NECCDC 2015

Northeast Collegiate Cyber Defense Competition

Blue Team Packet

March 20th – 22nd

School of Information Studies
SYRACUSE UNIVERSITY

Table of Contents

NECCDC 2015 Blue Team Packet

Welcome Letter

Dear NECCDC Competitors,

On behalf of Syracuse University and School of Information Studies (iSchool) I would like to welcome you to the eighth Northeast Collegiate Cyber Defense Competition (NECCDC). The iSchool is very excited to be hosting this event and we hope everyone enjoys their time here at Syracuse.

NECCDC would not be possible without the support it enjoys from everyone involved and our staff, volunteers and sponsors have worked very hard to make this an interesting, exciting, and challenging competition. We thank all of you for participating in this competition and wish you the best of luck.

Bahram Attaie
Director NECCDC 2015
Assistant Professor of Practice
School of Information Studies
Syracuse University

Competition Overview

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

The CCDC 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.

The 2015 NECCDC will select one winner and one alternate to represent the region in the CCDC for 2015. This year's CCDC is being held in San Antonio, Texas, April 24-26. More information on the CCDC can be found at the CCDC website: http://www.nationalccdc.org/ .

Competition Scenario

Skyhook Industries is an up and coming firm focused on restructuring and strengthening struggling organizations.   Targeted at midsized domestic firms with viable products and technologies, Skyhook lifts legacy management culture to a modern, efficient structure. Although small, the interest and investments in their approach is allowing them to expand.

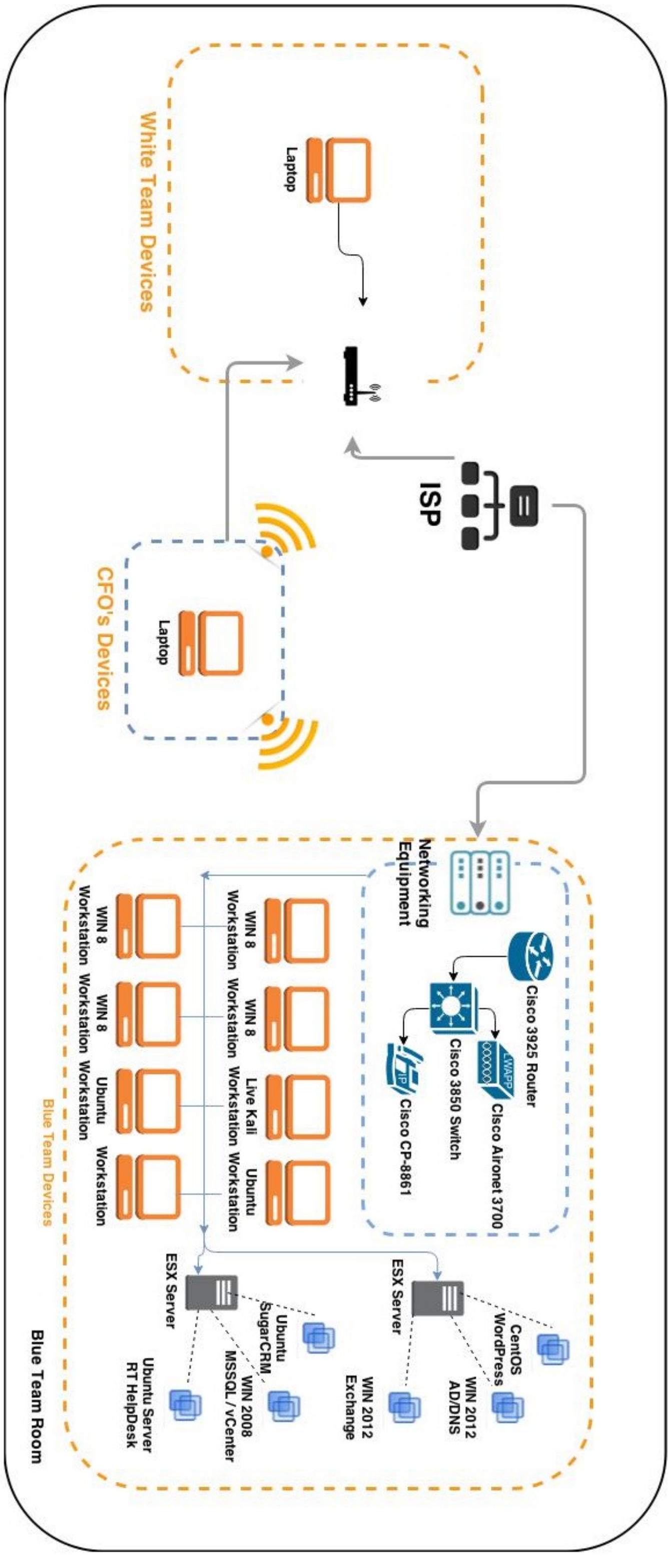
In an effort to acquire a specific talent pool as well as have success story to showcase their approach, they've acquired a struggling legacy management company named Enron. The acquisition has gone smoothly and Skyhook has started to move some of its administrative staff into the new location.

Since Skyhook was only interested in a percentage of current employees, much of the original company's staff was let go or left for "greener" pastures.   The cuts and departures included the entire IT staff. Skyhook's CIO, CEO and CFO are on site for the transition, and have brought your team in to evaluate the current state of the IT infrastructure. Have a seat at your new desk, login, and enjoy your new role at Skyhook Incorporated.

Skyhook: Lifting American companies into the future….

Enron’s Existing Network Topology

Our previous Technology Services employees created the following network map for you to reference.



Initial Services Scored for Enron’s Network

System	IP	Operating System	Scored Services
Vsphere	10.1.x.210	ESXi	Web /Uptime
Crm	10.1.x.203	Linux	Web
Website	10.1.x.212	Wordpress	Web
Ad	10.1.x.201	Windows	DNS / AD
exchange	10.1.x.202	Windows	SMTP / Web

*** x denotes team number

Each server is critical to the operation of Enron. Note that systems labeled as workstations and laptops must remain end-user systems and cannot be re-provisioned as server systems.

Services may be added to this list or removed from it via injects.

CCDC National Competition Rules

http://nationalccdc.org/index.php/competition/competitors/rules

Throughout these rules, the following terms are used:

- Gold Team/Operations Team - competition officials that organize, run, and manage the competition.
- White Team - competition officials that observe team performance in their competition area and evaluate team performance and rule compliance.
- Red Team - penetration testing professionals simulating external hackers attempting to gain unauthorized access to competition teams' systems.
- Black Team - competition support members that provide technical support, pick-up and deliver communications, and provide overall administrative support to the competition.
- Blue Team/Competition Team - the institution competitive teams consisting of students competing in a CCDC event.
- Team Captain - a student member of the Blue Team identified as the primary liaison between the Blue Team and the White Team.
- Team Co-Captain - a student member of the Blue Team identified as the secondary or backup liaison between the Blue Team and the White Team, should the Team Captain be unavailable (i.e. not in the competition room).
- Team representatives - a faculty or staff representative of the Blue Team's host institution responsible for serving as a liaison between competition officials and the Blue Team's institution.

1. Competitor Eligibility

A. Competitors in CCDC events must be full-time students of the institution they are representing.

   i. Team members must qualify as full-time students as defined by the institution they are attending.

   ii. Individual competitors may participate in CCDC events for a maximum of five seasons. A CCDC season is defined as the period of time between the start of the first state event and the completion of the National CCDC event. Participation on a team in any CCDC event during a given season counts as participation for that entire season.

   iii. A competitor in their final semester prior to graduation is exempt from the full-time student requirement and may compete in CCDC events as a part-time student provided the competitor has a demonstrated record of full-time attendance for the previous semester or quarter.

   iv. If a team member competes in a qualifying, state, or regional CCDC event and graduates before the next CCDC event in the same season, that team member will be allowed to continue to compete at CCDC events during the same season should their team win and advance to the next round of competition.

B. Competitors may only be a member of one team per CCDC season.

C. A team member may not participate in any role at CCDC events held outside the region in which their team competes during the same CCDC season.

D. Individuals who have participated in previous CCDC events in any role other than as a competitor must obtain eligibility approval from the director of the region in which their team competes prior to being added to the team roster. Once a candidate's eligibility has been approved they will remain eligible for all CCDC events during the same season.

2. Team Composition

A. Each team must submit a roster of up to 12 competitors to the competition director of the first CCDC event they participate in during a given CCDC competition season. Rosters must be submitted at least two weeks prior to the start of that event. All competitors on the roster must meet all stated eligibility requirements. No changes to the team roster will be permitted after the team competes in their first CCDC event. The competition team must be chosen from the submitted roster. A competition team is defined as the group of individuals competing in a CCDC event.

B. Each competition team may consist of up to eight (8) members chosen from the submitted roster.

C. Each competition team may have no more than two (2) graduate students as team members.

D. If the member of a competition team advancing to a qualifying, state, regional, or national competition is unable to attend that competition, that team may substitute another student from the roster in their place prior to the start of that competition.

E. Once a CCDC event has begun, a team must complete the competition with the team that started the competition. Substitutions, additions, or removals of team members are prohibited except for extreme circumstances.

   i. Team Representatives must petition the Competition Director in writing for the right to perform a change to the competition team.

   ii. The Competition Director must approve any substitutions or additions prior to those actions occurring.

F. Teams or team members arriving after an event's official start time, for reasons beyond their control, may be allowed to join the competition provided a substitution has not already been made. Event coordinators will review the reason for tardiness and make the final determination.

G. Each team will designate a Team Captain for the duration of the competition to act as the team liaison between the competition staff and the teams before and during the competition. In the event of the Team Captain's absence, teams must have an identified team liaison serving as the captain in the competition space at all times during competition hours.

H. An institution is only allowed to compete one team in any CCDC event or season.

3. Team Representatives

A. Each team must have at least one representative present at every CCDC event. The representative must be a faculty or staff member of the institution the team is representing.
B. Once a CCDC event has started, representatives may not coach, assist, or advise their team until the completion of that event (including overnight hours for multi-day competitions).
C. Representatives may not enter their team's competition space during any CCDC event.
D. Representatives must not interfere with any other competing team.
E. The representative, or any non-team member, must not discuss any aspect of the competition event, specifically event injections, configurations, operations, team performance or red team functions, with their team during CCDC competition hours and must not attempt to influence their team's performance in any way.

4. Competition Conduct

A. Throughout the competition, Operations and White Team members will occasionally need access to a team's system(s) for scoring, troubleshooting, etc. Teams must immediately allow Operations and White Team members' access when requested.
B. Teams must not connect any devices or peripherals to the competition network unless specifically authorized to do so by Operations or White Team members.
C. Teams may not modify the hardware configurations of competition systems. Teams must not open the case of any server, printer, PC, monitor, KVM, router, switch, firewall, or any other piece of equipment used during the competition. All hardware related questions and issues should be referred to the White Team.
D. Teams may not remove any item from the competition area unless specifically authorized to do so by Operations or White Team members including items brought into the team areas at the start of the competition.
E. Team members are forbidden from entering or attempting to enter another team's competition workspace or room during CCDC events.
F. Teams must compete without "outside assistance" from non-team members including team representatives from the start of the competition to the end of the competition (including overnight hours for multi-day events). All private communications (calls, emails, chat, texting, directed emails, forum postings, conversations, requests for assistance, etc) with non-team members including team representatives that would help the team gain an unfair advantage are not allowed and are grounds for disqualification and/or a penalty assigned to the appropriate team.
G. Printed reference materials (books, magazines, checklists) are permitted in competition areas and teams may bring printed reference materials to the competition.
H. Team representatives, sponsors, and observers are not competitors and are prohibited from directly assisting any competitor through direct advice,

"suggestions", or hands-on assistance. Any team sponsor or observers found assisting a team will be asked to leave the competition area for the duration of the competition and/or a penalty will be assigned to the appropriate team.

I. Team members will not initiate any contact with members of the Red Team during the hours of live competition. Team members are free to talk to Red Team members during official competition events such as breakfasts, dinners, mixers, and receptions that occur outside of live competition hours.

J. Teams are free to examine their own systems but no offensive activity against other teams, the Operations Team, the White Team, or the Red Team will be tolerated. This includes port scans, unauthorized connection attempts, vulnerability scans, etc. Any team performing offensive activity against other teams, the Operations Team, the White Team, the Red Team, or any global asset will be immediately disqualified from the competition. If there are any questions or concerns during the competition about whether or not specific actions can be considered offensive in nature contact the Operations Team before performing those actions.

K. Teams are allowed to use active response mechanisms such as TCP resets when responding to suspicious/malicious activity. Any active mechanisms that interfere with the functionality of the scoring engine or manual scoring checks are exclusively the responsibility of the teams. Any firewall rule, IDS, IPS, or defensive action that interferes with the functionality of the scoring engine or manual scoring checks are exclusively the responsibility of the teams.

L. All team members will wear badges identifying team affiliation at all times during competition hours.

M. Only Operations Team/White Team members will be allowed in competition areas outside of competition hours.

5. Internet Usage

A. Internet resources such as FAQs, how-to's, existing forums and responses, and company websites, are completely valid for competition use provided there is no fee required to access those resources and access to those resources has not been granted based on a previous membership, purchase, or fee. Only resources that could reasonably be available to all teams are permitted. For example, accessing Cisco resources through a CCO account would not be permitted but searching a public Cisco support forum would be permitted. Public sites such as Security Focus or Packetstorm are acceptable. Only public resources that every team could access if they chose to are permitted.

B. Teams may not use any external, private electronic staging area or FTP site for patches, software, etc. during the competition. Teams are not allowed to access private Internet-accessible libraries, FTP sites, web sites, network storage, email accounts, or shared drives during the competition. All Internet resources used during the competition must be freely available to all other teams. The use of external collaboration and storage environments such as Google Docs/Drive is prohibited unless the environment was provided by and is administered by competition officials. Accessing private staging areas or email accounts is grounds for disqualification and/or a penalty assigned to the appropriate team.

C. No peer to peer or distributed file sharing clients or servers are permitted on competition networks unless specifically authorized by the competition officials.
D. Internet activity, where allowed, will be monitored and any team member caught viewing inappropriate or unauthorized content will be subject to disqualification and/or a penalty assigned to the appropriate team. This includes direct contact with outside sources through AIM/chat/email or any other public or non-public services including sites such as Facebook. For the purposes of this competition inappropriate content includes pornography or explicit materials, pirated media files, sites containing key generators and pirated software, etc. If there are any questions or concerns during the competition about whether or not specific materials are unauthorized contact the White Team immediately.
E. All network activity that takes place on the competition network may be logged and subject to release. Competition officials are not responsible for the security of any information, including login credentials, which competitors place on the competition network.

6. Permitted Materials

A. No memory sticks, flash drives, removable drives, CDROMs, electronic media, or other similar electronic devices are allowed in the room during the competition unless specifically authorized by the Operations or White Team in advance. Any violation of these rules will result in disqualification of the team member and/or a penalty assigned to the appropriate team.
B. Teams may not bring any type of computer, laptop, tablet, PDA, cell phone, smart phone, or wireless device into the competition area unless specifically authorized by the Operations or White Team in advance. Any violation of these rules will result in disqualification of the team member and/or a penalty assigned to the appropriate team.
C. Printed reference materials (books, magazines, checklists) are permitted in competition areas and teams may bring printed reference materials to the competition as specified by the competition officials.

7. Professional Conduct

A. All participants, including competitors, coaches, White Team, Red Team, Ops Team, and Gold Team members, are expected to behave professionally at all times during all CCDC events including preparation meetings, receptions, mixers, banquets, competitions and so on.
B. In addition to published CCDC rules, Host Site policies and rules apply throughout the competition and must be respected by all CCDC participants.
C. All CCDC events are alcohol free events. No drinking is permitted at any time during competition hours.

D. Activities such as swearing, consumption of alcohol or illegal drugs, disrespectful or unruly behavior, sexual harassment, improper physical contact, becoming argumentative, willful violence, or willful physical damage have no place at the competition and will not be tolerated.
E. Violations of the rules can be deemed unprofessional conduct if determined to be intentional or malicious by competition officials.
F. Competitors behaving in an unprofessional manner may receive a warning from the White Team, Gold Team, or Operations Team for their first offense. For egregious actions or for subsequent violations following a warning, competitors may have a penalty assessed against their team, be disqualified, and/or expelled from the competition site. Competitors expelled for unprofessional conduct will be banned from future CCDC competitions for a period of no less than 12 months from the date of their expulsion.
G. Individual(s), other than competitors, behaving in an unprofessional manner may be warned against such behavior by the White Team or asked to leave the competition entirely by the Competition Director, the Operations Team, or Gold Team.

8. Questions, Disputes, and Disclosures

A. PRIOR TO THE COMPETITION: Team captains are encouraged to work with the Competition Director and their staff to resolve any questions regarding the rules of the competition or scoring methods before the competition begins.
B. DURING THE COMPETITION: Protests by any team must be presented in writing by the Team Captain to the White Team as soon as possible. The competition officials will be the final arbitrators for any protests or questions arising before, during, or after the competition. Rulings by the competition officials are final. All competition results are official and final as of the Closing Ceremony.
C. In the event of an individual disqualification, that team member must leave the competition area immediately upon notification of disqualification and must not re-enter the competition area at any time. Disqualified individuals are also ineligible for individual or team awards.
D. In the event of a team disqualification, the entire team must leave the competition area immediately upon notice of disqualification and is ineligible for any individual or team award.
E. All competition materials including injects, scoring sheets, and team-generated reports and documents must remain in the competition area. Only materials brought into the competition area by the student teams may be removed after the competition concludes.

9. Scoring

A. Scoring will be based on keeping required services up, controlling/preventing un-authorized access, and completing business tasks that will be provided throughout the competition. Teams accumulate points by successfully completing injects and maintaining services. Teams lose points by violating service level agreements, usage of recovery services, and successful penetrations by the Red Team.

B. Scores will be maintained by the competition officials and may be shared at the end of the competition. There will be no running totals provided during the competition. Team rankings may be provided at the beginning of each competition day.

C. Any team action that interrupts the scoring system is exclusively the responsibility of that team and will result in a lower score. Any team member that modifies a competition system or system component, with or without intent, in order to mislead the scoring engine into assessing a system or service as operational, when in fact it is not, may be disqualified and/or the team assessed penalties. Should any question arise about scoring, the scoring engine, or how scoring functions, the Team Captain should immediately contact the competition officials to address the issue.

D. Teams are strongly encouraged to provide incident reports for each Red Team incident they detect. Incident reports can be completed as needed throughout the competition and presented to the White Team for collection. Incident reports must contain a description of what occurred (including source and destination IP addresses, timelines of activity, passwords cracked, access obtained, damage done, etc), a discussion of what was affected, and a remediation plan. A thorough incident report that correctly identifies and addresses a successful Red Team attack may reduce the Red Team penalty for that event – no partial points will be given for incomplete or vague incident reports.

10. Remote/ Team Site Judging and Compliance

With the advent of viable remote access technologies and virtualization, teams will have the ability to participate in CCDC events from their respective institutions. This section addresses policy for proper engagement in CCDC events for remote teams.

A. One or more Remote Site Judge(s) must be assigned to the team site. At least one Remote Site Judge must be present at the remote site for the duration of the event in order to facilitate the execution of the CCDC. The qualifications of Remote Site Judge are the same as Event Judge. Subject to the specifications of the remote competition, the responsibilities of the Remote Site Judge may include the following:

   i. Be present with the participating team to assure compliance with all event rules
   ii. Provide direction and clarification to the team as to rules and requirements
   iii. Establish communication with all Event Judges and provide status when requested
   iv. Provide technical assistance to remote teams regarding use of the remote system
   v. Review all equipment to be used during the remote competition for compliance with all event rules

vi. Assure that the Team Captain has communicated to the Event Judges approval of initial system integrity and remote system functionality
vii. Assist Event Judges in the resolution of grievances and disciplinary action, including possible disqualification, where needed
viii. Report excessive misconduct to local security or police
ix. Assess completion of various injects based on timeliness and quality when requested by Event Judges
x. Act as a liaison to site personnel responsible for core networking and internet connectivity
xi. Provide direct technical assistance to teams when requested by Event Judges
xii. Provide feedback to students subsequent to the completion of the CCDC event

B. A recommendation for Remote Site Judge(s) is expected to be given from a Team representative of the participating institution to the CCDC Event Manager. Remote Site Judge(s) must not be currently employed, a student of, or otherwise affiliated with the participating institution, other than membership on an advisory board. CCDC Event Managers should also be apprised of a contact from the participating institution responsible for core networking and internet connectivity that will be available during the CCDC event. Remote teams are required to compete from a location with controlled access, i.e., a separate room or a portion of a room that is dedicated for use during the CCDC event. Workstations and internet access must comply with published requirements.

Northeastern Regional Competition Rules

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

Software Use

EULA violations are considered a serious offense and may result in disqualification:

i. No personal-only use or non-commercial trial software is allowed.
ii. Commercial trials or free use software (e.g. Apache License, GPL) are allowed.

Team Substitutions

Team are allowed to have 10 students named to their roster but only 8 can compete on a given day. Each day before the competition's start teams can declare up to 8 students who could compete for that day and no further substitutions will be allowed for that day.

Service Level Agreement

Physically disconnecting or powering-off of team network infrastructure is seen as a serious offense and will result in a point penalty roughly equivalent to 4 hours of downtime.

i. Reloading of network infrastructure requires notification and approval prior to service disruption.
ii. This policy extends to physical network connections for individual server systems.

Scoring Methodology

Final scores will be awarded using the following point distribution:

40%	Functional service uptimes and SLA violations as measured by the scoring engine.
40%	Successful completion of inject scenarios through the ISE.
20%	Incident Response and Red Team Activity

A system restore service is available to teams. This service has a minimum of 15 minutes lead time and could take 30 minutes. There will be a **penalty of 5% per restoration** against the final score for the service(s) restored.

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