MA-3CS

MACCDC 2023

E-COMMERCE & DISTRIBUTION

PRESENTED BY: Raytheon Technologies

RUN BY: MetaCTF

NATIONAL CYBERWATCH CENTER

03-31-23 – 04-01-23 19TH ANNUAL

2023 REGIONAL FINAL TEAMS

CAPITOL
Technology University

GEORGE MASON
UNIVERSITY

LIBERTY
UNIVERSITY

PennState

RUTGERS
THE STATE UNIVERSITY
OF NEW JERSEY

UMBC

UNIVERSITY of VIRGINIA

VIRGINIA TECH

SCHEDULE

Friday, March 31st

7:30am - 8:20am	Blue Team Check-In
8:30am - 8:50am	Morning Briefing (Proscenium)
9:00am - 5:00pm	Competition Day 1 (Black Box Theater)
11:00am - 1:00pm	C-level Meetings
1:00pm - 2:00pm	Lunch Break, Competition Paused
5:15pm - 6:00pm	Day 1 Debrief (Black Box Theater)
6:00pm – 6:30pm	Sponsor Introductions (Black Box Theater)
6:30pm - 9:30pm	Career Fair and Networking Event (Atrium and Conference Rooms)

Saturday, April 1st

8:30am - 8:50am	Morning Briefing (Proscenium)
9:00am - 4:00pm	Competition Day 2 (Black Box Theater)
11:00am - 1:00pm	C-level Meetings
1:00pm - 2:00pm	Lunch Break, Competition Paused
4:00pm – 5:00pm	Competition Breakdown
5:30pm - 6:30pm	Competition Debrief and Awards (Proscenium)

WELCOME

The Mid-Atlantic Collegiate Cyber Defense Competition is an annual event in which teams of college students compete against each other to defend computer networks from simulated attacks. The competition is designed to simulate real-world cybersecurity situations and test the skills of the students in a high-pressure, time-constrained environment.

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.

This competition consists of both a qualifying round and a regional final round. The virtual qualifying round took place on February 4th, and the top 8 teams from 26 participating universities advanced to the in-person regional competition at Prince George's Community College on March 31st - April 1st. The winner of the regional competition will advance to the national round.

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 starts 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.

This competition would not have been possible without the help of our sponsors and dedicated volunteers. We extend our sincere gratitude to those who have contributed to the success of this event over the years. Please take a moment to acknowledge the individuals who have worked tirelessly to prepare for this event.

2023 PARTICIPATING TEAMS

1. Bowie State University, Maryland
2. Capitol Technology University, Maryland *
3. Christopher Newport University (Team #1), Virginia
4. Christopher Newport University (Team #2), Virginia
5. College of Southern Maryland, Maryland
6. Community College of Baltimore County, Maryland
7. East Carolina University, North Carolina
8. George Mason University, Virginia *
9. James Madison University, Virginia
10. Liberty University, Virginia *
11. Marshall University, West Virginia
12. Messiah University, Pennsylvania
13. Millersville University, Pennsylvania
14. Northern Virginia Community College, Virginia
15. Old Dominion University, Virginia **
16. Pennsylvania State University, Pennsylvania *
17. Regent University, Virginia
18. Rowan College At Burlington County, New Jersey
19. Rutgers University, New Jersey *
20. Saint Vincent College, Pennsylvania
21. Towson University, Maryland
22. University of Maryland, Baltimore County (Team #1), Maryland *
23. University of Maryland, Baltimore County (Team #2), Maryland
24. University of Maryland, College Park, Maryland
25. University of Maryland, Global Campus, Maryland
26. University of Virginia (Team #1), Virginia *
27. University of Virginia (Team #2), Virginia
28. Virginia Tech, Virginia *
29. West Virginia University, West Virginia

* Team advanced to regional final round at Prince George's Community College.
** Team qualified to advance to the regional final round but could not attend the 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).

TERMINOLOGY

Gold Team: competition officials who orchestrate, run, and staff the event.

Black Team: competition officials who design and implement the competition infrastructure and provide overall technical and 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 roles during the competition.

Red Team: penetration testing professionals simulating external hackers attempting to gain unauthorized access to competition teams’ systems.

Orange Team: competition officials who serve as the end users of Blue Team systems and evaluate availability of services.

Blue Teams: the student teams competing in a CCDC event. Each team includes a Team Captain, who is the primary liaison between the Blue Team and the Gold/White Teams.

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.

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 server, and attending meetings. Injects will be scored by members of the White Team. If the inject is completed on time and to the standard required, the team will receive the appropriate number of points. Red Team activity can adversely affect a team's ability to complete injects. 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 and are not directly scored. At the conclusion of each competition day, the Red Team will rank each team from best to worst.

4. **C-level Meetings and CEO Reporting:** Each Team Captain will meet face-to-face with the executives of Hulk Bulk Shipping. During the initial meeting, the management will expect to be briefed on the status of the organization's information systems, the number of users impacted by downed systems, as well as other items the Team Captain will consider relevant for the CEO to know. At this initial meeting, each Team Captain will be given action items to complete within a fixed time. Items may include a written status report, a high-level remediation plan, a resource inventory, a request for prioritized additional resources subject to budget constraints, and other similar management considerations. Teams will be scored on oral presentation skills, writing skills, clarity of communicating the situation to a less-technical audience, and creativity in reacting to new information.

5. **Incident Response:** All Blue Teams must submit Incident Response reports to document and communicate the details of security incidents caused by the Red Team during the competition. The reports will be scored on timeliness, incident description, analysis & technical details, mitigation steps taken, and grammar & clarity.

6. **Orange Team:** The Orange Team represents the end-users and employees of Hulk Bulk Shipping. They will test services for functionality and data integrity every hour. The Orange Team will attempt to use the company services and communicate with the blue teams if they run into issues. The more orange team check points a team receives, the better.

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.

- 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 higher. 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.

Mid-Atlantic Collegiate
Cyber Defense Competition

ABOUT THE ORGANIZERS

METACTF

MetaCTF is a startup that focuses on hands-on, engaging, and practical cybersecurity training. It specializes in hosting and managing gamified security training such as CTF and Red vs. Blue events. MetaCTF helps organizations of all sizes, from Fortune 50 to higher education and nonprofits, to engage and educate employees on cybersecurity best practices, upskill their existing workforce, find new talent, and enhance their organizational cyber resilience.

https://metactf.com/

NATIONAL CYBERWATCH CENTER

Headquartered at Prince George's Community College, Maryland, the National CyberWatch Center is a consortium of higher education institutions, businesses, and government agencies focused on collaborative efforts to advance Information Security education and strengthen the national cybersecurity workforce.

https://www.nationalcyberwatch.org

SPONSORS & SUPPORTERS

Raytheon Technologies

NATIONAL CYBERWATCH CENTER

MetaCTF

NATIONAL SECURITY AGENCY
UNITED STATES OF AMERICA

UNITED

paloalto® NETWORKS

BATTELLE

SEALINGTECH®

CROWDSTRIKE

cisco
25 Years
Networking Academy

FORTRA

GDIT

Richweb

E-COMMERCE & DISTRIBUTION

MACCDC 2023

MACCDC