Regional Blue Team Packet

2/12/2019

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.

Regional Overview

The Northeast Collegiate Cyber Defence Regional 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. The 2019 Northeast Regional CCDC will take place March 15-17, 2019 at Champlain College, with the winner going on to represent the region at the National Competition being held April 23-25, 2019.

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.

- 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

Orange Team

Orange team members serve as users or managers in the blue team's organization. These trusted team members will be properly badged and identified by user name. When these personnel stop by, they will be afforded access to any systems where they have a user account.

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.

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.
9. Blue team rooms will be set up in college labs and classrooms. No computing or networking equipment and accessories from these classrooms may be used unless it is explicitly part of your original competition environment.

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 and we will be taking this very seriously.

NECCDC 2019 Competition Exceptions

- 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

Scoring Method

Half of your team's points will be earned by sustaining service uptime. The scoring engine will issue checks on a regular interval to determine your uptime. Each check is assigned a fixed amount of points, and your team will earn those points every time the scoring engine determines that the service is "Up". Services that do not pass checks will earn your team no points. If multiple checks in a row fail on a given service, each subsequent check that fails will result in a point loss due to SLA violation.

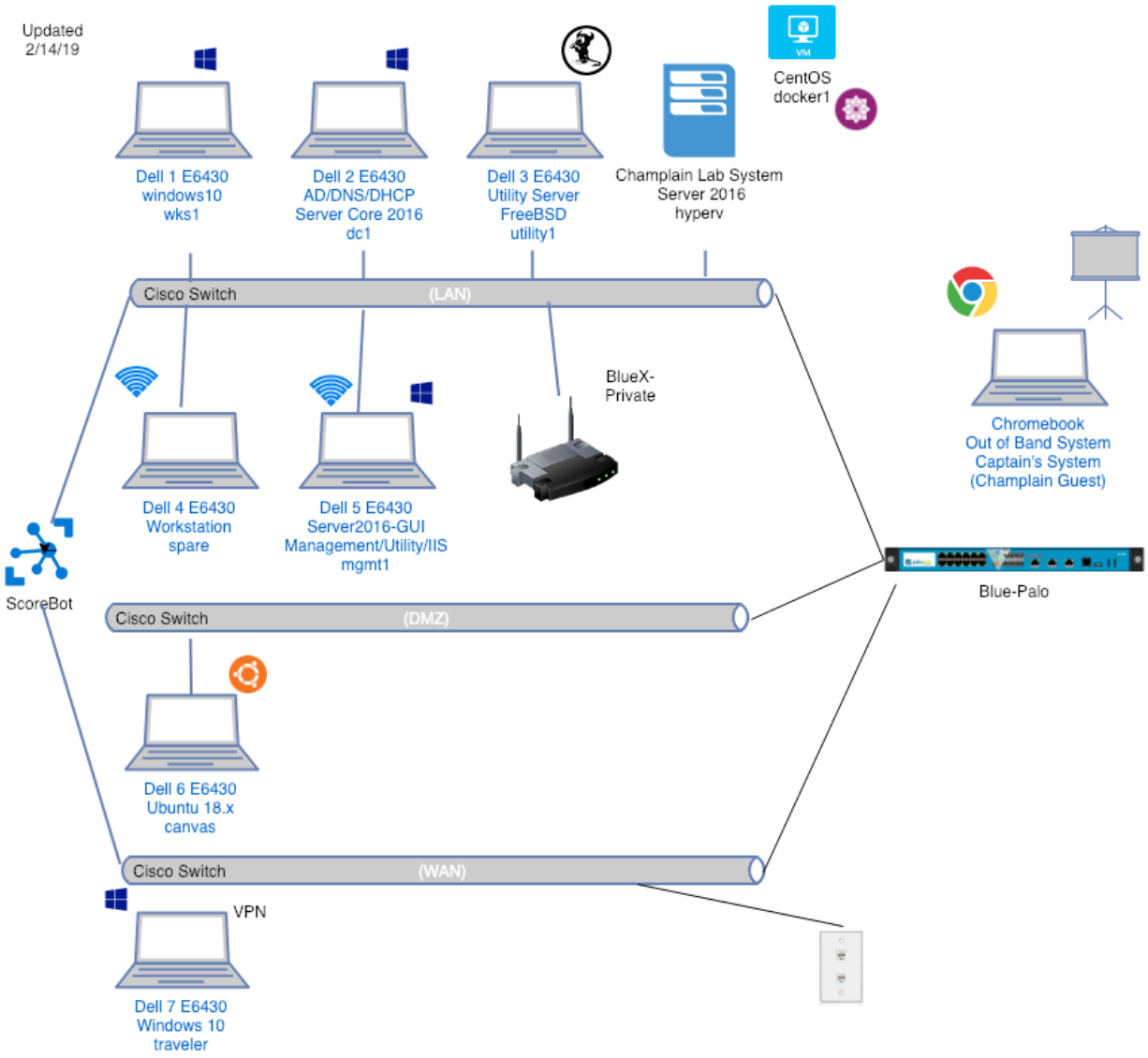
The other half of your team's points are earned by completing injects. Each inject is assigned a specific number of points due to a number of factors, such as business value, technical difficulty, and overall complexity. Given the general inject scores of teams in the qualifier, and that inject difficulty will be raised for regionals, we suggest teams invest additional resources into completing their injects at this years regionals.

Red Team activity can cost your team up to half of all possible points. Red team penalties are assessed based on the number and severity of successful incursions into your team's environment. You can recover up to 50% of points lost in each initial incursion with a detailed Incident Report. Periodically, each successful incursion will be re-assessed by the red team. If the incursion remains successful, the same penalty will be re-applied.

Competition Scenario

Your 8 person blue-team is the DevOps team for Software and Services company called StormSurge Software that hosts and supports 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 Canvas. The theme for this year's competition is resilience and recovery so keep that in mind as you prepare.

Competition Topology



NECCDC 2019 Regional Architecture (subject to change)

System Descriptions

Item	Description
blue-palo	A Palo Alto PA3050 Firewall with WAN, LAN, MGMT, and DMZ interfaces
switch	Internal Cisco Switch that virtually segments WAN, LAN and DMZ. This switch is out of scope for red and blue teams and should be considered infrastructure.
Wireless Access Point	OpenWRT Wireless Access Point that provides wireless connectivity to blue team LAN systems.
traveler	A Windows 10 WAN based remote worker that access internal stormsurge network resources via VPN.
canvas	A DMZ based server running CANVAS LMS, Postgres, Passenger Phusion and Apache
spare	Teams have wide discretion in using this system to assist in accomplishing their mission.
docker1	Virtualized CentOS docker server
hyperv	Server 2016 GUI running Microsoft HyperV. Hosts a file share of relevant ISO files.
wks1	Internal workstation. Domain joined and a DHCP client.
dc1	Server 2016 Core running active directory domain services, dns and dhcp
mgmt1	Server 2016 with a GUI that can be used to manage other systems. Also runs an internal Web Server
utility1	A freebsd server that can be used to bring up new or rehost existing services.
scorebot	This is a IoT internal scoring engine, it is out of scope for red and blue teams.

Schedule

TIme	Event	Venue	Notes
Friday, March 15, 2019			
8:30 AM	Team Registration	Hallway, Alumni Auditorium	
9:00 AM	Competition Opening	Alumni Auditorium	
9:30 AM	Blue Teams go to Rooms	Enroute to Joyce Hall	Escorted by White Team
10:00 AM	Competition Begins	Joyce Hall	
12:00 PM	Box Lunches	Joyce Hall	Teams will pick up Lunches in Joyce
6:00 PM	Day 1 Ends	Joyce Hall	
6:00 PM	Sponsor Only DInner	LCDI	6:00-7:30 PM
Saturday, March 16, 2019			
8:30 AM	Day 1 Recap and Admin	Alumni Auditorium	
9:00 AM	Blue Teams to Rooms	Joyce Hall	
9:15 AM	Competition Begins	Joyce Hall	
5:00 PM	Competition Ends	Joyce Hall	
5:30 PM	Recruiting Event	Champlain Room	5:30-7:30 PM
Sunday, March 17, 2019			
8:30 AM	Day 2 Recap and Admin	Champlain Room	
9:00 AM	CTF Mixed Teams	Champlain Room	
12:00 PM	Lunch	Champlain Room	HIghlights video, Q&A White and Red General Observations
1:00 PM	Awards Ceremony	Champlain Room	
1:30 PM	End of Competition	Champlain Room	

Logistics

Maps, Hotels, Parking Instructions can all be found at https://www.neccdc2019.org/resources/. Questions can be sent to neccdc@champlain.edu

Sponsors

NECCDC 2019 is made possible by the generous contribution of our sponsors whom include:

Platinum

Gold

Silver

COM | CODE

AIR FORCE CIVILIAN SERVICE

Forces. Joined.

Crowe

opentext™

Red River

CHARITABLE FOUNDATION


RSM
THE POWER OF BEING UNDERSTOOD
AUDIT | TAX | CONSULTING

Bronze


INVICTUS
INTERNATIONAL


Kivu


CROWDSTRIKE


vSOC
GUIDEPOINT SECURITY


People's United Bank
What know-how can do®


NuHarbor
SECURITY


vertek
accelerate to value


C2


ankura
COLLABORATION DRIVES RESULTS