

NORTHEAST COLLEGIATE CYBER DEFENSE COMPETITION



IN PARTNERSHIP WITH

RIT | **Rochester Institute
of Technology**

**NECCDC 2021 SEASON QUALIFIER
BLUE TEAM PACKET**

v1.0 | Revised 2021-01-08

CONTENTS

NORTHEAST COLLEGIATE CYBER DEFENSE LEAGUE	3
NECCDC 2021 SEASON	4
COMPETITION GOALS	4
QUALIFIER OVERVIEW	5
NECCDC 2021 SEASON SPONSORS	6
QUALIFIER EVENT SCHEDULE	7
SATURDAY, 23 JANUARY, 2021	7
COMPETITION ORGANIZATION	8
COMPETITION RULES	9
NCCDC RULE 5.f. Scripts, executables, tools, and programs written by active team members may be used in CCDC events	9
This will be allowed, provided:	9
IP Whitelisting	10
Competitor Authentication	10
SCORING OVERVIEW	11
NECCDC 2021 SEASON THEME	13
NECCDC 2021 SEASON SCENARIO	14
LETTER FROM MANAGEMENT	15
QUALIFIER INFRASTRUCTURE	16

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 volunteers and is funded by league sponsors and annual membership fees collected from participating Academic Institutions.

Find out more at: neccd.org

Follow on Twitter: @neccd

GitHub: github.com/NE-Collegiate-Cyber-Defense-League

NECCDC 2021 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 an 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 2021 Qualifier is managed by this year's regional competition host (Rochester Institute of Technology), 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 involves members of a news organizations' internal security team working to administer and secure both the data and systems of a regional office in the face of challenges posed by COVID-19. Competing teams are expected to manage the computer network, keep it operational, and prevent unauthorized access. Each team will be expected to maintain and provide public and internal services. Each team will start the competition with a set of identically configured systems.

The competition involves more than the application of technical skills. There are 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 NECCDC 2021 Qualifier in January (as well as the host institution's team) will have the opportunity to participate in the 2021 Northeast Regional CCDC, taking place March 19th through 21st, 2021 in virtual format through the Cyber Range and Training Center, part of the Global Cybersecurity Institute (GCI) within Rochester Institute of Technology (RIT) - the host organization for 2021.

NECCDC 2021 SEASON SPONSORS

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

Additional information regarding sponsorships for the NECCDC 2021 Season can be found at neccdl.org/neccdc/2021/sponsors

VIBRANIUM	
TBD (Reserved, in contracting)	

SILVER	
 Palo Alto Networks	Others TBD, in contracting

QUALIFIER EVENT SCHEDULE

SATURDAY, 23 JANUARY, 2021

TIME (EST, 24 Hour format)	ACTIVITY	NOTES
09:00	Blue Team Check-in begins	
10:00	Welcome Inject	
10:30	Competition Begins	Scoring starts and Blue Team access to environment systems enabled
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 the Competition Director. 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.

Red Team

Professional network penetration testers from 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 individual locations must have at least one (1) - ideally two (2) or more - remote site moderator(s) present within the virtual environment during active times of the competition provided by the Team Representative.
- Remote Moderators are responsible for:
 - Participating in one of the remote moderator orientation sessions offered by NECCDC
 - Understand how to use the required communication tools (e.g., Slack)
 - Submitting questions / requests from blue team to the Competition Project Manager
 - Ensuring that competition rules are followed and any violations are reported to the Competition Project Manager
 - Submit survey feedback based on competition / team observations near end of Qualifier (e.g., webform provided then)

- White Team senior staff will:
 - Supply and grade 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 to include the Director, logistics and sponsor relations coordinators

Orange Team

The competition staff that builds an integrated scenario storyline, corporate branding/image, and simulates user activities in a manner that integrates with and contextualizes Black and White team activities. The team also may include individuals who act as employees, clients, and other external acting parties, e.g., CISO, law enforcement that interact with systems and Blue Team during the competition experience.

COMPETITION RULES

NECCDC subscribes to the [National CCDC Rules](#), many of which have changed due to the online nature of the competition year.

NOTE: ** One important change from last year's National CCDC Rules is specifically addressed here**

NCCDC RULE 5.f. Scripts, executables, tools, and programs written by active team members may be used in CCDC events

This will be allowed, provided:

1. The scripts, executables, tools, and programs have been published as a publicly available resource on a public and non-university affiliated site such as GitHub or SourceForge for at least 3 months prior to their use in any CCDC event.
2. Teams must send the public links and descriptions of the team-written scripts, executables, tools, and programs to the appropriate competition director at least 30 days prior to their use in any CCDC event. Development must be “frozen” at time of submission with no modifications or updates until after the team competes in their last CCDC event of that season.

3. Teams must consent to the distribution of the submitted links and descriptions to all other teams competing in the same CCDC event where the team-written scripts, executables, tools, and programs will be used.

Because our Qualifier will take place on January 23, 2021, we requested and received an exception to rule 5.f.2 (30 days prior). **The NEW/FINAL date to register your public links and descriptions is 11:59 PM EST January 12, 2021. **These repositories must be frozen and no changes will be made to those after the submission cutoff**.** For example, teams can post a custom script, checklist, or documentation in a PUBLIC team GitHub repo. There must be no commits to that repo after the cutoff on Jan 12, 2021 (23:59). Teams seeking to take advantage of this opportunity will submit the link to their publicly-accessible repository via direct email to director@neccd.org. The Director will distribute the aggregate list of published links to all registered competitors by January 15, 2021.

IP Whitelisting

Prior to the competition, each competitor will register their IP address for whitelisting access to the VDI within RIT's Cyber Range. Exact details about VDI connections tests will be provided within 48 hour of the qualifier. In the meantime, further information is available here: <https://wiki.rit.edu/display/AcademicCloud/Accessing+the+GCI+Digital+Range+through+VDI>.

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 (reference Schedule on Page 7 of this Document).

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. 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 amount of points reduced as a result of Red Team activity.

System Scoring

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

Inject Scoring

Injects are business tasks provided to each team throughout the competition and make up half of the Blue Team 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. 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.

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 combining service and inject scoring. 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.

NECCDC 2021 SEASON THEME

The theme of the NECCDC 2021 Season is MOBILITY. Student competitors are expected to be able to implement and maintain technologies that improve an organization's mobility.

As the industry has seen in the last year, computer systems and the data they house can change location rapidly. Systems may need to be moved with little planning or forethought and that presents a unique set of challenges to those tasked with securing them. This is particularly true when security teams have little time, in advance, to secure the new location of these systems. Securing systems in a mobile landscape presents challenges to traditional security doctrine. Endpoint detection and identity management become paramount while perimeter security and the utilization of trusted systems become much harder. Similarly, supporting these systems and their users becomes more challenging.

Concepts involved in the theme of mobility include:

- The importance of understanding the security assumptions made in a highly mobile environment
- The relationship between host-based and network-based protections
- Evaluating trust relationships between systems in the environment
- Understanding the strategic objectives of adversaries in a highly mobile environment

Technologies and Processes that often help support mobility:

- Robust authentication and access control systems
- Strong endpoint detection and monitoring
- Inventories and asset management
- Incident response tools

NECCDC 2021 SEASON SCENARIO

The NECCDC 2021 Season scenario places student competitors as employees of NEWScrier.ORG. NewsCrier is a non-profit global news agency that is responsible for collecting and verifying news in many countries. During the NECCDC 2021 qualifying competition, you will be tasked with supporting the security needs of a smaller NewsCrier regional office following their transition to remote operations due to COVID-19. Teams that move on to the NECCDC regional competition will be working with the NewsCrier global security team supporting offices in multiple countries and additional critical NewsCrier systems.

LETTER FROM MANAGEMENT

From: Ivan Horvat
To: Remote Operations Security Support Team
Subject: WELCOME

Team:

Thank you for offering to step up and help support one of our smaller offices in this difficult time. This office, like the many of our offices, has recently moved to remote operations due to the prevalence of COVID-19 nearby. This has necessitated the deployment of many new technologies, such as a new VPN.

Our global security team has expressed some concerns about the security of this regional office. Because of the increasing rates at which news agencies are becoming targets of advanced threat actors, we have decided that systems used by our employees working from home and our field reporters should not be implicitly trusted. To address this, our operations team has begun utilizing Microsoft Azure Active Directory to authenticate remote users. So far, this deployment has been constrained to keep regional offices isolated while NewsCrier's legal and leadership teams determine a course of action for merging data from different regions.

Unfortunately, local COVID restrictions prevent local system and network administrators from being working on-site. Because on-site management is restricted, it is important to ensure that remote administration of NewsCrier systems can occur while simultaneously minimizing security risk. A system that is powered off may be unable to be restarted. Similarly, since on-site access is restricted, our operations team is not comfortable permitting changes to network security controls or network architecture because of the potential impact on the reporting.

It is critical that we ensure our systems are secured and allow for the distribution of accurate news during this difficult time. The public is relying on NewsCrier to keep it informed of many current events in an age ripe with the manipulation of information.

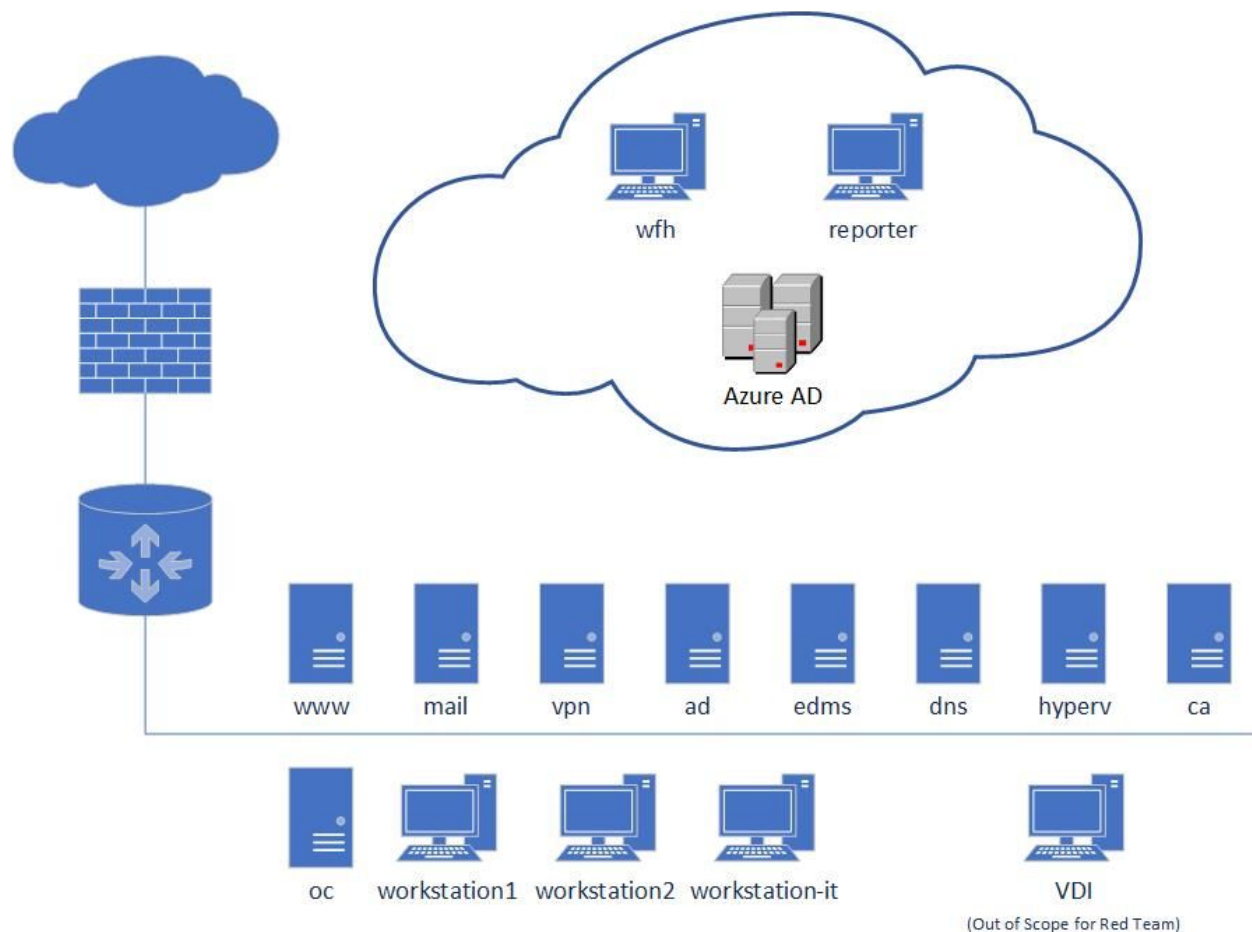
Respectfully,

Ivan Horvat
Global Security Manager
NewsCrier

QUALIFIER INFRASTRUCTURE

Employees of NewsCrier should be prepared to assess the various aspects of the client's infrastructure. Various technologies are known to be incorporated in the regional office's infrastructure, including, but not limited to:

Windows Server Core Microsoft Active Directory Microsoft IIS WAMP WMI and RDP Data Integrity Controls Hyper-V Certificate Authorities	Ubuntu Linux CentOS Linux Fedora Linux Linux-based DNS Mayan EDMS File signing Linux-based Email Systems Kerberos	Wireguard VPN Microsoft Azure VMs Microsoft Azure AD End-to-End Email Encryption
--	--	---



Note:

WFH = Work From home

OC = OwnCloud