepare for this competition and then take the next step towards becoming a cybersecurity professional.

Lastly, I want to wish you all good luck as this competition is very challenging, but I think you will find that the experience is greatly rewarding as well.

Best Wishes,

Scott Bell
PCDC Director

About the Competition

The Palmetto Cyber Defense Competition is a three-day Cyber Defense Competition in collaboration with the South Carolina Lowcountry Chapter of the Armed Forces Communications and Electronics Association (AFCEA), to be held on April 12-14, 2025. The PCDC is an event for the promotion of Cyber Security education and awareness. This competition is intended to energize local high schools & colleges to invigorate focused curriculum development for the type of technical skills that are needed in today’s fast paced & challenging cyber environment. We are introducing Cyber Security/Information Assurance (IA) technical skills at a much earlier age than ever before.

Event Objectives

- Provide an educational venue for cyber defense
- Foster teamwork & leadership
- Create awareness of cybersecurity careers
- Create awareness and understanding of real world cyber security scenarios
- Create interest in cyber security
- Promote cyber security education programs
- Provide student access to potential employers in fields related to cyber security
- Grow our current and future cybersecurity workforce

Competition Info	4
Competition Schedule	8
Event Concepts	9
Resources	10
PCDC Competition Roles	11
PCDC Rules	12
FAQs	20

Competition Overview

Each year the event is based on a particular themed scenario. The scenario description can be found on the PCDC website at PCDC-SC.com. The teams will assume the role of Blue Teams and will be responsible for operating a small network while protecting the network infrastructure from “Red Team” attacks. Throughout the competition, Blue Teams will be scored for accomplishing tasks while maintaining network/service availability as well as their ability to detect and respond to threats.

Students must be able to securely configure and protect their network. During the competition, teams will be expected to operate the business in addition to performing IT functions. This may include tasks such as responding to e-mails from customers, fulfilling customer orders received via e-mail, website, and other messaging services. These tasks may be trivial, however are crucial to competing in this competition. Business success is dependent on IT service availability. Teams must also be able to respond to requests (injects) such as the addition or removal of services while balancing security needs against business needs, or other tasks that cyber security professionals are expected to complete. Representatives of local technology companies seeking new talent will be present to observe the technical skills being exercised in this competition. We will also have the Southeast Region Collegiate HackWarz®@ PCDC competition.

Scenario

Welcome to Palmetto Crossing, a quaint town who prides itself on its “by citizens, for citizens” approach to utility offerings. Feeling financial pressure, Mayor Scott Bell instituted an early retirement program that resulted in the loss of all senior information system professionals and a crippling knowledge gap on system operations. With this information being public knowledge, the water, power, sewage, and internet offerings have become targets for various malicious actors who seek to leverage data breaches, ransomware, and control of utilities for financial and political gain. To combat this, the city Chief Information Officer (I can’t remember the name that’s always used) has begun hiring new teams to regain control of these systems in efforts to ensure the city’s utilities are protected and reliable once again. Join the Palmetto Crossing Department of Commerce team today and make public utilities great again!

High School Competition

The High School Competition will take place on Saturday 12 April. Ten South Carolina high schools will be participating in this event. The level of cyber defense knowledge that the students currently possess will vary depending on the programs and classes offered at the participating high schools. Therefore, PCDC provides at least 1 primary Blue Team Mentor to each school to work several hours each week to prepare the students for the competition. A mentor will also be available to each Blue Team to provide hands-off guidance during the competition. During the competition, only the assigned mentor or designated SMEs are allowed to provide the team guidance. Each high school will have one hour and thirty minutes to secure their network before the

Red Teams can attack. It is imperative that students comprising the Blue Teams make a commitment to spending time on their own to prepare for this competition through participation in school cyber clubs, reviewing Cyber Patriot Curriculum (on the Cyber Patriot web site) and/or working with their designated Blue Team mentors after school. This event will offer high school students the opportunity to gain hands-on real-world experience in the IA field and to collaborate with current IA college students, professors, and professionals. Three of the high schools competing are qualified based on their finishing in the top three in the last PCDC. The other seven high schools competing were qualified through their scores in the CyberPatriot National High School Cyber Defense Competition.

College Competition

The Collegiate Competition will take place on Sunday 13 April and will consist of up to 10 teams. The collegiate teams will prepare independently; however, several Q&A sessions will be held prior to the competition. The Red Team will utilize more sophisticated attacks during the College Day and will commence after 45 minutes. These conditions will allow the college participants to put their education to use with hands-on practice while also providing the opportunity to meet business leaders in the IA profession. During the college competition, systems may be pre-infected, and teams will need to perform the role of incident response to eradicate any present threats while maintaining services.

Pro Competition

The Pro Day competition will take place on Monday, 14 April and is held between a combination of industry and DoD teams. Up to 10 teams will compete and each team may have up to six members and a team lead. The Red Team will utilize the most sophisticated attacks during the College Day and will commence after 30 minutes. The event is to be treated as a competitive training opportunity. Pro teams must bring at least three members which can be supplemented with college students to bring the team up to full strength of six. Teams may also be supplemented with an additional two college students.

Awards

Each school team that wins first place will get to keep the Challenge Cup trophy until next year's competition, at which time it will be returned to be awarded to the next winning team. The top three teams will each receive a trophy as well, which is theirs to keep, and each team member will receive a medal for their achievement, cash towards scholarships and other prizes. The winning Pro Team receives a trophy, and its members get medals and prizes.

Q & A Sessions

Two Q&A sessions will be held for all participants in March.

Internship and Job Opportunities

Students are encouraged to submit their resume to the AFCEA POC, Greg Blackburn at PCDC@afceacharleston.org prior to the 29 March deadline. Resumes will be made available to corporate sponsors and technical companies providing the students with potential career opportunities and internships. There will also be a recruitment channel on Teams for students to post resumes and/or have them reviewed.

Southeast Collegiate Hack Warz® Competition (SCHWC)

Hack Warz® @ PCDC will be held on Saturday 12 April and will be open to all Colleges and Universities in the Southeast Region (Florida, Georgia, South Carolina, North Carolina, Mississippi, Alabama & Tennessee) on a first come, first serve basis. LCE's Hack Warz® is an event that's intended to help participants learn about security while also helping cybersecurity students hone their skills. The event is designed to be FUN and stretch the competitors' security muscle! Registration deadline will be 26 Feb for one team per school, after which schools will be allowed an additional team, space permitting. A total of 60 students will compete in teams of up to 3 students per school. Recruiters will be observing the competition. The winning team will receive a trophy, and each team member will receive valuable prizes such as blue tooth speakers and \$500 cash. Continuity Checks are scheduled to begin at 8:30 am followed by Opening ceremonies at 8:50 am with the competition starting at 9:00 am. The scoring will end at 2:30 pm with the closing ceremonies for Hack Warz® and PCDC running from 3:30 pm to 5:00 p

Questions

The links below provide useful information to assist you in preparing for this event. For the latest information on the event, including Frequently Asked Questions, please visit the PCDC webpage as well as its social media pages on Twitter and Facebook. For additional information of the event, including hotel information, please visit the PCDC site. If you have additional questions, please post to the Facebook page. Also, make sure to tell your friends and family to follow Facebook and Twitter during the competition to follow who is in the lead, what red team attacks are taking place, etc.

PCDC: <http://pcdc-sc.com> https:// also works

AFCEA: <http://charleston.afceachapter.org/>

Facebook:

<https://www.facebook.com/PalmettoCyberDefenseCompetition>

Twitter: <https://twitter.com/PalmettoCyber>

Cyber Patriot: <http://www.uscyberpatriot.org>

PROFESSIONALISM

The PCDC event is to be treated as a business environment. All participants are expected to behave professionally at all times during the PCDC event. Corporate sponsors will be observing the competition, many of whom are actively recruiting for employment. Competitors are advised to dress appropriately since you may be on camera for all to see and use professional language. Inappropriate behavior and speech will not be tolerated and will result in an individual or team removal from the event.

12 April: High School PCDC, Southeast Region Collegiate HackWarz, Cyber-in-the-Middle Schedule

- ❖ 7:45 am – 8:15 am: Connectivity Checks (PCDC/AWS Network & MS Teams) & Team Registration
- ❖ 8:15 am – 8:30 am: Blue Teams Briefing/Opening Ceremony
- ❖ 8:30 am – 10:00 am: Competition begins/Initial Injects/Secure the Network
- ❖ 8:30 am – 8:50 am: Hack Warz continuity checks
- ❖ 8:30 am – 9:00 am: Cyber-in-the Middle (CitM) Morning Session Sign-in
- ❖ 9:00 A.M. – 2:30 P.M.: Hack Warz at PCDC competition
- ❖ 9:00 am – 11:45 am: CitM Morning Session
- ❖ 10:00 am – 3:00 pm: PCDC Operate Network Under Hacker Attacks
- ❖ 12:45 am – 1:10 pm: CitM Afternoon Session Sign-in
- ❖ 1:10 pm – 3:40 pm: CitM Afternoon Session
- ❖ 3:00 pm – 3:25 pm: Red Team members visit Blue Teams
- ❖ 3:25 pm – 3:35 pm: Break/View Sponsor Booths
- ❖ 3:35 pm – 4:15 pm: Blue Team Presentations
- ❖ 4:15 pm – 4:25 pm: Red/Gold Team Debrief: POV, Common Mistakes
- ❖ 4:25 pm – 4:40 pm: Keynote Speaker: COL Linda Riedel, Deputy Director, Citadel DoD Cyber Institute Chief of Staff, South Carolina Army National Guard
- ❖ 4:50 pm – 5:30 pm: Awards / Closing Ceremony (PCDC & HackWarz)

13 April: Collegiate PCDC

- ❖ 7:45 am – 8:15 am: Registration
- ❖ 8:15 am – 8:30 am: Blue Teams Briefing/Opening Ceremony
- ❖ 8:30 am – 9:15 am: Competition Begins- Initial Injects / Secure the Network
- ❖ 9:15 am – 4:00 pm: Operate Network Under Hacker Attacks
- ❖ 4:00 pm - 4:10 pm: Red Team members visit Blue Teams
- ❖ 4:10 pm – 4:20 pm: Break/View Sponsor Booths
- ❖ 4:20 pm – 5:05 pm: Blue Team Presentations
- ❖ 5:05 pm – 5:15 pm: Red/Gold Team Debrief: POV, Common Mistakes
- ❖ 5:15 pm – 5:30 pm: Keynote Speaker: Katie Arrington, Deputy Chief Information Officer (CIO) for Cybersecurity & Chief Information Security Officer at DoD
- ❖ 5:30 pm – 5:50 pm: Awards / Closing Ceremony

14 April: Pro Day PCDC

- ❖ 7:45 am – 8:15 am: Registration
- ❖ 8:15 am – 8:30 am: Blue Teams Briefing/Opening Ceremony
- ❖ 8:30 am- 9:00 am: Scoring Begins, Secure the Network
- ❖ 9:00 am – 4:00 pm: Operate Network Under Hacker Attacks
- ❖ 4:00 pm - 4:15 pm: Red Team members visit Blue Teams
- ❖ 4:15 pm - 4:25 pm: Break/View Sponsor Booths/Networking
- ❖ 4:25 pm – 4:55 pm: Blue Team Briefs
- ❖ 4:55 pm – 5:05 pm: Red/Gold Team Debrief: Common Mistakes
- ❖ 5:05 pm – 5:25 pm: Keynote Speaker: Mr. Kevin Charlow, Executive Director (Acting), NIWC Atlantic
- ❖ 5:25 pm – 5:40 pm: Awards / Closing Ceremony

The PCDC event consists of several networking and security concepts. Below are some of the critical concepts that you and your team should familiarize yourself with while preparing to compete in the PCDC event. For each of these critical concepts, you should be familiar with how the concept applies to securing a network, reacting to incidents, and so on.

NOTE: This is not a comprehensive list and concepts on this list may not appear or be emphasized during this PCDC event.

1. **Perimeter Security.** How to use firewall products (network and host based) to include deployment, configuration, control of network traffic, log data analysis, maintenance, etc.
2. **Patching.** Software Patching. Manual, automatic, from repos, and individual files.
3. **Networking**
 - a. Traffic flow, switching, and routing
 - b. Drafting and/or reading a network diagram
4. **UNIX.** Flavors of UNIX/Linux, BSD, CentOS, Ubuntu
5. **Windows** – 10, 11 Server2016, and Server 2019, 2022
6. **User/Account Management.** Adding and deleting users on multiple Operating Systems and managing those user accounts.
7. **Services and Applications.** Email, DNS, Active Directory, FTP, HTTP, HTTPS, SSH, SCP, SMB, databases, web applications to include API calls
8. **Tools.** Port Scanners, Vulnerability Scanners, and software-based firewalls and IDSs.
9. **Database.** MySQL, MSSQL, MariaDB, PostgreSQL, and other common databases
10. **Security Onion**
11. **Docker Containers**
12. **Email Server.**
13. **Authentication.** Beyond just knowing how to change passwords in multiple environments, also understanding other forms of authentication.
14. **Authorization.** Modification of user and group permission sets across multiple technologies
15. **General**
 - a. Performing admin duties such as installing, securing, updating, troubleshooting, and maintaining the functionality of computer systems on a network.
 - b. Social Engineering

Below is an example list of web sites that contain information about concepts and tools that may be useful to competing teams during preparation for the PCDC event. The Cyber Patriot website offers several training modules at <http://www.uscyberpatriot.org/competition/training-materials/training-modules>.

NOTE: These pages are not being operated, managed, or maintained by PCDC affiliates.

WARNING: Some of these sites are run by the hacker community and should be visited at your own risk.

Administration

- <http://www.technicalinfo.net>
- <http://tldp.org/>
- <http://onlamp.com/>
- <http://technet.microsoft.com>
- <http://www.rootsecure.net/>
- <http://www.osboxes.org/>

Malware

- <http://www.malwarehelp.org>

Assessment

- <http://osvdb.org/>
- <http://packetstormsecurity.org/>
- <http://www.securityfocus.com/>
- <http://sectools.org>
- <http://www.insecure.org>

Perimeter

- <http://www.networkworld.com/topics/security.html>
- <http://www.owasp.org>

Incident Response and Forensics

- <http://www.cert.org>
- <http://www.first.org>
- <http://www.computerforensicsworld.com>
- <http://www.forensicfocus.com/>
- <http://www.e-evidence.info/>

General

- <http://www.scmagazineus.com>
- <http://www.sans.org/security-resources.php>
- <http://searchsecurity.techtarget.com/>
- <http://csrc.nist.gov/>
- <http://www.us-cert.gov/>
- <http://www.itsecurity.com/>
- <http://www.securitynewsportal.com/>

Gold Team: The competition officials that organize, score, run, and manage the competition.

White Team Judges: The competition officials that evaluate team performance and enforce rule compliance. They also pick-up, deliver communications, and provide overall administrative support to the competition.

Red Team: The penetration testing and ethical hacking professionals simulating external hackers attempting to gain unauthorized access to competition teams' systems.

Blue Team Preparation Mentor: The competition support members that provide technical and administrative support prior to the competition. This is only available to the high school teams.

Blue Team Competition Mentor: The Blue Team's assigned mentor for the day of the completion who will provide off-hands technical guidance. Often this is the same POC that assisted with the preparation mentoring. Note: Only the assigned PCDC mentor is permitted to provide the student's technical guidance. The school professors/mentors may make suggestions to the PCDC mentor but not to the students directly.

Blue Team Technical SMEs: In addition to the Blue Team Competition Mentors, there will be designated Blue Team Technical SME's that will be available during the competition to provide additional expertise as requested by the assigned Mentor (for example, if a team Mentor needs additional Linux help they can request assistance from the SME)

Blue Team / Competition Team: The college and high school competitive teams consisting of six students competing in the PCDC event.

Orange Team: Will perform activities on the event network. Could include place requests for the Blue Teams via Email, etc. Develops the injects/business operations requests that teams must perform during the event that are part of their overall score.

Team Captain: A student member of the Blue Team identified as the primary liaison between the Blue Team and the White Team. Will usually provide the 5-minute Blue Team de-brief (lessons learned, what you liked/disliked, etc.) at end of competition.

Team Co-Captain: A student member of the Blue Team identified as the backup liaison between the Blue Team and the White Team, should the Team Captain be unavailable (i.e. not in the competition area).

Team Representative: A faculty or staff representative of the Blue Team's host institution responsible for serving as a liaison between competition officials and the Blue Team's institution.

Trust: Blue Team members can trust competition staff on Blue, Gold or White Team staff teams as well as AFCEA or PCDC directors.

These competition rules are taken from the approved rules of the National Collegiate Cyber Defense Competition (CCDC) and are modified for this competition.

1. COMPETITION CONDUCT

- 1.1 Throughout the competition, trusted officials will occasionally need access to a team’s system(s) for scoring, troubleshooting, etc. Teams must immediately allow them access when requested.
- 1.2 All hardware related questions and issues should be referred to the White Team.
- 1.3 All private communications (calls, emails, chat, texting, forum posting, conversations, requests for assistance, etc.) with non-team members including team representatives, that would help the team gain an unfair advantage, are not allowed and are grounds for disqualification and/or a penalty assigned to the appropriate team. This includes conversations on cell phones or otherwise outside of the team’s competition area during breaks.
- 1.4 School representatives, sponsors, and observers are not competitors and are prohibited from directly assisting any competitor through direct advice, “suggestions”, or hands-on assistance. “Spying” on other teams is also prohibited as well as providing information to other competing teams.
 - 1.4.1 Any team sponsor or observers found assisting a team will be asked to leave the competition area for the duration of the competition and/or a penalty will be assigned to the appropriate team.
- 1.5 Team members will not initiate contact with members of the Red Team during the hours of live competition, unless requesting assistance/deal.
- 1.6 Team members are free to talk to Red Team members during official competition events (if in-person) such as breakfast, dinner, mixers, and receptions that occur outside of live competition hours.
- 1.7 Teams are free to examine their own systems but **no** offensive activity against other Blue Teams, the Gold Team, the White Team, the Red Team, or any global asset will be tolerated.
 - 1.7.1 This includes port scans, unauthorized connection attempts, vulnerability scans, etc.
 - 1.7.2 Any team performing such activity will be immediately **disqualified** from the competition.
- 1.8 If there are any questions or concerns during the competition about whether specific actions can be considered offensive in nature, contact the White Team before performing those actions. They will escalate it to Gold Team if necessary.
- 1.9 Teams are allowed to respond to suspicious / malicious activity including using active response mechanisms such as TCP resets.
 - 1.9.1 Any active mechanisms that interfere with the functionality of the scoring engine or scoring checks are exclusively the responsibility of the teams.

- 1.9.2 Any firewall rule, IDS, IPS, or defensive action that interferes with the functionality of the scoring engine or scoring checks are exclusively the responsibility of the teams.
- 1.9.3 Individuals wearing Blue, Black, Orange, Purple, Gold, White, or Media team badges are allowed in the Blue team areas. In addition, the PCDC Director may also be allowed in the Blue team areas as well as anyone he is escorting. (in-person events)
- 1.10 Red Team members may offer deals. Teams may accept or reject the deals.
- 1.11 The company Chief Information Officer (CIO) may make requests that should be honored.
- 1.12 Blue Teams may make reasonable requests of the White or Gold Teams. The request may or may not be granted.
- 1.13 Competing High School Blue Team members are not eligible to compete in the Collegiate or Pro Competitions.
- 1.14 Unauthorized personnel are not allowed in the teams' competition area.

2. PERMITTED AND PROHIBITED MATERIALS

- 2.1 No memory sticks, flash drives, removable drives, optical media, electronic media, or other similar electronic devices are allowed in the room during the competition unless specifically provided by the White Team in advance.
 - 2.1.1 Any violations of these rules will result in disqualification of the team member and/or a penalty assigned to the appropriate team.
- 2.2 Teams may not use a cell phone or other mobile device during the competition area unless specifically authorized by the White Team in advance.
 - 2.2.1 Any violations of these rules will result in disqualification of the team member and/or a penalty assigned to the respective team.
- 2.3 Printed reference materials (books, magazines, checklists) are permitted in competition areas and teams may bring printed or handwritten reference materials to the competition.
- 2.4 All competition materials must remain in the competition area, including injects, scoring sheets, and team-generated reports and documents.
- 2.5 Only materials brought into the competition area by the student teams may be removed after the competition concludes.
- 2.6 All materials provided to the teams must not be removed from the competition area unless authorized by the Gold Team or White Team.

3. PROFESSIONAL CONDUCT

- 3.1 In addition to published PCDC rules, Host Site policies and rules apply throughout the competition and must be respected by all PCDC participants.
 - 3.1.1 The use of tobacco is **prohibited** by students, staff, faculty, or visitors except in designated smoking areas. For the purpose of this procedure, tobacco is defined as any type of tobacco product including, but not limited to: cigarettes, cigars, cigarillos, pipes, hookahs, smokeless or spit tobacco

or snuff. This procedure also includes electronic-cigarettes of any type and any device that emits smoke or vapors or results in second hand smoke or vapors.

- 3.2 (in-person events only) Outside food is not permitted in Conference Center.
- 3.3 (in-person events only) No eating or drinking near equipment. Lunch and snacks will be provided but cannot be consumed near the equipment. Breaks may be taken as needed but the competition will be continuous throughout the day. It is recommended that only a few team members at a time take breaks.
- 3.4 Activities such as swearing, consumption of alcohol or illegal drugs, disrespectful or unruly behavior, sexual harassment, improper physical contact, becoming argumentative, willful violence, or willful physical damage have no place at the competition and will not be tolerated.
- 3.5 Violations of the rules can be deemed unprofessional conduct if determined to be intentional or malicious by competition officials.
- 3.6 Competitors behaving in an unprofessional manner may receive a warning from the White Team or Gold Team for their first offense. For egregious actions or for subsequent violations following a warning, competitors may have a penalty assessed against their team, be disqualified, and/or expelled from the competition site.
- 3.7 Individual(s), other than competitors, behaving in an unprofessional manner may be warned against such behavior by the White Team or asked to leave the competition entirely by the Gold Team.
- 3.8 (in-person events only) All team members will wear their competition badge identifying team affiliation at all times during competition hours.
- 3.9 (in-person events only) Only Gold and White Team members will be allowed in the competition areas outside of competition hours.

4. INTERNET USAGE

- 4.1 All Internet access will be based on a whitelist. Each competing schools should compile a list of website domains that they would like access to during the competition and submit them to their school's PCDC POC. Subject to approval, these domains will be added to the whitelist on competition day.
- 4.2 Internet resources such as FAQs, how-to's, existing forums and responses, and company websites, are completely valid for competition use provided there is no fee required to access those resources and access to those resources has not been granted based on a previous membership, purchase, or fee.
- 4.3 Only resources that could reasonably be available to all teams are permitted.
 - 4.3.1 For example, accessing Cisco resources through a Cisco.com account would not be permitted but searching a public Cisco support forum would be permitted.
 - 4.3.2 Public sites, such as Security Focus, are acceptable.
 - 4.3.3 Teams may not use any external, private electronic staging area or FTP site for patches, software, etc. during the competition. Violation of this rule is grounds for disqualification.

- 4.3.4 Teams are not allowed to access private Internet-accessible libraries, FTP sites, web sites, network storage, or shared drives during the competition.
 - 4.3.5 All Internet resources used during the competition must be freely available to all other teams.
 - 4.4 No peer-to-peer (P2P) or distributed file sharing clients or servers are permitted on competition networks unless specifically authorized by the competition officials.
 - 4.5 Internet activity, where allowed, will be monitored and any team member caught viewing inappropriate or unauthorized content will be subject to disqualification and/or a penalty assigned to the appropriate team.
 - 4.6 This includes direct contact with outside sources through AIM/chat/email or any other public or non-public services including sites such as Facebook.
 - 4.7 For the purposes of this competition, inappropriate content includes pornography or explicit materials, pirated media files, sites containing key generators and pirated software, etc.
 - 4.8 If there are any questions or concerns during the competition about whether or not specific materials are unauthorized, contact the White Team immediately.
 - 4.9 All network activity that takes place on the competition network may be logged and subject to release.
 - 4.10 Competition officials are not responsible for the security of any information, including login credentials, which competitors place on the competition network.

5. SCHOOL COMPETITOR ELIGIBILITY

- 5.1 Competitors may only be a member of one team per PCDC event.
- 5.2 Only invited academic institutions in the state of South Carolina are eligible.
- 5.3 Competitors in the Collegiate PCDC event must be full-time students of the college or university that they are representing.
 - 5.3.1 Team members must qualify as full-time students as defined by the college or university they are attending.
 - 5.3.2 A competitor in their final semester prior to graduation is exempt from the full-time student requirement and may compete in the PCDC event as a part-time student provided the competitor has a demonstrated record of full-time attendance for the previous semester or quarter.

6. TEAM COMPOSITION

- 6.1 Each school competition team may consist of between three (3) and six (6) eligible students.
- 6.2 Each collegiate competition team may have no more than one (1) graduate student as a team member.
- 6.3 If a member of a competition team is unable to attend the competition, that team may substitute another eligible student in their place prior to the start of that competition or compete without that member as long as the team consists of a minimum of three (3) members. A completed registration form is required for this substitution.

- 6.4 Once a PCDC event has begun, substitutions or additions of team members are prohibited. A team must complete the competition with the team that started the competition.
- 6.5 Each team will designate a Team Captain for the duration of the competition to act as the team liaison between the competition staff and the teams before and during the competition.
- 6.6 Each team will identify a Team Co-Captain for the duration of the competition to act as the team liaison in the absence of the Team Captain.
- 6.7 A Team Captain or Team Co-Captain must be in the competition space at all times during competition hours.
- 6.8 Each academic institution participating is only allowed to compete one team in the PCDC event, unless specifically cleared by the PCDC Director.
- 6.9 Pro Teams will have up to six (6) team members, one captain (1) and up to two (2) college students assigned. Additional college students may be assigned to bring a team up to full strength.

7. TEAM REPRESENTATIVES

- 7.1 (in-person event only) Each school team must have at least one representative present during the PCDC event.
- 7.2 The representative must be a faculty or staff member of the school the team is representing.
- 7.3 Once the PCDC event has started, representatives may not coach, assist, or advise their team until the completion of the event, unless authorized on a case-by-case basis by the assigned Blue Team Mentor or White Team Judge only on the high school competition day. If the assistance is authorized, the assistance must be hands-off.
- 7.4 Representatives must not interfere with any other competing team.
- 7.5 Each Collegiate Team Representative (faculty advisor) must avoid contact with their team during the PCDC competition hours and must not attempt to influence their team's performance in any way, except in the case of an emergency.
- 7.6 High School team representatives may be with their team during the PCDC competition hours but must NOT attempt to influence their team's performance in any way unless authorized as stated in 7.3

8. QUESTIONS, DISPUTES, AND DISCLOSURES

- 8.1 Team captains are encouraged to work with the Competition Point of Contact (POC) assigned to their school, as well as their school's staff to resolve any questions that arise prior to the competition regarding the rules of the competition or scoring methods.
- 8.2 Protests by any team during the competition must be presented in writing by the Team Captain or Co-Captain to the White Team as soon as possible.

- 8.3 The competition officials will be the final arbitrators for any protests or questions arising before, during, or after the competition. Rulings by the competition officials are final.
- 8.4 All competition results are official and final as of the Closing Ceremony of each day.
- 8.5 In the event of an individual disqualification, that team member must leave the competition area immediately upon notification of disqualification and must not re-enter the competition area at any time.
 - 8.5.1 Disqualified individuals are also ineligible for individual or team awards.
 - 8.5.2 In the event of a team disqualification, the entire team must leave the competition area immediately upon being notified of disqualification and is ineligible for any individual or team award.

9. SCORING

- 9.1 The up and down of services for all teams will be visible to everyone throughout the competition day.
- 9.2 Scores will be maintained by the Gold Team and will not be announced, even at the end of the competition.
- 9.3 Only the top three school rankings will be provided. For Pros, only the winner. Teams accumulate points by successfully completing injects, maintaining services, delivering products & detecting/responding to Red Team attacks.
- 9.4 Teams lose points by violating Service Level Agreements (SLAs), usage of recovery services, and successful penetrations by the Red Team.
- 9.5 Teams are scored on four main areas: Availability, Injects, Attacks, and Business Operations.
- 9.6 Availability is the act of maintaining functionality of required services throughout the competition. During the PCDC event, a set of critical services will be identified for teams to manage and always maintain. Those services are checked for functionality and availability throughout the competition – you gain points each time one of your services is “up” and functioning properly when it is checked. If one or more of your services are down for an extended period of time, your team will be assessed with an SLA violation, and you will lose points.
- 9.7 Injects are tasks assigned by the Orange Team. Blue Teams must address or respond to these injects during the competition. Injects range from the very simple, such as resetting a user’s password, to the complex, such as migrating web servers from IIS to Apache with zero down time. Many injects have a written portion, such as a report detailing actions taken by your team or the creation of a new business policy.
- 9.8 Injects are weighted – more complex and lengthier injects are worth more points than simple injects. Injects should be completed in the time allotted; late injects could potentially be scored and because injects chain together, it is prudent to complete all injects even if a deadline is missed. Details regarding credit for late injects will be provided the day of the competition.
- 9.9 Instructions on completing injects will be provided during the competition. All Injects will be delivered via an injects system such as Teams, website, Email, VOIP, and/or

Voice to the teams.

- 9.10 Blue Teams may request that systems be reverted to their original configuration before the competition began; however, there will be a maximum of two (2) reverts per machine and a revert action will cost the team points.
- 9.11 Attacks consist of Red Team activity such as gaining unauthorized access to a Blue Team's system. The Blue Team is responsible for controlling or preventing unauthorized access by the Red Team. Teams lose points to successful Red Team activity based on the nature of the activity and the level of access obtained.
- 9.12 Attack points may be regained if the team provides incident reports for each Red Team incident they detect. Incident reports can be completed as needed throughout the competition and sent to the Gold Team. Incident reports document a successful Red Team attack with a description of what occurred, a discussion of what was affected, and a remediation plan. A thorough incident report that correctly identifies a successful attack can reduce the penalty for that attack. A thorough report shall contain at a minimum the source IP address, the compromised system's IP address, the time that the attack occurred, and details of how the attack was identified. Vague or incomplete incident reports will be rejected.
- 9.13 Business operations will require each team to perform tasks that will be dependent on their services. These operations will require their services to not only be up, but they will need to be functional as well.
- 9.14 Any team action that interrupts the scoring system is exclusively the responsibility of that team and may result in a lower score. Should any question arise about scoring, the scoring engine, or how they function, the Team Captain should contact the White Team judge for their team to address this issue.
- 9.15 There will be no running totals provided during the competition.
- 9.16 At no time will questions about the status of the team's services or the team's current score be answered. Teams are expected to monitor their own performance throughout the competition.
- 9.17 Teams may request that systems be re-verted to their initial load only twice, but each time this is done, the team will be assessed a penalty.

10. RULE UPDATE – DMZ

- 10.1 The 2024 Competition introduces a new component, the Demilitarized Zone (DMZ). The DMZ will be used during the competition as a meeting space for Blue Team to interface with their respective Coach/Mentor.
- 10.2 Blue Teams may request a meeting by notifying a White Team member. If approved, one White Team member will escort the Blue Team Captain or Co-Captain (one or the other, not both) to the DMZ and another White Team member will escort the Coach/Mentor to the DMZ.
- 10.3 Meetings are intended to help Blue Teams work through an area that they are stuck. The Blue Team Captain or Co-Captain should be prepared to ask specific questions in the meeting, not ask for general help.
- 10.4 Only the Blue Team Captain or Co-Captain can request/attend a meeting in the

DMZ.

- 10.5** The Blue Team is only allowed to meet with their assigned Coach/Mentor.
- 10.6** A White Team member will be present for the entirety of the meeting. White Team reserves the right to request a Gold Team member to be present as well.
- 10.7** Meetings will be no longer than five (5) minutes, unless there is explicit permission from the White Team and/or Gold Team.
- 10.8** The Blue Team Captain or Co-Captain is allowed to ask the Coach/Mentor specific questions. The meetings are not to be used as “strategy” sessions. The Coach/Mentor cannot influence their team’s performance in any way, and may not offer suggestions on how to approach the remainder of the competition.
- 10.9** The White Team and Gold Team reserve the right to deny any meeting request and will provide an explanation to the Blue Team as to why.
- 10.10** Only one Blue Team is allowed in the DMZ at a time.
- 10.11** The DMZ will be available on a first-come, first-served basis, with the order tracked by White Team.
- 10.12** Blue Teams may request a meeting with the Gold Team in the DMZ, and the Gold Team may or may not accept.

Rule Violations: Any violation of competition rules and conduct can result in negative points toward the violating team’s score.

Q: What are Injects?

A: They are usually requests from company management requesting things from your team. They could be as simple as “Provide me a list of users who have access to the database system” or as involved as “Migrate the current mail server from Postfix to Exchange.” These are just examples as the actual injects will be provided the day of the competition at set times.

On the College and Pro days these tasks will differ and be more complex exercises related to cyber security.

Q: What is the most important aspect going into the competition?

A: Your team dynamics and the roles you assign each member are very important. Remember this is not a hacking competition: it’s a business competition. Don't put your most skilled technical person as the leader of the team. He/She will be busy handling business tasks. You want someone on your team that has good communication skills as your leader. You also want a strong team that works well together. Your team will be under stress during the event, teamwork helps to manage and control the situation.

Q: Do teams ever self-destruct, fall apart or quit the competition?

A: Yes, this happens at most Cyber Defense Competitions. It's due to various reasons. Mostly, the teams do not function as a single unit. Teamwork and persistence is crucial to successfully completing the competition.

Q: What do we do if we feel overwhelmed during the preparation and don't know what to do?

A: High School teams may consult with your assigned mentor and if he/she needs additional help they can request assistance from a Blue Team Technical SME. Collegiate teams are expected to be able to prepare on their own using resources at their school, however questions can always be sent via the Social Media sites.

Q: How will we be scored?

A: Scoring is based upon services, injects, and business operations.

Q: What is the single most important aspect of the competition?

A: This is a learning event. We are here to learn and have some fun at the same time. During a recent security talk regarding how to host a Capture the Flag (CtF), it was asked “How do you know what to do when you compete?” The reply was “Sit down, stare at the screen. Bang your head against the wall. You'll learn something.”

Q: Is the PCDC an Attack and Defend competition?

A: No, No, No. Absolutely not. If you come into the competition with that attitude, you will do poorly. This is an IT Business continuity competition. Your team will be the IT staff of a business. Your job will be to ensure business functionality and the security of the business's IT assets. The Red Team will simulate real world activity that could harm your IT assets and bring down your business.

Q: What information will I be given about my team's systems?

A: Teams will be provided a Blue Team Packet prior to the competition day. The packet will name the operating systems, root credentials to each system, a list of usernames and passwords, and the services that system was to provide (for example SSH, WWW, etc.).

Q: What will the blue team operating systems consist of?

A: An approximate equal mix of Windows and Unix/Linux operating systems. Windows systems for example may be a range from Windows 10 to Windows Server 2019. Unix/Linux systems for example may include several different distros of Linux, and BSD.

Q: What will our blue team network consist of?

A: The blue team network will consist of virtual machines hosting an array of operating systems, applications, and services installed hosted on an Amazon Web Services (AWS) virtualized infrastructure operated by the Gold Team. The laptops which will be used to access the virtualization systems are out of the scope of the competition for attacks.

Q: What will I need to manage as far as the virtualized servers?

A: You will need to know how to operate in AWS Workspaces where the Blue Team Network will reside. Your host machine will connect to the AWS utilizing common remote administration tools such as SSH and RDP.

Q: Will the competition involve social engineering?

A: Yes, the competition will involve social engineering.

Q: Will we have Internet access during the competition?

A: Yes, you will have access to the Internet during the competition. However, you will only be able to go to sites that have been approved on the "white list". If you have sites you would like to request to be placed on the whitelist prior to the competition, please notify your assigned POC. The tools and sites must be accessible and available for free to the general public. No special sites that require credentials or fees will be allowed. Note: It is not guaranteed that these sites will be approved and placed on the "white list". Sites hosted by any schools or individuals in the competition are also not allowed.

Q: What kind of tools will I have access to?

A: You will be able to use the Internet to access sites that have been placed on the whitelist to download tools. If you have specific tools you would like to request in advance, please let your assigned school mentor / POC know so we can include them for you. Also, see Security Onion below.

Q: Are the systems going to be working when we get access to them?

A: Yes, all the systems will be running and “functional” meaning they will be working and will be responding to the scoring checks – this is an operational network. That does not mean they will all be perfectly configured, or even intelligently configured.

Q: Will we know when our services are considered to be down?

A: The gold/white team will provide a simple display during the competition that shows the status of each of your core services (during the last status routine check).

Q: Can we bring our own system or networking device?

A: No, all equipment will be provided. Additionally, no personal electronic devices are allowed in the competition area. You are still encouraged to bring textbooks and hard copies of guides and manuals.

Q: How will the business injects work?

A: Each team will get instructions from the “CEO/CIO” throughout the competition, in the form of an inject, to complete within the specified amount of time. Completion of each inject within the time specified earns your team points. Partial credit may be given for injects turned in that are slightly late. The points awarded will depend on the complexity of each inject.

Q: How long will I have on the system before the red team is allowed to start attacking?

A: College teams will have approximately 45 minutes, and high school teams will have approximately 1 ½ hour before the red team will be allowed to actively attack. Pro teams will have 30 minutes to prepare before attacks. These times could vary the day of.

Q: Do we have to give a presentation at the end of the competition?

A: Yes. Each team's captain (or multiple people) will give a short 5-minute brief on what the team thought of the competition and recommend any changes for future. A PowerPoint can be used to share on your screen.

Q: How can we identify and respond to Red Team attacks?

A: You will be competing against professional hackers on a network that is definitely vulnerable, poorly secured, and possibly already hacked. A major tool that may assist you is Security Onion/Snort. Security Onion is a Linux distro for IDS (Intrusion Detection) and NSM (Network Security Monitoring). It contains multiple security tools, some of which may actually be configured. Being disciplined in your approach and how you use tools like Snort and the Security Onion will greatly help your chances of standing your ground against the pros and winning the competition. The pcdc-sc.com website already has study materials for Security Onion for high school students. Where to get Snort: <http://www.snort.org>. Also part of the Security Onion, <https://securityonion.net>!

Q: Should we accept deals from the Red Team?

A: Depends on the cost. Deals are improvised/negotiated, buyer beware. Some work out well, others, not so much.

The IP address spaces will vary based on team and a high-level topology diagram will be provided in the blue team packet. The previous years blue team packet in the documents section of the PCDC website can be used as a reference to get a general idea of what will be provided.

Trident Tech, North Charleston, SC 29406

<https://goo.gl/maps/oCxR6KJigGchtNTx7>

[Building 920 - Highlighted in yellow]

