2019 Northeast Collegiate Cyber Defence Competition

RESILIENCE & RECOVERY

Qualifier Blue Team Packet

v2 - 11-28-18

Northeast CCDC Mission and Objectives

The Northeast Collegiate Cyber Defense Competition (CCDC) provides an opportunity for qualified educational institutions in the Northeast to compete, and is part of a national organization (see www.nationalccdc.org) to provide a unified approach across nine regions across the country. Qualified educational institutions include those with information assurance or computer security curricula. The Northeast Collegiate Cyber Defense Competition 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.

Qualification Overview

The Northeast Collegiate Cyber Defence Qualifier will be managed by the NECCDC 2019 host, Champlain College. The competition is designed to test each student team's ability to secure a networked computer system while maintaining standard business functionality. The scenario involves team members simulating a group of employees from an IT service company that will initiate administration of an IT infrastructure. The 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 as described in the competition topology. Each team will start the competition with a set of identically configured systems.

The objective of the competition is to measure a team's ability to maintain secure computer network operations in a simulated business environment. This is not just a technical competition, but also one built upon the foundation of business operations, policy, 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 will be scored on the basis of their ability to detect and respond to outside threats, including cyber-attack while maintaining availability of existing network services such as mail servers and web servers, respond to business requests such as the addition or removal of additional services, and balance security against varying business needs. Qualifying teams from the 2019 NECCDC Qualifier will have the opportunity to participate in the 2019 Northeast Regional CCDC, March 15-17, 2019 at Champlain College.

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 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

Competition Team Identification

Blue Team

Student team representing a specific academic institution or major campus competing in this competition. Each team must submit a roster of up to 12 competitors to the Competition Manager. 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 Manager.

- Members and advisor sign a participation safety agreement if teams compete anywhere other than their academic institution
- Members and advisor sign a photo release document where applicable - have completed a minimum of one semester in the participating institution's networking or security curriculum
- Students should maintain a full time status at the time the competition is conducted.
- National rules apply (https://www.nationalccdc.org)

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 and
- Modify any acquired environment
- Assess the security of each Blue Team network
- Attempt to capture specific files on targeted devices of each Blue Team network
- Attempt to leave specific files on targeted devices of each Blue Team network

- Follow rules of engagement for the competition

White Team

Representatives from industry who serve as competition officials, judges, room monitors and security enforcement in the various competition rooms.

- Each team competing remotely from their academic institution must have a remote site judge on site, present during most active times of the competition.
- White team will supply and grade blue team tasks in the form of competition injects
- White team will adjudicate the scoring for the competition.
- The white team will 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.

Gold Team

The competition staff to include logistics and sponsor relations.

Network & Team Site Description

- Each competition network will be located remotely from the competition site, and will be logically isolated from all other competing Blue Teams. All Teams will access the competition network via a browser connection.
- Blue Teams will compete remotely from their own institution, in which case their institution must provide workstations with browsers that are compliant with the competition environment.
- Blue Teams competing from their own institution must do so from a dedicated, secure location where all team members are collocated together with the local site judge. Classrooms or conference rooms are considered ideal locations. The secure location is to have restricted access to only Blue Team members, remote site judges, local administrators and technical support.
- Competition workstations and servers are able to access the internet.
- The White Team and each respective Blue Team will communicate with each other via the deployed learning management system (CANVAS).
- Red Team activity may occur on internal networks or against exposed services in accordance with the competition rules of engagement. This activity may result in the loss of services.
- Each Blue Team network will be monitored by a scoring system operating within the remote network. An indication of services, as viewed by the scoring engine, will be made available to each Blue Team via a web interface.

A logical diagram of the team logical network is contained within this Team Packet. However, it is subject to change and /or modification as decided by the Competition Manager.

Schedule - 1/26/2019

Time	Activity	Notes
08:00 (EST)	Login Credentials distributed	vSphere login,
08:15-08:30	Zoom session and credential testing	
08:30	Welcome Inject	This will test access to vSphere and the Learning Management System
08:45	Competition Begins	All systems will be exposed and accessible
14:00	Competition Ends	
2:15 14:45	Debrief 1	Scheduling a debrief 2 in likely event that scoring is not complete.

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, Black Team and White Team members will occasionally need access to a team’s systems for scoring, troubleshooting, etc. Teams must allow Black Team and White Team member access when requested.
4. 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.
5. Teams must maintain specific services on the “public” IP addresses assigned to their team and stipulated by this document. Moving services from one public IP to another is not permitted unless directed to do so by an inject. Likewise, teams are not permitted to change the internal addressing or VLAN scheme of the competition network unless directed to do so by an inject.
6. 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. Changes to internal IP

addresses may affect any internal scoring, changes in IP addresses should be communicated to the White Team immediately. . It is the responsibility of the team to understand all the particulars of scoring a service when doing so.

7. Teams are not permitted to alter the system names or IP address of their assigned systems unless directed by an inject; this may affect the results of the scoring
8. Systems designated as user workstations within the competition network are to be treated as user workstations and may not be re-tasked for any other purpose by teams. Generally speaking, Windows 10 desktops and any linux system with a GUI is not to be used to run scored services.

Competition Rules

We will subscribe to the CCDC 2019 Rules with the following exceptions. One thing to note is that we will be using national rules (Rules 5 and 6) as they relate to external resources, private storage, staging of scripts etc… This is a departure from last year's local rules.

Remote Qualifier

- 8 Competitors only
- Coaches may be in the competition room but may passively observe only once the competition starts.
- Teams will need to arrange a remote site judge (no current affiliation with their institution). See section 10 of the CCDC 2019 Rules.

NECCDC 2019 Competition

- All teams will participate at Champlain College
- Teams may travel with 8 competitors and two alternates.
- Alternates may be switched in at the beginning of the competition day by informing the team's white team in-room judge
- Alternates may participate in team research and any overnight injects

Competition Scenario

Your 8 person blue-team is the DevOps team for Software and Services company that has developed and internally hosts a Learning Management System (LMS) that is used by multiple academic institutions. Among other services, the DevOps team is responsible for the security and operations of both internal enterprise services (DNS, DHCP, AD, Logging) as well as publicly exposed systems such as a Wiki and potentially a Bug tracking/submission system. The theme for this year's competition is resilience and recovery so keep that in mind as you prepare for the qualifier and subsequent competition.

Competition Topology

The qualifier environment has changed this year and will be hosted within Champlain College's Datacenter. Teams will access their respective environments through a vSphere FLEX or HTML5 Client. Team's should make sure that Flash Player is available on the systems used to access the qualifier environment. This topology and system description is provided in order that blue teams can begin preparation. This environment is subject to minor change

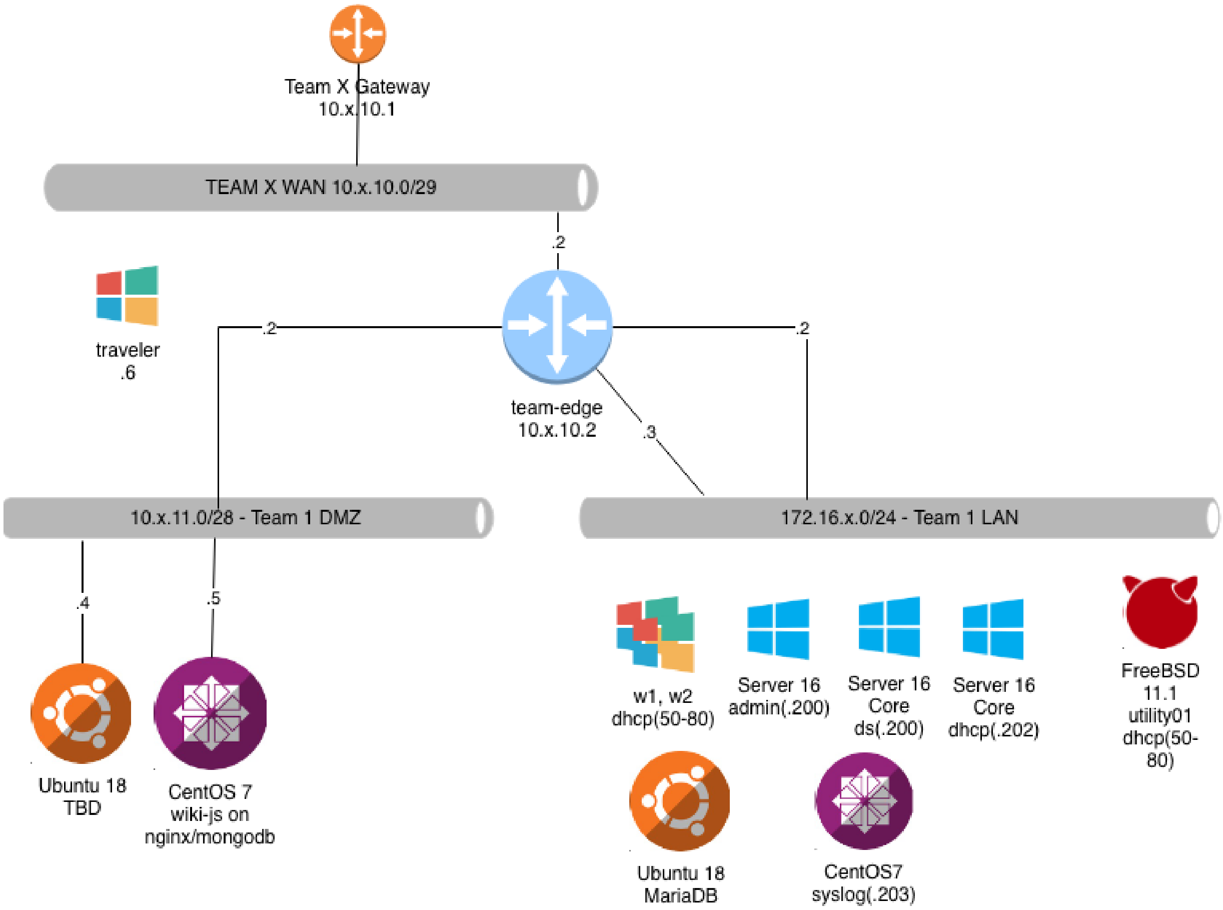

Figure 1. NECCDC 2019 Qualifier Architecture

System Descriptions

Item	Description
team-edge	A Palo Alto Virtual Firewall with WAN, LAN, MGMT, and DMZ interfaces. Registered teams will get a NETLAB training environment.
traveler	A Windows 10 VM on the Team's WAN
DMZ/Ubuntu 18 TBD	An exposed http based service
DMZ CentOS 7 wiki-js nginx/monogoDB	A corporate wiki used as a FAQ for external customers.
w1, w2	Windows 10 LTSB VMs that represent internal workstations. These are domain joined and get their Domain information from a DHCP server
Server 16 Admin	Server 2016 with a GUI that can be used to manage other systems.
Server 16 Core DS	Active Directory and DNS running on Server Core
Server 16 Core DHCP	DHCP Server running on Server Core
Ubuntu 18 Maria	A MariaDB Server
CentOS 7 Syslog	An rsyslog server
FreeBSD 11 Utility	A spare utility server that can be used to bring up new or rehost existing services.