Mid-Atlantic Collegiate
Cyber Defense Competition

2022 MACCDC Virtual Qualifying Round Team Packet

DRAFT v.02-03-22, 5:17pm EST

Presented by:

Raytheon Intelligence & Space

Run by:

NATIONAL CYBERWATCH CENTER

Mid-Atlantic Collegiate
Cyber Defense Competition

Table of Contents

Mid-Atlantic Collegiate
Cyber Defense Competition

CCDC Mission

“The goal of a Cyber Defense Competition is to provide hands-on application of information assurance skills; as such, they enhance students' understanding of both theory and practice. They provide students a laboratory in which to experiment, just as in other fields of science. They fulfill the same role as capstone projects in a traditional engineering program (i.e., projects that allow students to synthesize and integrate knowledge acquired through course work and other learning experiences into a project usually conducted in a workplace). The competition combines legal, ethical, forensics, and technical components while emphasizing a team approach. Such experiential education increases the knowledge and expertise of future professionals who may be in a position to contribute to the secure design and operation of critical information and its supporting infrastructure" (from Exploring a National Cyber Security Exercise for Colleges and Universities, Ron Dodge, Lance J. Hoffman, Daniel Ragsdale, and Tim Rosenberg, 2004).

Competition Objectives

- Build a meaningful mechanism by which institutions of higher education may evaluate their programs.
- Provide an educational venue in which students can apply the theory and skills they have learned in their course work.
- Foster a spirit of teamwork, ethical behavior, and effective communication both within and across teams.
- Open a dialog and awareness among participating institutions and students.

Competition Goals

1. To promote fair and equitable standards for cyber defense and technology-based competitions that can be recognized by industry.
2. To evaluate the defensive and responsive skills of each team under exact hardware, software application, and operating system configurations using a joint academic and industry rating scale.
3. To demonstrate the effectiveness of each participating institution’s academic security program.
4. To be executed by a preponderance of industry professionals.
5. To have industry recognition, participation, and acceptance of each competition.
6. To rate the effectiveness of each competition against a predefined standard of competition rules.
7. To provide a cooperative and competitive atmosphere among industry partners and academia in cyber defense education.
8. To provide recognition for participating teams.

9. To increase public awareness of academic and industry efforts in cyber defense education.

Qualifying Round Overview

Now in its 17th year, the MACCDC consists of both a qualifying and regional final engaging full-time undergraduate and graduate degree-seeking students, representing four-year universities and community colleges from Delaware, the District of Columbia, Maryland, New Jersey, North Carolina, Pennsylvania, Virginia, and West Virginia. Since its inception, over 3,500 students have participated in the MACCDC.

The MACCDC is presented by Raytheon Intelligence and Space and organized and run by the National CyberWatch Center, headquartered at Prince George's Community College.

The competition is designed to test each student team's ability to secure networked systems while maintaining standard business functionality. Each year's scenario involves team members simulating a group of employees from a fictitious company that will initiate administration of an IT infrastructure. The teams are expected to manage the systems, keep them operational, and prevent unauthorized access. Each team will start the competition with a set of identically configured systems. This is not just a technical competition, but also one built upon the foundation of business operations, policies, and procedures. A technical success that adversely impacts the business operation will result in a lower score as will a business success which results in security weaknesses.

Student teams are scored on their ability to detect and respond to outside threats, while maintaining availability of existing network and application services, responding to business requests, AKA *injects*, and balancing security against varying business needs. For more, see **Scoring** section below.

The following qualifying round teams will compete on February 5th from 11am-5pm EST (all teams will compete at the same time):

1. Bowie State University, MD
2. Capitol Technology University, MD
3. Community College of Baltimore County, MD
4. Christopher Newport University, VA
5. Drexel University, PA
6. East Carolina University, NC
7. George Mason University, VA
8. James Madison University, VA
9. Liberty University, VA
10. Marshall University, WV

11. Millersville University, PA
12. Northern Virginia Community College, VA
13. Old Dominion University, VA
14. Penn State University, PA
15. Rutgers University, NJ
16. Saint Vincent College, PA
17. Towson University, MD
18. University of Maryland Baltimore County (2 teams), MD
19. University of Maryland College Park, MD
20. University of Maryland, Global Campus, MD
21. University of Pittsburgh, PA
22. University of Virginia, VA
23. West Virginia University, WV

The top eight teams from the virtual qualifying round will advance to the MACCDC Regional Finals March 17-19.

Competition Team Identification

Throughout this document, the following terms are used:

- **Gold/Operations Team**: Competition officials that organize, run, and manage the competition. Responsibilities include, but are not limited to:
  - Administration and staffing of the event
  - Work with industry partners to orchestrate the event
  - Design, implement, and administer the competition infrastructure
  - Manage scoring elements and determine final standings
  - Has the authority to dismiss any team, team member, or visitor for violation of competition rules, inappropriate, and/or unprofessional conduct
  - Make provision for awards and recognition
  - Manage debrief to teams subsequent to the conclusion of the competition
  - **Main Point of Contact**: Casey W. O'Brien, MACCDC Regional Director, maccdc@nationalcyberwatch.org; Discord [Gold Team] Casey O'Brien
- **Black Team**: Competition support members that create the competition's infrastructure, provide technical support, and provide overall administrative support to the competition.
- **White Team**: Competition officials that observe team performance in their competition area and evaluate team performance and rule compliance. White team volunteers assess the competition team's ability to maintain their network and service availability based upon a business inject and a scoring instrument, delivering inject scenarios, scoring of injects, issuing or controlling the timing of injects, etc. White Team members

present in the competition room(s) will assist judges by observing teams, confirming proper inject completion, report issues, and assure compliance of rules and guidelines.

- **Blue Teams**: The institution competitive teams consisting of students competing in a CCDC event.
- **Team Captain**: A student member of the Blue Team identified as the primary liaison between the Blue Team and the Gold/White Teams.
- **Team Co-Captain**: A student member of the Blue Team identified as the secondary or backup liaison between the Blue Team and the Gold/White Team, should the Team Captain be unavailable (i.e., not in the competition room).
- **Team Representatives**: 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.
- **Red Team**: Penetration testing professionals simulating external hackers attempting to gain unauthorized access to competition teams' systems.

Communications During the Event

Discord is the main communications platform for the 2022 MACCDC Qualifying Round (excluding a few emails here and there). Invite link: https://discord.gg/zfnjAb8Gdh. Be sure to check out the #readme channel once logged in for naming conventions.

Competition Rules

Competition rules (http://nationalccdc.org/index.php/competition/competitors/rules) are applicable to all participants of the MACCDC. They provide structure for the makeup of student teams, permitted actions during competition play, guidelines for scoring, and contingencies for handling disputes. They also document expectations for appropriate conduct during the entire time participants are guests at a host site or are competing from their academic institution. Coaches, Remote Site Judges, and all student participants are expected to know and follow all CCDC rules and guidelines. Coaches and team captains are responsible for deploying the competition rules to the remaining members of their team. Host sites reserve the right to stipulate additional rules conforming to local policies and guidelines. Access to the competition stadium environment (both virtual and/or in-person) implies their acknowledgement of competition rules and their commitment to abide by them.

Rule Updates:

- 2.a. Each team must submit a roster of up to 12 competitors to the designated registration system. Rosters must be submitted by published deadlines and include a coach who is a staff or faculty member of the institution the team is representing. All competitors on the roster must meet all stated eligibility requirements. No changes to the team roster will be permitted after the team competes in their first CCDC event. The

competition team must be chosen from the submitted roster. A competition team is defined as the group of individuals competing in a CCDC event.

- *New*:
  - 5.f.iv. Team written tools, scripts, or executables that use resources outside of the competition environment other than simple DNS lookups are prohibited (i.e. tools that use cloud services or cloud processing outside of the competition environment are prohibited).
  - 5.f.v. Team written tools, scripts, or executables that transmit data outside of the competition environment (such as log data) must be declared to competition officials at least 30 days prior to their use in any CCDC event. Teams must obtain written authorization from competition officials prior to using these tools in any CCDC event. Approval or rejection of these tools is at the sole discretion of competition officials.

Scenario: Maritime

Over the past 17 years, the MACCDC has innovated, developed, and sought to create an original experience for not only the student teams, but all participants. Introducing scenarios that imitate life adds a dimension of realism and fun: healthcare IT, free and secure elections, natural disasters, mass transit, and banking, to name a few.

Student (Blue) teams will be working for the fictitious company, *Cyber Cargo*, a multinational maritime transportation organization bound by geographical constraints, political regulation, and commercial interests:

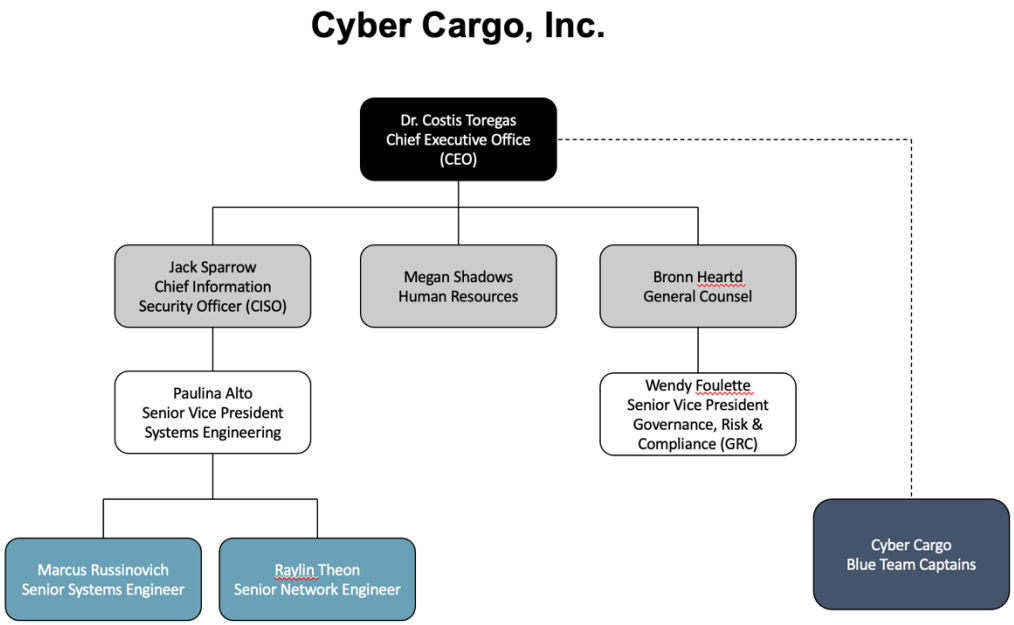

Fig. 1: Cyber Cargo Org Chart

Scoring

Scoring is based on keeping required services up, controlling/preventing unauthorized access, and completing business tasks (injects) that will be provided throughout the competition. Teams lose points by violating Service Level Agreements (SLAs), using recovery services, and successful penetrations by the Red Team.

Scores are maintained by the Gold/Operations Team, working in conjunction with the Black, Red, and White Team leads. Individual tracking of services may be available to respective teams during the competition. Blue Team members should use available service tracking reports and internal testing to assess the integrity of their networks and systems. Blue Team members should refrain from making direct requests to the Black or White Teams for routine service verification.

Scoring Metrics:

1. **Services**: All scored services must remain up and available, with a high degree of integrity. All services are given a predefined point value and will be checked periodically using Service Round Checks. The actual number of service rounds is not disclosed prior to or during the competition. For each service that passes the necessary check, the team will receive the appropriate number of points for that service. The more service points a team receives, the better.

2. **Injects**: Throughout the competition, Blue Teams will be presented with injects. An inject is any assigned task to be completed in the assigned amount of time. Inject types vary and point totals are based on the difficulty and time sensitivity of the task. Tasks may contain multiple parts. Sample injects include creating policy documents, making technical changes to a system, and attending meetings. Injects can be delivered through any number of methods, including electronically and orally. Injects will be scored by a White Team member. If the inject is completed on time and to the standard required, the Blue Team will receive the appropriate number of points. Unless indicated otherwise, the Team Captain may assign injects to specific team members for completion. Red Team activity can adversely affect a team's ability to complete injects. It is the Blue Teams' responsibility to maintain system availability. No extra time or point credit will be given for injects that are not completed because of inability to access a system. The more inject points a team receives, the better.
3. **Red Team Activity**: The activities performed by the Red Team have an impact on many of the scoring categories. It is imperative that Blue Teams work to prevent Red Team activities. The Red Team will have specific goals during the event (e.g., compromising a server, stealing data). All Red Team activities are meant to disrupt or misinform. At the conclusion of each competition day, the Red Team will rank order each team from best to worst.

4. **Service Level Agreements (SLAs)**: Each failed check of a service carries a 10%-point penalty of the service's maximum point value assessed on the next successful check of that service, up to a maximum of a 50% penalty. Each successful service check mitigates a single 10%-point penalty until 100% is restored. For example:
    a. Service A: 100 points (up), 0 points (down), 0 points (down), 80 points (up), 90 points (up), 0 points (down), 80 points (up), 0 points (down), 0 points (down), 0 points (down), 0 points (down), 0 points (down), 50 points (up), 60 points (up)
    b. Service B: 100 points (up), 100 points (up), 0 points (down), 0 points (down), 80 points (up), 90 points (up), 100 points (up), 100 points (up), 100 points (up), 100 points (up), 100 points (up), 0 points (down), 90 points (up), 0 points (down)
5. **Recovery Services**: In the event of system lock or failure, teams can request that a virtual machine (VM) be reset to a known good state (*revert to snapshot*). Teams are allowed one (1) free revert total for the entire event, per team. Each additional request for a VM snapshot revert will carry a 10% point penalty in the total service score for the event.

Calculating Scores:

- All Blue Teams start with zero points.
- Raw scores are used for the above scoring metrics, excluding the Red Team (which uses an ordinal scale, see next).

- Blue Teams are ranked using an *ordinal scale*, which is a measurement scale that assigns values to objects based on their ranking with respect to one another. For example, a first-place finish in the service scoring metric warrants an ordinal score of 1, a second-place finish warrants an ordinal score of 2, and on. This process is repeated for all the scoring metrics.
- The ordinal scores from all the scoring metrics are then totaled for each Blue Team, yielding a *combined ordinal score*, which is used to rank the Blue Teams from first through last place. The winning Blue Team will be determined based on the lowest combined ordinal score obtained during the competition time.
- In the event of a tie for first place, the team with the highest raw combined inject and service score breaks the tie.

Competition Topology

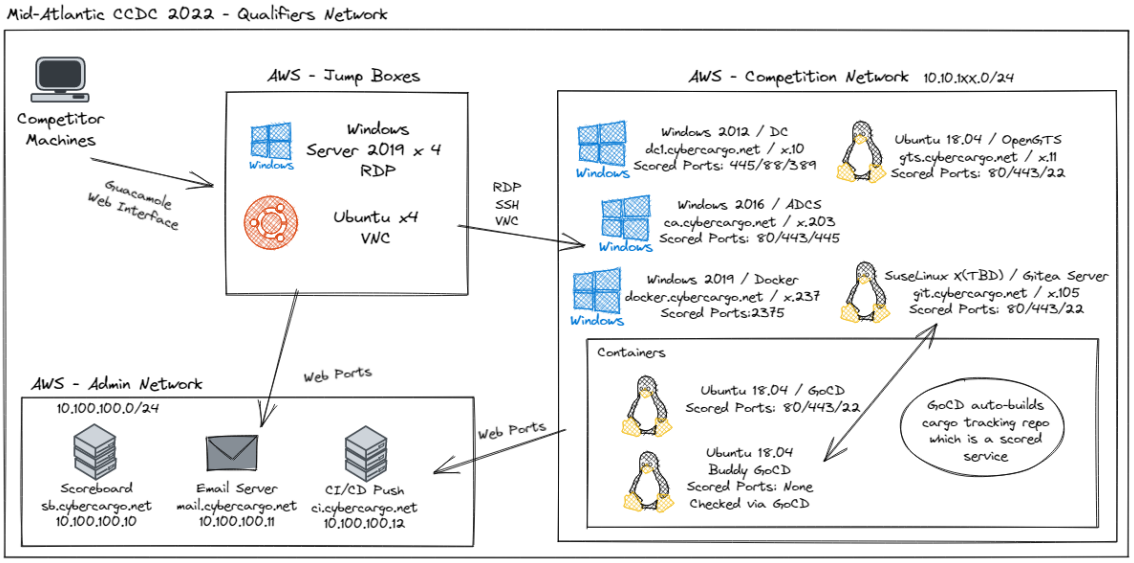

Fig. 2: Competition Network Topology

IP Range	OS	Functionality
TBD	Win Server 2019: 4 total	Remote Desktop Protocol (RDP)
	Ubuntu 20.04: 4 total	Virtual Network Computing (VNC)

Table 1: AWS Jump Box Table

AWS Admin Network: 10.100.100.0/24		
Hostname	**IP Address**	**Functionality**
sb	10.100.100.10	Scoreboard
mail	10.100.100.11	Email Server
ci	10.10.100.12	Continuous integration (CI)/Continuous Delivery (CD) System

Table 2: AWS Admin Network Table

AWS Competition Network: 10.10.1xx.0/24			
Hostname	**IP Address**	**OS/Functionality**	**Scored Ports (Subject to Change)**
dc1	10.10.1xx.10	Win Server 2012: Domain Controller (DC)	88, 389, 445
gts	10.10.1xx.11	Ubuntu 18.04: GPS Tracking System	22, 80, 443
git	10.10.1xx.105	SUSE Linux (version TBD): Gitea Server	22, 80, 443
ca	10.10.1xx.203	Win Server 2016: AD Certificate Services (ADCS)	80, 443, 445
docker	10.10.1xx.237	Win Server 2019: Docker	22, 80, 443, 2375

Table 3: AWS Competition Network Table

Functional Services

In addition to being up and accepting connections, the services must be functional and serve the intended business purpose. At random intervals, the following services (subject to change) will be tested for functionality and content where appropriate:

HTTP

Hypertext Transfer Protocol (HTTP). A request for a specific web page will be made. Once the request is made, the result will be stored in a file and compared to the expected result. The returned page must match the expected content for points to be awarded.

HTTPS
Hypertext Transfer Protocol Secure (HTTPS). A request for a page over SSL will be made. Again, the request will be made, the result stored in a file, and the result compared to the expected result. The returned page needs to match the expected file for points to be awarded.

RDP
Remote Desktop (RDP). A specified user will attempt to log in via RDP to the service. This will simulate an employee working from home. If a desktop appears, the check will be successful. Each successful test of RDP functionality will be awarded points.

SMB
Server Message Block (SMB). A specified user will attempt to connect to and read a designated file from the remote host. This file will then be hashed and compared against the expected value. This will simulate an employee accessing shares on the network. Each successful file read, and integrity test will be awarded points.

DNS
Domain Name System (DNS). DNS lookups will be performed against the DNS server. Each successfully served request will be awarded points.

MySQL
MySQL (Database). A connection to the database will be made with a specified user and a query will be run. The output of the query will be compared and each correctly answered query will be awarded points.

SSH
Secure Shell (SSH). A connection to the server will be made with a specified user, and commands will be executed as that user. The output of the commands and the ability to connect will be scored, with points awarded upon successful execution.

LDAP
Lightweight Directory Access Protocol (LDAP). An authenticated query to the Active Directory LDAP service will be performed. Each successfully performed query will be awarded points.

Kerberos

A user will need to connect and successfully authenticate using Kerberos authentication.

DOCKER
The docker service (which commonly runs on port 2375) refers to the Docker Daemon. A request will be made against this Remote API and the Docker Daemon is expected to respond with appropriate information about the state of the docker service on the host. An appropriate response will be awarded points.

Initial Connection

There are two (2) separate systems that are used to provide the services and scoring necessary to meet the goals of the MACCDC:

System 1, AWS Jump Boxes: This is how teams access the competition network. Teams will access an Apache Guacamole Web interface in their browsers, which lets them connect over both RDP for GUI access to Windows jump hosts, as well as VNC to the Linux jump hosts.

IP addresses, usernames, and passwords for the Jump Hosts/Guacamole portal will be provided prior to the competition for connectivity testing via the private Discord channels for each team.

System 2, Scoreboard. This will only be accessible (via a browser) internally to the competition network.

Usernames and passwords for the Scoreboard will be provided prior to the competition via the private Discord channels for each team.

Systems

1. Each team will start the competition with identically configured systems.
2. Teams may not add or remove any computer, printer, or networking device from the designated competition area (where applicable).
3. Teams should not assume any competition system is properly functioning or secure.
4. Throughout the competition, Gold and White Team members will occasionally need access to a team's systems for scoring, troubleshooting, etc. Teams must allow Gold and White Team member access when requested.
5. Network traffic generators may be used throughout the competition to generate traffic on each team's network. Traffic generators may generate typical user traffic as well as suspicious or potentially malicious traffic from random source IP addresses throughout the competition.

6. Teams must maintain specific services on the “public” IP addresses assigned to their team and stipulated in this document. Moving services from one public IP to another is not permitted unless directed to do so by an inject or the Gold/Operations team. Likewise, teams are not permitted to change the internal addressing or Virtual Local Area Networking (VLAN) scheme of the competition network unless directed to do so by an inject or the Gold/Operations team.
7. Teams may re-task servers, moving a service from one server to another as long as the outside "public" IP address of the service remains the same. It is the responsibility of the team to understand all the particulars of scoring a service when doing so.
8. Teams are not permitted to alter the system names or IP address of their assigned systems unless directed by an inject or the Gold/Operations team; this may affect the results of the scoring mechanism.
9. Systems designated as user workstations within the competition network(s) are to be treated as user workstations and may not be re-tasked for any other purpose by teams.
10. Teams may not modify the hardware configurations of workstations used to access the competition network (where appropriate).
11. Servers and networking equipment may be re-tasked or reconfigured as needed.
12. Red Team activity will be active throughout the event. At no time will the Red Team have access outside the Cyber Stadium perimeter.
13. Each Blue Team network will be monitored by a scoring system. An indication of services, as viewed by the indigenous scoring engine, may be made available to each Blue Team via the Scoreboard range.
14. While every effort is made to provide a stable and well-defined competition topology, it is subject to change and/or modification as decided by the MACCDC Regional Director and Gold/Operations team Lead.

Questions and Disputes

1. Team captains are encouraged to work with their site judge and White team staff to resolve any questions or disputes regarding the rules of the competition or scoring methods before the competition begins. Protests by any team will be presented by the Team Captain to the Regional Director as soon as possible. The Regional Director (in consultation with the Gold/Operations/White/Red teams) will be the final arbitrator for any protests or questions arising before, during, or after the competition and rulings by the competition officials are final.
2. 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. Disqualified individuals are also ineligible for individual awards or team trophies.

3. In the event of a team disqualification, the entire team must leave the competition area immediately upon notice of disqualification and is ineligible for any individual or team award.

Aftermath

Members of the MACCDC Gold, White, and Red Teams strive to make the MACCDC an enriching experience. All management and administrative teams are open to feedback and suggestions for improvement after the completion of the competition. This may include areas of concern or dissatisfaction.

Whether feedback is positive or negative, participants are forbidden from publishing, posting on the Internet, or publicly communicating details of the competition other than what is available at www.nationalccdc.org or maccdc.org.

Institutions that fail to adhere to this rule may be refused participation in future competitions. Institutions may publish, post on the Internet, or publicly communicate news stories of a general nature about the MACCDC, and may also enumerate participating teams and winners.

Errata

Date/Time:

- 01-22: 4:00pm EST:
  - Fixed misc. typos
- 01-27-22: 9:00am EST:
  - Fixed formatting issues
- 01-31-22:
  - 1:30pm EST:
    - Page 10: Renamed Fig. 3 and Fig. 4 to Table 1 and Table 2 respectively
    - Page 10: Updated Table 1 to reflect changing the two CentOS Jump Boxes to Ubuntu 20.04, due to stability issue
  - 3:48pm EST:
    - Page 2: Updated Table of Contents

        - Page 10: Added Table 2
        - Page 11: Renamed Table 2 > Table 3

- 02-03-22:
    - 5:17pm EST:
        - Page 2: updated Table of Contents
        - Page 12: Added DOCKER to Functional Services list