

2015 Southeast Collegiate Cyber Defense Qualification Competition (SECCDQC)



**Qualification Competition
Team Packet
DRAFT**

**For March 7, 2015 &
March 14, 2015**

Includes Materials © CSSIA 2015, © SECCDC 2015 and © National CCDC

Table of Contents

Contents

Southeast CCDC Mission and Objectives	3
Qualification Overview	3
Competition Goals	3
Competition Team Structure	3
Competition Rules.....	5
2015 Rules.....	5
Initial Connection & the Start Flag.....	13
Network & Team Site Description	17
EMAIL System Client Configuration	18
Schedule - Times are EST	22
www.halcorp.biz Document Repository.....	22
Systems	23
Competition Rules: Acknowledgement & Agreement	23
Competition Scoring	24
Functional Services	25
Business Tasks.....	25
Questions and Disputes	26
Aftermath.....	26
Competition Topology	27
Connection Testing	29
Team Competition Dates	29
Sponsors:.....	30
Appendix - Addressing Access Problems to NETLAB+™ Systems	31

Southeast CCDC Mission and Objectives

The Southeast Collegiate Cyber Defense Qualifying Competition (SECCDC) provides an opportunity for qualified educational institutions in the Southeast to compete as part of the national CCDC organization (see www.nationalccdc.org) to provide a unified approach across nine regions of the country. Qualified educational institutions include those with information assurance or computer security curricula. The Southeast 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 Southeast Collegiate Cyber Defence Qualification Competition (SECCDQC) is coordinated by the KSU Coles Center for Information Security Education (CISE), and operated using infrastructure and resources provided by the Center for Systems Security and Information Assurance (CSSIA) at Moraine Valley Community 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 services: a web site, a secure web site, an email server, a database server, an online curriculum server, and workstations used by simulated sales, marketing, and research staff as 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-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 top eight (8) qualifying teams from the 2015 SECCDQC will have the opportunity to participate in the 2015 Southeast Regional CCDC (SECCDC), April 7 & 8, 2015, at Kennesaw State University.

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 Structure

- **Blue Team** – A 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 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 – Dr. Whitman.

- 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 and SECCDC Regional rules apply; www.nationalccdc.org
- **Red Team** – Professional network penetration testers from industry approved by the competition director and industry representatives
 - 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 judges, remote site 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.
 - Judges will assess the competition team's ability to maintain their network and service availability based upon a business inject and a scoring instrument, delivering inject scenarios, scoring of injects, creating log entries, securing log files, issuing or controlling the timing of injects, etc. White Team members present in the competition room will assist judges by observing teams, confirming proper inject completion, report issues, and assure compliance of rules and guidelines.
- **Gold Team** – Comprised of the Competition Manager, the host site Chief Administrator, as well as representatives from industry and academia who make up the administration team both in planning and during the exercises. Responsibilities include, but are not limited to,
 - Administration and staffing of the cyber defense competition
 - Works with industry partners to orchestrate the event
 - Has the authority to dismiss any team, team member, or visitor for violation of competition rules, inappropriate or unprofessional conduct
 - Makes provision for awards and recognition
 - Manages debrief to teams subsequent to the conclusion of the competition
 - Serves as the final authority on scoring decisions or issues relating to equity or fairness of events or activities
 - Cannot be from any institution that has a competing Blue team or have any interest in any team outcome
 - Ideally, should be a representative from industry or law enforcement
 - Final authority of all judging decisions, including assessment of final scores and winners of the competition

- **Black Team** – Tech support and hospitality – assists with any technical needs necessary to maintain the integrity of the competition. Assists with ancillary functions – greeters, food service, local directions.

Competition Rules

Notes:

- These rules reflect the National CCDC Rules committee review of all rules, and are effective as of the date of this packet.
- SECCDC Specific rules are clearly marked and prefaced with SECCDC.
- SECCDQC (Qualification) competition rules are clearly marked and prefaced with SECCDQC.

Introduction

The following Rules apply to institutions competing in the Southeast Collegiate Cyber Defense Competition and are based on, and reflect changes made to, the National Collegiate Cyber Defense Competition as of January 2015. Updates will be provided as available.

All institution teams, including student competitors and university representatives, must comply with these rules. Failure to do so can result in penalties ranging from points against the team, individual or team disqualification, individual or team expulsion, individual or team suspension or banishment from future competitions, to law enforcement involvement.

All individuals associated with the competition must sign a compliance agreement and disclosure waiver prior to being allowed to attend the competition.

Areas where the SECCDC rules differ from the National CCDC rules are highlighted in italics. Some rules are duplicated for emphasis.

2015 Rules

The following are the approved national rules for the 2015 CCDC season. Please refer to the official rules for your specific CCDC event for any local variations.

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. (*SECCDC: a.k.a. Room Judges*)
- 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.

NEW RULES FOR 2015 SECCDC ARE 1.c. and 1.d.

Minor revisions to 2.a.i.

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. 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.
 - i. *SECCDC Supplemental Rule: Final team rosters are due to the SECCDC Competition organizers at least 72 hours prior to the start of the SECCDQC (the Virtual Prequalification Competition), however changes may be WITHIN the roster up through the start of the competition, and between events as needed. Local Room Judges information must be provided at least 2 weeks prior to the SECCDQC.*
- 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.

- i. *SECCDC Supplemental Rule: During a competition, only the Team Captain, or in the Captain's absence the Co-Captain, may interact with the White Team, unless a team member has specifically been approached by the White Team. All correspondence, questions or issues must follow this chain of command Team Captain (or Co-Captain) to White Team to Gold Team/Operations. Violation of this chain of command MAY result in a points penalty against the competition team.*
- ii. *SECCDC Supplemental Rule: All questions regarding the competition organization, its systems and operations, including responses to competition injections, should be addressed to the competition organization's chief information officer. Questions regarding the competition or its rules should be addressed to competition officials. Violation of this separation of duties MAY result in a points penalty against the competition team.*
- 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.
 - i. *SECCDC Supplemental Rule: The institutional representative must remain in the area designated during competition hours. Should the institutional representative need to leave the competition area, they must ensure that they notify the operations center and leave a contact number in case of emergencies.*

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.
 - i. *SECCDC Supplemental Rule: For technical support, such as a system reset, Black team members will require access to systems. These individuals will only be allowed access if accompanied or specifically authorized by a Gold Team/Operations or White Team member.*
 - ii. *SECCDC Supplemental Rule: For the qualification competition, the local judge may inspect all systems for rules compliance at any time before, during or after the competition.*
- 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.
 - i. *SECCDC Supplemental Rule: If a competition team is provided with supplemental equipment in the competition room, and that equipment is specifically designated as support for the team's competition efforts, it is preauthorized for connection to the competition network and systems (e.g. USB hard drive, flash drive, printer).*
 - ii. *SECCDC Supplemental Rule: For the qualification competition, the host institution may stage replacement equipment in the competition rooms. This equipment cannot be used until authorized by SECCDC competition officials, after the team reports a systems failure and has*

made every effort to recover the initial equipment. Once authorized, the local judge will supervise the installation of replacement equipment, and inspect it for unauthorized materials prior to allowing it to be used by the local team.

- 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.
 - i. *SECCDC Supplemental Rule: This includes items brought into the competition rooms by the Blue teams 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.
 - i. *SECCDC Supplemental Rule: Each team is restricted to two (2) standard business file boxes (approx. 12 x 12 x 18) of hard copy/printed material. Refer also to rule 4.d. and 4.d.i.*
- 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. *SECCDC Supplemental Rule: Team representatives, sponsors, and observers are prohibited from entering team areas without direct supervision of the Competition officials (Gold Team). Institutions wishing to photograph students during the competition must be escorted by a Gold Team representative, and must photograph the team from outside the competition area. For the qualification competitions Institutions may "stage" competition photographs before or after the competition hours. For the onsite competition, an official event photographer (Black team) will take pictures of all teams and make them available after the competition.*
- 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.
 - i. *SECCDC Supplemental Rule: For the SECCDC on-site regional competition, all Internet access is by proxy server. In order to access any external Web site, Blue Teams must submit a candidate proxy list at least 2 weeks prior to the competition. This list will be reviewed, and only authorized sites added to the proxy list.*
 - ii. *SECCDC Supplemental Rule: Once the competition has started, additions to the proxy list may be requested via a properly formatted request to the CIO.*
 - iii. *SECCDC Supplemental Rule: The proxy list will not be shared with any competition team. If a team wishes to access a particular site, they must request it in advance. Support sites for operating systems used during the competition will be pre-configured in the Proxy Server. Teams will be notified of these sites.*
 - iv. *SECCDC Supplemental Rule: For the Qualification competition, Internet access will be monitored and enforced by local judges.*
- 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.
 - i. *SECCDC Supplemental Rule: For the onsite regional, all event logs are subject to public review and release subsequent to the following conditions: Should a competition team desire to view their own logs, the Team Representative may submit a request to competition officials after the competition has ended. Teams desiring to review the logs from other teams must submit a valid, legitimate reason in order to gain access.*

- ii. *SECCDC Supplemental Rule: Competition logs may be provided to external entities for non-profit research and investigation, if a legitimate request is received within 60 days of the competition.*
- iii. *SECCDC Supplemental Rule: All logs will be destroyed 60 days after the competition.*

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.
 - i. *Supplemental SECCDC Rule: All cellular calls, texts, smart phone usage, and so on must be made and received/viewed outside of the team's competition space and must not be used to receive outside assistance.*
 - ii. *Supplemental SECCDC Rule: For the qualification competition, should the team representative desire to provide USB flash drives for the team's use they must notify the Competition Director in advance, and attest that the devices were wiped clean prior to the completion, and only issued after the start of the competition.*
- 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.
 - i. *SECCDC Supplemental Rule: For the qualification competition, all equipment to be used for the competition must be the property of the host institution. No student owned or supplied equipment may be connected to local systems or the competition networks. The team representative and local judge will inspect the local systems and attest to their status.*
- 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.
 - i. *SECCDC Supplemental Rule: (See Rule 4.g. for restrictions on the quantity of printed materials which may be brought into the competition area).*
- d. *SECCDC Supplemental Rule: If a competition team member with a documented disability requires special equipment to compete, the Team Representative must notify competition officials at least 30 days prior to the competition to facilitate the evaluation and authorization of needed equipment. Failure to do so MAY result in the student team member not being able to use the needed equipment during the competition.*

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.**
 - i. *SECCDC Supplemental Rule: White team members will notify the Gold Team of a protest immediately and forward ALL formally submitted protests from the Team Captain for review and arbitration.*
 - ii. *SECCDC Supplemental Rule: Any team representative that approaches a competition official during the competition to register a complaint or protest on behalf of their competition team will be asked to leave the competition area.*
- 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.
- f. *SECCDC Supplemental Rule: AFTER THE COMPETITION: any team member that behaves unprofessionally in their public comments about the event may be prohibited from competing in future CCDC events and/or referred to their host institutions for student misconduct.*

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 intention, 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 **properly formatted** 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.

- i. *SECCDC Supplemental Rule: incident reports must use the specified format, and must be submitted within 2 hours of the incident in order to receive any reduction in Red Team penalty.*
- ii. *SECCDC Supplemental Rule: Some incidents are “seeded” throughout SECCDC equipment, such as planted malware or inappropriate material. Since these Incident reports are not directly affiliated with a Red Team action, these incident reports are scored and points earned added to the team’s total, UNLESS they correspond to a graded injection, in which case any modification of scoring will be made to that injection.*

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. 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.
- b. 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 (*SECCDC: before and*) 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
- c. 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.

11. Local Competition Rules

The local competition rules section is unique to each specific CCDC competition. Please refer to the official rules for

your CCDC event for more information.

Initial Connection & the Start Flag

The 2015 SECCDC Qualifying Event will use the Cyber Stadium powered by NETLAB⁺.

Using the Cyber Stadium to compete is simple and straightforward. There are two separate systems that are used which interact to provide the services and communication necessary to meet the goals of the SECCDC.

System 1 - ISE (Inject Scoring System)/Team Portal - This system is totally separate from the competition environment and is used by Blue Teams to display current services, as viewed by the indigenous scoring engine, communicate to the White Team, and receive notifications.

NOTE: THIS SYSTEM WILL NOT BE USED FOR INJECTIONS - ONLY COMPETITION SUPPORT (TROUBLE TICKETS/SERVICE STATUS).

This system is accessed via a browser,

ccdcadmin1.morainevalley.edu

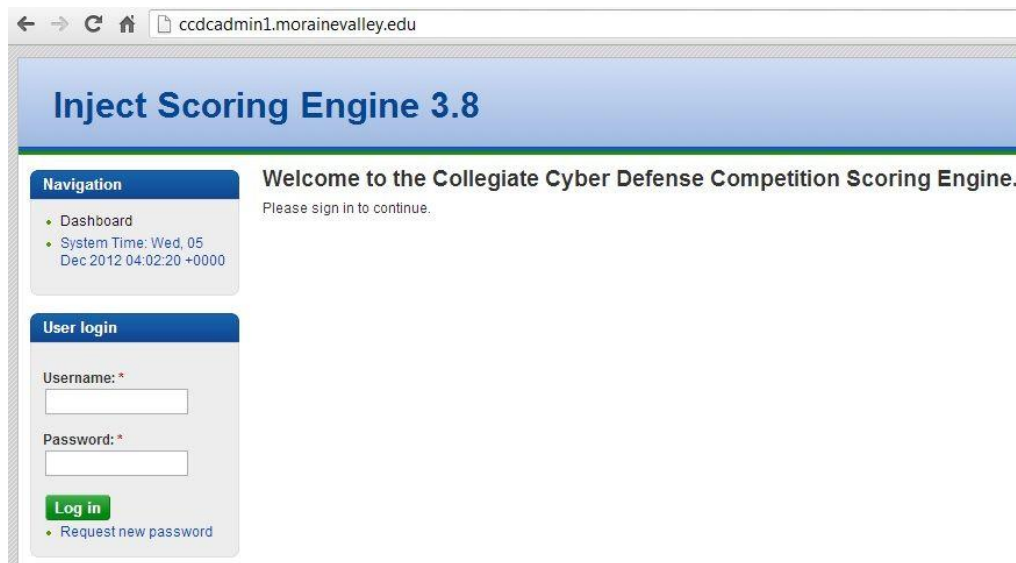
Note that CSSIA supports additional ISE/Team Portals,

ccdcadmin2.morainevalley.edu

ccdcadmin3.morainevalley.edu

ccdcadmin4.morainevalley.edu

Follow the instructions from your competition manager for the specific ISE/Team Portal that will be used for your CCDC Qualifier. You will be emailed the connection address for COMPETITION SYSTEMS on the morning of the competition, and credentials prior to the competition. You will be allowed to test your connection to the competition network at least a week prior to the competition.



The screenshot shows a web browser window with the address bar displaying 'ccdcadmin1.morainevalley.edu'. The page title is 'Inject Scoring Engine 3.8'. The main content area has a blue header with the title. Below the header, there is a 'Navigation' sidebar on the left with links to 'Dashboard' and 'System Time: Wed, 05 Dec 2012 04:02:20 +0000'. The main content area has a 'Welcome to the Collegiate Cyber Defense Competition Scoring Engine.' message and a 'Please sign in to continue.' prompt. Below this is a 'User login' section with fields for 'Username: *' and 'Password: *', a 'Log in' button, and a link to 'Request new password'.

Students should login to the ISE first to initiate communication with the competition staff. There is one account per team that may be used to connect to the ISE where multiple logins using the same account is permissible. The accounts are,

team1 (team.a), team2 (team.b), team3 (team.c),

The team password required to access the ISE is distributed, along with team assignment, by a competition manager prior to the scheduled start of the competition. When first connecting to the ISE, a member of the team should check for an initial communications, usually identified as “Welcome” or something similar. The task simply sends a response back to the competition coordinators, signaling that access to the ISE has been successful, and that the responding team is ready to compete.

At the same time the team must email operations@seccdc.org using the competition email system to indicate they are online and ready to compete.

Once the competition staff has verified that all teams are ready to compete, or have provided ample time to respond, the competition staff will forward an email, providing the team password (applicable to all accounts for a particular team) required to access...

System 2 - The NETLAB⁺ / myVLAB Competition Stadium system used to access and manage the competition network. This too is accessed via a browser,

myvlab1.morainevalley.edu



Client requirements for the Blue Team workstations must conform to NDG guidelines. See, <http://www.netdevgroup.com/products/requirements/>

Generally the client requirements are easily met with simple browser and java plug-in. The bandwidth requirement is 256 kb/s up and down per client minimum. Ports 80, 2201 must be allowed outbound. A 10 Mb/s minimum synchronous service is recommended.

It is the responsibility of each participating school to assure that client requirements are met, and that proper internet service is provided.

NISGTC Virtualization Center

myVLAB 1

myVLAB1 @ Moraine Valley Community College

**Virtual Labs supported by Department of Labor
TAACCCT Grant #TC-22525-11-60-A-48**

To access, you need a user ID and password, assigned by your instructor or local system administrator.

Personal firewall software can interfere with this application. If you experience login or port test failures, please disable your firewall software to determine if this is causing the problem.

Browser security settings can interfere with required features. It is recommended that you add the IP address (or host name) of this site to your browser's trusted site list. This application uses Java™, JavaScript, Cookies, Popup Windows, and IFRAMES. Please adjust your browser settings accordingly.


Username

Password

Login

[Forgot Password?](#)

POWERED BY



Experience has shown that access problems may persist even though nominal client requirements are met. Certain combinations of OS/browser/java work better than others. Teams should experiment during times provided ahead of the competition to "tune" their clients for optimal operation, and assure that their local network properly supports the NETLAB+™ environment.

For more guidance towards addressing connectivity issues to the myVLAB environment, see the Appendix - Addressing Access Problems to NETLAB+™ Systems, at the end of this document.

There are eight accounts per team that may be used to connect to the Cyber Competition Stadium. For team1 (Team.A) they are,

v1u1, v1u2, v1u3,, v1u8

Accounts for other teams follow the same pattern. For team2 (Team.B) the accounts are,

v2u1,

Once authenticated you will be asked to change your password and confirm a few details regarding your profile. Remember your new password! Subsequently you should see a lab reservation for your competition network, similar to the following:

ID	Date /Time	Description	Pod
9264	NOW Fri Jan 17, 2014 3:44PM - Thu Jan 23, 2014 5:00PM	Team M: vTeam 13 User 1, vTeam 13 User 2, vTeam 13 User 3, vTeam 13 User 4, vTeam 13 User 5, vTeam 13 User 6, vTeam 13 User 7, vTeam 13 User 8 Class: .CCDC State 2014 CCDC 2014	CCDC 2014 Team 13 CCDC Team Pod
	ENTER LAB		

Each team member can click on '**ENTER LAB**' for their respective lab/pod reservation to gain access to their competition network. The competition network topology, shown later in this document, should be clearly visible. Access individual VMs simply by clicking on them.

When leaving the myVLAB environment, **DO NOT CLICK I'M DONE**. This will end your reservation, and shut down your systems. Upon rescheduling, your systems will revert back to the initial state of the competition.

NISGTC Virtualization Center

myVLAB 1



Lab Access

MyNETLAB Logout

 ddurkee

CCDC 2014 Team 13 4356 minutes remaining

I'M DONE

Topology

Action

Status

Connections

CCDC 2014

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.
- Each competition network will therefore be physically and logically isolated from the hosting organization's network.
- Each competing Blue Team will be provided a set of workstations at a host site that are logically and physically isolated from other Blue Teams in order to access respective remote competition networks via the internet. Alternatively, Blue Teams may compete from their own institution, in which case their institution must provide workstations in conformance with aforementioned requirements. 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 a trouble ticket and response application, the ISE/Team Portal, residing at Moraine Valley Community College.
- Red Team activity may be either externally or internally sourced with respect to the remote competition network. At no time will the Red Team have access outside the remote NETLAB+™ environment.
- Each Blue Team network will be monitored by a scoring system operating within the remote network. An indication of services, as viewed by the indigenous scoring engine, will be made available to each Blue Team via the ISE/Team Portal.
- 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 Director.

EMAIL System Client Configuration

The SECCDC uses an external email system “@seccdc.org” to coordinate all communications to/from the teams and judges. Teams need simply access and log into the Web based email client to ensure effective communications and the receipt of competition injections.

These instructions are provided to allow teams and judges to connect to the competition email server for the purposes of exchanging information related to the 2015 SECCDC Preliminary Qualification Competition. The accounts provided are to be used exclusively for the competition and should not be used to communicate to accounts other than the addresses provided.

Once configured team and judges MUST NOT change the passwords associated with the accounts. These accounts are monitored and logged from competition operations. Any modification to the accounts other than those listed in this document MAY result in teams and judges not receiving critical communications and could result in Teams receiving points penalties.

Standard SECCDC Email Accounts: (Feel free to add these to your address book, once you have logged into and configured your team’s email account).

team.X@seccdc.org (where X=the team letter e.g. team.a, team.b...)

judge.X@seccdc.org (where the Judge’s letter matches the team’s letter)

operations@seccdc.org (SECCDC Operations account used to communicate with Judges, teams should only use when real-world issues affect their competitive status (Emergency in building or with team), or when submitting a requested email check,

hal.cio@seccdc.org (HAL’s CIO – used for all team questions that are “in-game”

hal.ciso@seccdc.org (HAL’s CISO – used to send and receive work assignments to/from the team. Note this email account is not directly monitored, only archived. The “Automatic CC” setup described below ensures a copy of all work assignment and your team’s response go to your local Judge who verifies the work has been accomplished and assigns a score (Full Credit, Partial Credit, No Credit). Points are then assigned by Operations, and revealed after all teams have competed.

hal.change@seccdc.org (HAL’s Chief Change Officer (CCO) used for questions regarding change management logs, activities and related issues.

NOTE: In order to avoid teams accidentally “Replying to All” and sending their work assignments to other teams, all emails will come FROM hal.ciso@seccdc.org, and be addressed TO: hal.cio@seccdc.org, with all teams and judges blind carbon copied (BCC). Teams will still treat each memo/email as if it were addressed directly “TO” them. If teams properly configure the “Automatically CC to Address(es):” as described here, your judge will still get a copy of your work. Make sure you are replying to hal.ciso@seccdc.org when responding, and attach your work product in a properly formatted memo.

Initial Log-in and Configuration

1. Using a Web browser go to www.seccdc.org/sm to access the SquirrelMail client.
2. Enter your team username and password. Note: all teams use a standardized username and password:
 - a. Username: team.X
 - b. Password: team.X.#### (where #### is a unique 4 digit code assigned to the team). This will be given to the institutional reps approximately one week prior to the team’s competition date.
3. You will see the primary SM client:

Folders
Last Refresh:
Thu, 8:28 pm
(Check mail)

INBOX
INBOX.Drafts
INBOX.Sent
INBOX.Trash

Show Notify Popup

Current Folder: **INBOX** [Sign Out](#)

[Compose](#)
[Addresses](#)
[Folders](#)
[Options](#)
[Search](#)
[Help](#)
[SquirrelMail](#)

[Toggle All](#)
Viewing Messages: 1 to 2 (2 total)

Move Selected To:

INBOX
Move
Forward

Transform Selected Messages:

Read
Unread
Delete

From	Date	Subject
<input type="checkbox"/> HAL CISO	Thu, 6:40 pm	Test
<input type="checkbox"/> SECCDC Operations	Thu, 6:38 pm	Test

[Toggle All](#)
Viewing Messages: 1 to 2 (2 total)

4. First, configure a few basic options as shown: Select **Options**, then **Personal Information**, then configure as shown:

Folders
Last Refresh:
Sat, 12:21 pm
(Check mail)

INBOX
INBOX.Drafts
INBOX.Sent
INBOX.Trash

Show Notify Popup

[Compose](#)
[Addresses](#)
[Folders](#)
[Options](#)
[Search](#)
[Help](#)
[SquirrelMail](#)

Options - Personal Information

Name and Address Options

Full Name: Team X (State University)

E-mail Address: team.x@seccdc.org

Reply To:

Signature:

Ima Student
Captain,
HAL Team X
(State University)

All emails used in the seccdc.org email system are in support of the SECCDC academic competition. They do not represent a real-world organization.

Multiple Identities: [Edit Advanced Identities](#) (discards changes made on this form so far)

Timezone Options

Your current timezone: Same as server

Reply Citation Options

Reply Citation Style: No Citation

User-Defined Citation Start:

User-Defined Citation End:

Signature Options

Use Signature: ☒

Prefix Signature with '--' Line: ☒

Additional CC address(es) for all messages: judge.X@seccdc.org

Additional BCC address(es) for all messages:

Submit

5. **NOTE: A FAILURE TO ENTER YOUR JUDGES EMAIL IN THE "ADDITIONAL CC ADDRESS(ES) FOR ALL MESSAGES" FIELD MEANS YOUR JUDGE DOESN'T GET YOUR REPORTS, WHICH MEANS YOUR TEAM DOES RECEIVE CREDIT FOR ANY WORK ASSIGNMENTS!**
6. Submit your changes.
7. While still in the **Options** page, select **Display Preferences**. Configure as shown:

Folders
Last Refresh:
Sat, 12:21 pm
(Check mail)

INBOX
INBOX.Drafts
INBOX.Sent
INBOX.Trash

Show Notify Popup

[Compose](#) [Addresses](#) [Folders](#) [Options](#) [Search](#) [Help](#) [Sign Out](#) [SquirrelMail](#)

Options - Display Preferences

General Display Options

Theme:

Custom Stylesheet:

Language:

Use Javascript:

Mailbox Display Options

Number of Messages per Page:

Enable Alternating Row Colors: ☒

Enable Page Selector: ☒

Maximum Number of Pages to Show:

Always Show Full Date: ☐

Length of From/To Field (0 for full):

Length of Subject Field (0 for full):

Show Message Preview Pane: ☒

Split Preview Pane Vertically: ☐

Message Preview Pane Size:

Always Refresh Message List: ☒

When Using Preview Pane: ☒

8. You may select a color theme as you desire.
9. **Display Preferences** continued here:

Folders
Last Refresh:
Sat, 12:21 pm
(Check mail)

INBOX
INBOX.Drafts
INBOX.Sent
INBOX.Trash

Show Notify Popup

Options - Message Display and Composition

Wrap Incoming Text At:

Width of Editor Window:

Height of Editor Window:

Location of Buttons when Composing:

Address Book Display Format:

Format of Addresses Added From Address Book:

Show HTML Version by Default: ☒

Enable Forward as Attachment: ☒

Include Me in CC when I Reply All: ☒

Enable Mailer Display: ☒

Display Attached Images with Message: ☐

Enable Printer Friendly Clean Display: ☐

Enable Mail Delivery Notification: ☒

Compose Messages in New Window: ☒

Width of Compose Window:

Height of Compose Window:

Prepend Signature before Reply/Forward Text: ☐

Strip signature when replying: ☐

Prefix for Original Message when Replying:

Cursor Position when Replying:

Sort by Received Date: ☒

Folders
Last Refresh:
Sat, 12:31 pm
(Check mail)

INBOX
INBOX.Drafts
INBOX.Sent
INBOX.Trash

[Show Notify Popup](#)

Address Autocompletion

Search Contacts As You Type: ☒

Only Search Personal Contacts: ☐

Pre-load Contacts: ☒ (Faster lookup but slower loading)

Match Case: ☐

Match Only Beginning Of Contact Fields: ☐

Search Contact Nicknames: ☒

Search Contact Full Names: ☒

Search Contact Email Addresses: ☒

Number Of Characters Typed To Trigger Search:

Select Contact Upon Tab Press: ☒

Default Email Composition Format: ☐ Plain Text ☒ HTML


Only Reply In HTML When Viewing HTML Format: ☐ Yes ☒ No (Always Attempt To Reply In HTML)

Only Allow Unsafe Images In HTML Replies When Viewing Unsafe Images: ☒ Yes ☐ No (Always Include Unsafe Images)

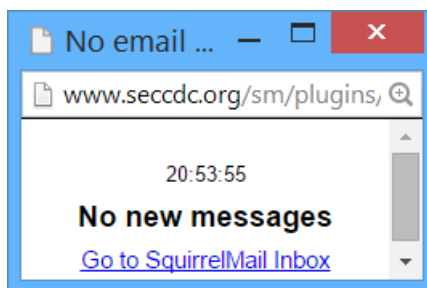
Notify Popup Options

New mail check period (minutes):

Play sound: ☒



10. Submit your changes. Note: you may need to log out and back into your email account for some options to activate.
11. Note the email times are by default set to the server time which is Eastern Standard Time (EST). When your team receives an email you should see a simple popup and hear a sound, which you can click to go into your Inbox. Note: First click the **"Show Notify Popup"** text on the left side of the email page and look for a pop-up blocked symbol next to the URL. Allow popups from www.seccdc.org if you see one. Sometimes this works, sometimes not – it is the team's responsibility to monitor their email account for incoming messages/assignments.



12. Once the account is configured, send an email to operations@seccdc.org to verify connectivity. Someone will respond as soon as possible.
13. During the competition, multiple team members may log into and monitor your email account simultaneously. If you are unable to access the email account during pre-competition testing, use another account to send to infosec@kennesaw.edu with detailed descriptions of your error messages.

Do not use other email accounts during the competition, nor are you allowed to forward seccdc.org messages to outside email accounts.

Schedule - Times are EST

Saturday 7 & 14 March 2015

9:00am	Team judges review competition systems to ensure within rules. Once judges are finished, teams allowed to access remote system; Teams send a “ready” email to operations@seccdc.org and receive competition system account information, as needed.
9:30am	Team access the ISE/Team Portal and respond to any information requests
10:00am	Start of Competition; scoring begins
6:00pm	Competition ends/Scoring ends

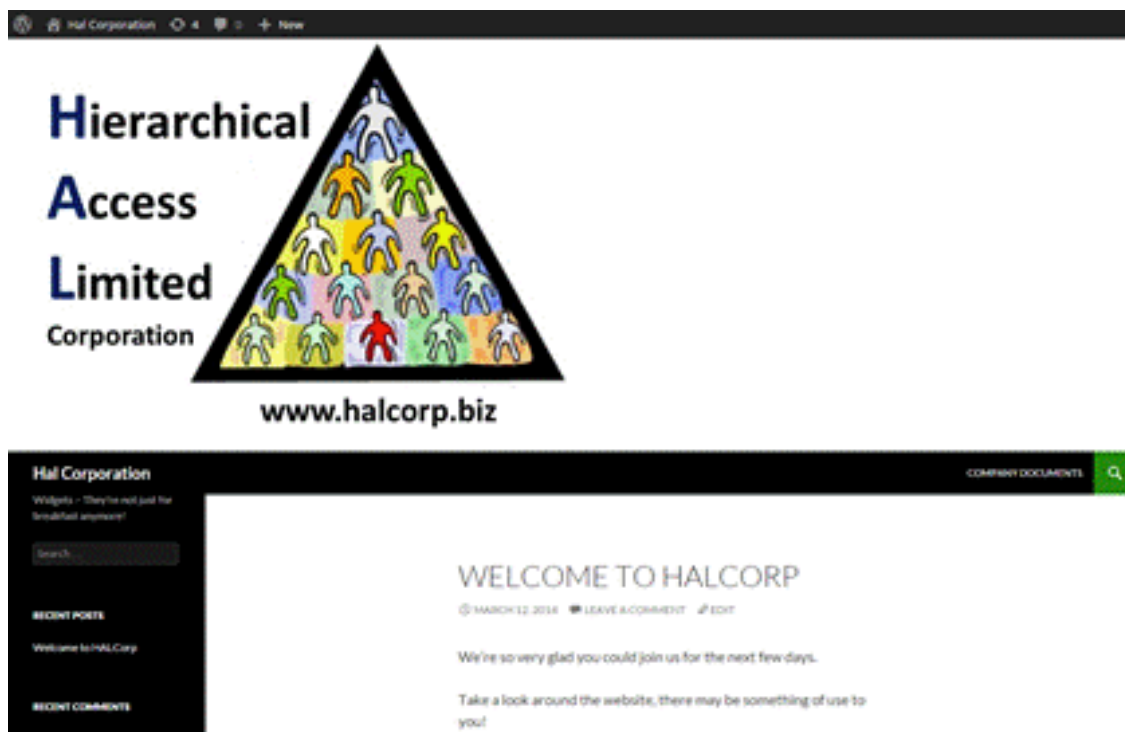
Teams are responsible for coordinating meals and rotating out of the competition for breaks. Institutional reps and non-competition team members must leave the competition room once the competition begins.

Sunday 15 March 2015

NLT 5pm Announcement of Winners Details on team performance will be provided as soon as available.

www.halcorp.biz Document Repository

A large collection of “corporate policies and documents” has been staged for use in the SECCDC competitions. You may locate them at www.halcorp.biz. These are for your use preparing for, and during, the competition. To access the “private” collection simply click on the “**Company Documents**” link on the right/center of the opening page, and enter the password: **Halprivate1!** when prompted. You may then click any of the hyperlinks to download the associated document.



Systems

1. Each team will start the competition with identically configured systems.
2. Teams may not add or remove any computer, printer, or networking device from the designated competition area.
3. This document provides the overall system architecture, network configuration, and initial set-up of the competition.
4. Teams should not assume any competition system is properly functioning or secure.
5. 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.
6. 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.
7. 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.
8. 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. It is the responsibility of the team to understand all the particulars of scoring a service when doing so.
9. 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 mechanism.
10. In the event of system lock or failure, teams will be able to perform a complete restoration from within the administration console of the remote system. This will reset any system to its initial starting configuration. The number of system restorations will be tracked and negatively impact scores at the discretion of the White Team. Teams should also consider that system restoration will take time.
11. 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.
12. Teams may not modify the hardware configurations of workstations used to access the competition network.
13. Servers and networking equipment may be re-tasked or reconfigured as needed.

Competition Rules: Acknowledgement & Agreement

Competition rules are applicable to all participants of the SECCDQC. They provide structure for the makeup of student teams, permitted actions during competition play, guidelines for scoring, and contingencies for handling disputes. They also document expectations for appropriate conduct during the entire time participants are guests at a host site, or are competing from their academic institution. Team advisors and all student participants are expected to know and follow all CCDC rules and guidelines. Access to the myVLAB competition environment implies their acknowledgement of competition rules and their commitment to abide by them.

Team advisors and team captains are responsible for deploying the competition rules to the remaining members of their team. Host sites reserve the right to stipulate additional rules conforming to local policies and guidelines.

Competition Scoring

1. Scoring will be based on keeping required services up, controlling/preventing un-authorized access, mitigating vulnerabilities, and completing business tasks that will be provided throughout the competition. Teams accumulate points by successfully completing injects, maintaining services, and by submitting incident reports. Teams lose points by violating service level agreements, usage of recovery services, and successful penetrations by the Red Team.
2. Scores will be evaluated by the White Team (Room Judges) maintained by the Gold Team (Competition Officials). Individual tracking of services will be available to respective teams during the competition. Blue Team members should use available service tracking reports and internal testing to assess the integrity of their network. Blue Team members should refrain from making direct requests to the White Team for routine service verification.
3. Any team action that interrupts the scoring system is exclusively the fault of that team and will result in a lower score. Should any question arise about specific scripts or how they are functioning, the Team Captain should immediately contact the competition officials to address the issue.
4. Any team that tampers with or interferes with the scoring or operations of another team's systems will be disqualified.
5. Teams are required to provide incident reports for each Red Team incident they detect. Incident reports can be completed as needed throughout the competition and submitted to the White Team. Incident reports must contain a description of what occurred (including source and destination IP addresses, timelines of activity, passwords cracked, etc), a discussion of what was affected, and a remediation plan. The White Team will assess scores for incident report submission based on clarity, thoroughness, and accuracy. The White Team may also, at their discretion, assess negative scores for frivolous, unnecessary, or excessive communication.
6. The winner will be based on the highest score obtained during the competition. Point values are broken down as follows:

2000 pts	Functional services uptime as measured by scoring engine
4000 pts	Successful completion of inject scenarios (task assignments) will result in varying points, depending upon the importance or complexity of the inject scenario
Up to -2000 pts	Successful Red Team Attacks (less effective Incident Response Reporting mitigation)

Precise points breakdown will be determined by the Gold Team/Competition Officials. Max competition score is 6000 pts.

Functional Services

Certain services are expected to be operational at all times or as specified throughout the competition. In addition to being up and accepting connections, the services must be functional and serve the intended business purpose. At random intervals, certain services will be tested for function and content where appropriate.

HTTP

A request for a specific web page will be made. Once the request is made, the result will be stored in a file and compared to the expected result. The returned page must match the expected content for points to be awarded.

HTTPS

A request for a page over SSL will be made. Again, the request will be made, the result stored in a file, and the result compared to the expected result. The returned page needs to match the expected file for points to be awarded.

SMTP

Email will be sent and received through a valid email account via SMTP. This will simulate an employee in the field using their email. Each successful test of email functionality will be awarded points.

FTP

Successful access to a database will be tested via the FTP protocol. Some indication of database integrity will also be examined.

DNS

DNS lookups will be performed against the DNS server. Each successfully served request will be awarded points.

Business Tasks

Throughout the competition, each team will be **emailed** identical business tasks (a.k.a. injects). Points will be awarded based upon successful completion of each business task. Tasks will vary in nature and points will be weighted based upon the difficulty and time sensitivity of the assignment. Tasks may contain multiple parts with point values assigned to each specific part of the tasking. Each business task will have a specific time period in which the assignment must be completed. Business tasks may involve modification or addition of services. Room judges may ask for verification of task completion. Cooperation fully with their requests.

All business tasks (injects) will come from hal.ciso@seccdc.org. All responses to business tasks should be properly formatted on HAL letterhead and **attached** to replies to the original email request.

All questions should be directed to hal.cio@seccdc.org. Interact with these accounts as if you were dealing directly with a corporate executive.

Questions and Disputes

1. Team captains are encouraged to work with the local site judge and contest staff to resolve any questions or disputes regarding the rules of the competition or scoring methods before the competition begins. Protests by any team will be presented by the Team Captain to the competition officials as soon as possible. Competition Gold Team officials will be the final arbitrators for any protests or questions arising before, during, or after the competition and rulings by the competition officials are final.
2. 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 awards or team trophies.
3. 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.

Aftermath

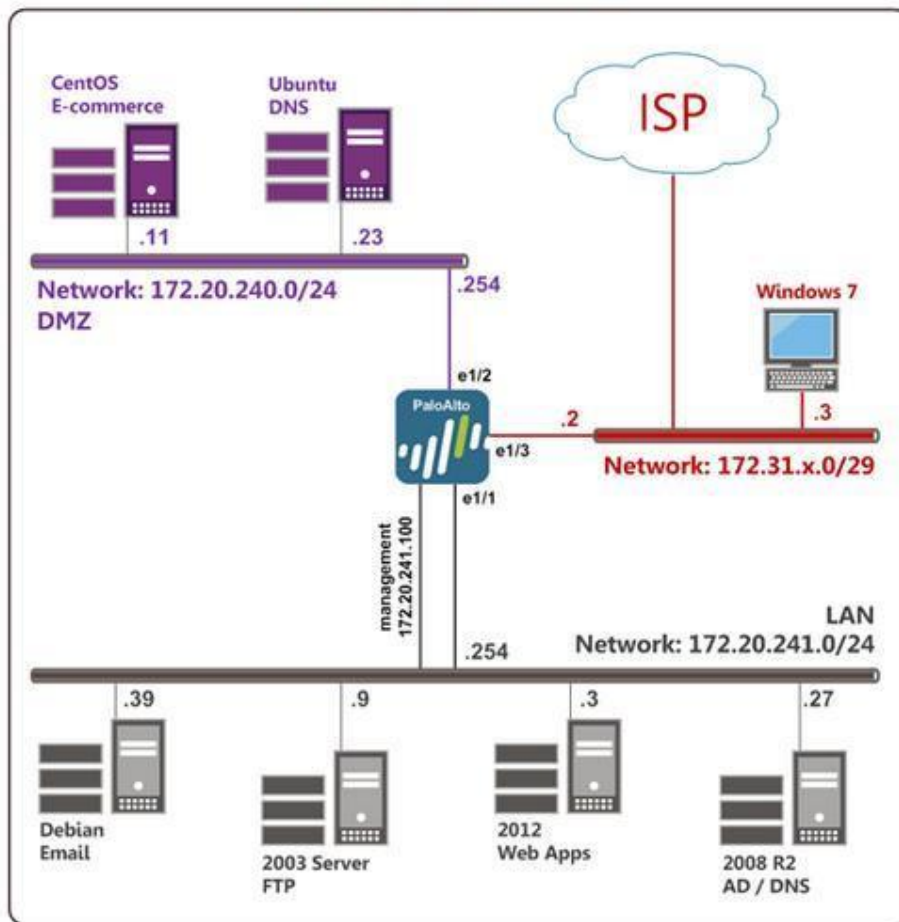
Members of CSSIA, CISE - Gold, White, Red, and Black Teams strive to make the SECCDQC an enriching experience. All management and administrative teams are open to feedback and suggestions for improvement after the completion of the competition. This may include areas of concern or dissatisfaction.

Whether feedback is positive or negative, participants are forbidden from publishing, posting on the internet, or publicly communicating details of the competition other than what is available at www.cssia.org. They are also forbidden from publishing, posting on the internet, or publicly communicating assessments of the State CCDC, nor assessments of the performance of any team, nor speculations concerning different possible outcomes. Institutions that fail to adhere to this rule may be refused participation in future competitions.

Institutions may publish, post on the internet, or publicly communicate news stories of a general nature about the SECCDQC, and may also enumerate participating teams and winners.

Competition Topology

CCDC 2015



- Teams have access to 8 VMs – 6 servers, 1 workstation, and the Palo Alto firewall.
- All servers, workstations, and Palo Alto firewall are virtual machines under the management of NETLAB™.
- Teams do not have access to the underlying layer 2 switch.
- The firewall shown in the topology is a Palo Alto VM, version 6.0.7, which is licensed by Palo Alto.

You can access the Palo Alto VM either directly, which yields a command window, or via a browser 172.20.241.100 from any of the LAN VMs.

admin/changeme

Note that this is different from the default username/password that you may have used in an MSEC+ pod.

- Each team has the following Palo Alto internal addresses:

LAN, e1/1	172.20.241.254/24
DMZ, e1/2	172.20.240.254/24

- Core IP addresses are the following:

Team	Palo Alto e1/3 Outbound to Core	Core connection to Palo Alto	"Public" IP pool
1	172.31.21.2/29	172.31.21.1	172.25.21.0/24
2	172.31.22.2/29	172.31.22.1	172.25.22.0/24
3	172.31.23.2/29	172.31.23.1	172.25.23.0/24
4	172.31.24.2/29	172.31.24.1	172.25.24.0/24
5	172.31.25.2/29	172.31.25.1	172.25.25.0/24
6	172.31.26.2/29	172.31.26.1	172.25.26.0/24
7	172.31.27.2/29	172.31.27.1	172.25.27.0/24
8	172.31.28.2/29	172.31.28.1	172.25.28.0/24
9	172.31.29.2/29	172.31.29.1	172.25.29.0/24
10	172.31.30.2/29	172.31.30.1	172.25.30.0/24
11	172.31.31.2/29	172.31.31.1	172.25.31.0/24
12	172.31.32.2/29	172.31.32.1	172.25.32.0/24
13	172.31.33.2/29	172.31.33.1	172.25.33.0/24
14	172.31.34.2/29	172.31.34.1	172.25.34.0/24
15	172.31.35.2/29	172.31.35.1	172.25.35.0/24
16	172.31.36.2/29	172.31.36.1	172.25.36.0/24
17	172.31.37.2/29	172.31.37.1	172.25.37.0/24
18	172.31.38.2/29	172.31.38.1	172.25.38.0/24
19	172.31.39.2/29	172.31.39.1	172.25.39.0/24
20	172.31.40.2/29	172.31.40.1	172.25.40.0/24

- Services provided by the servers in the topology are expected to have the same last octet of the IP address for internal and external “Public”.

This table, minus the ‘public’ translations is accessible on the topology tab of NETLAB+™, via the “Show Lab Content” on the lower right.

VM Label	Major Service	Internal IP	Public IP or pool	Account	initial pwd
CentOS E-Commerce	HTTP/S; FTP	172.20.240.11	172.25.20+team#.11	root	changeme
Ubuntu DNS	DNS	172.20.240.23	172.25.20+team#.23	root	changeme
2003 Server FTP	SQL	172.20.241.9	172.25.20+team#.9	administrator	changeme
Debian Email	Email	172.20.241.39	172.25.20+team#.39	administrator	changeme
2012 Web Apps	Web Apps	172.20.241.3	172.25.team#.3	administrator	!changeme01
2008 R2 AD/ DNS	AD/DNS	172.20.241.27	172.25.20+team#.27	administrator	changeme
Palo Alto		172.20.241.100	172.25.20+team#.100	admin	changeme
Windows 7 Workstation		172.31.20+team#.2/29	NA	administrator	changeme

Palo Alto training is scheduled for teams on the Friday prior to their respective competition day, 3/6 & 3/13, 1-5pm EST. Entire team rosters can attend via a single WebEx with overhead and speakers. A single account per team can have hands on access to the Palo Alto VM. Details will be provided as they become available.

Pertinent guides are available to ccdc students to work with the PA firewall.

Password: ccdc2015

GlobalProtect_Admin_Guide_v6.0.pdf	http://64.107.13.125:2201/fbsharing/RIRSu1dt
PAN-OS-6.0-Admin-Guide.pdf	http://64.107.13.125:2201/fbsharing/prasNKlO
PAN-OS-6.0-web-interface-ref.pdf	http://64.107.13.125:2201/fbsharing/0UVa5RuX
WildFire_Administrator_Guide-6.0.pdf	http://64.107.13.125:2201/fbsharing/SBNpntGI

Connection Testing

The SECCDQC Gold Team will coordinate connection testing sessions. We will be in contact with team representatives to allow them to select a specified number of testing sessions (as time permits). These sessions will allow teams to verify connectivity and communications with the competition systems. Testing systems are NOT representative of competition systems.

Team Competition Dates

Saturday March 7, 2015

Kennesaw State University
Montreat College
Trident Technical College
University of Central Florida
University of North Carolina Charlotte
University of North Carolina Wilmington
University of North Georgia
University of South Alabama
University of South Carolina
University of South Florida
University of Tennessee at Chattanooga
University of West Florida

Saturday March 14, 2015

Albany State University
Clemson University
College of Charleston
Columbus State University
Daytona State College
Eastern Tennessee State University
Florida State University
Georgia Regents University
Lipscomb University
Mercer University
Middle Georgia State College
Tennessee Technological University

Sponsors:

For CSSIA	
	National Science Foundation, http://www.nsf.gov/
	SecureWorks, http://www.secureworks.com
	CSSIA, http://www.cssia.org/
FOR SECCDC (and its qualifier – SECCDQC)	
	Department of Homeland Security
	Raytheon
	National Security Agency
	Akamai
	INSCOM
	SPAWARs

Appendix - Addressing Access Problems to NETLAB+™ Systems

The NETLAB+™ platform from Network Development Group drives the remotely accessible Cyber Stadiums housed in the data center at Moraine Valley Community College (MVCC) used to host competitions and provide training. It is a proven system for access control provided the requirements are met. See, <http://www.netdevgroup.com/products/requirements/>

Generally the client requirements are easily met with simple browser and java plug-in.

Some browsers will simply download the script upon granting permission. The script then needs to be executed.

The bandwidth requirement likewise seems very reasonable at 256 kb/s up and down. Ports 80, 2201 must be allowed outbound.

Experience has shown that a significant majority of remote clients are able to access NETLAB+™ without incident. Nevertheless, it is not uncommon that difficulties are encountered using the NETLAB+™ platform. Problems may be a result of,

- poor network connectivity between the remote user and the data center at MVCC
- poor performance of the Viewer with some combinations of OS/browser/java

In addition to these problems it is imperative that VMWare Tools be maintained. A drifting cursor will result if VMWare Tools are removed.

For a team of 8 for the CCDC, the requirements call for a minimum of 2 Mb/s per team access bandwidth. Based on experience, CSSIA recommends 10 Mb/s service for competitions. The reason for this is more than just margin. The 256 kb/s requirement is for the typical user with a few open sessions. It is not unusual for competitors to have numerous open sessions that demand greater bandwidth. In passing, it is a good strategy to close sessions that will not be in use for an extended time. New sessions, with proper connectivity, open quickly when needed.

Bandwidth by itself is not determinative, and under many circumstances bandwidth is gauged by *download* speed. Note here **it is imperative to have a synchronous service**. Likewise, responsiveness of the services is also important without undue latency. Though a definitive metric for latency and packet loss is wanting, many of these difficulties are shown via a pathping test from the remote (windows) host accessing the stadium (and not from a VM within the stadium).

```
>pathping {cyber stadium url such as cyberlab.morainevalley.edu}
```

On Linux hosts use the mtr command in place of pathping.

```
#mtr --report {cyber stadium url such as cyberlab.morainevalley.edu}
```

Note that this test may be performed without authenticating into the stadium as long as the url is active. Care should be taken when performing a pathping test to make sure the command completes, which may take several minutes. Experience has shown that connections with more than a few percent loss will have performance problems. Certainly 4% or more packet loss on such a test will clearly be attended with poor performance on the NETLAB+™ platform.

MVCC continues to monitor data center performance which has been provisioned to easily support hundreds of remote connections. The problem of network connectivity is usually at the local institution from which the connection is made.

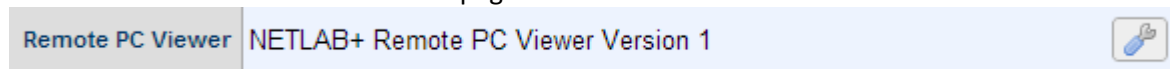
Though there may seem to be adequate bandwidth, local institutions must assure synchronous service without undue filtering.

There may be a need for special provisioning at local institutions, even bypassing filters and firewalls for dedicated traffic to the stadium(s). Towards this end it is helpful to note the level of trust and the benign nature of traffic coming from the stadium(s). Though malicious traffic may be present in the competition or lab environment supported by the NETLAB+™ platform, it is impossible for this traffic to make its way back to remotely connecting sites.

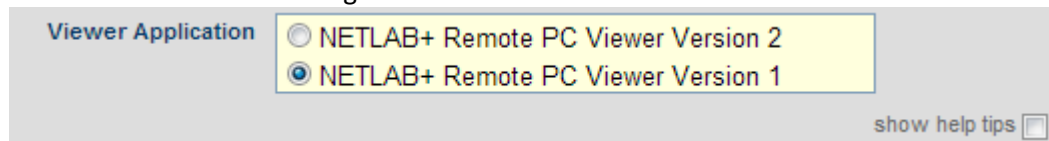
Rarely, a remote site will experience difficulty due to packet loss somewhere in route in the big white cloud, and is not a result of faults either at the local site or MVCC. Institutions must contact their ISP to address such difficulties. Even with excellent connectivity, there may still be problems with using the NETLAB+™ platform. The NETLAB+™ viewer has been programmed using java, and is sensitive to the specific combination of OS/browser/java version being used. With each update of java, the NETLAB+™ viewer may be affected.

Better response is often obtained simply by changing to a different browser. If this is unsuccessful, users may revert back to Viewer 1 instead of the default Viewer 2.

To change to Viewer 1, from the MyNETLAB page on the NETLAB+™ system, click on 'Profile' menu option or icon. Look for 'Remote PC Viewer' on the Profile page.



Click on the button on the right and select Viewer 1.



Fortunately most users accessing the NETLAB+™ platform do not experience difficulty. Hopefully the suggestions documented here will be helpful for those who do.