Mid-Atlantic Collegiate
Cyber Defense Competition

2023 Qualifying Round
Blue Team Packet

Last modified: 1/28/23, 6:30pm ET

Presented by

Raytheon
Intelligence & Space

Run by

MetaCTF

NATIONAL
CYBERWATCH
CENTER

Table of Contents

Overview

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.

Competition Teams

Throughout this document, the following terms will be used:

- **Gold/Operations Team**: Competition officials who organize, run, and manage the competition. Responsibilities include, but are not limited to:
    - Administer, staff, and orchestrate the event.
    - 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.
- **Black Team**: Competition support members who design and implement the competition infrastructure, provide technical support, and provide overall administrative support to the competition.
- **White Team**: Competition officials who evaluate team performance, ensure rule compliance, deliver and score injects, and volunteer in various other positions during the competition.
- **Blue Teams**: The student teams 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 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.

MACCDC Overview

The MACCDC is one of the 9 regional CCDC events in the United States. Now in its 18th year, our region represents 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.

MACCDC consists of both a qualifying round and a regional final round. The 2023 virtual qualifying round will be held on February 4th. The top 8 teams will advance to the in-person regional competition held at the Price George’s Community College in Largo, MD on March 31st - April 1st.

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 who must “inherit-and-defend” 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, also known as injects, and balancing security against varying business needs. For more details, see the Scoring section below.

Virtual Qualifying Round

Communications

Excluding a few emails here and there, *Discord (https://discord.gg/mtpS3en4zT) will be the main communications platform for the 2023 Qualifying Round*. Be sure to check out the #readme channel once logged in for naming conventions.

For questions during the competition, the team captain or coach can open a ticket in Discord. Please follow the instructions in the #readme channel.

Primary Gold/Operations Team point of contact:
Discord: [Gold Team] Roman Bohuk
Email: roman@metactf.com

Primary Black Team point of contact:
Discord: [Black Team] Rob Fuller

Schedule

Friday, February 3rd, 2023

7:00pm Qualifying round overview session, Q&A, and access troubleshooting

Zoom Link:
https://us02web.zoom.us/j/81347206779?pwd=Zk04NWhhcGxPTlRSR3ZKcys2ZWNUQT09

Meeting ID: 813 4720 6779
Passcode: 189521
Phone: +1 (646) 931-3860

Saturday, February 4th, 2023

11:00am Qualifying round start
5:00pm Qualifying round end
7:30pm Winner Announcements & Debrief

Zoom Link:
https://us02web.zoom.us/j/88656565244?pwd=NmwzN1NVNnBhOHR2eWxkK2JuaUo1QT09

Meeting ID: 886 5656 5244
Passcode: 341251
Phone: +1 (646) 931-3860

Teams

Teams from the following schools will compete in the 2023 qualifying round. *The list will be published after MACCDC registration deadline.*

1. -
2. -
3. -
4. -
5. -
6. -
7. -
8. -
9. -
10. -

CCDC Rules

Mid-Atlantic CCDC follows the competition rules established by the National CCDC (http://nationalccdc.org/index.php/competition/competitors/rules). They provide structure for the makeup of student teams, permitted actions during competition play, 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.

Qualifiers 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.

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.
    a. **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:
        i. Service A: 100 points (up), 0 points (down), 0 points (down), 80 points (up), 90 points (up), 0 points (down), 0 points (down), 0 points (down), 0 points (down), 0 points (down), 50 points (up), 60 points (up)

ii. 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), 0 points (down), 90 points (up)

It is possible that there will be no SLA penalties during the qualifying round. Please stay tuned for updates.

b. **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.

c. **Black Team Agent (BTA).** Every host on the competition network will be running a special Black Team Agent service that will be used to help score machine uptime, service uptime, and red team activity.

i. The BTA needs to be able to reach the scoring server via HTTPS (port 443) at the IP address 10.250.250.11. BTA check-ins will be reported on the scoreboard.

ii. If the BTA is disabled or blocked from reaching the scoring server, severe point penalties will be applied.

iii. The BTA will be running as the root or Administrator user and installed as an auto-start service named `bta` on all platforms.

iv. The Red Team has been instructed not to inject into or tamper with the BTA in any way.

v. Any attempt by Blue Teams to tamper with, impersonate, or hinder communication of the BTA will result in heavy point penalties or disqualification.

vi. The BTA may perform additional checks on local network services such as SMB, HTTP, LDAP, and SSH. These additional checks will be made locally only (i.e. to localhost), so no additional ports need to be opened for the BTA for it to function properly. Any questions about the BTA should be asked before the competition starts.

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.

a. Sample injects include creating policy documents, making technical changes to a system, and attending meetings.

b. Injects can be announced through any number of methods, including electronically and orally. Inject submission instructions are covered later in this document.

c. 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. Different injects may have different point values.

   d. No points will be awarded for the inject if the inject is submitted late.
   e. Unless indicated otherwise, the Team Captain may assign injects to specific team members for completion.
   f. Red Team (or Blue 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.

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 each team from best to worst.

Calculating Scores

- Raw scores are used for the above scoring metrics, excluding the Red Team.
- Blue Teams will be assigned a rank for each scoring metric using standard competition ranking, 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. Same raw scores will have the same rank. For example, four teams with scores of 2000, 1750, 1750, and 1500, will be ranked 1, 2, 2, and 4 respectively. This process will be repeated for all the scoring metrics, excluding the Red Team.
- 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, the team with the higher raw inject score will place better. If there's still a tie, the raw service score and then the Red Team ranking will be used as secondary and tertiary tie breakers respectively.

Scenario & Infrastructure

Hulk Bulk Shipping

Hulk Bulk Shipping is a leading online retail and distribution company. Operating globally, the company offers a wide range of products and services to customers around the world from many third-party sellers.

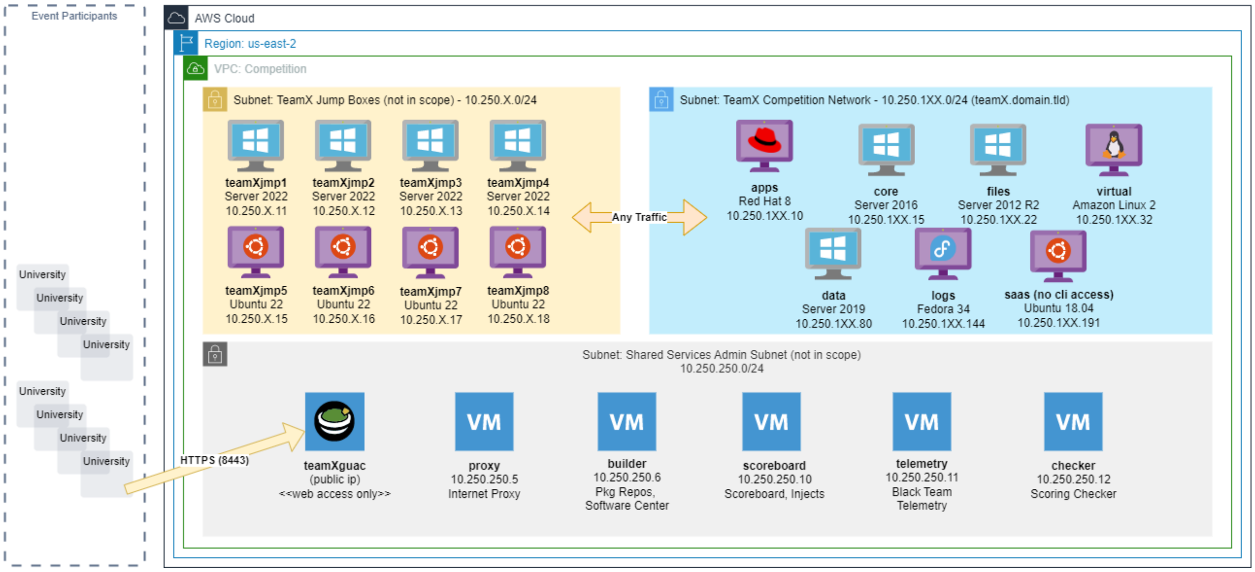
In addition to its e-commerce operations, "Hulk Bulk Shipping" also boasts an efficient and reliable delivery service. With a network of warehouses and fulfillment centers around the world, the company is able to get purchases to customers quickly and efficiently, no matter where they are located.

Due to a recent breach, the company underwent a major restructuring of its IT department, and a new IT team was brought in to replace the former team.

The new IT team is tasked with securing and defending the company's network while also ensuring that business operations can continue smoothly.

Competition Topology

Each team will be responsible for managing and protecting the 7 in-scope virtual machines in their network. They are listed in the “TeamX Competition Network” in the diagram below.



Scored Services

The in-scope virtual machines may contain one or more scored services that will be periodically checked by the scoring service. 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:

The list of services will be provided after the registration deadline to all teams at the same time.

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.

Qualifiers Logistics, Clarifications, and Additional Rules

1. For the qualifying round, teams are not allowed to configure firewall rules on any of the systems that block any inbound or outbound IP addresses or ranges. This includes the team's local network.
2. Some competition machines may contain sensitive data or PII belonging to the fictitious company or its customers. This data may be necessary to complete service checks or injects and a leak of this data by the Red Team may also negatively impact the team's Red Team Activity rank. Teams are not forbidden from moving this data to other in-scope devices, but it may impact their ability to pass some service checks or complete some injects.
3. Please refer to the Scoring section above for more information about the new Black Team Agent. Neither the Blue nor the Red Teams are allowed to tamper with this service in any way.
4. Internet access from within the virtual machines will be limited during qualifiers. Participants will likely be able to download updates from the standard package repositories on their Linux systems, but other downloads will be restricted. Please submit requests for any tools, software, GitHub repositories, etc. that you might want to use during the competition here as issues: https://github.com/init6security/DownloadRequestList/issues. Explain why you want to use the tool and make sure it hasn't already been submitted by another team. Please limit the number of requests to under 15 per team. You may submit more requests, but we might not check them. Please refer to section 5.f. in the National CCDC rulebook for clarifications about requirements for tools written by team members. Requested and approved resources will be available for download from the competition network for all teams. There is no guarantee that your request will be approved.
5. You are allowed to restart your virtual machines as many times as you want with no point penalties (except points lost by your critical services being down while the machine is rebooting). Refer to the Scoring section for penalties if you need to completely reset a VM to its original state.
6. You are not allowed to transfer files from outside the competition network (i.e. from your personal laptops, servers) into the competition virtual machines and vice versa.
7. If you participated in previous MACCDC competitions, you may be familiar with incident response reports. These will not be collected or scored during the Qualifying Round.

Systems

1. Each team will start the competition with identically configured systems.
2. Teams should not assume any competition system is properly functioning or secure.
3. 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.

4. Network traffic generators may be used by competition organizers 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.
5. 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.
6. The competition topology is subject to change.

Questions and Disputes

1. Team captains are encouraged to work with their remote 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

- 1/28/23 6:30pm – Fix qualifier date from Feb 5th to Feb 4th and Zoom session from Feb 4th to Feb 3rd in the “Schedule” section