# Southeast Collegiate Cyber Defense Competition

## 2013 Southeast Collegiate Cyber Defense Competition

**a regional competition in the**

NATIONAL COLLEGIATE CYBER DEFENSE COMPETITION

# Team Packet
# FINAL

# Table of Contents

# History

On February 27 and 28, 2004, a group of educators, students, government and industry representatives gathered in San Antonio, Texas, to discuss the feasibility and desirability of establishing regular cyber security exercises with a uniform structure for post-secondary level students. During their discussions this group suggested the goals of creating a uniform structure for cyber security exercises might include the following:

1. Providing a template from which any educational institution can build a cyber security exercise
2. Providing enough structure to allow for competition among schools, regardless of size or resources
3. Motivating more educational institutions to offer students an opportunity to gain practical experience in information assurance

The group also identified concerns related to limiting participation to post-secondary students, creating a level playing field to eliminate possible advantages due to hardware and bandwidth differences, having a clear set of rules, implementing a fair and impartial scoring system, and addressing possible legal concerns.

In an effort to help facilitate the development of a regular, national level cyber security exercise, the Center for Infrastructure Assurance and Security at the University of Texas at San Antonio hosted the first Collegiate Cyber Defense Competition (CCDC) for the Southwestern region in May 2005. In June 2005, they presented their experiences at the Colloquium for Information System Security Education (CISSE) (see http://www.ncisse.org). Members of the Kennesaw State University's Center for Information Security Education attended their presentation and recognized the insight and foresight of the UTSA faculty. They immediately volunteered to create a similar event at KSU in 2006, to provide a regional competition to recognize the best team in the Southeast, and to work to sponsor that team to a National Competition which will be developed by UTSA from its regional experiences.

Since the first SECCDC in 2006, KSU has hosted the first SECCDC, with the exception of 2007.

This document provides the background information and rules governing the teams that will participate in the Southeast Collegiate Cyber Defense Competition (SECCDC), a regional implementation of the Collegiate Cyber Defense Competition. Currently there are no state competitions; as such this competition is open to all institutions in the following states: Alabama, Florida, Georgia, Kentucky, Mississippi, Tennessee, South Carolina and North Carolina.

Any questions or concerns associated with these rules and regulations should be directed to Dr. Mike Whitman, Director of the KSU Center for Information Security Education and Chair of the SECCDC Advisory Board. Comments from team coaches are encouraged; however, the KSU Center reserves the right to formulate the competition in a manner best suiting their interpretation of the CCDC.

Special thanks go to the UTSA Center for Infrastructure Assurance and Security for their permission and support in providing materials to support the SECCDC.

# Overview

While similar to other cyber defense competitions in many aspects, the SECCDC, as part of the CCDC, is unique in that it focuses on the operational aspect of managing and protecting an existing network infrastructure. While other exercises examine the abilities of a group of students to design, configure, and protect a network over the course of an entire semester, this competition is focused on the more operational task of assuming administrative and protective duties for an existing "commercial" network. Teams will be scored based on their ability to detect and respond to outside threats, maintain availability of existing services such as mail servers and web servers, respond to business requests such as the addition or removal of additional services, and balance security needs against business needs.

Teams involved in this competition include:

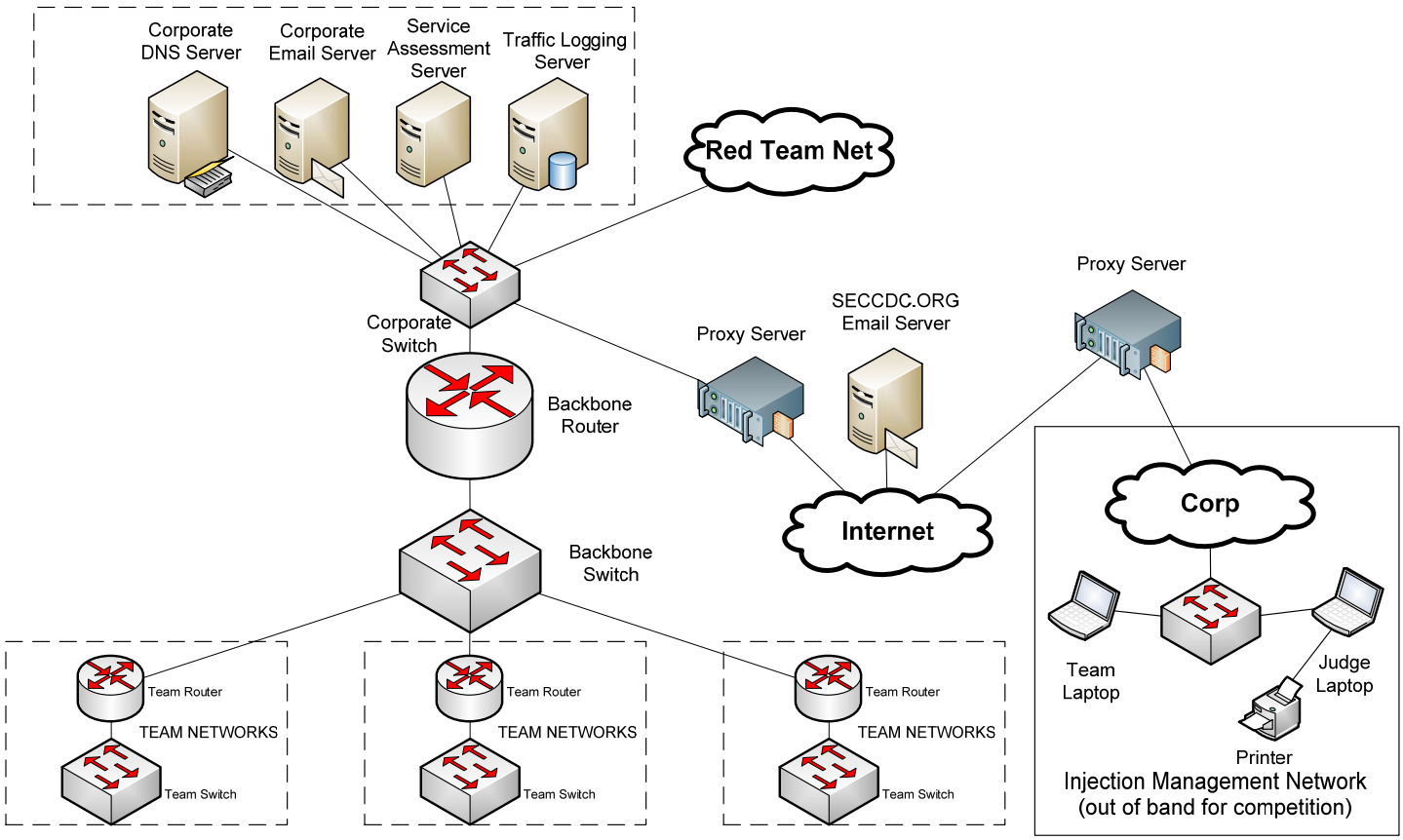
- Blue teams – (student team/competition team) student teams consisting of graduate and undergraduate students from regional institutions who will compete in the SECCDC.
- Red team – (op for/pen team) a group of information security professionals from volunteer commercial organizations who have offered their skills to assess the abilities of the teams to defend their networks and systems. The Red team will conduct periodic probes, scans and attempted penetrations of the academic teams.
- White team – (judges) a group of information technology and information security academics and professionals who will serve as judges and referees. Each academic team will be assigned a White team judge who will assess the academic teams' ability to secure their network segment and systems, and who will periodically query the team as to their actions and provide "injections" designed to challenge the teams' implementation. Academic teams are advised not to argue or question the White team, only answer when queried. The White teams also include individuals who assess the readiness of team services.
- Gold team –(operations) the administrative faculty and professionals who will conduct the exercise, control the flow and timing of the events and injections, and who will serve as mediators for disputes and challenges. Academic teams are advised not to interact with the Gold team except during challenges and mediations. White team judges will handle these interactions on behalf of the teams.
- Black team - competition support team, volunteers who handle technical and administrative support for the event.

To create a fair and even playing field:

- Each team will begin with a functionally equivalent set of hardware and software provided by the competition. Each team will be given a small, pre-configured, operational network with 5 to 8 servers (physical or virtual) and 4 to 6 workstations they must configure, secure and maintain.
- Each team will be located on a dedicated internal network. Each team's network will be connected to a competition network allowing equal bandwidth and access for scoring and red team operations. This also allows tight control over competition traffic.
- Each team will be provided with the same objectives and tasks. Each team will be given the same set of business objectives and tasks at the same time during the course of the competition.
- Only the assigned academic team members, and White and Gold team members will be allowed inside their competition areas. Each team will be assigned their own workspace during the competition and only the members of the academic student team will be allowed in this area during the competition. This eliminates the potential influence of coaches or mentors during the competition.
- A non-biased red team will be used: An impartial, volunteer, commercially-experienced red team will be used during the competition.

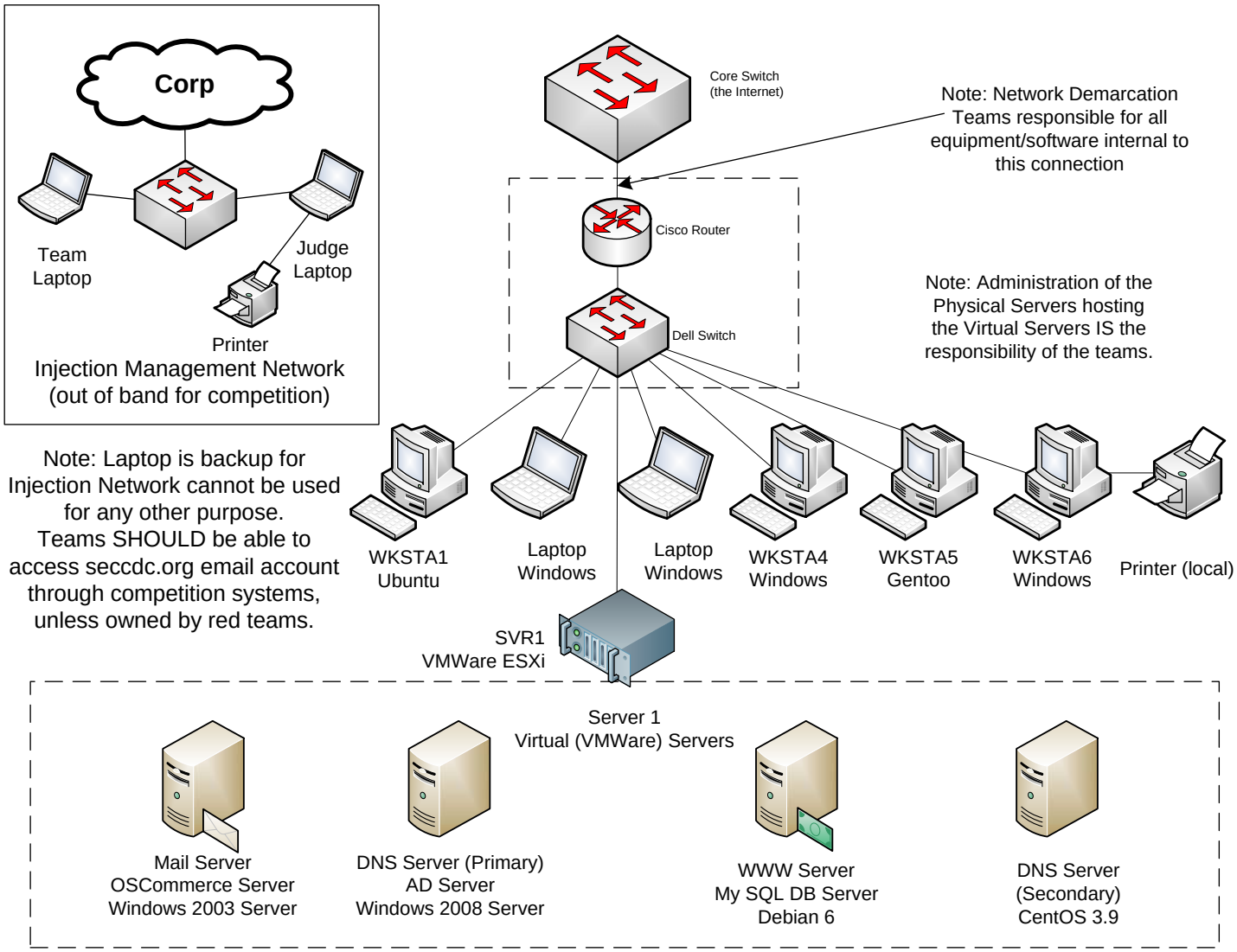
# Logical Network Diagrams

Overall Competition Network Layout (note: subject to change prior to competition)




The competition network will be completely standalone with proxied external connectivity. Global servers, the red team network, the white team network, and each team network will be connected to a central switch that will be maintained by the white team. Note: Designations for Switches/Routers are subject to change.

Individual Team Layout (note: subject to change prior to competition)




Each team network will be connected to the central router through their own individual router. Each team will be provided with proxy Internet access that may be used for research, software downloads, etc. Any web locations the team feels they need access to during the competition, that are not already provided, may be requested through the organization CIO as described in the rules.

Teams may NOT bring systems or electronic media (flash drives, CDs, cell phones, PDAs etc.) with them to connect to their competition network. However, additional hardware, software (open-source and freeware) and networking components will be available for each team to use to create additional network protection resources. Teams will be provided with ***access to installation images*** or access to stored materials (ISOs or VMImages) for multiple versions of commonly available operating systems.

# Schedule

**Tues, March 5 (NOTE: DINNER ON DAY 1 IS PROVIDED, BUT NOT LUNCH)**

11:00 AM Sign-in opens. Teams will gather in room SCIENCE 109 (, College of Science and Math Building - connected to the Clendenin Building) for registration and opening remarks.

11:30 PM Opening announcements. Teams judges lead teams to their areas before start of competition.

12:00 PM ***Competition begins:*** Academic teams are provided the opportunity to examine the configuration of their systems and networks, "offline". This means there will be no red team and no services scored. Teams begin updating and modifying their configuration to meet their initial requirements. There will be business injections issued and scored on Day 1, however.

***4:00 PM*** ***"Offline" period ends. Teams formally scored on services and subject to red team operations.***

5:00 PM Dinner will be available in the dining area. Announcement will be made when snacks are available. Competition IS NOT suspended for meals. Students must rotate out for meals. No food or drink is allowed in the competition areas.

8:00 PM ***End Day 1,*** teams must leave the competition area and may not remove any items.

**Wednesday, March 6 (NOTE: LUNCH AND SNACKS ARE PROVIDED ON DAY 2)**

8:45 AM Teams gathered in room SC 109 (College of Science and Math) for day 2 announcements. Team judges lead to their team to their areas 5 minutes before competition start.

9:00 AM ***Competition Day 2*** begins.

12:00 PM Lunch will be available in the dining area. Announcement will be made when snacks are available. Competition IS NOT suspended for meals. Students must rotate out for meals. No food or drink is allowed in the competition areas.

5:00 PM ***End Day 2,*** teams must leave the competition area and may not remove any competition components from their areas.

**Thursday, March 7 (NOTE: LUNCH AND RECEPTION SNACKS PROVIDED ON DAY 3)**

8:45 AM Teams gathered in room SC 109 (College of Science and Math) for day 3 announcements. Team judges lead to their team to their areas 5 minutes before competition start.

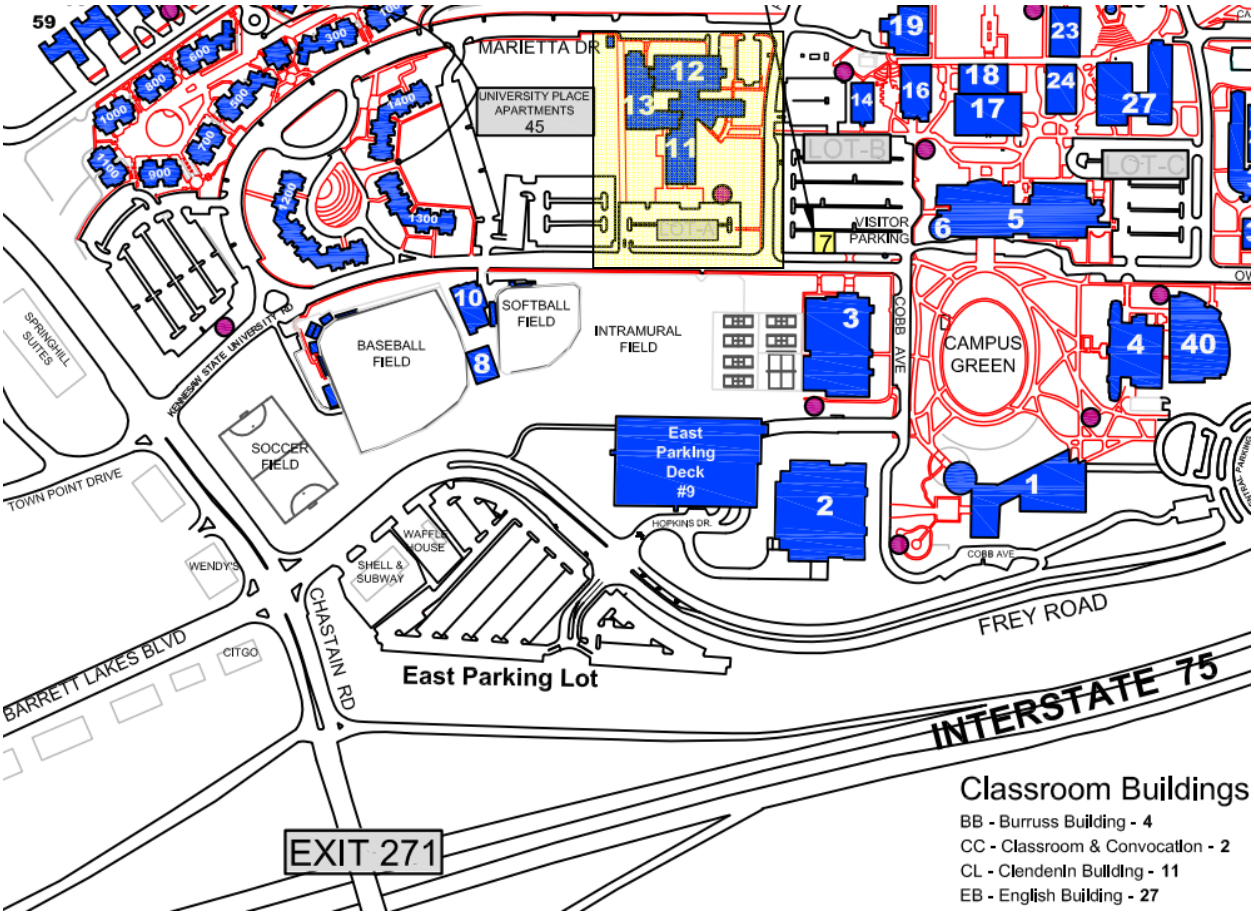
9:00 AM ***Competition Day 3*** begins.

12:00 PM Lunch will be available in the dining area. Announcement will be made when snacks are available. Competition IS NOT suspended for meals. Students must rotate out for meals. No food or drink is allowed in the competition areas.

2:00 PM ***Competition End.*** Sponsored reception in SC 109 and atrium. Snacks provided.

4 PM Presentations and discussion by ALL Teams – including student teams in the Science Building Room 109. Awards ceremony immediately follows.

**6 PM EVENT CONCLUDES**




**Teams may park in Lot A *due south of Bdlg 11) as KSU is on spring break the week of the competition. Start in Bdlg 12, SC 109 then teams will be moved to Bdlg 11 (Clendenin) for actual competition.**

# Competition Rules

Note: 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:*

All institutions, including student competitors and university representatives, must comply with these rules. Failure to do so can result in penalties ranging from points against the student 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.

## COMPETITION RULES

### 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 2013. 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.

### 2013 Rules

The following are the approved national rules for the 2013 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: 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.

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.

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.
        *i. SECCDC Supplemental Rule: Rosters are due to the SECCDC Competition organizers by Jan 15 of the competition year, however changes may be made to the roster up through two weeks prior to the first competition (the Virtual Prequalification Competition).*
    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, substitutions or additions of team members are prohibited. A team must complete the competition with the team that started the competition.
    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 Operations (SECCDC: Gold) Team. 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.

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 (support) team members will require access to systems. These individuals will only be allowed access if accompanied by an Operations (SECCDC: Gold) or White Team member.*
        ii. *SECCDC Supplemental Rule: For the virtual preliminary qualification competition, the local judge may inspect all systems to rules compliance 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.*
        ii. *SECCDC Supplemental Rule: For the virtual preliminary 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 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.
        i. *SECCDC Supplemental Rule: Each team is restricted to two (2) standard business file boxes (approx 10 x 12 x 18) of printed material. Note that this material must remain in the competition room until the end of 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. 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 virtual preliminary qualification competitions Institutions may "stage" competition photographs before or after the competition hours. For the onsite competition, an official event photographer 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, 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. These requests will take between 30 minutes to 2 hours to process, depending on the CIO's schedule.*

*iii. SECCDC Supplemental Rule: At no time will the proxy list 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 Virtual Preliminary Qualification competition, Internet access will be 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, 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 is prohibited unless the environment was provided by and is administered by competition officials. Accessing private staging areas 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 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. 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.

*i. SECCDC Supplemental Rule: For the virtual preliminary qualification competition, all equipment to be used for the competition must be the property of the host institution. No student-owned equipment may be connected to competition networks, even if the competition network is not directly controlled by SECCDC competition officials.*

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 45 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.

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.

*i. 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. Should any question arise about scoring, the scoring engine, or how they function, 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.

*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.*

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 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.

# Scoring

The winner will be based on the highest score obtained during 22 total hours of competition time ***(8 on Day 1, 9 on day 2 and 5 on Day 3)***. During this competition a team may accumulate a total maximum of 6,000 points, plus bonuses, minus penalties. Accumulated point values are broken down as follows:

- Functional services (based on periodic polling interval of core services): 2000 points
- Successful completion of business tasks: Awarded points will vary by task for a possible total of 2000 points
- Red team assessments: Red teams will attempt to penetrate the student teams' systems, assessing penalty points for successful attacks, against each team's maximum score of 2000 points. The red team will have access to the services availability information to assist them in the determination of their scores. Student teams may mitigate these penalties by up to 50% with effective, timely and properly formatted incident reporting.

Penalties may be awarded for extended service outages, improperly formatted communications, or other activities determined by the Gold team to warrant such.

**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 semi-random intervals, certain services will be tested for function and content where appropriate. Each successfully served request will gain the team points.

**HTTP:** A request for a specific web page may be made. Once the request is made, the result will be compared to the expected result. Results must match expected content for points to be awarded.

**HTTPS:** A request for a page over SSL may be made. Again, the request will be made, the result compared to the expected result. The returned page needs to match the expected file for points to be awarded.

**SMTP:** Email may 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.

**SSH:** An SSH session may be initiated to simulate a vendor account logging in on a regular basis to check error logs. Each successful login and log check will be awarded points.

**SQL:** An SQL request may be made to the database server. The result will be stored and compared against an expected result. Each successfully served SQL request will be awarded points.

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

The official list of required services will be provided at the start of the competition.

Each of the required services operates under a Service Level Agreement and teams will be assessed penalties for extended outages of any critical service. For example, if a critical service is down continuously for 1 hour,

the team will be assessed a 50 point penalty **per service**. The specific number of service checks used during the competition will be addressed by competition officials prior to the start of the event.

**Business Taskings (Injections)**
Throughout the competition, each team will be presented with identical business taskings. Points will be awarded based upon successful completion of each business tasking or part of a tasking, in a timely manner. Taskings will vary in nature and points will be weighted based upon the difficulty and time sensitivity of the tasking. ***Tasks may contain multiple parts with point values assigned to each specific part of the tasking.***

Some examples:

- Opening an FTP service for 2 hours given a specific user name and password
- Closing the FTP after the 2 hours is up
- Creating/enabling new user accounts
- Auditing a user's activities through system logs
- Installing new software package on CEO's desktop within 30 minutes

Each "injection" tasks will include time restrictions associated with the task. Teams can prioritize their efforts based on outstanding requests. Upon completion of tasks, the tasks assignment sheets will be signed by the team Captain and returned to the White team judge, who will note the time that the event was completed. The assignments will then be assessed by the Gold team. *Some* assignments *may* have "late" point values beyond the due date/time, so completion of all assignments is recommended. If teams elect NOT to complete a tasking, and submit a properly formatted legitimate business explanation as to why, to the requestor in a timely manner, they *MAY* receive partial or complete credit for the assignment.

SAMPLE MEMORANDUM (full memorandum includes specifics on task and time to complete)

EXERCISE TOP SECRET
2013 SECCDC DOCUMENT

# Internal Memorandum

**To:** InfoSec Branch Team
**CC:**
**From:** Paul Alexander, CISO
**Date/Task #:** 3/5/2013 #03-02
**Re:** Welcome

Hierarchial Access Limited
WWW.HAL.COM

---

Welcome team:

I would like to echo the CIO's comments. You've got a tough job ahead.

***Effective 2013 – Team networks will be able to access the seccdc.org email server for injections/tasks. In addition, an external administrative network will be used as a fail-safe backup for Injections. Team members will be expected to monitor the administrative network for official communications from headquarters and upload responses. While the Team SHOULD be able to access the email server containing the team's account receiving tasks, the team is responsible for making sure that even if their competition network goes down, someone monitors the administrative network. This administrative network will be independent of the competition network and not subject to Red Team actions. Teams are similarly prohibited from modifying this outside network and systems connected to it.***

NOTE: All communications from HAL Headquarters WILL BE on Internal Memorandum letterhead. Any communications the team sends or receives that are NOT on Internal Memorandum letterhead will be considered invalid and be discarded. The Red Team MAY attempt social engineering electronically but is specifically PROHIBITED from physical interaction with the teams. Almost all communications will originate from the CISO (with the exception of the initial memo).

# Red Team

**Red Team Actions**
Successful Red Team actions will result in penalties that reduce the affected team's score. Red Team actions include:

- Obtaining root/administrator level access to a team system
- Obtaining user level access to a team system (shell access or equivalent)
- Recovery of userids and passwords from a team system (encrypted or unencrypted)
- Recovery of one or more sensitive files or pieces of information from a team system (configuration files, corporate data, etc.)
- Recovery of customer credit card numbers
- Recovery of personally identifiable customer information (name, address, and credit card number)
- Recovery of encrypted customer data or an encrypted database

Red Team actions are scored on a **per system** and **per method** basis – a buffer overflow attack that allows the Red Team to penetrate a team's system will only be scored once for that system; however, a different attack that allows the Red Team to penetrate the same system will also be scored. Only the highest level of account access will be scored per attack – for example, if the Red Team compromises a single user account and obtains root access in the same attack the penalty will be points for root level access and not combined points for root and user level access.

Other Red Team actions are cumulative. For example, a successful attack that yields root level access and allows the downloading of userids and passwords will result in an additional point penalty.

Red Team points will be deducted from the 2000 max points each team begins with. Penalties include:

- Obtaining root/admin level access to a system: - 40 points
- Recovery of userids and passwords from a team system (encrypted or unencrypted): -40 points

- Recovery of one or more critical files or pieces of information from a team system (customer credit card numbers, personally identifiable customer information, virtual images): - 80 points
- Other miscellaneous attacks, harassment, web site defacement and Denial of Service attack (not-network based) on team system: -20 points

Note: The Red team will attack each system multiple times throughout the competition, but must successfully attack at intervals greater than 2 hours to take additional penalty points for attacking a system. In other words, the Red Team cannot take points for gaining admin access to a system , then come back 30 minutes later, before the teams realizes this, and take additional points for gaining admin access to the same system.

Student teams can mitigate these penalties with effective, efficient incident reporting. ***Incident reports must be properly formatted, and submitted within 2 hours of the attack to receive credit.***

# Team Requirements

**Logs**

All student teams will be expected to maintain two logs:

1) Change management log (1 log per team - spreadsheet). When a student performs a task, they should immediately make an entry to the change management log detailing the following:
   - what task was performed, (i.e. changed a password, installed software etc)
   - when it was performed (i.e. 12:45 PM 3/10/2010)
   - on what machine it was performed (i.e. IP 10.10.10.10 or CEO's Client PC)
   - what specifically was done (i.e. changed password) – **note: the actual password will be stored in the confidential storage log, not the change management log.**
   - why it was performed (i.e. in response to injection or because it was good business practice)

   Failure to document modifications and updates in the change management log could result in point penalties. This log will be kept in electronic form (spreadsheet). Teams may be required to submit logs as requested by the organizational change management officer.

   ***There will be scheduled meetings for all changes after the "offline" period. All teams are expected to queue planned changes and have them formally approved before implementing, unless they are specifically told otherwise in the request document. Additional information will be provided during the in-briefing.***

2) Confidential Password Storage Log

   Student teams will also be provided with a confidential storage log notebook. ALL system usernames and passwords MUST be stored in this document, and should be considered secure for the purposes of the competition. Periodically White Team Judges and/or Gold Team admins will check these logs to determine if the team is vigilant in storing their usernames/passwords.

   Penalties for failing to do so will range from 10 points per system user account to 100 points per server that is inaccessible due to unavailable username/password (injection based or other) without a recorded username/password. Teams should make a concerted effort to **neatly** organize and maintain these logs to

facilitate review. If the White team cannot read an entry in the storage log, the team will be penalized as if the entry were missing.

During the competition, certain services are assessed based on a pre-configured username/password. The Gold team will brief the teams on which accounts require coordination with the CIO/Ops. *Teams wishing to change these accounts must carefully coordinate these changes with CIO/Ops or else risk losing credit for down services.* Details on how to request these changes will be provided at the start of the competition.

## Recommended Reading List

Note this list is not meant to be comprehensive but a baseline for programs to use in preparing for the SECCDC.

Various publications from:
DHS National Checklist Program Repository: http://web.nvd.nist.gov/view/ncp/repository

NIST Special Publications: http://csrc.nist.gov/publications/nistpubs/index.html

Microsoft Security Guides for Security Compliance Management Toolkit Series:
http://technet.microsoft.com/en-us/library/cc677002.aspx

Team Institution Representatives should address any questions or concerns to the competition coordinator: Dr. Mike Whitman at mwhitman@kennesaw.edu.

**Student team members should NOT contact competition officials directly.**