Team Packet

March 16-18, 2018

University of New Hampshire

Welcome Letter

Competitors,

On behalf of the University of New Hampshire, I would like to welcome you to the 11th Annual Northeast Collegiate Cyber Defense Competition (NECCDC). Cyber security continues to become an ever more important part of our national security efforts and this competition is one of most important events in training our future cyber security experts.

We are very grateful to all of our sponsors as well as to The University of Texas at San Antonio (UTSA) for their guidance, event templates and materials. Our staff, volunteers, and sponsors have worked hard to make this an interesting, exciting, and challenging competition.

This event has three goals: 1) Provide practical cyber security experience for college students. 2) Provide sponsors candidates that understand how to run a modern (cloud based) Security Operation Center (SOC). 3) Select the best team to represent the Northeast at Nationals.

The winner of this contest will receive travel expenses to compete at the National Collegiate Cyber Defense Competition to be held in April 2018 in San Antonio, Texas.

We encourage you to spend some time with members of the other teams to enhance your learning experience. We wish the very best of luck to each of you and your teams! Many thanks to you for participating in this competition.

Ken Graf, Event Director
Department of Computer Science
University of New Hampshire

Schedule

Friday – March 16, 2018

9:00 AM	Team Registration	Huddleston
9:30 AM	Opening Announcements	Huddleston
10:00 AM	Competition Starts	Kingsbury
Noon	Box Lunch in team rooms	Kingsbury
6:00 PM	**Competition Day 1 Ends**	Kingsbury
6:30 PM	Recruiting event – Hors d'oeurves	Huddleston

Saturday – March 15, 2018

9:00 AM	Breakfast	Huddleston
9:30 AM	Day 1 recap	Huddleston
10:00 AM	Competition Starts	Kingsbury
Noon	Box Lunch in team rooms	Kingsbury
6:00 PM	**Competition Ends**	Kingsbury
6:30 – 9:00 PM	Team mixer - Dinner	Huddleston

Sunday – March 16, 2018

8:30 AM	Continental Breakfast	Huddleston
9:00 AM	CTF/Panopoly (Open teams)	Huddleston
11:00 AM	White and Red team feedback	Huddleston
Noon	Luncheon	Huddleston
1PM	Awards Ceremony	Huddleston

Directions

The NECCDC is being held in Durham, New Hampshire, at the University of New Hampshire. The building for the event is Kingsbury Hall.

Directions to University of New Hampshire's Kingsbury Hall
33 Academic Way, Durham, NH 03824

UNH is located off NH Route 4

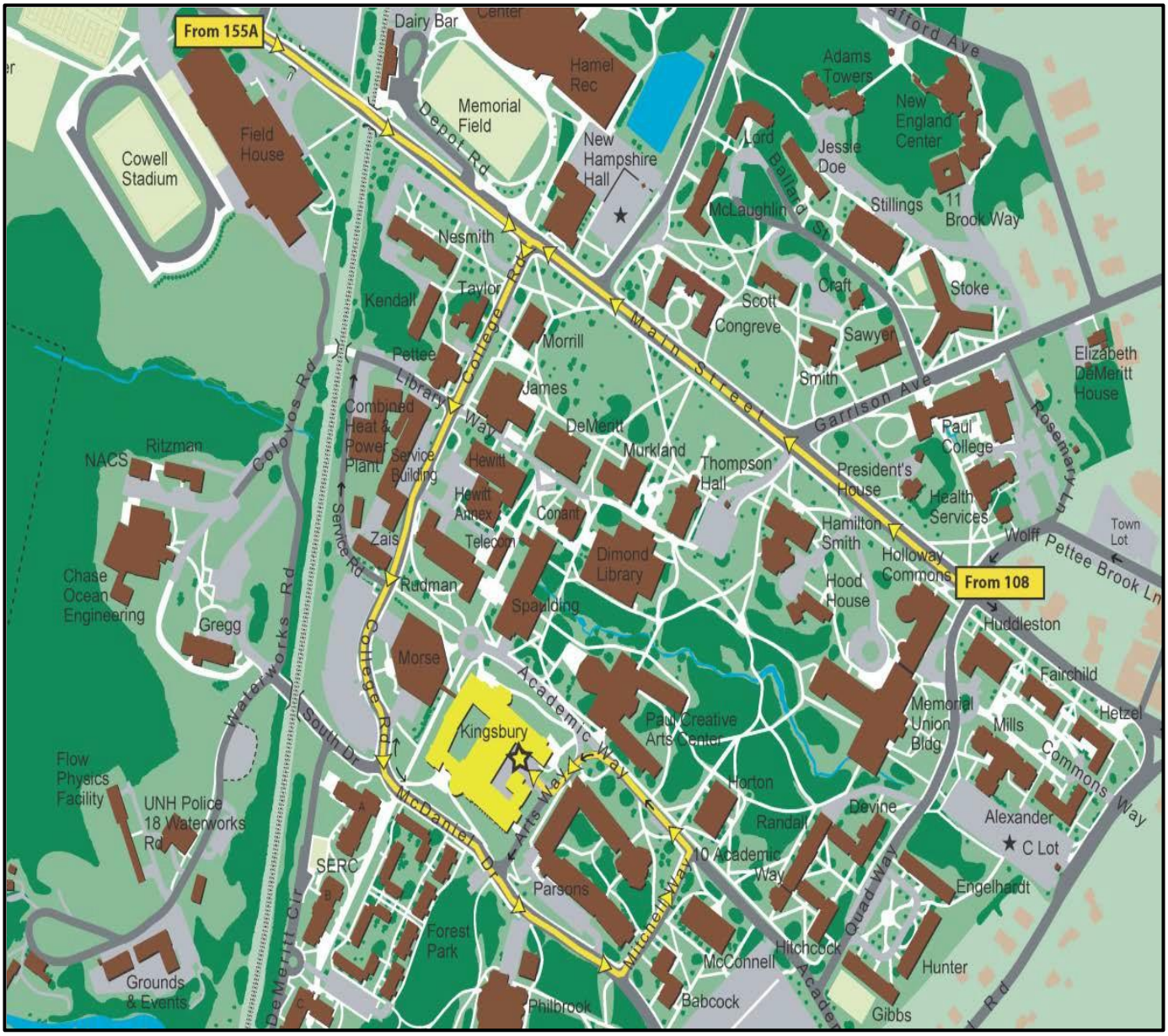
From I-95 South (Maine), take Exit 5 (in NH) to the Spaulding Turnpike (Route 16N), then take Exit 6W (Route 4 West) towards Durham to the Exit for Route 108. Follow Route 108 until you reach Main Street (intersection where 108 turns East you will stay straight). Refer to Mapquest map below.

From I-95 North (Mass.), take Exit 4 (in NH) (left hand exit) to the Spaulding Turnpike (Route 16N), then take Exit 6W (Route 4 West) towards Durham to the Exit for Route 108. Same as above.

From the West, take Route 101 East to Exit 7 (Route 125 North). Follow Route 125 North to the traffic circle. Take Route 4 East to the Durham Exit (2 miles)(Route 155A). Continue on Main Street until you take a right on College Road.

Additional map/directions can be found at:
http://www.unh.edu/transportation/visitor/directions.htm.

University of New Hampshire Campus Map



Hotel Information

Below are suggested hotels located less than 10 miles from the University of New Hampshire in Durham, NH.

Holiday Inn Express Durham
2 Main Street
Durham, NH 03824
(603) 868-1234
Approximately .5 miles from campus
http://www.ihg.com/holidayinnexpress/hotels/us/en/durham/durnh/hoteldetail

Homewood Suites Dover
21 Members Way
Dover, NH 03820
Approximately 6 miles from campus
(866) 678-6350
http://homewoodsuites3.hilton.com/en/hotels/new-hampshire/homewood-suites-by-hilton-dover-PSMDVHW/index.html

Hampton Inn
9 Hotel Drive
Dover, NH 03820
603-526-5600
Approximately 7 miles from campus
http://hamptoninn3.hilton.com/en/hotels/new-hampshire/hampton-inn-dover-PSMDOHX/index.html

Comfort Inn & Suites
10 Hotel Drive
Dover, NH 03820
(603)
Approximately 6.4 miles from campus
http://www.comfortinndover.com/

Competition Overview

The Northeast Collegiate Cyber-Defense Competition (NECCDC) is the regional qualifier for the National Collegiate Cyber-Defense Competition (NCCDC). The northeast region represents institutions in the states of New York, Maine, New Hampshire, Vermont, Massachusetts, Rhode Island, and Connecticut.

The NECCDC will select one winner and one alternate to represent the region. This year's CCDC is being held in San Antonio, Texas..

More information on the CCDC can be found at the CCDC website:

http://www.nccdc.org/

The NCCDC represents a collection of defense-only competitions in cyber-security. The competition is designed to test each student team's ability to secure a networked computer system while maintaining standard business functionality. 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 services per company policy and mission. 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-attacks, 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

Corporate Profile

Your team, along with a new CIO, has been hired to take over the Security Operations Center (SOC) for **TBD**. At the request of major stake holders, including the Department of **TBD**, the previous SOC team was let go after confidential and proprietary research documents surfaced online.

As the new SOC team, you will be tasked with securing the network, providing forensics while maintaining SOC services.

Specific scenarios for qualifying and regionals will be provided just prior to the event

Network Description

There two components to the competition network design. A developer/operations (DevOps) center and scored services deployed to the cloud.

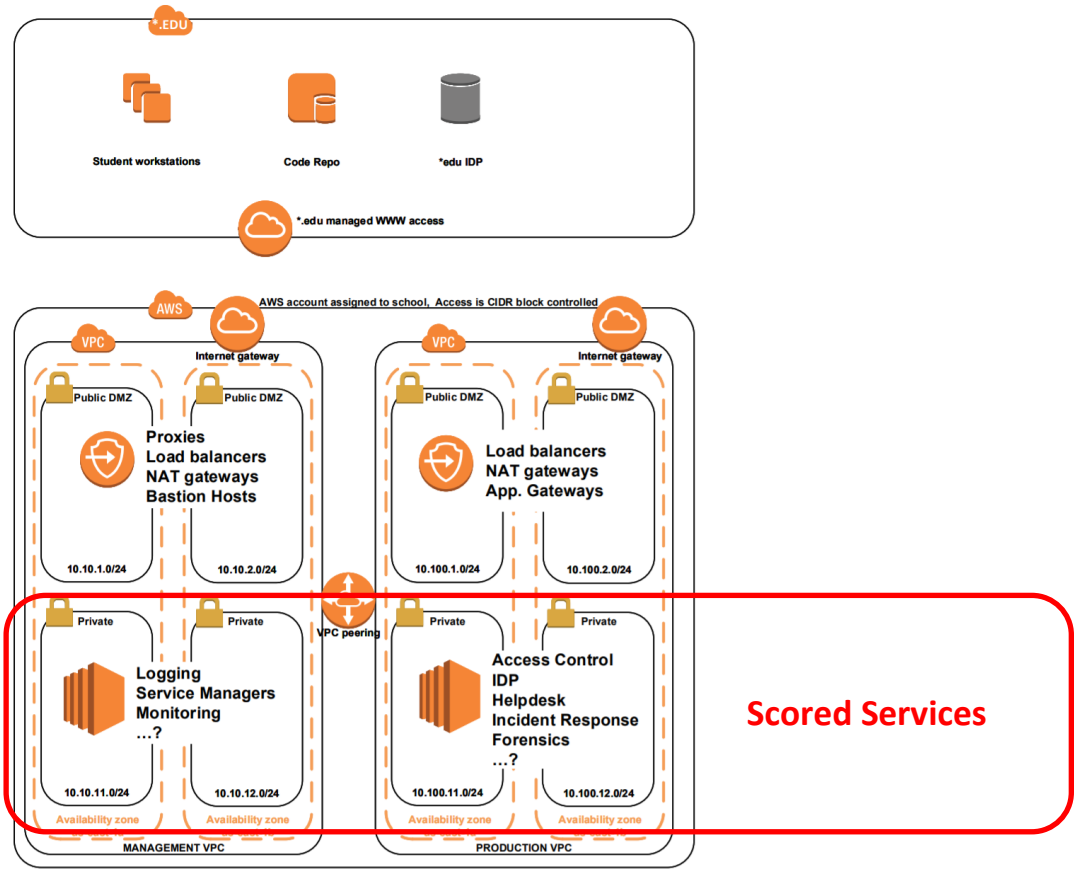
For practice and qualifying rounds each school will need to provide the DevOps systems with HTTP/SSH/RDP access to the scored services hosted in AWS. At the regional DevOps systems will be provided for you by UNH. DevOps detail for the regional to be provided prior to the event.

For all rounds all scored services will be run in the cloud (AWS)

All rounds will use the same AWS network configuration for scored services. The source for this configuration is maintained at:
https://github.com/kengraf/neccdc2018automation

Note: the scored services for each phase of competition will change and the scored services will not be maintained in the above Github repository.

Note: This event is focused on secure operations not AWS knowledge. Your efforts should be focused on securing the services not any specific AWS technology.



Possible scenarios

The following list is not comprehensive, but every team should at a minimum have a plan for addressing the following injects:

- Create Centralized Logging System
- Lock Down the Wireless Network
- OS/Runtime Vulnerability Scanning
- Create Bastion (Jump Host) Infrastructure
- Develop Incident Response Procedures
- Implement Privileged Account Management
- Track Elevation of Privileges
- Install an Outbound Proxy
- Create Incident Report Template
- Provide Recommendations for System Monitoring
- Harden Network Cryptography
- Provide Recommendations for Alerts
- Implement Alerts
- Implement Security Event Tracking
- Implement Incident Response Tooling
- Implement a network packet capturing system
- Manage Windows Admin Account Alerts
- Create Dashboards
- Implement an API Gateway / Application Firewall
- Provide Situation Reports
- Provide Forensic Investigations

Northeast Regional Rules

In an effort to properly prepare winning team for the national CCDC, the NECCDC makes use of national CCDC competition rules with the following clarifications/modifications:

1. **Software Use**
    a. EULA violations are considered a serious offense and will result in disqualification:
    b. Do not use any software that requires a paid license.
    c. All software for the regional event will be properly licensed by the regional organizer.
2. **Team Membership**
    a. The Northeast regional allows up to 12 students (2 graduate) from each school to attend the regional event.
    b. Only 8 students may participant on any given day, for both qualifying and regional rounds.
    c. Substitutions may be made at the beginning of the day, but not during the day.

Scoring

This year's regional introduces changes to how teams are scored. In an effort to 1) match nationals. 2) Create a more transparent assessment model. The following weighted point distribution matches scoring at the national level.

Final scores will be awarded using the following point distribution:

50%	Functional service uptimes and SLA violations as measured by the scoring engine.
50%	Successful completion of approximately 30 inject scenarios.

Note: Red team activity is not a direct component of scoring this year. With that said; red team activity will generate inject scenarios that are scored, and if proper defenses/configurations are not maintained, red team activity will result in service outages and SLA violations.

A system restore service is available to teams. This service has a minimum of 15 minutes lead time. There will be a **penalty of 5% per restoration** against the final score for this service.

Note: This penalty does not apply to restoration due to hardware failure.