PRESENTS THE

NORTHEAST COLLEGIATE CYBER DEFENSE COMPETITION

IN PARTNERSHIP WITH

HOSTED BY

NECCDC 2023 SEASON QUALIFIER
BLUE TEAM PACKET
v.1 | Revised 2023-01-13

CONTENTS

NORTHEAST COLLEGIATE CYBER DEFENSE LEAGUE

The Northeast Collegiate Cyber Defense League (NECCDL) is an administrative body whose sole purpose is to facilitate the smooth running of NECCDC regardless of hosting institution. The League is operated by academic volunteers and is funded by league sponsors and annual membership fees collected from participating Academic Institutions.

Find out more at: neccdl.org
Follow on Twitter: @neccdl
GitHub: github.com/NE-Collegiate-Cyber-Defense-League

We would like to thank UMass Lowell for hosting the qualification infrastructure for this season!

NECCDC 2023 SEASON

The Northeast Collegiate Cyber Defense Competition (NECCDC) is designed to provide a controlled competitive environment that will permit each participating institution to assess their students' depth of understanding and operational competency in managing the challenges inherent in protecting enterprise network infrastructure and business information systems. NECCDC provides an opportunity for qualified educational institutions in the Northeast to compete in this environment and is part of a national organization (see www.nationalccdc.org), which provides a unified approach for nine regions across the country. Qualified educational institutions include those with information assurance or computer security curricula.

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 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 (and related) programs
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 the area of cyber defense education
8. To provide recognition for participating teams
9. To increase public awareness of academic and industry efforts in the area of cyber defense education
10. To facilitate the pipeline for the next-generation cybersecurity workforce
11. Develop competitor skills to respond to modern cybersecurity threats

QUALIFIER OVERVIEW

The NECCDC 2023 Qualifier is managed by this year's regional competition host (UMass Lowell), with strong contributions from the wider team at NECCDL. The competition is designed to test each competing team's ability to secure a networked computer system while maintaining standard business functionality. The scenario is a medium-sized Software-as-a-Service (SaaS) company that is migrating to cloud infrastructure. The organization has a small number of clients with a specific set of services. If its new cloud launch goes well, it could expand its services in the future!

The competition involves more than the application of technical skills. It is also one built upon the foundation of business operations, policy, and procedures. A technical success that adversely impacts business operations will result in a lower score, as will a business success that results in security weaknesses.

Qualifying teams from the NECCDC 2023 Qualifier in January will have the opportunity to participate in the NECCDC 2023 Regional, expected to take place March 10 - 12, 2023 at UMass Lowell - the host organization for 2023.

NECCDC 2023 SEASON SPONSORS

NECCDC would not be possible without the generous support of our sponsors!

Additional information regarding sponsorships for the NECCDC 2023 Season can be found at https://neccdl.org/neccdc/2023/howtosponsor/ and https://neccdl.org/neccdc/2023/sponsors/

VIBRANIUM
Raytheon Intelligence & Space

SILVER
Networking Academy
paloalto NETWORKS Cybersecurity Academy
RSM

NECCDC 2023 SEASON SPONSORS, CONT'D.

BRONZE	
FORTRA	BATTELLE It can be done
NuHarbor SECURITY	

SUPPORTERS
no starch press
With extra support from Jason E

OTHERS? HELP CONNECT US WITH POTENTIAL SPONSORS!
Others TBD, in contracting. **Let us know if you have someone you know who is interested in sponsoring!** **Have them contact sponsor@neccdl.org for more information.**

QUALIFIER EVENT SCHEDULES

- Please be in Discord and On-Site ~20 minutes prior to Check-in
- Have Webcam/video capacity + Student ID for authentication
- Have fresh Public IPs for team members (most search engines will display it via “what is my ip”)
- Work with your Team’s Moderator(s) - if your coach hasn’t already, make sure they submit moderator contact information for training and coordination. The original deadline is Jan 14, 2023.

COMPETITION (Game Points) == SATURDAY, 28 JANUARY, 2023

TIME (EST, 24-Hour format)	ACTIVITY	NOTES
09:00	Blue Team Check-in Begins in Discord	Have student ID accessible
09:30	Welcome Inject	Injects in Google Classroom
10:00	Competition Begins	Scoring starts and Blue Team access to environment systems enabled. Credentials are shared in Discord team channels.
14:30	Competition Ends	Blue Team access to environment systems will be disabled.

COMPETITION ORGANIZATION

Blue Team

Student team representing a specific academic institution or major campus competing in the NECCDC. Each team must submit a roster of up to 12 competitors to National CCDC via: https://www.nationalccdc.org/index.php/competition/competitors/registration (due by Jan 20, 2023). Each competition team may consist of up to eight (8) members chosen from the submitted roster. The remainder of the roster is for substitution in the event a member of the active competition team cannot compete. Substitution in the competition team requires approval from the Competition Director.

- Students should maintain a full-time status (as defined by the participating institution) at the time the competition is conducted. Coaches are responsible for ensuring that participating students have the status needed to participate, and recommend two (2) or more moderators. See National CCDC rules for full eligibility criteria.

- Technical access issues and the like should be **@BlackTeam** in Discord in your specific Team channel for infrastructure-related questions. If competitors are unsure about other questions, then they should ask their room moderators.

Red Team

Professional network penetration testers from the industry, approved by the Competition Director, and industry representatives who:

- Scan and map the network of each competition team - Attempt to penetrate the defensive capabilities of each Blue Team network
- Modify any acquired environment
- Assess the security of Blue Team networks
- Attempt to capture and/or modify specific files on targeted devices of Blue Team networks
- Attempt to leave specific files on targeted devices of each Blue Team network
- Document and provide feedback for competitors/organizers to evaluate performance
- Follow Rules of Engagement for the competition

White Team

Representatives who serve as competition officials, moderators and rule enforcement in the various competition rooms.

- Each team competing remotely from their home institutions must have at least one (1), ideally two (2) or more, site moderator(s) present at the blue team location as well as within the virtual environment during active times of the competition provided by the Team Representative.
- Moderators are responsible to perform tasks such as:
    - Undertake/Review moderator training offered by NECCDC
    - Gain familiarity on using the required communication tools (e.g. Discord)
    - Submit questions/requests from the blue team members to the designated communication #channels
    - Check rosters to authenticate competitors at check-in
    - Ensure that competition rules are followed and any violations or situations of concern are reported to the White Team senior staff
    - Submit survey feedback based on competition/team observations near the end of Qualifier (e.g., webform provided in Discord)
- White Team senior staff will:
    - Supply and score Blue Team tasks in the form of competition injects
    - Adjudicate the scoring for the competition
    - Have a chief judge responsible for final decisions with regard to scoring

Black Team

Competition technical support, the Black Team deploys and maintains the physical and virtual competition environments, as well as the service scoring engine and possible related SLA violations.

Gold Team

The competition staff includes the Director, logistics, and sponsor relations coordinators.

Orange Team

The competition staff builds an integrated scenario storyline and simulates user activities in a manner that integrates with and contextualizes Black and White team activities. The Orange Team is also responsible for the corporate branding and image of the contest. The team also may include individuals who act as employees, clients, and other external acting parties, e.g., C-suite personnel, law enforcement agents, etc. These actors may interact with infrastructure systems and the Blue Team members during the competition experience.

COMPETITION RULES

NECCDC subscribes to the National CCDC Rules, which have been continuously updated in recent years. In particular, Article 7 on Professional Conduct which applies to competitors and non-competitors alike. Not only is this expected in today's workforce, we truly strive to create a fun and safe professional + technical learning environment every year.

The Director will update a list of published Blue Team GitHub links for Qualifier. Besides these approved repositories, teams are not allowed to use any other privately team-developed staging materials.

IP Allowlisting

Prior to the competition, each competitor registered their IP address for allowlisting access to the remote access solution within the competition environment. Remote access will be achieved through a VPN connection. Tools such as RDP and/or SSH may be used by competitors to manage their hosts.

Competitor Authentication

Competitors will be expected to show a valid/current student ID, issued by their educational institution to authenticate during the qualifier check-in as well as public IPv4 address verification. Authentication will be done by room moderators on-site.

Blue team members should ask for rule clarifications through their room moderators at any time. Scenario-based activities can take a wide variety of paths, so if there is any doubt or need for clarification on injects or other competition-related events, make sure to check with room moderators who can relay questions to appropriate competition staff.

Questions and Answers

We maintain a set of updated Questions and Answers, publicly available here: FAQ.

SCORING OVERVIEW

Blue Teams gain points throughout the competition in two (2) categories using the following point distribution:

50%	System Scoring

50%	Inject Scoring

Both service uptime and completion of injects are equally important. As with any business, systems often have different risks and criticality. Additionally, any disabling/disconnection of network services is considered unauthorized and thus, depending on severity and service criticality, might incur appropriate SLA violations. The more points Blue Teams can gain, the better.

Additionally, successful Red Team Activity will subtract up to 50% of points from a team's possible total points:

- 50%	Red Team Activity

The more points Blue Teams can prevent the Red Team from taking away, the better.

Accurate and high-quality Incident Reports will reduce the number of points reduced as a result of Red Team activity.

System Scoring

System availability and integrity make up half of the Blue Team's final score. This scoring consists of service checks that happen on a predetermined interval. Each successful check will increase point totals (depending on service criticality). Unsuccessful checks will not add or decrease point totals.

Inject Scoring

Injects are business tasks provided to each team throughout the competition and make up half of the Blue Team's final score. Injects are typically provided to teams in the form of communication from a supervisor/stakeholder, a project work order, or a break/fix ticket. Injects may not always explicitly outline specific deliverables expected. It is the responsibility of the Blue Team to interpret the request and respond professionally. Questions can be asked for clarification via moderators or directly to White Team or Black Team. Some injects may be scored objectively, while other injects may be scored on a ranked scoring model. Injects may not all have the same point value, and are weighted based on items such as complexity and time required to complete. The specific point value for each inject is not disclosed to the Blue Team. Injects have their own deadlines, and injects submitted past deadlines do not earn points. Keep in mind that the Google Classroom clock may be different from your system time and can experience lag when submitting.

Red Team Activity

Successful Red Team activity is subtracted from Blue Team total points. Red Team Activity has a ceiling and may not take away more than half of the total possible points from the combined service and inject scores. Accurate, evidence-based, and professional Incident Reports submitted by the Blue Team may provide the opportunity to reclaim Red Team points for specific

Red Team activity. However, very low-quality Incident Reports may result in additional points awarded towards Red Team Activity and Blue Teams should only submit Incident Reports they have confidence in (detailed in National's Rule 9.d). A standardized Incident Report document is provided below and teams are encouraged to utilize the document to submit Incident Reports.

Incident Response Template

Please feel free to use this Incident Response Template, or use a similar professional IR report which captures data referenced in National Rules 9.d.

Tips for Effective IR Reports

- Submit IR reports when incidents occur in order to potentially reduce future Red Team impacts
- Ensure any executive summaries and business impact analyses are appropriately written for the intended audience (try not to include too much technical jargon)
- When writing, ensure that it is professional and includes enough necessary information and depth while not including any extraneous information
- When discussing business impact, ensure that you accurately identify the effects on the business
- Attempt to accurately determine the root cause
- Once an incident has occurred, you want to perform remediation. Any actions taken towards remediation/prevention should be detailed.
- Make sure that you include relevant screenshots, visuals & evidence
- Think about whether what you are experiencing is really due to Red Team activity or due to a misconfiguration/actions taken by the team

NECCDC 2023 SEASON THEME

The theme of NECCDC 2023 is “Resilient Cloud Infrastructures”. Modern cloud providers, containerization, and orchestration technologies have enabled organizations to massively scale their infrastructures. At the same time, the presence of availability zones has enabled organizations to guarantee high availability (> 99.99%) of critical services.

These massively scalable, highly available, and public infrastructures present unique security challenges that require innovative security solutions. This year’s qualifier and regional competition will focus on the multitude of techniques that ensure enterprise network uptime, security, and flexibility—even when operating at a massive scale.

Blue Teams will need to maintain, secure, and scale highly available services while also juggling compliance with service-level agreements.

Core Focus -

- Resiliency
- High Availability
- Distributed File Systems
- Vulnerability management
- CI/CD pipelines
- Endpoint security

NECCDC 2023 SEASON SCENARIO

This year's qualifier and regional competition will focus on the multitude of techniques that ensure enterprise network uptime, security, and flexibility – when operating at a massive scale. These ideas will be critical to the success of the organization Blue Teams will be supporting, Prometheus Group. The company is scaling its business to have greater reach and flexibility for existing and future customers. These goals will only materialize if all of these ideas can come together and be operationalized well.

Blue Teams will need to maintain, secure, and scale highly available services while also juggling compliance with service level agreements. Teams will be expected to follow modern best practices such as CI/CD; modern technologies such as Docker containers; and orchestration frameworks such as Docker Swarm to create robust, secure, and dedicated services for Prometheus' clients.

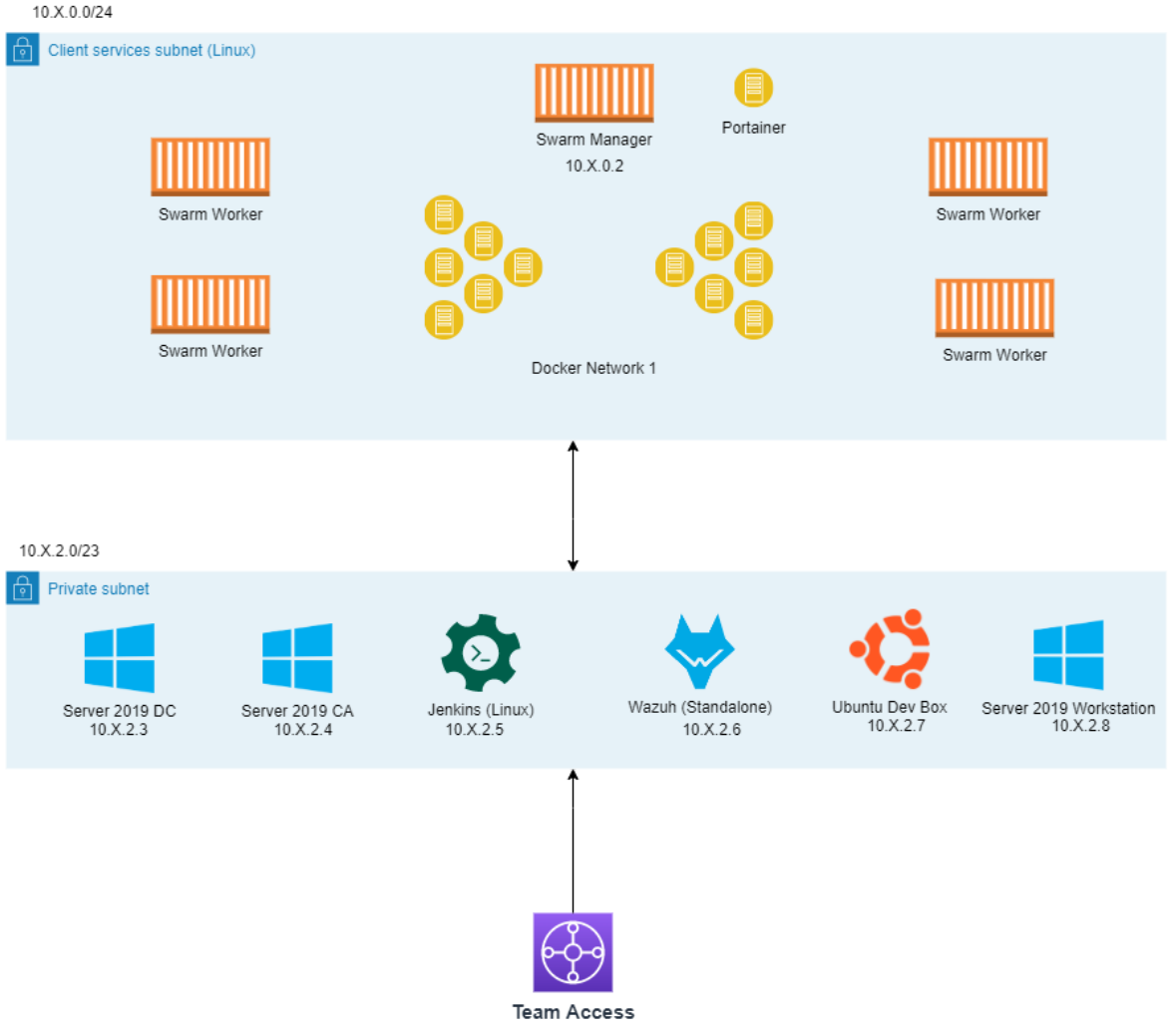
QUALIFIER INFRASTRUCTURE

Employees of Prometheus Group should be prepared to assess the various aspects of the organization's infrastructure. Technologies that may be found in the company's infrastructure include*:

Windows Server 2019	Docker	Container Networking
Microsoft Active Directory	Docker Swarm	HAProxy
Microsoft IIS	Ubuntu	Harbor
WMI, SSH, and RDP	RHEL	MySQL
Certificate Authorities	Wazuh	MariaDB
Kerberos	Podman	MongoDB
Windows based DNS	Jenkins	Nginx
Alpine Linux	Git	NextCloud
Amazon Linux 2	Ansible	RocketChat

* The focus will be on containerized versions of applications.

Remote Access will be provided by Black Team to allow teams to connect to the Qualifier environment from their personal/campus computers on-site at the host institution. **It is critical that teams use the beta period to test and validate this remote access solution.** Additional details on testing/setup instructions will be provided by competition staff as we get closer to the date of the Qualifier.**See Appendix I for a larger version of the Qualifier Infrastructure Diagram (below) on Page 17.**



LETTER FROM MANAGEMENT

From: Dade Murphy
To: DevSecOps Team
Subject: Team Reorganization

Team:

The company's growth is on an upward trajectory and we're all excited about the new product launch where we're offering a bespoke private collection of collaborative/productivity tools for customers! We've seen companies getting hit left and right with security incidents, so we want to make sure that we're putting our best foot forward for this launch. We wouldn't want to have any negative press during this critical time period for the company.

As you know, we are migrating to cloud infrastructure and exploring the use of containerization for efficiency/effectiveness. Through this endeavor, we're hoping to expand our limited set of services as well as attract more clients. We expect to be able to onboard a new customer this month and need to make sure their launch also goes smoothly. If this goes well, we can apply the lessons learned to the next customer in the queue.

Thanks so much for being a part of our team and we look forward to you growing together with us as we take this new step toward our future as an organization.

Kind Regards,

Dade Murphy, CIO
Prometheus Group

APPENDIX I: Larger Version of Qualifier Infrastructure Diagram