2020 SECCDC Collegiate Cyber Defense Qualification Competition (SECCDQC)

Southeast Collegiate Cyber Defense Competition

KENNESAW STATE UNIVERSITY
INSTITUTE FOR CYBERSECURITY WORKFORCE DEVELOPMENT

Team Packet
DRAFT
(01/30/20)

Prelim Date:
February 22, 2020

© CSSIA & SECCDC

Table of Contents

Contents

SECCDC Mission and Objectives

The Southeast Collegiate Cyber Defense Qualification Competition (SECCDQC, "the qualifier", the "prelim") provides an opportunity for qualified educational institutions in the Southeast U.S. to compete as part of a national security competition (see www.nationalccdc.org). Qualified educational institutions include those accredited institutions of higher education with information security, information assurance, cybersecurity or computer security related curricula in the states of Alabama, Florida, Georgia, Mississippi, North Carolina, South Carolina, and Tennessee. The Southeast Collegiate Cyber Defense Competition provides a controlled competitive environment that will permit each participating institution to assess their students' depth of understanding and operational competency in managing the challenges inherent in protecting an enterprise network infrastructure and business information systems.

Qualification Overview

Effective Fall 2020, the SECCDQC is managed by the Institute for Cybersecurity Workforce Development at Kennesaw State University, Georgia. The competition tests each student team's ability to secure a networked computer system while maintaining standard business functionality. The scenario involves team members simulating a group of employees from an IT service company that will initiate administration of an IT infrastructure. The teams are expected to manage the computer network, keep it operational, and prevent unauthorized access. Each team will be expected to maintain and provide public services, including, but not limited to: a web site, a secure ecommerce site, an email server, a database server, a domain name server and workstations used by simulated sales, marketing, and research staff as per company policy and mission. Each team will start the competition with a set of identically configured systems.

The objective of the competition is to measure a team's ability to maintain secure computer network operations in a simulated business environment. While this is a technical competition, it is built upon the foundation of business operations, policy, and procedures. A technical success that adversely affects the business operation will result in a lower score as will a business success that results in security weaknesses.

The performance of the student teams will be assessed on their ability to detect and respond to outside threats, including cyber-attack while maintaining availability of existing network services such as mail servers and web servers, respond to business requests such as the addition or removal of additional services, and balance security against varying business needs.

Qualifying teams from the 2020 SECCDQC will have the opportunity to participate in the 2020 Southeast Regional CCDC, April 1-2 at Kennesaw State University.

Competition Goals

1. To promote fair and equitable standards for cyber defense and technology based competitions that can be recognized by industry
2. To evaluate the defensive and responsive skills of each team under matching and specific hardware, software application, and operating system configurations using a joint academic and industry rating scale
3. To demonstrate the effectiveness of each participating institution's academic security program
4. To be staffed by a joint team of academic sponsors and industry professionals
5. To have industry recognition, participation and acceptance
6. To rate the effectiveness of each competitor team against a predefined standard of competition rules
7. To provide a cooperative and competitive atmosphere among industry partners and academia in the area of cyber defense education
8. To provide recognition for participating teams
9. To increase public awareness of academic and industry efforts in the area of cyber defense education

Competition Team Identification

- **Blue Team** - student team representing a specific academic institution or major campus competing in this competition; each team must submit a roster of up to 12 competitors to the Competition Manager. Each competition team may consist of up to eight (8) members chosen from the submitted roster. The remainder of the roster is for substitution in the event a member of the active competition team cannot compete. Substitution in the competition team requires approval from the Competition Manager.

    - Rules specific to the Southeast Region can be found at www.seccdc.org (also available at cyberinstitute.kennesaw.edu/seccdc/). National rules are available at www.nationalccdc.org.

- **Red Team** – Professional network penetration testers from industry approved by the competition director and industry representatives
    - Scan and map the network of each competition team
    - Attempt to penetrate the defensive capabilities of each Blue Team network and modify any acquired environment
    - Assess the security of each Blue Team network
    - Attempt to capture specific files on targeted devices of each Blue Team network
    - Attempt to leave specific files on targeted devices of each Blue Team network
    - Follow rules of engagement for the competition

- **White Team** – Representatives from industry who serve as competition judges, remote site judges, room monitors and security enforcement in the various competition rooms.

  Each team competing remotely from their academic institution must have a remote site judge on site, present during most active times of the competition.

Judges will assess the competition team's ability to maintain their network and service availability based upon a business task and a scoring instrument, delivering task scenarios, scoring of tasks, creating log entries, securing log files, issuing or controlling the timing of tasks, etc. White Team members present in the competition room will assist judges by observing teams, confirming proper task completion, report issues, and assure compliance of rules and guidelines.

- **Gold Team** – Comprised of the Competition Manager, the host site Chief Administrator, as well as representatives from industry and academia who make up the administration team both in planning and during the exercises. Responsibilities include, but are not limited to,
    - Administration and staffing of the cyber defense competition
    - Works with industry partners to orchestrate the event
    - Has the authority to dismiss any team, team member, or visitor for violation of competition rules, inappropriate or unprofessional conduct
    - Makes provision for awards and recognition
    - Manages debrief to teams subsequent to the conclusion of the competition
    - Serves as the final authority on judging and scoring decisions or issues relating to equity or fairness of events or activities and winners of the competition
    - If teams travel to another site, the Gold Team manages activities such as:
        - Greet people
        - Organize food
        - Assist in setting up the competition
        - Assist with hotel / travel arrangements

Initial Connection & Start Flag

Using a NETLAB$^{+™}$ VE powered Cyber Stadium to compete is simple and straightforward. There are two separate systems that are used which interact to provide the services and communication necessary to meet the goals of the CCDC.

System 1 - ISE/Team Portal

This system is totally separate from the competition environment and is used by Blue Teams to display current services, as viewed by the indigenous scoring engine, and communicate to the Competition Support Team, and receive certain notifications. **This system is NOT used for Business Tasks for the SECCDC Prelim, the competition email system is.**

This system is accessed via a browser,

ccdcadmin1.morainevalley.edu

Note that CSSIA supports additional ISE/Team Portals,

ccdcadmin2.morainevalley.edu
ccdcadmin3.morainevalley.edu
ccdcadmin4.morainevalley.edu

Follow the instructions from your competition manager for the specific ISE/Team Portal that will be used for your CCDC Qualifier. Likely ccdcadmin1 will be used for section 1 (AM Session), ccdcadmin2 for section 2 (PM Session).

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

> team1, team2, team3, etc… up to team20.
> *<NOTE: these numbers are different than the email assignments (@seccdc.org) and should not be confused>*

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

At the start of the competition session, the competition officials will release a second communication, providing the team password (applicable to all accounts for a particular team) required to access the Competition Stadium systems.

System 2 - The NETLAB+™ VE Competition Stadium

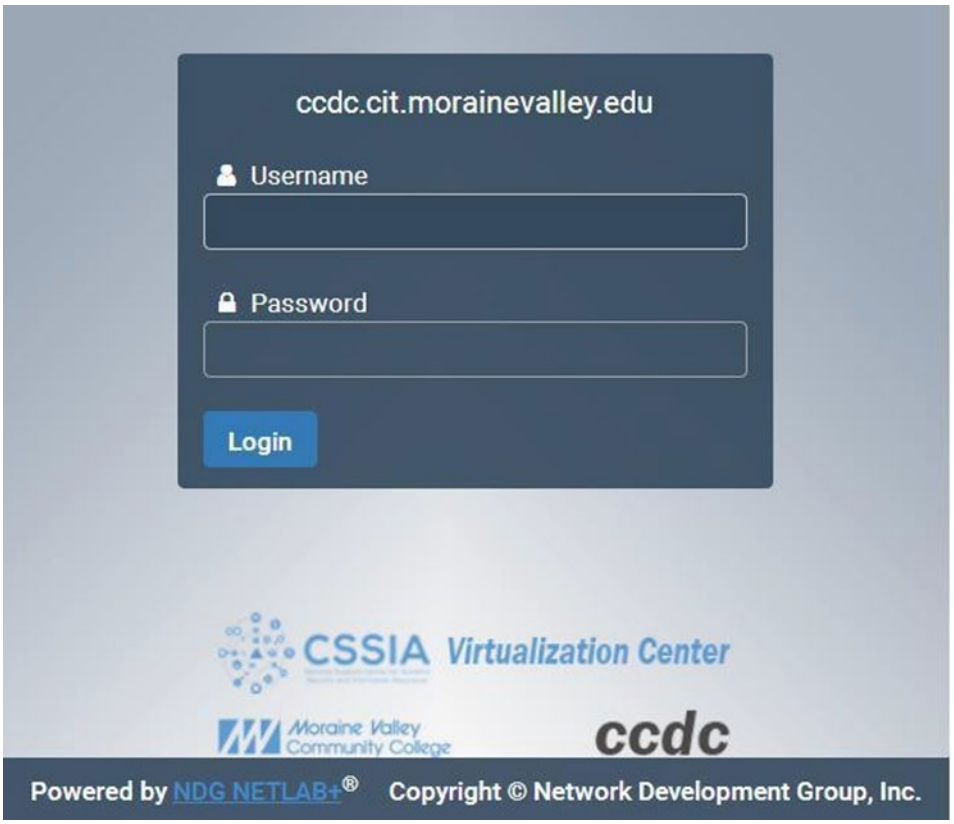
This is the system used to access and manage the competition network. This too is accessed via a browser:

ccdc.cit.morainevalley.edu

Generally, the client requirements are easily met with simple browser. The bandwidth requirement is 256 kb/s up and down per client minimum. **Ports 80, 443 must be allowed outbound.** A 10 Mb/s

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

The Competition Stadium login screen is shown below.



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

There are eight accounts per team that may be used to connect to the Cyber Competition Stadium. For team1 they are:

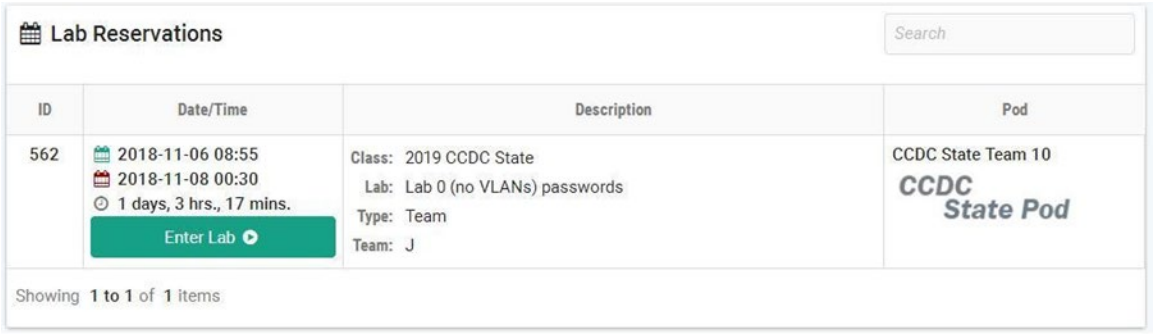
v1u1, v1u2, v1u3, v1u4, v1u5, v1u6, v1u7, v1u8

Accounts for other teams follow the same pattern. For team20 the accounts are:

V20u1, v20u2, v20u3, v20u4, v20u5, v20u6, v20u7, v20u8

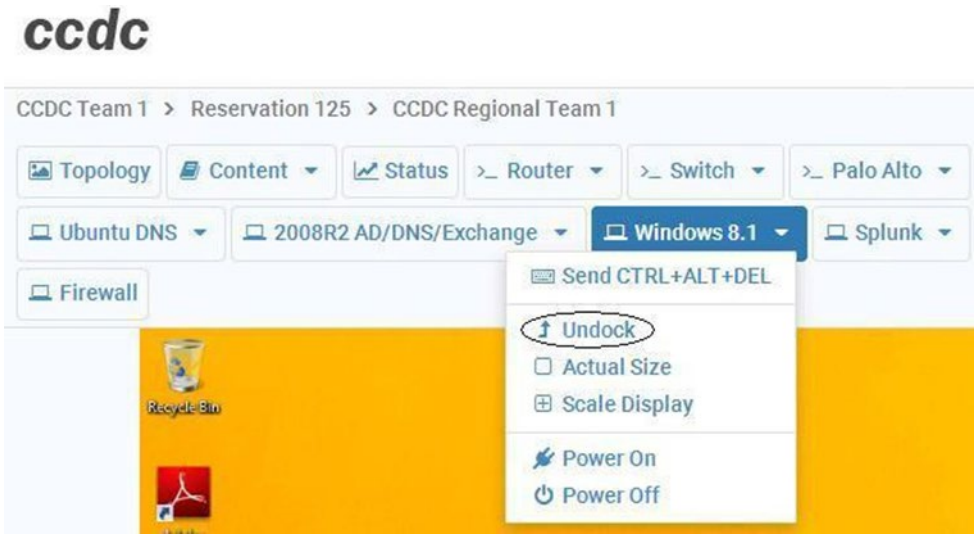
Note that teams initially only have access to the ISE/Team Portal.
Team assignments are issued prior to the event so the proper accounts are known. The password needed to access the Competition Stadium is issued by the ISE via an inject to inform teams of their initial password applicable for all team accounts.

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



Each team member can click on 'ENTER LAB' for their respective lab/pod reservation to gain access to their competition network. The competition network topology, shown later in this document, should be clearly visible. To access individual VMs simply click on the respective VM name at the top of the screen.

Users might wish to work on a VM in a separate window which they can do by the 'Undock' feature.



Summary of Events/Timetable for Competition Session

- Week prior to competition – team receives email, ISE and test VM credentials, confirms login to seccdc.org email systems and conducts connectivity test with competition systems.
- 1 Hour prior to start of session – room judge inspects systems.
- 30 minutes prior to start of session – team assumes control of local systems, log into competition email and ISE systems and reports ready to compete.
- At start of competition – NetLab VM credentials released *through ISE system*. The initial task email will be sent *through the SECCDC email system at* ***http://halinc.biz***. Competition sessions last 5 hours.

Network & Team Site Description

- Each competition network will be located remotely from the competition site and will be logically isolated from all other competing Blue Teams. All Teams will access the competition network via a browser connection.
- Each competition network will therefore be physically and logically isolated from the hosting organization's network.
- Each competing Blue Team will compete from their own institution and from a dedicated, secure location where all team members are collocated **together with the local site judge**. Computer Labs, classrooms or conference rooms are considered ideal locations. The secure location is to have restricted access to only Blue Team members, remote site judges, local administrators and technical support. Competition workstations must be able to access the internet.
- The White Team and each respective Blue Team will communicate with each other via Web-based email (@halinc.biz). Blue teams will communicate technical support issues to the host team via the ISE/Team Portal, residing at Moraine Valley Community College.
- Red Team activity may be either externally or internally sourced with respect to the remote competition network. At no time will the Red Team have access outside the remote NETLAB+™ environment.
- Each Blue Team network will be monitored by a scoring system operating within the remote network. An indication of services, as viewed by the indigenous scoring engine, will be made available to each Blue Team via the ISE/Team Portal.
- A logical diagram of the team logical network is contained within this Team Packet. However, it is subject to change and /or modification as decided by the Competition Manager.

Schedule – Note: All Times are Eastern Time Zone

Saturday, February 22, 2020
Note that the prelim sessions are 5 hours in duration, with 2 sessions/day. Teams will only compete in 1 of these sessions as assigned:

Timeline:
Session 1 (AM Session):

8:00am	Team judges review competition systems to ensure within rules. Once judges are finished, teams allowed to access remote system; Teams send a "ready" email to operations@seccdc.org.
8:30am	Team access the ISE/Team Portal system at **ccdcadmin1.morainevalley.edu** and respond to any information requests
9:00am	Start of Competition; Teams will receive competition system account credentials for the NetLab+/VM Competition Arena (ccdc.cit.morainevalley.edu) ***through*** the ISE/Team Portal system (ccdcadmin1); Scoring begins
2:00pm	Competition session ends/Scoring ends

Session 2 (PM Session):

2:00pm	Team judges review competition systems to ensure within rules. Once judges are finished, teams allowed to access remote system; Teams send a "ready" email to operations@seccdc.org and receive competition system account information, as needed.
2:30pm	Team access the ISE/Team Portal system at **ccdcadmin2.morainevalley.edu** and respond to any information requests
3:00pm	Start of Competition; Teams will receive competition system account credentials for the NetLab+/VM Competition Arena (ccdc.cit.morainevalley.edu) ***through*** the ISE/Team Portal system (ccdcadmin2); Scoring begins
8:00pm	Competition session ends/Scoring ends

Teams are responsible for coordinating meals and rotating out of the competition for breaks. Everyone except for active room judges and competition team members must leave the competition room once the competition begins.

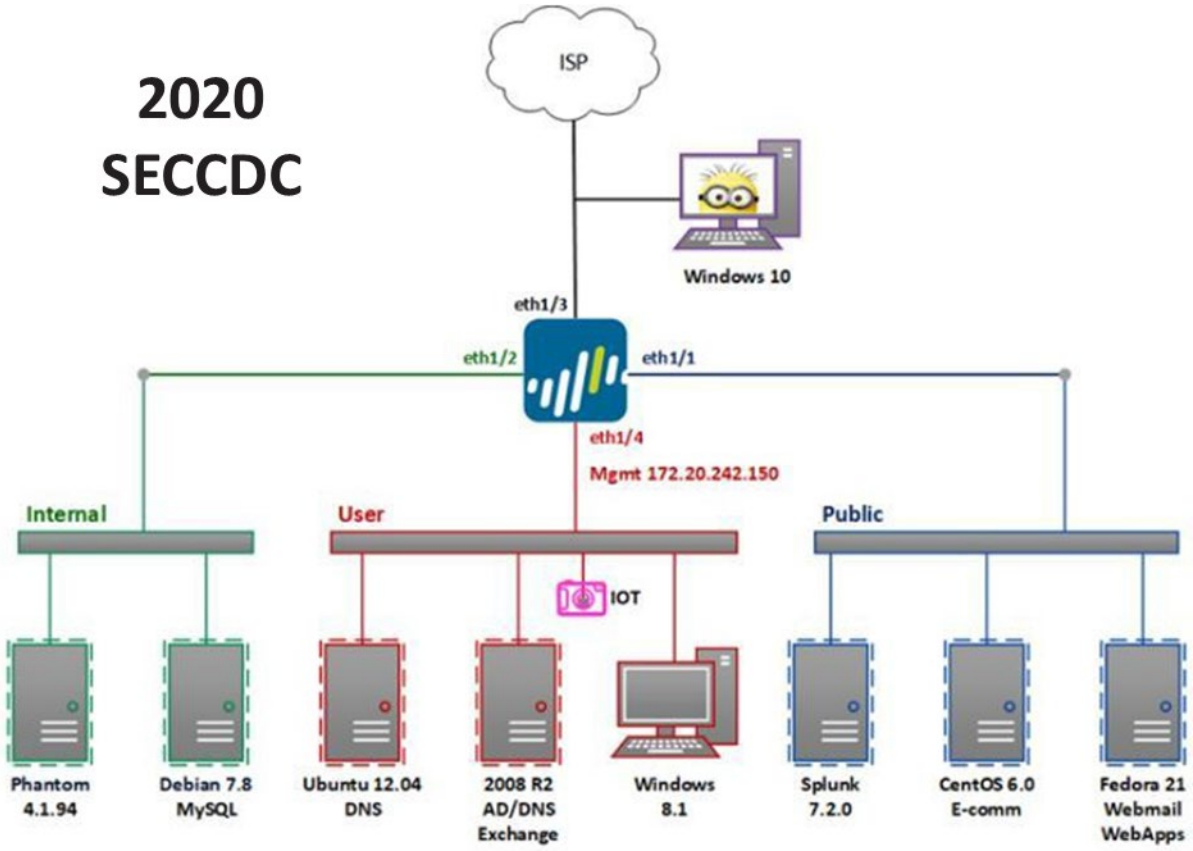
An announcement of the top 8 teams to be invited to the on-site regional in April will be made by 5pm **Friday, Feb. 28, 2020**. Details on team performance will be provided as soon as available.

Systems

1. Each team will start the competition with identically configured systems.
2. Teams may not add or remove any computer, printer, or networking device from the designated competition area.
3. This document provides the overall system architecture, network configuration, and initial set-up of the competition.
4. Teams should not assume any competition system is properly functioning or secure.

5. Throughout the competition, Green Team and White Team members will occasionally need access to a team's systems for scoring, troubleshooting, etc. Teams must allow Green Team and White Team member access when requested.
6. Network traffic generators may be used throughout the competition to generate traffic on each team's network. Traffic generators may generate typical user traffic as well as suspicious or potentially malicious traffic from random source IP addresses throughout the competition.
7. Teams must maintain specific services on the "public" IP addresses assigned to their team and stipulated by this document. Moving services from one public IP to another is not permitted unless directed to do so by a task. Likewise, teams are not permitted to change the internal addressing or VLAN scheme of the competition network unless directed to do so by a task.
8. Teams may re-task servers, moving a service from one server to another as long as the outside "public" IP address of the service remains the same. It is the responsibility of the team to understand all the particulars of scoring a service when doing so.
9. Teams are not permitted to alter the system names or IP address of their assigned systems unless directed by a task; this may affect the results of the scoring mechanism.
10. In the event of system lock or failure, teams will be able to perform a complete restoration from within the administration console of the remote system. This will reset any system to its initial starting configuration. The number of system restorations will be tracked and negatively impact scores at the discretion of the White Team. Teams should also consider that system restoration will take time.
11. Systems designated as user workstations within the competition network are to be treated as user workstations and may not be re-tasked for any other purpose by teams.
12. Teams may not modify the hardware configurations of workstations used to access the competition network.
13. Servers and networking equipment may be re-tasked or reconfigured as needed.

Competition Topology



- Teams have access to 10 VMs – 7 servers, 2 workstations, and the Palo Alto firewall.
- All servers, workstations, and Palo Alto firewall are virtual machines under the management of NETLAB+™ VE.
- Teams do not have access to the underlying layer 2 switch.
- The firewall shown in the topology is a Palo Alto VM, version 8.0.0, which is licensed by Palo Alto.

  You can access the Palo Alto VM either directly, which yields a command window, or via a browser 172.20.242.150 from any of the User LAN VMs. The PA user/password are,

  admin/changeme

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

- Each team has the following Palo Alto internal addresses:

Internal, e1/2	172.20.240.254/24
User, e1/4	172.20.242.254/24
Public, e1/1	172.20.241.254/24

- Core IP addresses are the following:

Team #	Palo Alto e1/3 Outbound to Core	Core connection to Palo Alto	"Public" IP pool
01	172.31.21.2/29	172.31.21.1	172.25.21.0/24
02	172.31.22.2/29	172.31.22.1	172.25.22.0/24
03	172.31.23.2/29	172.31.23.1	172.25.23.0/24
04	172.31.24.2/29	172.31.24.1	172.25.24.0/24
05	172.31.25.2/29	172.31.25.1	172.25.25.0/24
06	172.31.26.2/29	172.31.26.1	172.25.26.0/24
07	172.31.27.2/29	172.31.27.1	172.25.27.0/24
08	172.31.28.2/29	172.31.28.1	172.25.28.0/24
09	172.31.29.2/29	172.31.29.1	172.25.29.0/24
10	172.31.30.2/29	172.31.30.1	172.25.30.0/24
11	172.31.31.2/29	172.31.31.1	172.25.31.0/24
12	172.31.32.2/29	172.31.32.1	172.25.32.0/24
13	172.31.33.2/29	172.31.33.1	172.25.33.0/24
14	172.31.34.2/29	172.31.34.1	172.25.34.0/24
15	172.31.35.2/29	172.31.35.1	172.25.35.0/24
16	172.31.36.2/29	172.31.36.1	172.25.36.0/24
17	172.31.37.2/29	172.31.37.1	172.25.37.0/24
18	172.31.38.2/29	172.31.38.1	172.25.38.0/24
19	172.31.39.2/29	172.31.39.1	172.25.39.0/24
20	172.31.40.2/29	172.31.40.1	172.25.40.0/24

- VM data are as follows:

	Version	IP	Username	Password
INTERNAL				
Phantom	4.1.94	172.20.240.10	root admin (Web UI)	!Password123 !Password123
Debian 7.8 MySQL	Debian 7.8	172.20.240.20	root sysadmin	!Password123 !Password123
USER				
Ubunbtu 12.04 DNS	Ubunbtu 12.04	172.20.242.10	sysadmin	!Password123
2008 R2 AD/DNS/Exchange	2008 R2	172.20.242.200	administrator	!Password234
Windows 8.1	Windows 8.1	172.20.242.100	binddn	!Password123
PUBLIC				
Splunk	7.2.0	172.20.241.20	root admin (Web UI)	changemenow changeme
CentOS 6.0 E-comm	CentOS 6.0	172.20.241.30	root	!Password123
Fedora 21 Webmail/WebApps	Fedora 21	172.20.241.40	root	!Password123
Palo Alto	PAN OS 8.0.0	172.20.242.150	admin	changeme
Windows 10	Windows 10	172.31.xx.5	minion	kingbob

This table is accessible on the topology tab of NETLAB+™ VE, via the “Content” upper left. Specific NAT translations are as follows:

INTERNAL	Local IP	'Public' IP*
Phantom	172.20.240.10	172.25.20+team#.97
Debian MySQL	172.20.240.20	172.25.20+team#.20
USER		
Ubuntu DNS	172.20.242.10	172.25.20+team#.23
2008 R2 AD/DNS/Exchange	172.20.242.200	172.25.20+team#.27
Windows 8.1	172.20.242.100	dynamic
PUBLIC		
Splunk	172.20.241.20	172.25.20+team#.9
CentOS E-Comm	172.20.241.30	172.25.20+team#.11
Fedora Webmail/WebApps	172.20.241.40	172.25.20+team#.39

**Thus 'Public' IP addresses will be in the range of 172.25.21.XX (for team 1) to .40.XX (for team 20).*

- Teams should be attentive to monitor inject requests and notifications via the Team Portal/ISE.
- Red Team activity will be active throughout the event. At no time will the Red Team have access outside the Cyber Stadium perimeter. Neither will the Red Team be given direct access to any Team network or local system directly via the NDG NETLAB+™ VE system.
- Each Blue Team network will be monitored by a scoring system operating within the remote network. An indication of services, as viewed by the indigenous scoring engine, will be made available to each Blue Team via the Team Portal/ISE.

- **While every effort is made to provide a stable and well defined competition topology, it is subject to change and /or modification as decided by the CCDC Competition Director.**

Functional Services

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

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

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

Webmail-HTTP
Email service via HTTP will be tested. Note that for such services numerous accounts may be used, selected randomly throughout the competition.

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

POP3
Proper delivery of email will be tested.

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

Precise delineation of services is subject to change. Take note of scored services during the event from the ISE.

Business Tasks

Throughout the competition, each team will be presented with identical business tasks, **delivered via the seccdc.org email system**. Points will be awarded based upon successful completion of each business task. Tasks will vary in nature and points will be weighted based upon the difficulty and time sensitivity of the assignment. Tasks may contain multiple parts with point values assigned to each specific part of the task. Each business task may have an indication of relative importance or value assigned and a specific time period in which the assignment must be completed. Business tasks may involve modification to or addition of services.

Competition Rules: Acknowledgement & Agreement

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

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

See www.seccdc.org (cyberinstitute.kennesaw.edu) and www.nationalccdc.org for a complete set of rules.

Internet Usage

1. Competition systems will have access to the Internet for the purposes of research and downloading patches. Internet activity will be monitored and any team member viewing inappropriate or unauthorized content will be immediately disqualified from the competition. This includes direct contact with outside sources through AIM/chat/email or any other non-public services. For the purposes of this competition inappropriate content includes pornography or explicit materials, pirated media files or software, 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.
2. 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 purchase or fee. Only resources that could reasonably be available to all teams are permitted. Teams may not use any external, private electronic staging area or FTP site for patches, software, etc. during the competition. All Internet resources used during the competition must be freely available to all other teams.
3. Public sites such as Security Focus or Packetstorm are acceptable. Only public resources that every team could access if they chose to are permitted. No peer to peer or distributed file sharing clients or servers are permitted on competition networks.
4. All network activity that takes place on the competition network may be logged and is subject to release. Competition officials are not responsible for the security of any personal information, including login credentials that competitors place on the competition network.

Scoring

1. Scoring will be based on keeping required services up, controlling/preventing un-authorized access, mitigating vulnerabilities, and completing business tasks that will be provided throughout the competition. Teams accumulate points by successfully completing tasks, maintaining services, and by submitting incident reports. Teams lose points by violating service level agreements, usage of recovery services, and successful penetrations by the Red Team.
2. Scores will be maintained by the White Team. Individual tracking of services will be available to respective teams during the competition. Blue Team members should use available service tracking reports and internal testing to assess the integrity of their network. Blue Team members should refrain from making direct requests to the White Team for routine service verification.
3. Any team action that interrupts the scoring system is exclusively the fault of that team and will result in a lower score. Should any question arise about specific scripts or how they are functioning, the Team Captain should immediately contact the competition officials to address the issue.
4. Any team that tampers with or interferes with the scoring or operations of another team's systems will be disqualified.
5. Teams are required to provide incident reports for each Red Team incident they detect. Incident reports can be completed as needed throughout the competition and submitted to hal.cio@seccdc.org within the SECCDC email system. Incident reports must contain a description

of what occurred (including source and destination IP addresses, timelines of activity, passwords cracked, etc.), a discussion of what was affected, and a remediation plan. The White Team will assess scores for incident report submission based on clarity, thoroughness, and accuracy. The White and Gold Teams may also, at their discretion, assess negative scores for frivolous, unnecessary, or excessive communication.

6. The winner will be based on the highest score obtained during the competition. Point values are broken down as follows:

25%	Functional services uptime as measured by scoring engine (number of successful assessments divided by total number of assessments)
50%	Successful completion of task scenarios will result in varying points, depending upon the importance or complexity of the task scenario
25%	Incident Response and Red Team Assessment

The formula used is:
Service uptime (up to 100 pt.) + Tasks total (up to 200 pts.) – [Red team penalties (up to 100 pts.) less IR mitigation (up to 50% of Red Team penalties)] /3. The resulting score is on a zero to 100 scale. Teams earning less than Zero points will be normalized to zero points.

Precise percentage breakdown and any penalties for rules or policy violations will be determined by the Gold Team.

Questions and Disputes

1. Team captains are encouraged to work with the local site judge and competition staff to resolve any questions or disputes regarding the rules of the competition or scoring methods before the competition begins. Protests by any team will be presented by the Team Captain to the competition officials as soon as possible. Competition Gold Team officials will be the final arbitrators for any protests or questions arising before, during, or after the competition and rulings by the competition officials are final.
2. In the event of an individual disqualification, that team member must leave the competition area immediately upon notification of disqualification and must not re-enter the competition area at any time. Disqualified individuals are also ineligible for individual awards or team trophies.
3. In the event of a team disqualification, the entire team must leave the competition area immediately upon notice of disqualification and is ineligible for any individual or team award.

Post Prelim Activity

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

Whether feedback is positive or negative, participants are forbidden from publishing, posting on the internet, or publicly communicating details of the competition other than what is available at www.cssia.org or www.seccdc.org. They are also forbidden from publishing, posting on the internet, or publicly communicating details or assessments of the Preliminary CCDC, or assessments of the performance of any team, or speculations concerning different possible outcomes. Institutions that fail to adhere to this rule may be refused participation in future competitions.

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

2020 Sponsors:

PLATINUM SPONSOR

Raytheon

GOLD SPONSOR

IBM

GOLD SPONSOR

paloalto NETWORKS

GOLD SPONSOR

AIR FORCE CIVILIAN SERVICE

GOLD SPONSOR

SPAWAR Systems Center ATLANTIC

SILVER SPONSOR

SAIC Redefining Ingenuity

CSSIA National Support Center for Systems Security and Information Assurance