

*Collegiate Cyber
Defense Competition*



Western Regional
Collegiate Cyber Defense Competition

Qualification Team Packet

January 31, 2015

Contents

Western Regional CCDC Mission and Objectives	3
Qualification Overview	3
Competition Goals	3
Competition Team Identification.....	4
Competition Rules: Acknowledgement & Agreement	5
Schedule - Times are PST	5
Initial Connection & the Start Flag.....	6
Network & Team Site Description	8
Systems	9
Functional Services	9
Business Tasks.....	10
Questions and Disputes	10
Summary	10
Appendix - Addressing Access Problems to NETLAB+™ Systems	11
2015 NCCDC Rules with WRCCDC local rules at bottom	12

Western Regional CCDC Mission and Objectives

The Western Regional Collegiate Cyber Defense Competition (CCDC) provides an opportunity for qualified educational institutions in the Western Regional to compete, and is part of a national organization (see www.nationalccdc.org) to provide a unified approach across nine regions of the country. Qualified educational institutions include those with information assurance or computer security curricula. The Western Regional Collegiate Cyber Defense Competition is designed to provide a controlled competitive environment that will permit each participating institution to assess their students' depth of understanding and operational competency in managing the challenges inherent in protecting an enterprise network infrastructure and business information systems.

Qualification Overview

The Western Regional Collegiate Cyber Defense Qualification Competition (WRCCDQC) is designed to test each student team's ability to secure a networked computer system while maintaining standard business functionality. The scenario involves team members simulating a group of employees from an IT service company that will initiate administration of an IT infrastructure. The teams are expected to manage the computer network, keep it operational, and prevent unauthorized access. Each team will be expected to maintain and provide public services: a web site, a secure web site, an email server, a database server, an online curriculum server, and workstations used by simulated sales, marketing, and research staff as per company policy and mission. Each team will start the competition with a set of identically configured systems.

The objective of the competition is to measure a team's ability to maintain secure computer network operations in a simulated business environment. This is not just a technical competition, but also one built upon the foundation of business operations, policy, and procedures. A technical success that adversely impacts the business operation will result in a lower score as will a business success which results in security weaknesses.

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

The top 8 teams from the 2015 WRCCDQC will have the opportunity to participate in the 2015 Western Regional CCDC, March 26-29, 2014, hosted at Cal Poly Pomona.

Competition Goals

1. To promote fair and equitable standards for cyber defense and technology based competitions that can be recognized by industry
2. To evaluate the defensive and responsive skills of each team under exact hardware, software application, and operating system configurations using a joint academic and industry rating scale
3. To demonstrate the effectiveness of each participating institution's academic security program

4. To have industry recognition, participation and acceptance of each competition
5. To rate the effectiveness of each competition against a predefined standard of competition rules
6. To provide a cooperative and competitive atmosphere among industry partners and academia in the area of cyber defense education
7. To provide recognition for participating teams
8. To increase public awareness of academic and industry efforts in the area of cyber defense education

Competition Team Identification

National CCDC rules apply with only a couple modifications for local use. Please refer to National rules for complete information: www.nationalccdc.org

- **Blue Team** – a unique 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 WRCCDC Lead Judge. 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 WRCCDC Lead Judge.
- **Red Team** – Professional network penetration testers from industry approved by the WRCCDC Executive Team
 - 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 and academia who serve as competition judges, remote site judges, room monitors and security enforcement in the various competition rooms.

Judges will assess the competition team's ability to maintain their network and service availability based upon a business inject and a scoring instrument, delivering inject scenarios, scoring of injects, creating log entries, securing log files, issuing or controlling the timing of injects, etc.

Each team competing remotely from their academic institution must have a remote site judge on site, present during most active times of the competition. Remote Site Judges, representing White Team members, will be present in the competition room to assist judges by observing teams, confirming proper inject completion, report issues, and assure compliance of rules and guidelines.

- **Lead Judge**
 - Serves as the final authority on scoring decisions or issues relating to equity or fairness of events or activities
 - Final authority of all judging decisions, including assessment of final scores and winners of the competition
- **Gold Team** – Comprised of the Competition Manager, the host site Chief Administrator who make up the administration team both in planning and conducting 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
- **Black Team** – Tech support – assists with any technical needs necessary to maintain the integrity of the competition.

Competition Rules: Acknowledgement & Agreement

Competition rules are applicable to all participants of the WRCCDQC. 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 WRCCDC Virtual Competition Stadium 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.

Schedule - Times are PST

WRCCDC Qualifier Schedule

Friday Night Distribution of ISE/Team Portal passwords & WebEx Invite

Saturday

7:00am Join WebEx meeting

7:30am Team access the ISE/Team Portal and respond to the Welcome inject

7:45am NetLab credentials distributed via ISE

8:00am	Start Flag of Competition; scoring begins
2:00pm	Competition ends/Scoring ends
2-3:00pm	Debrief

Winners might be announced before the end of the competition day. However, if necessary, an email announcement will be issued within a few days after the competition.

Initial Connection & the Start Flag

Using a NETLAB⁺ 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 (Inject Scoring System)/Team Portal

This system is totally separate from the competition environment and is used by Blue Teams to display current services, as viewed by the indigenous scoring engine, communicate to the White Team, and receive inject tasks and notifications. This system is accessed via a browser.

<https://fry.wrccdc.csupomona.edu>

Follow the instructions from your competition manager should the specific ISE/Team Portal change.

The screenshot shows the 'Inject Scoring Engine 3.8' login interface. At the top, a blue header bar contains the title. Below this, a navigation sidebar on the left lists 'Dashboard' and 'System Time: Wed, 05 Dec 2012 04:02:20 +0000'. The main content area features a 'Welcome to the Collegiate Cyber Defense Competition Scoring Engine.' message with a 'Please sign in to continue.' prompt. Below the welcome message is a 'User login' section with fields for 'Username: *' and 'Password: *', a green 'Log in' button, and a link for 'Request new password'.

Students should login to the ISE first to initiate communication with the competition judges.

There is one account per team that may be used to connect to the ISE where multiple logins using the same account is permissible. The accounts are,

team1, team2, team3,

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 inject task, usually identified as "Welcome" or something similar. The task simply requests a response back by creating a

submission in the ISE to the competition judges, signaling that access to the ISE has been successful, and that the responding team is ready to compete.

Once the competition judges have verified that all teams are ready to compete, or have provided ample time to respond, the competition judges will release a second inject, providing the team password (applicable to all accounts for a particular team) required to access,

System 2 - The NETLAB+™ / WRCCDC Virtual Competition Stadium

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

<http://bender.wrccdc.csupomona.edu>

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

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

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

NDG **NETLAB+®** (VMware)

Username

Password

Login

[Forgot Password?](#)

POWERED BY

NDG

NETLAB+®

NETLAB+® provides remote access to lab equipment and curriculum. To access, you need a user ID and password, assigned by your instructor or local system administrator.

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

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

System	Web Browser	Version	Status
Windows	Mozilla Firefox	3.6.15	Supported
	Internet Explorer	8.0.6	Supported
	Apple Safari	5.0.2	Beta
	Google Chrome	7.0.517	Beta
Mac	Mozilla Firefox	3.6.15	Supported
	Apple Safari	5.0.2	Beta
Linux	Mozilla Firefox	3.6.15	Supported


Copyright © [Network Development Group, Inc.](#) The programs included herein are subject to a restricted use license and can only be used in conjunction with this application.

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

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

There are eight accounts per team that may be used to connect to the WRCCDC Virtual Competition Stadium. These will be handed out in the ISE right before the competition begins.

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

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

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 should be clearly visible after entering the lab. Access individual VMs simply by clicking on them.

When leaving the WRCCDC Virtual Competition Stadium environment, **don't hit WE'RE DONE**. This will end your reservation, and shut down your systems. Upon rescheduling, your systems will revert back to the initial state of the competition.

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.
- Blue Teams may compete from their own institution, in which case their institution must provide workstations in conformance with aforementioned requirements. Blue Teams competing from their own institution must do so from a dedicated, secure location where all team members are collocated together with the local site judge. Classrooms or conference rooms are considered ideal locations. The secure location is to have restricted access to only Blue Team members, remote site judges, local administrators and technical support. Competition workstations and servers inside NETLAB environment are able to access the internet but are restricted by an established whitelist.
- The White Team and each respective Blue Team will communicate with each other via the NetLab chat (Black Team), WebEX (White Team & Gold Team), the ISE/Team Portal and phone.
- All red team activity will originate within the competition environment. Any such activity sourced from outside RFC1918 address space should immediately be brought to the attention of the white and black teams for further investigation.

- 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.

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. Teams should not assume any competition system is properly functioning or secure.
4. Throughout the competition, Black Team and White Team members will occasionally need access to a team's systems for scoring, troubleshooting, etc. Teams must allow Black Team and White Team member access when requested.
5. 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.
6. Teams must maintain specific services on the "public" IP addresses assigned to their team and stipulated by this document. Moving services from one public IP to another is not permitted unless directed to do so by an inject.
7. 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.
8. 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. Teams should also consider that system restoration will take time.
9. 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.
10. Teams may not modify the hardware configurations of workstations used to access the competition network.
11. Servers and networking equipment may be re-tasked or reconfigured as needed.

Functional Services

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

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

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

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

FTP - Successful access to a file repository will be tested via the FTP protocol with authentication. Some indication of file integrity will be examined.

DNS - DNS lookups will be performed against the DNS server. A DNS name will be requested, and any response will be validated against an accepted value, usually a known IP address. Each successfully served request will be awarded points.

Business Tasks

Throughout the competition, each team will be presented with identical business tasks. Points will be awarded based upon successful completion of each business task. Tasks will vary in nature and points will be weighted based upon the difficulty and time sensitivity of the assignment. Tasks may contain multiple parts with point values assigned to each specific part of the tasking. Each business task 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 or addition of services.

Questions and Disputes

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

Summary

All Competition Organizers - Gold, White, Red, and Black Teams - strive to make the WRCCDQC 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 WRCCDC.org. They are also forbidden from publishing, posting on the internet, or publicly communicating assessments of the WRCCDQC, nor assessments of the performance of any

team, nor speculations concerning different possible outcomes. Institutions that fail to adhere to this rule may be refused participation in future competitions.

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

Appendix - Addressing Access Problems to NETLAB+™ Systems

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

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

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

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

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

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

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

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

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

```
>pathping {cyber stadium url such as bender.wrccdc.csupomona.edu }
```

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

```
#mtr --report {cyber stadium url such as bender.wrccdc.csupomona.edu }
```

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

The problem of network connectivity is usually at the local institution from which the connection is made. Though there may seem to be adequate bandwidth, local institutions must assure synchronous service without undue filtering.

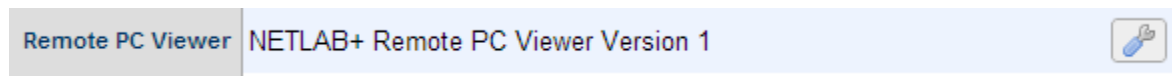
There may be a need for special provisioning at local institutions, even bypassing filters and firewalls for dedicated traffic to the stadium(s). Towards this end it is helpful to note the level of trust and the benign nature of traffic coming from the stadium(s). Though malicious traffic may be present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

Rarely, a remote site will experience difficulty due to packet loss somewhere in route in the big white cloud, and is not a result of faults either at the local site or Cal Poly Pomona. Institutions must contact their ISP to address such difficulties.

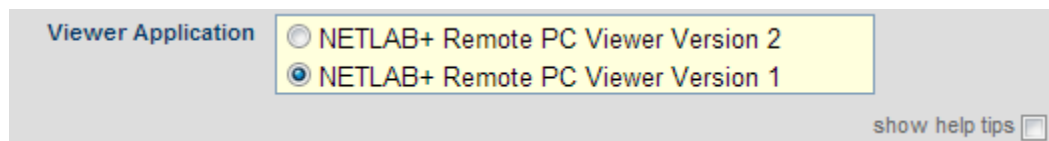
Even with excellent connectivity, there may still be problems with using the NETLAB+™ platform. The NETLAB+™ viewer has been programmed using java, and is sensitive to the specific combination of OS/browser/java version being used. With each update of java, the NETLAB+™ viewer may be affected.

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

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



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



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

2015 NCCDC Rules with WRCCDC local rules at bottom

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

Throughout these rules, the following **terms** are used:

- Gold Team/Operations Team/Executive Team - competition officials that organize, run, and manage the competition.

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

1. Competitor Eligibility

- Competitors in CCDC events must be full-time students of the institution they are representing.
 - Team members must qualify as full-time students as defined by the institution they are attending.
 - 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.
 - 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.
 - 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.
- Competitors may only be a member of one team per CCDC season.

2. Team Composition

- a. Each team must submit a roster of up to 12 competitors to the competition director of the first CCDC event they participate in during a given CCDC competition season. Rosters must be submitted at least two weeks prior to the start of that event. All competitors on the roster must meet all stated eligibility requirements. No changes to the team roster will be permitted after the team competes in their first CCDC event. The competition team must be chosen from the submitted roster. A competition team is defined as the group of individuals competing in a CCDC event.
- 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. Competition Director will review the reason for tardiness and make the final determination.
- g. Each team will designate a Team Captain for the duration of the competition to act as the team liaison between the competition staff and the teams before and during the competition. In the event of the Team Captain's absence, teams must have an identified team liaison serving as the captain in the competition space at all times during competition hours.
- h. An institution is only allowed to compete one team in any CCDC event or season.

3. Team Representatives

- a. Each team must have at least one representative present at every CCDC event. The representative must be a faculty or staff member of the institution the team is representing.
- b. Once a CCDC event has started, representatives may not coach, assist, or advise their team until the completion of that event (including overnight hours for multi-day competitions).
- c. Representatives may not enter their team's competition space during any CCDC event.
- d. Representatives must not interfere with any other competing team.

- e. The representative, or any non-team member, must not discuss any aspect of the competition event, specifically event injections, configurations, operations, team performance or red team functions, with their team during CCDC competition hours and must not attempt to influence their team's performance in any way.

4. Competition Conduct

- a. Throughout the competition, Operations and White Team members will occasionally need access to a team's system(s) for scoring, troubleshooting, etc. Teams must immediately allow Operations and White Team members' access when requested.
- b. Teams must not connect any devices or peripherals to the competition network unless specifically authorized to do so by Operations or White Team members.
- c. Teams may not modify the hardware configurations of competition systems. Teams must not open the case of any server, printer, PC, monitor, KVM, router, switch, firewall, or any other piece of equipment used during the competition. All hardware related questions and issues should be referred to the White Team.
- d. Teams may not remove any item from the competition area unless specifically authorized to do so by Operations or White Team members including items brought into the team areas at the start of the competition.
- e. Team members are forbidden from entering or attempting to enter another team's competition workspace or room during CCDC events.
- f. Teams must compete without "outside assistance" from non-team members including team representatives from the start of the competition to the end of the competition (including overnight hours for multi-day events). All private communications (calls, emails, chat, texting, directed emails, forum postings, conversations, requests for assistance, etc) with non-team members including team representatives that would help the team gain an unfair advantage are not allowed and are grounds for disqualification and/or a penalty assigned to the appropriate team.
- g. Printed reference materials (books, magazines, checklists) are permitted in competition areas and teams may bring printed reference materials to the competition.
- h. Team representatives, sponsors, and observers are not competitors and are prohibited from directly assisting any competitor through direct advice, "suggestions", or hands-on assistance. Any team sponsor or observers found assisting a team will be asked to leave the competition area for the duration of the competition and/or a penalty will be assigned to the appropriate team.
- i. Team members will not initiate any contact with members of the Red Team during the hours of live competition. Team members are free to talk to Red Team members during official competition events such as breakfasts, dinners, mixers, and receptions that occur outside of live competition hours.
- j. Teams are free to examine their own systems but no offensive activity against other teams, the Operations Team, the White Team, or the Red Team will be tolerated. This includes port scans, unauthorized connection attempts, vulnerability scans, etc. Any team performing offensive activity against other teams, the Operations Team, the White Team, the Red Team, or any global asset will be immediately disqualified from the

competition. If there are any questions or concerns during the competition about whether or not specific actions can be considered offensive in nature contact the Operations Team before performing those actions.

- k. Teams are allowed to use active response mechanisms such as TCP resets when responding to suspicious/malicious activity. Any active mechanisms that interfere with the functionality of the scoring engine or manual scoring checks are exclusively the responsibility of the teams. Any firewall rule, IDS, IPS, or defensive action that interferes with the functionality of the scoring engine or manual scoring checks are exclusively the responsibility of the teams.
- l. All team members will wear badges identifying team affiliation at all times during competition hours.
- m. Only Operations Team/White Team members will be allowed in competition areas outside of competition hours.

5. Internet Usage

- a. Internet resources such as FAQs, how-to's, existing forums and responses, and company websites, are completely valid for competition use provided there is no fee required to access those resources and access to those resources has not been granted based on a previous membership, purchase, or fee. Only resources that could reasonably be available to all teams are permitted. For example, accessing Cisco resources through a CCO account would not be permitted but searching a public Cisco support forum would be permitted. Public sites such as Security Focus or Packetstorm are acceptable. Only public resources that every team could access if they chose to are permitted.
- b. Teams may not use any external, private electronic staging area or FTP site for patches, software, etc. during the competition. Teams are not allowed to access private Internet-accessible libraries, FTP sites, web sites, network storage, email accounts, or shared drives during the competition. All Internet resources used during the competition must be freely available to all other teams. The use of external collaboration and storage environments such as Google Docs/Drive is prohibited unless the environment was provided by and is administered by competition officials. Accessing private staging areas or email accounts is grounds for disqualification and/or a penalty assigned to the appropriate team.
- c. No peer to peer or distributed file sharing clients or servers are permitted on competition networks unless specifically authorized by the competition officials.
- d. Internet activity, where allowed, will be monitored and any team member caught viewing inappropriate or unauthorized content will be subject to disqualification and/or a penalty assigned to the appropriate team. This includes direct contact with outside sources through AIM/chat/email or any other public or non-public services including sites such as Facebook. For the purposes of this competition inappropriate content includes pornography or explicit materials, pirated media files, sites containing key generators and pirated software, etc. If there are any questions or concerns during the competition about whether or not specific materials are unauthorized contact the White Team immediately.

- e. All network activity that takes place on the competition network may be logged and subject to release. Competition officials are not responsible for the security of any information, including login credentials, which competitors place on the competition network.

6. Permitted Materials

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

7. Professional Conduct

- a. All participants, including competitors, coaches, White Team, Red Team, Ops Team, and Gold Team members, are expected to behave professionally at all times during all CCDC events including preparation meetings, receptions, mixers, banquets, competitions and so on.
- b. In addition to published CCDC rules, Host Site policies and rules apply throughout the competition and must be respected by all CCDC participants.
- c. All CCDC events are alcohol free events. No drinking is permitted at any time during competition hours.
- d. Activities such as swearing, consumption of alcohol or illegal drugs, disrespectful or unruly behavior, sexual harassment, improper physical contact, becoming argumentative, willful violence, or willful physical damage have no place at the competition and will not be tolerated.
- e. Violations of the rules can be deemed unprofessional conduct if determined to be intentional or malicious by competition officials.
- f. Competitors behaving in an unprofessional manner may receive a warning from the White Team, Gold Team, or Operations Team for their first offense. For egregious actions or for subsequent violations following a warning, competitors may have a penalty assessed against their team, be disqualified, and/or expelled from the competition site. Competitors expelled for unprofessional conduct will be banned from future CCDC competitions for a period of no less than 12 months from the date of their expulsion.

- g. Individual(s), other than competitors, behaving in an unprofessional manner may be warned against such behavior by the White Team or asked to leave the competition entirely by the Competition Director, the Operations Team, or Gold Team.

8. Questions, Disputes, and Disclosures

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

9. Scoring

- a. Scoring will be based on keeping required services up, controlling/preventing unauthorized 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 in order to mislead the scoring engine into assessing a system or service as operational, when in fact it is not, may be disqualified and/or the team assessed penalties. Should any question arise about scoring, the scoring engine, or how scoring functions, the Team Captain should immediately contact the competition officials to address the issue.
- d. Teams are strongly encouraged to provide incident reports for each Red Team incident they detect. Incident reports can be completed as needed throughout the competition and presented to the White Team for collection. Incident reports must contain a

description of what occurred (including source and destination IP addresses, timelines of activity, passwords cracked, access obtained, damage done, etc), a discussion of what was affected, and a remediation plan. A thorough incident report that correctly identifies and addresses a successful Red Team attack may reduce the Red Team penalty for that event – no partial points will be given for incomplete or vague incident reports.

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

35-50%	Functional services uptime as measured by scoring engine
35-50%	Successful completion of inject scenarios will result in varying points, depending upon the importance or complexity of the inject scenario
10-20%	Incident Response and Red Team Assessment

Precise percentage breakdown will be determined by the White Team.

10. Remote/ Team Site Judging and Compliance

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

- a. One or more Remote Site Judge(s) must be assigned to the team site. At least one Remote Site Judge must be present at the remote site for the duration of the event in order to facilitate the execution of the CCDC. The qualifications of Remote Site Judge are the same as Event Judge. Subject to the specifications of the remote competition, the responsibilities of the Remote Site Judge may include the following:
- i. Be present with the participating team to assure compliance with all event rules
 - ii. Provide direction and clarification to the team as to rules and requirements
 - iii. Establish communication with all Event Judges and provide status when requested
 - iv. Provide technical assistance to remote teams regarding use of the remote system
 - v. Review all equipment to be used during the remote competition for compliance with all event rules
 - vi. Assure that the Team Captain has communicated to the Event Judges approval of initial system integrity and remote system functionality
 - vii. Assist Event Judges in the resolution of grievances and disciplinary action, including possible disqualification, where needed
 - viii. Report excessive misconduct to local security or police
 - ix. Assess completion of various injects based on timeliness and quality when requested by Event Judges

- x. Act as a liaison to site personnel responsible for core networking and internet connectivity
 - xi. Provide direct technical assistance to teams when requested by Event Judges
 - xii. Provide feedback to students subsequent to the completion of the CCDC event
- b. A recommendation for Remote Site Judge(s) is expected to be given from a Team representative of the participating institution to the CCDC Event Manager. Remote Site Judge(s) must not be currently employed, a student of, or otherwise affiliated with the participating institution, other than membership on an advisory board. CCDC Event Managers should also be apprised of a contact from the participating institution responsible for core networking and internet connectivity that will be available during the CCDC event. Remote teams are required to compete from a location with controlled access, i.e., a separate room or a portion of a room that is dedicated for use during the CCDC event. Workstations and internet access must comply with published requirements.

11. WRCCDC Rule exceptions to NCCDC Rules

Remote Site Judges cannot be directly affiliated with the team or any member of the team. They are allowed to be a campus IT tech, a faculty member from a different concentration or a sponsor.