Southeast Collegiate Cyber Defense Competition

2018 Southeast Collegiate Cyber Defense Competition

a regional competition in the

NATIONAL COLLEGIATE CYBER DEFENSE COMPETITION

SECCDC On-Site Regional Competition Team Packet

<FINAL 3/21/2018>

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 cybersecurity 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 cybersecurity 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.cisse.info). 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, to be developed by UTSA from its regional experiences.

Since the first SECCDC in 2006, KSU has hosted every SECCDC, except 2007, where the director served as a primary consultant.

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, Mississippi, Tennessee, South Carolina and North Carolina.

In 2012, the SECCDC implemented a qualification competition, the SECCDQC, as a virtual preliminary qualification to the on-site SECCDC. This competition identifies the top eight (8) teams to be invited to the on-site during KSU's spring break week.

Special thanks go to the UTSA Center for Infrastructure Assurance and Security for their permission and support in providing materials to support the SECCDC, and to Dr. David Durkee and the Moraine Valley Community College's National Center for Systems Security and Information Assurance for their assistance in conducting the Prelim.

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:

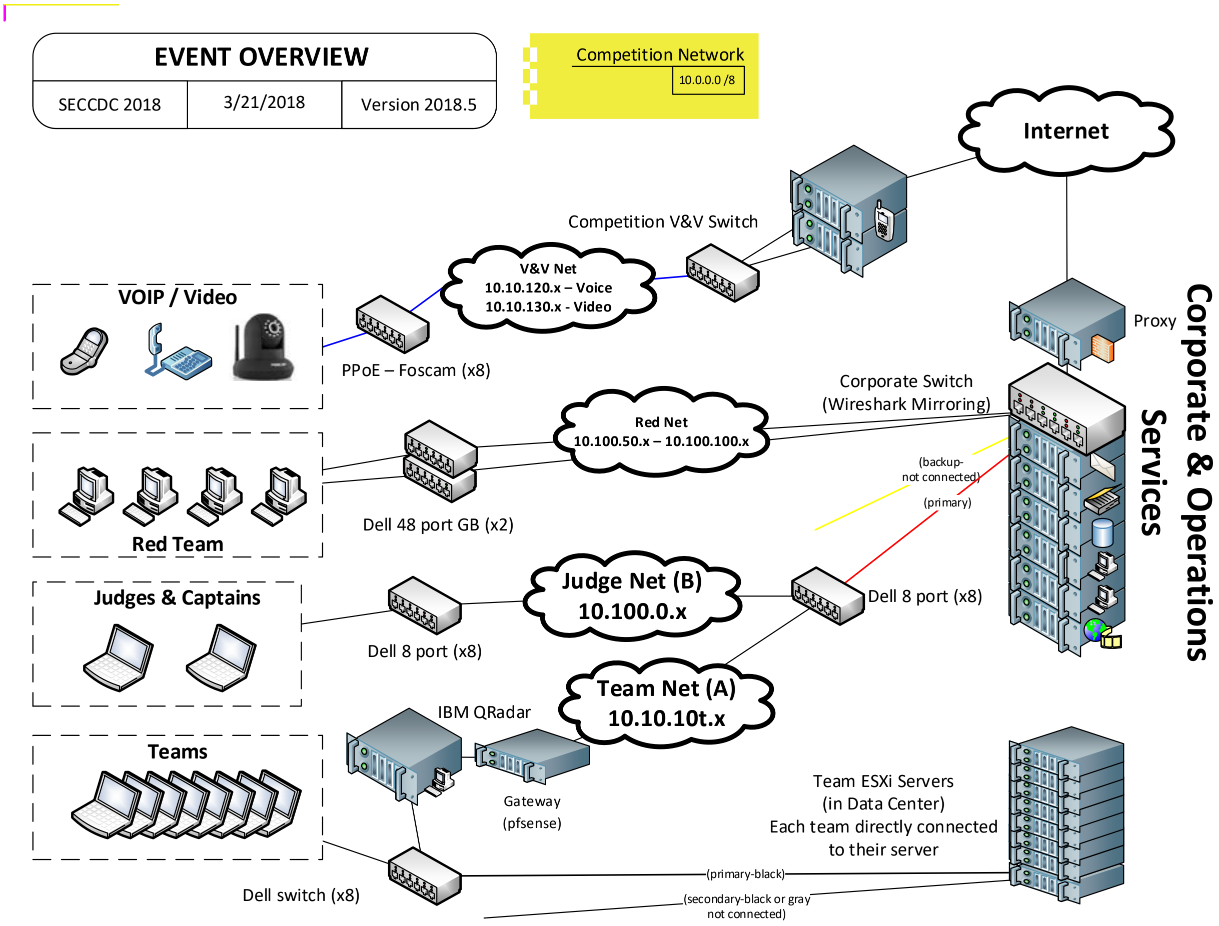
- Gold Team/Operations Team - competition officials that organize, run, and manage the competition.
- White Team - competition officials that observe team performance in their competition area and evaluate team performance and rule compliance.
- Red Team - penetration testing professionals simulating external hackers attempting to gain unauthorized access to competition teams' systems.
- Orange Team – a subset of the Red Team dedicated to providing advice and support to the Blue Teams.
- 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).
- Institutional representatives – (team representative) a faculty or staff employee of the Blue Team's host institution responsible for serving as a liaison between competition officials and the Blue Team's institution and team.

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 a number of servers (physical or virtual) and 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 Blue 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. Black team members not simply collecting mail must be escorted in competition areas by White or Gold team members.
- A non-biased red team will be used: An impartial, volunteer, commercially-experienced red team will be used during the competition.

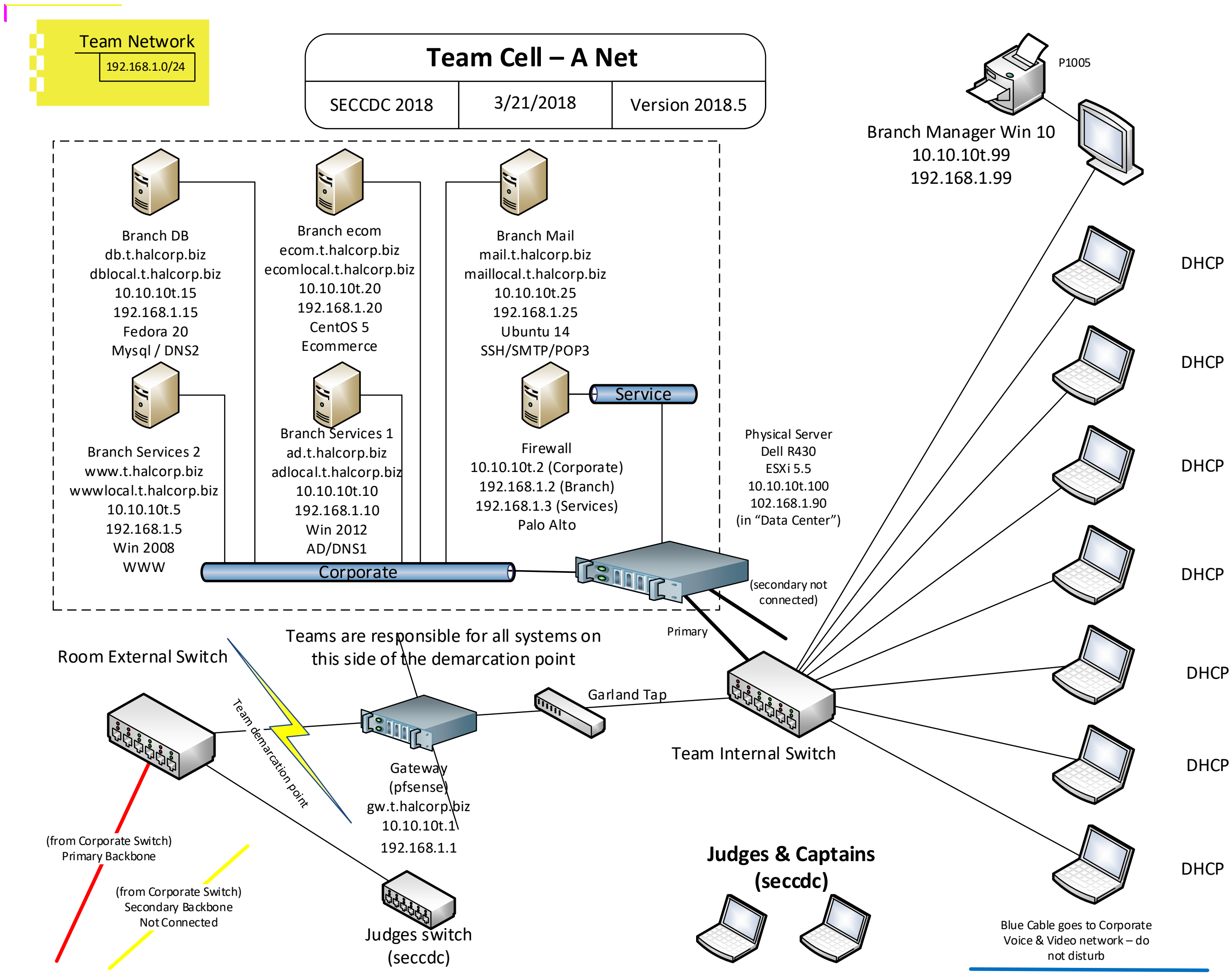
Logical Network Diagrams

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



The competition network will be completely standalone with external connectivity via a proxy server. Corporate 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 gold team, and which will be subject to logging and monitoring.   Note: This diagram and the competition network is subject to change.

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



Each team network will be connected to the central router/switch through their own individual router or switch. Each team will be provided with Internet access via a proxy server 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/CISO 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 MAY 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 VM Images) for implemented operating systems.

Schedule

Monday, April 2

9:00 AM Sign-in opens. Teams will gather in room BB 151, Burruss Building - home of the Coles College of Business - for registration and opening remarks.

White Team judges meet teams outside their areas before start of competition.

10:00 AM ***Competition begins:*** Teams are provided 2 hours (until 12PM) to examine and revise the configuration of their systems and networks, under "emergency change conditions". This does NOT mean will be no red team activities or services scored. Scoring on services and injections begin immediately, and the Red Team shows up when the Red Team shows up. Teams begin updating and modifying their configuration to meet their initial requirements.

12:00 PM Lunch will be available in the 1st Floor Atrium. Announcement will be made when meals are available. Competition IS NOT suspended for meals. Students must rotate out for meals. No food or drink is allowed in the competition areas or hallways outside the rooms.

2:30 PM Snacks will be provided – same rules and conditions as lunch.

5:00 PM Dinner will be provided – same rules and conditions as lunch.

8:00 PM ***End Day 1 Competition.*** Teams must leave the competition area and must not remove any items.

8:05 PM End of day debrief in BB 151.

8:30 PM Teams released from competition.

Tuesday, April 3

9:30 AM Teams gather in room BB 151 for day 2 announcements.

White Team judges lead teams to their areas 5 minutes before competition start.

10:00 AM ***Competition Day 2*** begins.

12:00 PM Lunch will be available in the BB 1st Floor Atrium. Announcement will be made when meals are available. Competition IS NOT suspended for meals. Students must rotate out for meals. No food or drink is allowed in the competition areas or hallways outside the rooms.

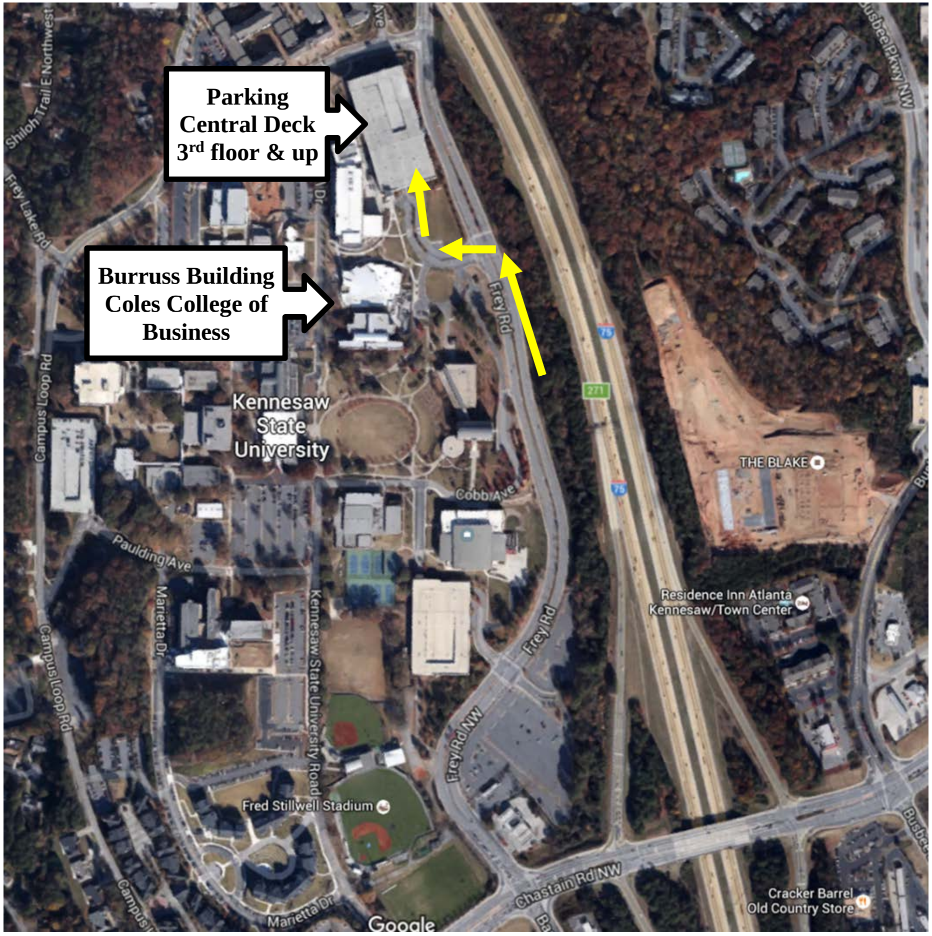
2:00 PM ***Competition Ends.*** Sponsors & red team reception in BB 1st Floor atrium. Refreshments provided and sponsored by IBM.

4:00 PM Presentations and awards in BB 151.

5:00 PM EVENT CONCLUDES

Travel & Lodging

Thanks to the generosity of our sponsors, this year we will be providing hotel rooms for interested teams at one of three local properties. Teams not desiring to take advantage of this offer, should contact the SECCDC Director as soon as possible so that the remaining rooms may be redistributed to other teams, or the reservations cancelled. Due to the severe lack of room availability, the rooms provided are based on a 2 person occupancy all in 2 bed, non-smoking rooms. We are only able to provide 5-6 rooms per team for up to 9 team members and the institutional rep. Should additional facilities be needed, we can recommend several other hotels nearby that MAY have space available. It will then be up to the institution to secure additional reservations. We regret the lack of rooms, but it is a physical space limitation, not a budget issue.
Team representatives will receive details on confirmation and other information prior to the competition. To reach the competition facility from the hotel, take Chastain Road across I-75 to Frey Road (1st intersection after I-75). Take a right on Frey Road, drive past the first parking deck to Parliament Garden Way. Turn left on Parliament Garden Way and then proceed straight into the Central Deck. Teams may park at no cost on the 3rd floor or higher. Parking in the visitor lot may incur parking fees. Burruss is walking distance south from the Central Deck. See Map below for details.



Event begins with check-in in BB 151. Teams will be escorted to the 3rd floor for start of competition.
(Maps available from http://www.kennesaw.edu/maps/docs/kennesaw_2d_map.pdf)

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.
- There are no new rule(s) for 2018.
- For the 2018 on-site, we will be maintaining complete "immersion" in the case organization. Judges will be referred to as "auditors", and ALL questions not related to "auditing guidelines" (competition rules) MUST go to the CIO or CISO. Teams should refrain from separating "competition" functions from "corporate" functions. Only in extreme circumstances will event participants "break character" to interact with team members.

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 December 1, 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.

SECCDC Rules (as of Jan 2016)

The following are the approved national rules for the 2018 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.
- *SECCDC: Orange Team – select individuals serving to simulate customers and employees of the fictional organization.*
- Team Captain - a student member of the Blue Team identified as the primary liaison between the Blue Team and the White Team.
- Team Co-Captain - a student member of the Blue Team identified as the secondary or backup liaison between the Blue Team and the White Team, should the Team Captain be unavailable (i.e. not in the competition room).
- Team representatives - a faculty or staff representative of the Blue Team's host institution responsible for serving as a liaison between competition officials and the Blue Team's institution.

1. **Competitor Eligibility**
    a. Competitors in CCDC events must be full-time students of the institution they are representing.
        i. Team members must qualify as full-time students as defined by the institution they are attending.
        ii. Individual competitors may participate in CCDC events for a maximum of five seasons. A CCDC season is defined as the period of time between the start of the first state event and the completion of the National CCDC event. Participation on a team in any CCDC event during a given season counts as participation for that entire season.
        iii. A competitor in their final semester prior to graduation is exempt from the full-time student requirement and may compete in CCDC events as a part-time student provided the competitor has a demonstrated record of full-time attendance for the previous semester or quarter.
        iv. If a team member competes in a qualifying, state, or regional CCDC event and graduates before the next CCDC event in the same season, that team member will be allowed to continue to compete at CCDC events during the same season should their team win and advance to the next round of competition.
    b. Competitors may only be a member of one team per CCDC season.
    c. A team member may not participate in any role at CCDC events held outside the region in which their team competes during the same CCDC season.
    d. Individuals who have participated in previous CCDC events in any role other than as a competitor must obtain eligibility approval from the director of the region in which their team competes prior to being added to the team roster. Once a candidate's eligibility has been approved they will remain eligible for all CCDC events during the same season.

2. **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. SECCDQC/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 by the date specified in the Call for Teams.
    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. *SECCDQC/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. *SECCDQC/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. *SECCDQC 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. *SECCDQC 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. SECCDQC/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. SECCDQC/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 (a White team member) 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 any system outside the team's assigned network(s), including those of other CCDC teams, will be tolerated. Any team performing offensive activity against any system outside the team's assigned network(s) 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. SECCDQC 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 SECCDQC 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. *SECCDQC 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 may be asked to leave the competition area.*
      iii. *SECCDQC Supplemental Rule: The competition director reserves the right to correct an error of fact after the prelim qualification event, in order to ensure that the most deserving teams are invited to the on-site SECCDC regional event. All reasonable and prudent care will be taken to ensure such corrections are made quickly and with the utmost respect for the institutions affected.*
   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.

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.

REMINDER: Do not delete, modify or otherwise interact with any account, folder or drive labeled seccdc or SECCDC. These are competition scoring/function systems and any unauthorized interaction MAY result in a team penalty or disqualification. Note that obscuring or tampering with systems or application log files to these resources is also not allowed.

Scoring

The winner will be based on the highest score obtained during scheduled competition times. During this competition a team may accumulate points from task assignments, successful service assessments, business operations and reports. Teams will lose points from penalties and successful red team operations. Accumulated score values are broken down as follows:

- Service Assessments (based on periodic polling interval of core services): Team scores will be based on calculated "up time" assessed as the total number of successful service checks divided by the total number of checks. Scores will be converted to a 100 points scale.
- Business tasks (injections): Awarded points will vary by task. Scores will total to a maximum of 200 points, weighting business tasks twice as much as service assessments.
- Business operations (separate assignments and expected reports): Teams are expected to successfully report key activities not directly tied to an injection. These include, but are not limited to:
  - Change management meeting and reporting,
  - Incident response reporting,
  - Auditing and compliance reporting,

  …all in accordance with "corporate" policy.

  Failure to report expected activities will result in penalties against the service and injection scores.
- Red team assessments: Red teams will attempt to penetrate the student teams' systems. Red team operations will be divided into two categories: organized crime and hacktivist, as discussed later on in the Red Team section of this document. Red team organized crime members will focus on theft of critical information, which will result in points penalties against the teams. Red team hacktivists will focus on disruption of team services, which will be reflected in the teams' service assessments (SLAs). Teams may mitigate up to 50% of red team penalties through timely and accurate Incident Response reporting, in accordance with the simulated case organization (HAL) policy.

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

Scores for each category will be converted to a 100 points scale for each category, with the final total calculated as (Tasks plus Service uptime minus (Red Team Penalties less IR reporting) minus Misc. Penalties) divided by three, resulting in a maximum score of 100 (200 + 100 – 0 – 0)/3 = 100. This method is consistent with previous competitions.

Functional Service Level Assessments (SLAs)

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. Servers and services are assess through multiple measures including checking by service, IP address and DNS resolution, with the assessments averaged to determine up time.

Services that are assessed MAY include the following (actual details to be shared at competition in-briefing):

HTTP (Static Web): 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. Web sites will undergo random testing with penalties against the service assessment if failing.

HTTPS (Ecommerce): A request for a page over SSL may be made. Again, the request will be made, the result compared to the expected result. Ecommerce sites will undergo random testing with penalties against the service assessment if failing.

SMTP (Email): Email may be sent and received through a valid email account via SMTP. This will simulate an employee in the field using their email. Email accounts will undergo random testing with penalties against the service assessment if failing.

SQL (Database): An SQL request may be made to the database server. The result will be stored and compared against an expected result.

DNS: DNS lookups may be performed against the DNS server.

AD (Active Directory): Login attempts may be made against the AD server.

Each service is typically assessed through multiple methods including DNS lookup, IP validation and a direct access method.

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

Business Tasks (Injections/Tasks/Assignments)

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

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 task 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. If teams elect NOT to complete a task, and submit a properly formatted legitimate business explanation as to why, to the requestor in a timely manner, they *MAY* receive credit for the assignment.

All injections will come from the HAL Work Management System tasks@halcorp.biz (not the CISO/CIO email accounts). All injections that specify a ***written report*** must include an attachment that is properly formatted using the HAL memorandum template. Injections that do not specify a written report may be answered with a professionally written email. All correspondence must be professionally written as if communicating with actual corporate executives. Failure to do so may result in loss of points on a task and/or penalties.

All communications must be professionally written, using professional business language, in complete sentences, without spelling or grammar errors.
All emails from the team will be configured to automatically bcc the team's room judge email account (judge.#@halcorp.biz) where the # is the team's assigned letter. If teams modify the email configuration they may disable this function. If the judge does not receive a copy of the team's outbound response to a business task, they will not score that assignment.

Teams are still expected to maintain their local "halcorp.biz" email accounts, and monitor the team "help@" local email account.

CM: All changes not explicitly approved under "emergency change conditions" must be deferred until the next change meeting. **Teams must notify the CIO by email within 30 minutes of intent to defer a task until after the next change meeting.** Teams that to not properly prepare their change requests for a particular task to be delivered at the next change meeting will find it will not be approved, costing the team the points for that task. Teams should bring all current CM documents ***to every CM meeting*** and be prepared to turn in copies for review and scoring.

IR: Teams are encouraged to print out copies of the IR form for use in documenting incidents as soon as they are detected. Teams should complete and submit the form ***by email to ciso@halcorp.biz*** once the incident has been resolved and control of systems regained. Teams have 3 hours from detection of incident to report. Incomplete or late IR reports, or reports not directly tied to a real incident (red team) will not receive credit.

Any CM or IR submissions not made via the appropriate channel will not be scored.

THIS WAS THE ACTUAL FIRST INJECTION FROM THE 2016 SECCDC. THE 2018 FIRST INJECTION WILL BE SIMILAR, BUT MAY CONTAIN ADDITIONAL ASSIGNMENTS. THIS CONTAINS MULTIPLE WORK ASSIGNMENTS, EACH OF WHICH MUST BE ANSWERED SEPERATELY (by hitting reply all to the assignment email).

Subject: Task #16.4-01 & -02

Sorry I'm not able to meet you in person, but we're really swamped right now, between the technical issues we've been experiencing lately, and the personnel changes. Bottom line is your team has been hired to get a remote branch's network and systems up and running as quickly as possible. As I'm sure you will discover shortly, the network and systems were hastily and poorly installed. Alan Hake, our CEO has asked that I relay his welcome and requested you to do the very best job you can in getting your branch's systems and networks optimally configured.

I'm hoping your team can get also your HAL email service up quickly and we can communicate via our own systems. In the meantime, we're using an auxiliary network for the halcorp.biz domain. So until you hear otherwise from me, you will receive work assignments from our workflow management system via the hal.tasks@halcorp.biz email account. Please respond to that account when submitting your work. You can access your team's email client from any web browser. Note that each team shares an email client, and that these clients are pre-configured. Take care not to modify the configuration.

Pay particular attention to how you respond to tasks both in email and written reports. We only accept "professionally written and complete responses". Professionally written and complete responses (emails and reports) provide clear responses to the assignment. They are well written using complete sentences, proper grammar and correct spelling. Responses should begin by addressing the assignment given, specify that the assignment has been completed, and then provide any requested details. You will not receive full credit for assignments that are not responded to with professional communications. If your work specifies a ***written*** report, please use HAL letterhead and attach it to your return email. If an assignment just asks you to respond, then you can include your information in the body of the email.

Many of the documents you will need during your assignment here at HAL can be downloaded from our online repository at www.halcorp.biz. To access the "private" collection simply click on the "Company Documents" link on the right/center of the opening page, and when prompted, enter the password: "Halprivate1!" (without quotes). You may then click any of the hyperlinks to download the associated document.

The following are your first official tasks – note all official HAL tasks are tracked with our brand new workflow numbering system - #16.4-01 would indicate the first task for April 2017, etc.

Task # 16.4-01: Update, patch and harden all systems – submit Change Management (CM) forms when all systems complete and operational.

> You've inherited a set of servers and a firewall. Many of them are out of date or poorly configured. You need to update, patch and harden all systems in accordance with best industry practices. While Change Controls have authorized emergency change conditions until 2PM (the time of the first CM meeting), you must document all changes to systems in the appropriate CM forms and submit the forms (one per server/device) by email before 2PM. Be explicit and detailed. All CM policies and forms can be downloaded from the halcorp.biz site. Email the CIO with the completed CM forms when finished and no later than 2PM. Note: any task you receive before 2PM should be considered pre-authorized under emergency change procedures, and should be included in your CM forms. *If you finish this task before you receive a task and it is still before 2PM, just update the CM forms and submit the revised CM forms with the task response email. Also plan to bring copies of all your CM forms to date to the 2PM Change management meeting (more information follows).*

Task # 16.4-02: Add users to all systems

> We've found that the last team failed to add all users to the systems. At a minimum you must get ALL LOCAL HAL employees, including your team set up with accounts on the EMAIL and AD servers. You will find the phone directory and the company org chart on the halcorp.biz site. Use these to populate the accounts. Note: you may find accounts already configured within your systems. These are most likely administrative accounts associated with our consulting company. Do not delete without permission. Email the CIO when finished and no later than two (2) hours from now.

(Memo continues…)

Why are we showing you an example of the first assignment? Three reasons:

1. Few teams successfully accomplish all parts of the complete assignment.
2. It's a great example of a multi-task memo.
3. Several teams fail to catch the strict requirement that all communications (emails and written reports) must be "professionally written and correct" (a.k.a. "well-written and comprehensive").

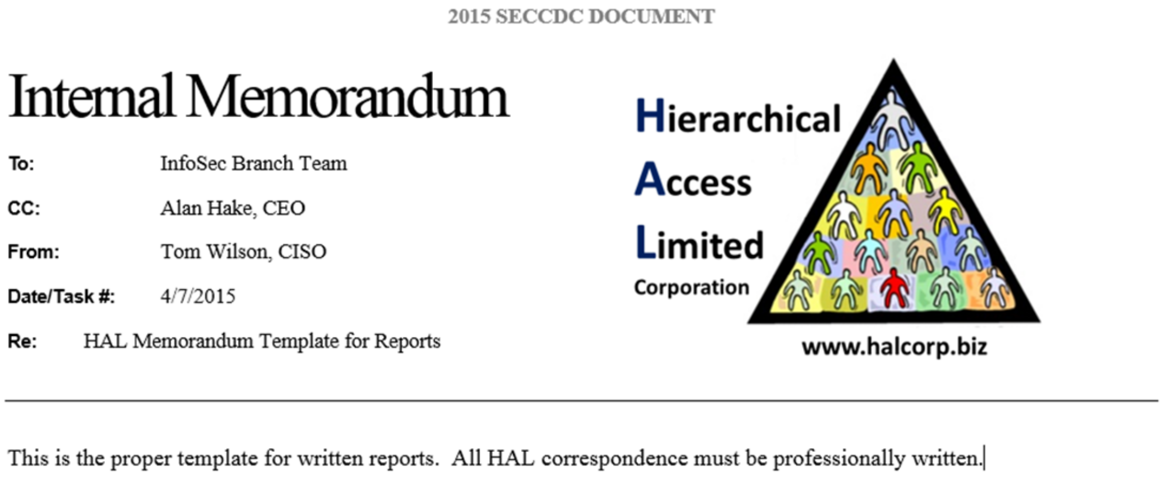
No seriously, very few teams have completed this assignment in its entirety! Why? They may not read it carefully enough, and then it's "easier said than done". The assignment shown included 2 tasks:

1. Report when all servers are configured and operational. This is the "easier said than done" part. Red teams tend to not want your systems operational, so before you can get them all up and running, they go back down. Red teams will start when you do, so you'll just have to do your best to get the servers/services up and running long enough to report them.
2. Add all Local HAL employees to select servers. During previous competitions we were constantly asked – "How can I change the passwords for users that aren't in the Active Directory?" Our answer? Did you add them to the Active Directory at the beginning of the competition? (Silence). You have to add all users to both the Email and Active Directory servers (and any other server they should have accounts on) within the time limit. That's the first task assigned. Even if there are already some users present (which may be part of the scoring system, so confirm before removing), add ALL the LOCAL users. "But where do I get their names from?" Where else? Org Chart? We give it to you; use it!
3. The actual first injection for the 2018 season will begin very similarly to this email, but will contain additional assignments. Read each email carefully!

All questions directly related to the competition rules maybe asked by the Team Captain/Co-Captain to the White Team/Room Judge. All other questions should be directed to the HAL CIO – Paula Alexander via email cio@halcorp.biz, or by phoning the CIO's office if the need is time sensitive – *hint be extra professional on the phone*. Some reports may require you to email the HAL CISO, same advice.

Competition questions not related to the in-game organization should be clearly specified in the subject of the email – e.g. "Competition question: Failure of initial VM image". Refer to the section on Help Desk Requests to the CIO for more information on all tech support requests, including image resets (scrubs).

SAMPLE MEMORANDUM TEMPLATE



2015 SECCDC DOCUMENT

Internal Memorandum

To: InfoSec Branch Team

CC: Alan Hake, CEO

From: Tom Wilson, CISO

Date/Task #: 4/7/2015

Re: HAL Memorandum Template for Reports

Hierarchical
Access
Limited
Corporation
www.halcorp.biz

This is the proper template for written reports. All HAL correspondence must be professionally written.

Business Operations and Reports (Reports)

While Business Tasks are discrete events directly tied to a work task memorandum, business operations and reports are ongoing and routine expectations of each team. Throughout the competition, each team will be expected to review and comply with "corporate" policy documents, including change management and incident response). Most of these documents are available on the halcorp.biz WordPress site. There will be planned meetings and activities that team members are expected to attend, perform, and comply with. Failure to meet these expectations successfully will result in team penalties or fail to remediate points from a red team attack. For example:

- Appointing team change management and incident response officers and reporting to HQ,
- Attending change management and incident response meetings (prepared),
- Submitting properly prepared change management forms indicating successful completion of initial configuration of critical servers/services to HQ within the specified time frame,
- Reporting of identified incidents using properly prepared forms within the specified time,
- Successfully passing a random compliance audit,
- Other reporting requirements …

Penalties or Points will be assessed based upon performance in each business requirement or part of a task. Teams will understand which category the assessment will be awarded on based on the source and type of memorandum or directive received. For example, a memo from the CIO asking the team to install a specific piece of software or hardware would be a business task/injection, while a memo from the Corporate Change Management Officer reminding the teams to submit change management forms, or from the Corporate Computer Security Incident Response Team leader reminding the teams to make scheduled meetings would most likely be business operations & reporting requirement. Just as with Tasks, reports will vary in nature and points will be weighted based upon the difficulty and time sensitivity of the task.

Most tasks will contain multiple parts with point values assigned to each specific part of the task. Some tasks are prerequisites to others, so teams should make every effort to complete all tasks, even if late.

Competition Communications

The competition will use the halcorp.biz email server at **http://mail.halcorp.biz** for all communications and assignments. In addition, an external administrative network will be used as a fail-safe backup for email communications. Team members will be expected to monitor equipment on 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 through competition systems, the team is responsible for making sure that even if their competition network goes down, someone monitors the administrative network for email communications. This administrative network will be independent of the competition network and not subject to Red Team actions. **Teams are similarly prohibited from using or modifying this outside network and systems connected to it, for ANY purpose other than the receipt and response to competition communications.** Software MAY be configured on these systems to restrict use.

NOTE: All assignments from HAL Headquarters WILL BE from the **tasks@halcorp.biz** workflow management email account. Any assignments the team receives or responses to assignments the team sends or receives that are from **tasks@halcorp.biz** or other corporate HAL officer via the halcorp.biz service will be considered invalid and be discarded. The CIO, Chief Change Officer may issue supplemental assignments via their halcorp.biz accounts, but all official injection assignments will come from **tasks@halcorp.biz.** Always select "REPLY ALL" when responding.

The Red Team MAY attempt social engineering by phone, email or IM, but is specifically PROHIBITED from physical interaction with the teams. All official communications will originate from "Corporate" officers, whose accounts will not be spoofed.

White Team Judges

White Team Composition

White Team judges will provide answers to rules questions, and monitor team rules for potential violations. The White team is NOT technical support for competition systems. All competition system and "corporate" questions should be addressed to the CIO/CISO as appropriate.

- In the on-site Regional Competition, there will be two categories of White Team Judges used in the on-site competition:
  - Room "Auditors" – who will remain in the team rooms and assess BITs, and
  - Roving "Auditors" – who will move room to room and conduct audits and random assessments as part of BORs.

Teams will not attempt to interfere with either set of Judges and will respond to questions quickly and openly. Only the team Captain, or in their absence, the Co-Captain should interact directly with the room judge, unless asked a question by the Judge.

Do not attempt to use the Judge's laptop or printer.

Red Team

Red Team Actions

Successful Red Team actions will be divided into two major categories, which guide the impact of their actions on team operations. These categories are:

- Organized crime red team operations: red team operations in this category will result in penalty points for successful attacks, against each team's score. The focus of organized crime red team operations is the penetration of systems with the intent to steal critical information. Each server/service will have designated critical information, so organized crime red team operations focus on
    - Recovery of user IDs 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

  The maximum penalty for this red team category will be managed so as not to exceed 2000 points for the competition. 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, which will be mapped directly to a red team attack. Incident reports not tied to a discrete red team attack in this category will not be scored.

- Hacktivist red team operations: red team operations in this category will focus on disruption of service. Successful red team hacktivist operations will include:
    - Disabling critical server accounts (such as the root/admin account),
    - Corruption of key server files,
    - Modification of server functions or configurations
    - Disabling of assessed services.

  Since the result of successful action in this category will result in losses in the service assessments category, there is no separate penalty. Effective, timely and properly formatted incident reports of hacktivist attacks will earn the team points in the BOR category.

Red Team actions are assessed 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.

In general, red teams will deduct points from the team's total for each instance of the following:

- Red team get admin/root on the system (got root?)
- Red team can deny service to a system (Change passwords, etc.)
- Red team retrieves "critical data" (employee/customer data etc.)
- Red team miscellaneous harassment (web site defacement, etc.)

These points are *per system/per incident*; meaning that a multiple system, repeat attack could have a devastating impact on the team's score.

Teams can mitigate red team actions with effective, efficient incident reporting. ***Incident reports must be properly formatted, and submitted within 2 hours of the attack to receive credit.***
Policies and procedures are available, as well as templates for reports. Successful IR reporting may mitigate up to *50%* of red team attack penalties.

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 penalized a team by 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 again.

Red Team Mentors

Red Team mentors will visit each team room from time to time to provide assistance, mentorship and advice. Teams may specifically request "penetration testing consultant" assistance from the CIO, however depending on the assistance requested and/or provided there may be a penalty for their involvement. If the red team visits a team room, they will be accompanied by a white or gold team member. Teams are to treat them as if they were white team judges, allowing all reasonable and professional accommodation and respect. Red team mentors have volunteered to help teams in need.

Green Badge Visitors and VIPs

From time to time select VIPs and visitors wearing green badges will visit each team room from time to time to observe team performance. Teams should ignore these visitors and not directly interact at all. Should a visitor wearing a green badge ask a question of a competition team member, please notify the white team immediately. If the visitor is accompanied by a white team or gold team member, you may respond when asked. We will make every effort to ensure that visitors do not impact the operations of the teams and the competition, however many visitors represent sponsors who make the competition possible, so we would like to accommodate them when possible.

Team Documentation Requirements

Logs

All student teams will be expected to maintain two sets of logs assessed as part of the competition:

1) **Change management log** (1 log per team – using the provided spreadsheet template). 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 4/2/2018)
- 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 points lost on BOR assessments. 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. Bring an extra copy of your CM documentation to every CM meeting, and expect to turn it in for review and scoring.

2) **Password Storage Log**

Student teams will also be provided with a "confidential" storage log spreadsheet. ALL system usernames and passwords MUST be stored in this document. **Handwritten password logs will not be accepted.** Teams are expected to keep electronic copies of these logs and print them at the end of each business day, or upon request. The hard copy binders used to house these documents should be considered secure for the purposes of the competition. Periodically, White Team "auditors" will audit these logs to determine if the team is vigilant in storing their usernames/passwords.

The password log will be randomly audited and assessed. Scores will focus on successfully recorded user and admin account credentials. 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. *Teams wishing to change these accounts must carefully coordinate these changes with CIO.* Details on how to request these changes will be provided at the start of the competition.

Competition Email System

The SECCDC uses an external email system “http://mail.halcorp.biz” 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 2018 SECCDC event. 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 teams 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 your team’s email account).

hal_x@halcorp.biz (where x=the team letter e.g. hal_a, hal_b…).
judge_x@halcorp.biz (where the Judge’s letter matches the team’s letter).
operations@halcorp.biz (SECCDC Operations account used to communicate with Judges), teams should not use except when responding to a requested email check.
cio@halcorp.biz (HAL’s CIO – used for **ALL** team questions that are “in-game”, including helpdesk requests and proxy server requests.
ciso@halcorp.biz (HAL’s CISO – used for “in-game” interaction, including Incident Reports, and emailed change management documentation).

tasks@halcorp.biz (HAL’s “workflow management system” – used to send and receive work assignments to/from the team. Note this email account is not directly monitored, only archived. The “Automatic BCC” 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, No Credit). Points are then assigned by Operations, and revealed after all teams have competed.

NOTE: In order to avoid teams accidentally “Replying to All” and sending their work assignments to other teams, all emails will come FROM tasks@halcorp.biz, and will be addressed TO: cio@halcorp.biz, with all teams and judges blind carbon copied (BCC). Teams will still treat each memo/email as if it were addressed directly “TO” them. Make sure you are replying to tasks@halcorp.biz when responding, and professionally write your email responses, attaching your any written reports in properly formatted memos where appropriate.

Your email accounts will be pre-configured and passwords provided. It’s the same RoundCube system used during the Prelim, so no supplemental training is needed. Teams have a local email system which they must also monitor, especially a “help” account contained therein.

During the competition, multiple team members may log into and monitor your corporate email account simultaneously. If you are unable to access the email account during the competition, call the CIO’s phone extension or submit a help desk ticket through the service desk.

Do not use other email accounts during the competition (other than those provided on your local competition servers), nor should you attempt to forward halcorp.biz messages to outside email accounts. Doing so will automatically result in points penalties and/or possible disqualification.

Document Repository

A large collection of “corporate policies and documents” has been staged for use in the SECCDC competitions at http://files.halcorp.biz. Advanced copies have been provided to your institutional reps through the SECCDC Portal. These are for your use preparing for, and during, the competition. Note the policies and procedures are subject to change.

Competition Service Support

Team will email the CIO (cio@halcorp.biz) for helpdesk requests, questions and other required communications. Teams will email the CISO for incident response reports and Change Management related questions.
Note: Unless otherwise noted, change management documents will be hand delivered at scheduled change management meetings.

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 infosec@kennesaw.edu.

Student team members should NOT contact competition officials directly. All communications to competition officials must come from the institution representatives.