



# **2020 MACCDC Virtual Qualifying Round Team Packet**

## **FINAL**

**v.03-20-20**

## Table of Contents

|                                     |    |
|-------------------------------------|----|
| CCDC Mission                        | 3  |
| Competition Objectives              | 3  |
| Qualifying Round Overview           | 3  |
| Competition Goals                   | 5  |
| Competition Team Identification     | 6  |
| Initial Connection & the Start Flag | 7  |
| Systems                             | 11 |
| Competition Rules                   | 12 |
| Scoring                             | 20 |
| Functional Services                 | 21 |
| Business Tasks                      | 22 |
| Questions and Disputes              | 22 |
| Aftermath                           | 22 |
| Competition Topology                | 23 |

## CCDC Mission

"The goal of a Cyber Defense Competition is to provide hands-on application of information assurance skills; as such, they enhance students' understanding of both theory and practice. They provide students a laboratory in which to experiment, just as in other fields of science. They fulfill the same role as capstone projects in a traditional engineering program (i.e., projects that allow students to synthesize and integrate knowledge acquired through course work and other learning experiences into a project usually conducted in a workplace). The competition combines legal, ethical, forensics, and technical components while emphasizing a team approach. Such experiential education increases the knowledge and expertise of future professionals who may be in a position to contribute to the secure design and operation of critical information and its supporting infrastructure" (from Exploring a National Cyber Security Exercise for Colleges and Universities, Ron Dodge, Lance J. Hoffman, Daniel Ragsdale, and Tim Rosenberg, 2004).

## Competition Objectives

- Build a meaningful mechanism by which institutions of higher education may evaluate their programs
- Provide an educational venue in which students are able to apply the theory and skills they have learned in their course work
- Foster a spirit of teamwork, ethical behavior, and effective communication both within and across teams
- Open a dialog and awareness among participating institutions and students.

## Qualifying Round Overview

Now in its 15th year, the MACCDC consists of both a virtual qualifying round and a face-to-face regional final round engaging full-time undergraduate and graduate degree-seeking students, representing four-year universities and community colleges from Delaware, the District of Columbia, Maryland, New Jersey, North Carolina, Pennsylvania, Virginia, and West Virginia. In the past 14 years, over 2,300 students have participated in the MACCDC.

The Mid-Atlantic Collegiate Cyber Defense Competition Qualifier (MACCD) is managed by the National CyberWatch Center, headquartered at Prince George's Community College. The 2020 MACCDC will be run in conjunction with the Center for Systems Security and Information Assurance (CSSIA) at Moraine Valley Community College in Palos Hills, IL.



The competition is designed to test each student team's ability to secure networked systems while maintaining standard business functionality. The scenario involves team members simulating a group of employees from a fictitious company that will initiate administration of an IT infrastructure. The teams are expected to manage the systems, keep them operational, and prevent unauthorized access. Each team will be expected to maintain and provide public services, provided by CSSIA (e.g., a web site, an email server, a database server). 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, while maintaining availability of existing network services (e.g., mail servers, web servers), respond to business requests (e.g., the addition or removal of additional services), and balance security against varying business needs.

The qualifying round teams will have the opportunity to compete on March 21st in one of two time slots: **pay attention to your Team Number assignment below, as it relates to the Core IP Address Table (p. 24) and the URL used to access System 1 (p. 7-8):**

1. 9am-2pm EDT:
  - Team 1: Bloomsburg University of Pennsylvania, PA
  - Team 2: Capitol Technology University, MD
  - Team 3: Community College of Baltimore County, MD
  - Team 4: Delaware Technical Community College, DE
  - Team 5: Drexel University, PA
  - Team 6: East Carolina University, NC
  - Team 7: Frederick Community College, MD
  - Team 8: George Mason University, VA
  - Team 9: James Madison University, VA
  - Team 10: Liberty University, VA
  - Team 11: Marshall University, WV
  - Team 12: Millersville University, PA
  - Team 13: Northern Virginia Community College (Team 1), VA
  - Team 14: Northern Virginia Community College (Team 2), VA

2. 3pm-8pm EDT:

- Team 1: Pennsylvania State University, PA
- Team 2: Polytechnic University of Puerto Rico, Puerto Rico
- Team 3: Saint Vincent College, PA
- Team 4: Towson University, MD
- Team 5: University of Maryland Baltimore County (Team 1), MD
- Team 6: University of Maryland Baltimore County (Team 2), MD
- Team 7: University of Maryland College Park, MD
- Team 8: University of Maryland Global Campus, MD
- Team 9: University of Virginia (Team 1), VA
- Team 10: University of Virginia (Team 2), VA
- Team 11: University of Virginia College at Wise, VA
- Team 12: Virginia Commonwealth University, VA
- Team 13: West Virginia University, WV
- Team 14: Wilmington University, DE

The top eight (8) teams from the virtual qualifying round will advance to the MACCDC Regional Finals April 2-4, **which will be virtual as well.**

## Competition Goals

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

## Competition Team Identification

Throughout this document, the following terms are used:

- **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 (Casey W. O'Brien). 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.
  - Members and advisor(s) sign a participation safety agreement if teams compete anywhere other than their academic institution
  - Members and advisor (s) sign a photo release document where applicable
  - Students have completed a minimum of one semester in the participating institution's curriculum
  - Students should maintain a full-time status at the time the competition is conducted
  - National rules apply (see also below): [www.nationalccdc.org](http://www.nationalccdc.org)
- **Red Team** - Professional network penetration testers from industry, approved by the competition director and industry representatives:
  - Scan and map the network of each competition team
  - Attempt to penetrate the defensive capabilities of each Blue Team network and modify any acquired environment
  - Assess the security of each Blue Team network
  - Attempt to capture specific files on targeted devices of each Blue Team network
  - Attempt to leave specific files on targeted devices of each Blue Team network
  - Follow rules of engagement for the competition
- **White Team** - Representatives from industry who serve as competition judges, remote site judges, room monitors and security enforcement in the various competition rooms.

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

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

- **Chief Judge:**
  - Serves as the final authority on scoring decisions or issues relating to equity or fairness of events or activities
  - Cannot be from any institution that has a competing Blue team or have any interest in any team outcome
  - Ideally, should be a representative from industry or law enforcement
  - Final authority of all judging decisions, including assessment of final scores and winners of the competition
- **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
  - Along with Industry White Team approves the Chief Judge
  - 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
  - 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
- **Green Team** - Tech support and hospitality - assists with any technical needs necessary to maintain the integrity of the competition. Assists with ancillary functions - greeters, food service, local directions.

## Initial Connection & the Start Flag

Using a NETLAB<sup>+</sup>™ 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 (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.

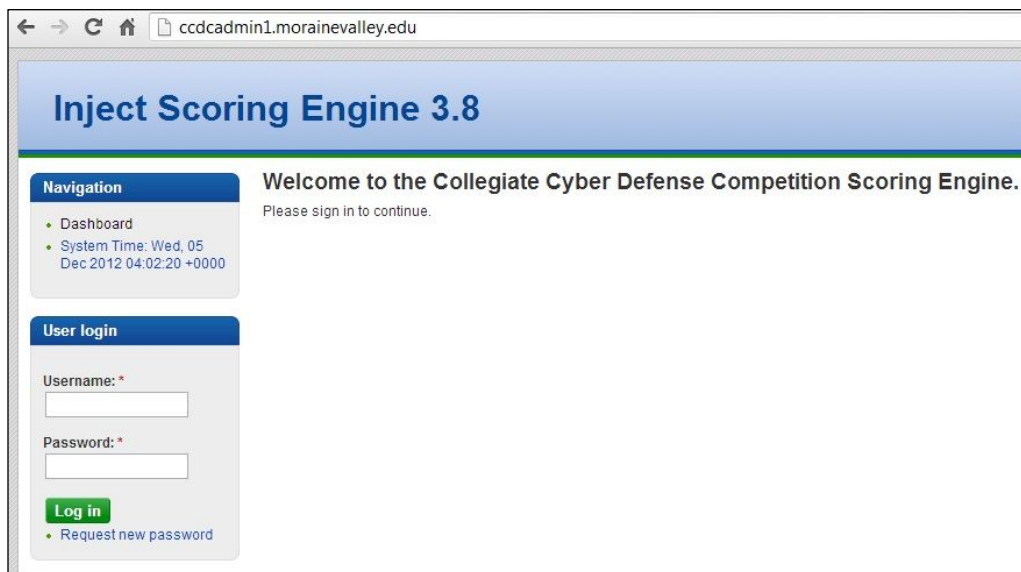
This system is accessed via a browser and looks as follows:

**For teams competing from 9am-2pm ET, use:**

**ccdcadmin2.morainevalley.edu**

**For teams competing from 3-8pm ET, use:**

**ccdcadmin3.morainevalley.edu**



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

**Students should login to the ISE first.** 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 was distributed in the email this FINAL team packet was attached to. Team assignments are on pages 4-5 above.**

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 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<sup>+</sup>™ VE Competition Stadium system used to access and manage the competition network. This too is accessed via a browser:

**ccdc.cit.morainevalley.edu**

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

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:

ccdc.cit.morainevalley.edu

Username

Password

Login

CSSIA Virtualization Center

Moraine Valley Community College

ccdc

Powered by NDG NETLAB+® Copyright © Network Development Group, Inc.

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





v1u1, v1u2, v1u3, ..., v1u8

Accounts for other teams follow the same pattern. For team2 the accounts are:

v2u1, ....

**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.

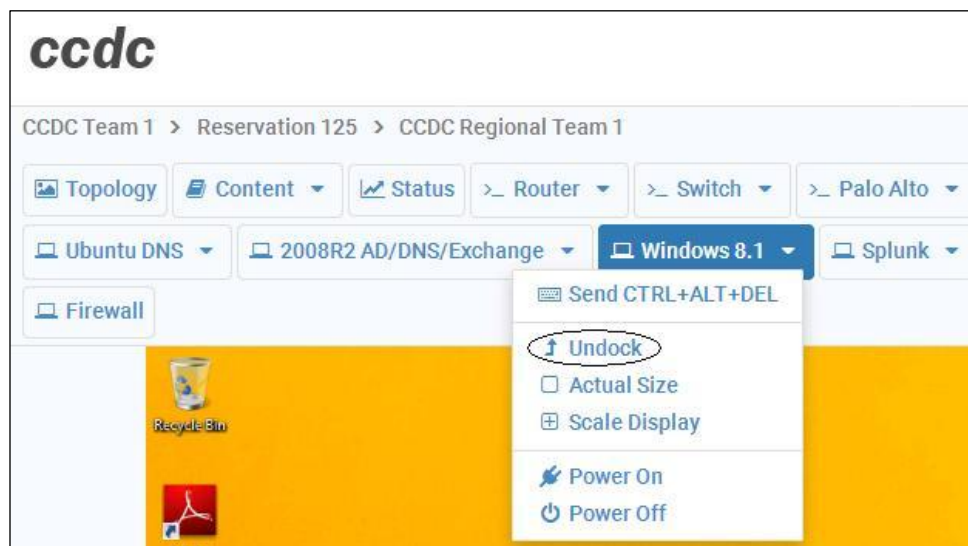
Once authenticated you will be asked to change your password and confirm a few details regarding your profile. Remember your new password! Subsequently you should see a lab reservation for your competition network, similar to the following:

| <div>  <b>Lab Reservations</b> <div>Search</div> </div> |  |  |   |
|--|--|--|---|
| ID   | Date/Time  | Description  | Pod   |
| 562  | <div>  2018-11-06 08:55<br/>  2018-11-08 00:30<br/>  1 days, 3 hrs., 17 mins.           </div> <div>Enter Lab</div> | Class: 2019 CCDC State<br>Lab: Lab 0 (no VLANs) passwords<br>Type: Team<br>Team: J | CCDC State Team 10<br><b>CCDC State Pod</b> |
| Showing 1 to 1 of 1 items  |  |  |   |

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:



## 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 an inject. Likewise, teams are not permitted to change the internal addressing or VLAN scheme of the competition network unless directed to do so by an inject.
8. Teams may re-task servers, moving a service from one server to another as long as the outside "public" IP address of the service remains the same. It is the responsibility of the team to understand all the particulars of scoring a service when doing so.
9. Teams are not permitted to alter the system names or IP address of their assigned systems unless directed by an inject; this may affect the results of the scoring mechanism.
10. In the event of system lock or failure, teams will be able to perform a cold boot from within the administration console of the remote system. This will not reset any system to its initial starting configuration. Teams do not have the ability to revert/snapshot/scrub a VM, nor will Tech Support scrub a device. There are no scrubs for the Qualification Round of the MACCDC.
11. Systems designated as user workstations within the competition network are to be treated as user workstations and may not be re-tasked for any other purpose by teams.
12. Teams may not modify the hardware configurations of workstations used to access the competition network.
13. Servers and networking equipment may be re-tasked or reconfigured as needed.

## Competition Rules

Competition rules are applicable to all participants of the MACCDC. 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 competition stadium 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.

### 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.
- 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.
- 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. Team Composition

- Each team must submit a roster of up to twelve (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.
- Each competition team may consist of up to eight (8) members chosen from the submitted roster.

- Each competition team may have no more than two (2) graduate students as team members.
- 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.
- 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.
  - Team Representatives must petition the Competition Director in writing for the right to perform a change to the competition team.
  - The Competition Director must approve any substitutions or additions prior to those actions occurring.
- 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.
- 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.
- An institution is only allowed to compete one team in any CCDC event or season.

### 3. Team Representatives

- 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.
- 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).
- Representatives may not enter their team's competition space during any CCDC event.
- Representatives must not interfere with any other competing team.
- 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

- 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.

- Teams must not connect any devices or peripherals to the competition network unless specifically authorized to do so by Operations or White Team members.
- 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.
- 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.
- Team members are forbidden from entering or attempting to enter another team's competition workspace or room during CCDC events.
- 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.
- Printed reference materials (books, magazines, checklists) are permitted in competition areas and teams may bring printed reference materials to the competition.
- 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.
- 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.
- 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.
- 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.

- All team members will wear badges identifying team affiliation at all times during competition hours.
- Only Operations Team/White Team members will be allowed in competition areas outside of competition hours.

#### 5. Internet Usage

- 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 are acceptable. Only public resources that every team could access if they chose to are permitted.
- 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.
- No peer to peer or distributed file sharing clients or servers are permitted on competition networks unless specifically authorized by the competition officials.
- 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.
- 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

- 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.
- 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.
- 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

- 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.
- In addition to published CCDC rules, Host Site policies and rules apply throughout the competition and must be respected by all CCDC participants.
- All CCDC events are alcohol free events. No drinking is permitted at any time during competition hours.
- 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.
- Violations of the rules can be deemed unprofessional conduct if determined to be intentional or malicious by competition officials.
- 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.
- 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

- **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.
- **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.
- 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.
- 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.
- 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

- 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 usage of recovery services (e.g., resetting a virtual machine) and successful penetrations by the Red Team.
- Scores will be maintained by the competition officials and may be shared a few days after the event. There will be no running totals provided during the competition.
- Any team action that interrupts the scoring system is exclusively the responsibility of that team and will result in a lower score. Should any question arise about scoring, the scoring engine, or how they function, the Team Captain should immediately contact the competition officials to address the issue.
- 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.

#### 10. Remote Team Site Judging and Compliance

- **Because of the unfolding COVID-19 situation, many schools have implemented restrictions on gathering in a single place, have restricted all travel, have extended spring break, or have cancelled classes all together. It is OK for each participant from a school to compete from their own location. It is also not practical to have a remote site judge at each participant's location. An alternative is to implement some form of video conferencing that's shared with each participant, coach, and site judge.**
- The responsibilities of the Remote Site Judge may include the following:
  - Assure compliance with all event rules
  - Provide direction and clarification to the team as to rules and requirements
  - Establish communication with all Event Judges and provide status when requested
  - Provide technical assistance to remote teams regarding use of the remote system
  - Review all equipment to be used during the remote competition for compliance with all event rules
  - Assure that the Team Captain has communicated to the Event Judges approval of initial system integrity and remote system functionality
  - Assist Event Judges in the resolution of grievances and disciplinary action, including possible disqualification, where needed
  - Report excessive misconduct to local security or police
  - Assess completion of various Injects based on timeliness and quality when requested by Event Judges
  - Act as a liaison to site personnel responsible for core networking and internet connectivity
  - Provide direct technical assistance to teams when requested by Event Judges
  - Provide feedback to students subsequent to the completion of the CCDC event
- 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

- Unless otherwise stated below, the rules of the National Collegiate Cyber Defense Competition will serve as the official rules of the Mid-Atlantic Collegiate Cyber Defense Competition all-inclusive and unaltered.

#### 12. Red Team Attack Rules

- Attack surface is the entire network.
- No physical attacks without prior approval.
- No physical contact with any blue team player during the competition.
- If contact is necessary with a white team, black team, or a competition staff member, red team members must identify themselves as a member of the red team.
- No Distributed Denial of Service (DDoS) attacks.
- No attacks that are not recoverable by blue team action or recoverable only through a virtual machine revert to snapshot or rebuild performed by the operations team.

## Scoring

1. Scoring will be based on keeping required services up, controlling/preventing unauthorized access, mitigating vulnerabilities, and completing business tasks that will be provided throughout the competition. Teams accumulate points by successfully completing injects, maintaining services, and by submitting incident reports. Teams lose points by usage of recovery services (e.g., reset a virtual machine) 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 the White Team. Incident reports must contain a description of what occurred (including source and destination IP addresses, timelines of activity, passwords cracked, etc.), a discussion of what was affected, and a remediation plan. The White Team will assess scores for incident report submission based on clarity, thoroughness,

and accuracy. The White Team may also, at their discretion, assess negative scores for frivolous, unnecessary, or excessive communication.

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

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

Precise percentage breakdown will be determined by the White Team.

## 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. Precise services to be scored are configured by the scoring management team, but will be delineated via the ISE/Team Portal.

### 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.

### POP3

POP3 connections will be performed against the system using usernames from Active Directory. Once connected a series of commands will be run and the output examined. Correct responses will be awarded points.

## **DNS**

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

## **Business Tasks**

Throughout the competition, each team will be 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.

## **Aftermath**

Members of CSSIA, Gold, White, Red, and Green Teams strive to make the MACCDC enriching experiences. 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.

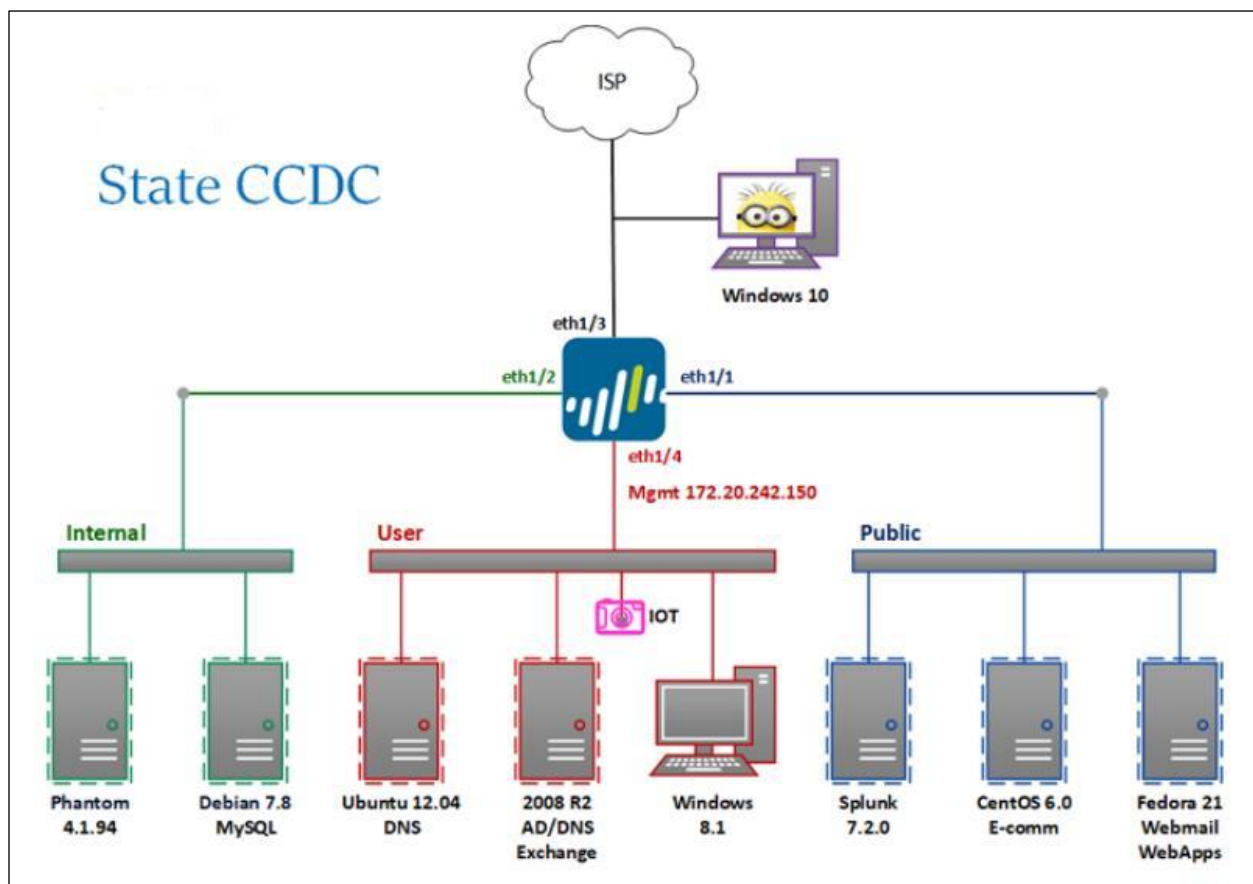
Whether feedback is positive or negative, participants are forbidden from publishing, posting on the internet, or publicly communicating details of the competition other than what is available at [www.cssia.org](http://www.cssia.org) and [maccdc.org](http://maccdc.org). They are also forbidden from publishing, posting on

the internet, or publicly communicating assessments of the State CCDC, nor assessments of the performance of any team, nor speculations concerning different possible outcomes.

Institutions that fail to adhere to this rule may be refused participation in future competitions.

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

## Competition Topology



- Teams have access to 10 VMs: 7 serves, 2 workstations, and the Palo Alto firewall
- There is no IOT device for the virtual qualifying round
- All servers, workstations, and the Palo Alto firewall are virtual machines under the management of NETLAB<sup>+</sup>™ 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

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



- VM data are as follows:

|                  | Version    | IP            | Username               | Password                     |
|------------------|------------|---------------|------------------------|------------------------------|
| <b>INTERNAL</b>  |            |               |                        |                              |
| Phantom          | 4.1.94     | 172.20.240.10 | root<br>admin (Web UI) | !Password123<br>!Password123 |
| Debian 7.8 MySQL | Debian 7.8 | 172.20.240.20 | root<br>sysadmin       | !Password123<br>!Password123 |

|                         |              |                |               |              |
|-------------------------|--------------|----------------|---------------|--------------|
| <b>USER</b>             |              |                |               |              |
| Ubuntu 12.04 DNS        | Ubuntu 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 |

|                           |              |                |                        |                         |
|---------------------------|--------------|----------------|------------------------|-------------------------|
| <b>PUBLIC</b>             |              |                |                        |                         |
| Splunk                    | 7.2.0        | 172.20.241.20  | root<br>admin (Web UI) | changemenow<br>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 |
|                         |                |                    |
| <b>USER</b>             |                |                    |
| 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            |
|                         |                |                    |
| <b>PUBLIC</b>           |                |                    |
| 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 |

- 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 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 MACCDC Competition Director