

# **Regional Final Team Packet**

**v.03-29-20**

# Table of Contents

Regional Final Overview	3
CCDC Mission	3
Competition Objectives	3
Scenario: Artificially Intelligent Institute (AII)	4
Blue Teams	4
Schedule	5
Competition Team Identification	6
Rules	6
Scoring	13
Systems	15
Initial Connection & the Start Flag	16
Competition Range Information	21
Functional Services	24

## Regional Final Overview

The MACCDC Regional Final is managed by the National CyberWatch Center (NCC), headquartered at Prince George's Community College, and run in conjunction with the Center for Systems Security and Information Assurance (CSSIA) at Moraine Valley Community College in Palos Hills, IL.

## 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

## Scenario: Artificially Intelligent Institute (All)

Each year, the MACCDC develops a new exercise scenario and implements cutting-edge technologies that mimic those in the real world. This year's scenario involves student teams working for the Artificially Intelligent Institute (All), pronounced *eye*.

All is a multinational corporation with offices in the Mid-Atlantic region. As a leading provider of advanced AI surveillance tools to intelligence and law enforcement agencies, as well as private-sector organizations, the main business driver of All is to show how new surveillance capabilities are transforming government's and organization's monitoring capabilities.

As part of their duties, Blue Teams are expected to defend their systems against aggressors. Early intelligence reports suggest that rouge Hackistanian antagonist are interested in stealing All's intellectual property, source code, and customer database. Hackers contracted and working directly for the country of Hackistan are also interested in disrupting IoT devices on-premises at the various All regional offices.

## Blue Teams

The following teams will be competing in the 2020 MACCDC Regional Final - NOTE: **pay special attention to your Team Number assignment below, as it relates to the Core IP Address Table on (p. 21):**

- Team 1: George Mason University, VA
- Team 2: James Madison University, VA
- Team 3: Liberty University, VA
- Team 4: Marshall University, WV
- Team 5: Pennsylvania State University, PA
- Team 6: University of Maryland Baltimore County, MD
- Team 7: University of Maryland College Park, MD
- Team 8: University of Virginia, VA

The winning team will represent the Mid-Atlantic Region in the National CCDC, April 25-26.

NOTE: the second-place team from the MACCDC will compete in a Wild Card Round on April 6<sup>th</sup>. The winner of that round will advance to the National CCDC as well.

## Schedule

### Thursday, April 2

12:00pm - 1:00pm

Sponsors' Briefings to Teams (Zoom):

<https://zoom.us/j/670839882>

+16465588656,,670839882# US (New York)

+16699006833,,670839882# US (San Jose)

Meeting ID: 670 839 882

1:00pm - 3:30pm

Job Fair (Virtual Breakout Rooms)

### Friday, April 3

7:30am - 8:30am

Blue Team Check-In (Zoom):

<https://zoom.us/j/668816456>

+16465588656,,668816456# US (New York)

+16699006833,,668816456# US (San Jose)

Meeting ID: 668 816 456

8:30am - 8:50am

Opening Competition Briefing (Zoom):

9:00am - 5:00pm

Competition Day 1 (Virtual Stadium)

11:00am - 1:00pm

CEO Meetings (Zoom)

5:30pm

Day 1 Debrief (Zoom)

### Saturday, April 4

7:30am - 8:30am

Blue Team Check-In (Zoom):

<https://zoom.us/j/212077917>

+16465588656,,212077917# US (New York)

+16699006833,,212077917# US (San Jose)

Meeting ID: 212 077 917

8:30am - 8:50am

Morning Briefing (Zoom)

9:00am - 5:00pm

Competition Day 2 (Virtual Stadium)

10:00am - 12:00pm

CEO Meetings (Zoom)

5:00pm

Competition Ends

6:30pm - 7:30pm

Debrief and Awards Ceremony (Zoom)

## Competition Team Identification

Throughout this document, the following terms are used:

- **Black Team:** competition support members that provide technical support and provide overall administrative support to the competition
- **Blue Team/Competition Team:** the institution competitive teams consisting of students competing in a CCDC event
- **Operations (Ops) Team:** competition officials that organize, run, and manage the competition. The Competition Director is part of this team
- **Red Team:** penetration testing professionals simulating external hackers attempting to gain unauthorized access to Competition Teams' systems
- **Team Captain:** a student member of the Blue Team identified as the primary liaison between the Blue Team and the Ops and White Teams
- **Team Co-Captain:** a student member of the Blue Team identified as the secondary or backup liaison between the Blue Team and the Ops and White Teams, should the Team Captain be unavailable
- **Team Representatives:** a faculty or staff representative of the Blue Team's host institution responsible for serving as a liaison between the Ops Team and the Blue Team's institution
- **White Team:** competition officials that evaluate Blue Team performance and rule compliance.

## Rules

1. Competitor Eligibility
  - a. 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 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 or regional CCDC event and graduates before the next CCDC event in the same season, that team member will be allowed to continue to compete at CCDC events during

the same season should their team win and advance to the next round of competition.

- b. Competitors may only be a member of one team per CCDC season.
- c. A team member may not participate in any role at CCDC events held outside the region in which their team competes during the same CCDC season.
- d. Individuals who have participated in previous CCDC events in any role other than as a competitor must obtain eligibility approval from the director of the region in which their team competes prior to being added to the team roster. Once a candidate's eligibility has been approved, they will remain eligible for all CCDC events during the same season.

## 2. Team Composition

- a. 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.
- 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, 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.
  - 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.
- f. Teams or team members arriving after an event's official start time, for reasons beyond their control, may be allowed to join the competition provided a substitution has not already been made. Event coordinators will review the reason for tardiness and make the final determination.
- g. Each team will designate a Team Captain for the duration of the competition to act as the team liaison between the competition staff and the teams before and during the competition. In the event of the Team Captain's absence, teams must have an identified team liaison serving as the captain in the competition space at all times during competition hours.

- 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, Ops and White Team members will occasionally need access to a team's system(s) for scoring, troubleshooting, etc. Blue Teams must immediately allow Ops and White Team members' access when requested.
- b. Blue Teams must not connect any devices or peripherals to the competition network unless specifically authorized to do so by Ops or White Team members.
- c. Blue Teams may not remove any item from the competition area unless specifically authorized to do so by Ops or White Team members, including items brought into the team areas at the start of the competition.
- d. Blue Team members are forbidden from entering or attempting to enter another team's competition workspace during CCDC events.
- e. Blue 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 Blue Team.
- f. Printed reference materials (books, magazines, checklists) are permitted in competition areas and Blue Teams may use printed reference materials during the competition.
- g. Blue 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 Blue 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 Blue Team.

- h. Blue Team members will not initiate any contact with members of the Red Team during the hours of live competition. Blue Team members are free to talk to Red Team members during official competition events such as the Job Fair or online Debrief/Awards ceremony.
- i. Blue 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 Blue 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 Ops or White Team before performing those actions.
- j. Blue Teams are allowed to use active response mechanisms (e.g., 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 Blue 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 Blue Teams.
- k. Only Ops or White Team members will be allowed in competition areas/Virtual Stadium outside of competition hours.

## 5. Internet Usage

- a. Internet resources (e.g., 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 Blue Team could access if they chose to are permitted.
- b. Teams may not use any external, public or private electronic staging area or FTP site for patches and software 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 (e.g., Google Docs/Drive) is prohibited unless read access is given to the Competition Director prior to the start of the competition on Day 1 and that access remains available during the entire event.
- c. No peer to peer or distributed file sharing clients or servers is permitted on competition networks unless specifically authorized by the Ops Team.
- d. Internet activity, where allowed, will be monitored and any Blue 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 IM/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, pirated software, etc. If there are any questions or concerns during the competition about whether or not specific materials are unauthorized contact the Ops or 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 Ops 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. 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 Ops Team.

#### 7. Professional Conduct

- a. All participants, including competitors, coaches, Remote Site Judges, Ops Team, White Team, and Red 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, local and host 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 Ops 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. 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 Ops Team or asked to leave the competition entirely by the Competition Director.

#### 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 Blue Team must be presented in writing by the Team Captain to the Ops 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 Awards 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, completing business tasks that will be provided throughout the competition, meeting with the All CEO, and the quality and accuracy of submitted incident response reports.
- b. Scores will be maintained by the competition officials and may be shared at the end of the competition. There will be no running totals provided during the competition. Team rankings may be provided at the beginning of each competition day.
- c. Any team action that interrupts the scoring system is exclusively the responsibility of that team and will result in a lower score. Should any question arise about scoring, the scoring engine, or how they function, the Team Captain should immediately contact the Ops Team to address the issue.
- d. 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 presented to the Ops 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

- a. 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.
- b. Because of the ongoing COVID-19 pandemic, team participants are required to compete from their own location. Workstations and internet access must comply with published requirements.
- c. A minimum of one Remote Site Judge must be assigned to a Blue Team and must be virtually present for the duration of the event in order to facilitate the execution of the CCDC. Team Captains must send the Competition Director (via email) the Remote Site Judge's first/last name, email, and phone number by 5pm ET on Thurs. April 2<sup>nd</sup>.
- d. Subject to the specifications of the remote competition, the responsibilities of the Remote Site Judge may include the following:
  - Be present with the participating team to assure compliance with all event rules
  - Provide direction and clarification to the team as to rules and requirements
  - Establish communication with the Ops Team and provide status updates 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 Ops Team approval of initial system integrity and remote system functionality
  - Assist the Ops and White Teams in the resolution of grievances and disciplinary action, including possible disqualification, where needed
  - Report excessive misconduct to the Ops Team
  - Assess completion of various injects based on timeliness and quality when requested by the Ops or White Teams
  - Act as a liaison to the Ops Team responsible for core networking and Internet connectivity
  - Provide direct technical assistance to teams when requested by the Ops Team

- Provide feedback to students subsequent to the completion of the CCDC event
- A recommendation for the Remote Site Judge is expected to be given from a Team representative of the participating institution to the MACCDC Competition Director. A Remote Site Judge must not be currently employed, a student of, or otherwise affiliated with the participating institution, other than membership on an advisory board.

#### 11. Local Competition Rules

- a. The rules stated in this Team Packet will serve as the official rules of the 2020 MACCDC.

#### 12. Red Team Attack Rules

- a. Confine attack activity to the official target list located on the ScoreBot player page.
- b. No physical attacks without prior approval.
- c. No physical contact with any Blue Team player during the competition.
- d. 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.
- e. No Distributed Denial of Service (DDoS) attacks.
- f. 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 Ops Team.

## Scoring

All Blue Teams start with zero points. Blue Teams are ranked against each other in order of highest (best) to lowest score.

#### Scoring Metrics:

1. **Services:** All scored services must remain up and available, with a high degree of integrity. All services are given a predefined point value and will be checked periodically using Service Round Checks. The actual number of service rounds is not disclosed prior to or during the competition. For each service that passes the necessary check, the team will receive the appropriate number of points for that service. The more service points a team receives, the better.

2. **Injects:** Throughout the competition, the Blue Team will be presented with injects. An inject is any assigned task to be completed in the assigned amount of time. Inject types vary and are weighted based on the difficulty and time sensitivity of the task. Tasks may contain multiple parts. Sample injects include creating policy documents, making technical changes to a system, and attending meetings. Injects can be delivered through any number of methods, including electronically and orally. Injects will be scored by a White Team member. If the inject is completed on time and to the standard required, the Blue Team will receive the appropriate number of points. Unless indicated otherwise, the Team Captain may assign injects to specific team members for completion. Red Team activity can adversely affect a team's ability to complete injects. It is the Blue Teams' responsibility to keep their systems available. No extra time or point credit will be given for injects that are not completed because of inability to access a system. The more inject points a team receives, the better.
3. **Red Team Activity:** The activities performed by the Red Team have an impact on many of the scoring categories. It is imperative that Blue Teams work to prevent Red Team activities. The Red Team will have specific goals during the event. Sample goals include compromising a server, stealing data, and modifying injects. All Red Team activities are meant to disrupt or misinform. At the conclusion of each competition day, the Red Team will rank order each team from best to worst.
4. **CEO Reporting:** Each Team Captain will meet face-to-face with the CEO of the competition (see Schedule above). During the initial meeting on Day 1 (ten minutes, timed), the CEO will expect to be briefed on the current status of the All's information systems, the number of users impacted by downed systems, as well other items the Team Captain will consider relevant for the CEO to know. At this initial meeting, each Team Captain will be given action items to complete within a fixed time. Items may include a written status report, a high-level remediation plan, a resource inventory, a request for prioritized additional resources subject to budget constraints, and other similar management considerations.

During the second meeting on Day 2 (ten minutes, timed), each Team Captain will meet with the CEO and will have a chance to present responses to what was covered in the first meeting on Day 1 and provide updates on any changes that transpired.

Each team will be scored using the following metrics:

- Oral presentation and writing skills
- Clarity of communicating the situation
- Ability to rise above technobabble
- Creativity in reacting to new information

The more CEO points a team receives, the better.

5. **Incident Response:** All Blue Teams must submit at least four Incident Response forms and open two cases with the Incident Response officials in attendance (they are part of the White Team). Incident response forms will be provided. Instructions for submitting these forms will be provided during the initial team briefing on Day 1. Incident response forms will be scored based on coherence and technical accuracy/depth. 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.

### Calculating Scores:

- Raw scores are used for the above scoring metrics, excluding the Red Team (which uses an ordinal scale, see next).
- Blue Teams are ranked using an ordinal scale, which is a measurement scale that assigns values to objects based on their ranking with respect to one another. For example, a first-place finish in the service scoring metric warrants an ordinal score of 1, a second-place finish warrants an ordinal score of 2, up to an eighth-place finish warranting an ordinal score of 8. This process is repeated for all of the scoring metrics.
- The ordinal scores from all of the scoring metrics are then totaled for each Blue Team, yielding a combined ordinal score, which is used to rank the Blue Teams from first through eighth place. The winning Blue Team will be determined based on the lowest combined ordinal score obtained during the competition time.
- In the event of a tie for first place, the team with the highest raw combined inject and service score will win.

## Systems

1. Each Blue Team will start the competition with identically configured systems.
2. Blue 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. Blue Teams should not assume any competition system is properly functioning or secure.
5. Throughout the competition, Ops and White Team members will occasionally need access to a team's system(s) for scoring, troubleshooting, etc. Blue Teams must allow the Ops and White Team member(s) access when requested.
6. Network traffic generators may be used throughout the competition to generate traffic on the competition 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. Blue 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, Blue 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. Blue 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 Blue Team to understand all the particulars of scoring a service when doing so.
9. Blue 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, Blue 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. Blue Teams do not have the ability to revert/snapshot/scrub a VM, nor will the Ops Team scrub a device. There are no scrubs for the MACCDC Regional Final – *this may get changed; stay tuned.*
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 Blue Teams.
12. Blue 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.

## Initial Connection & the Start Flag

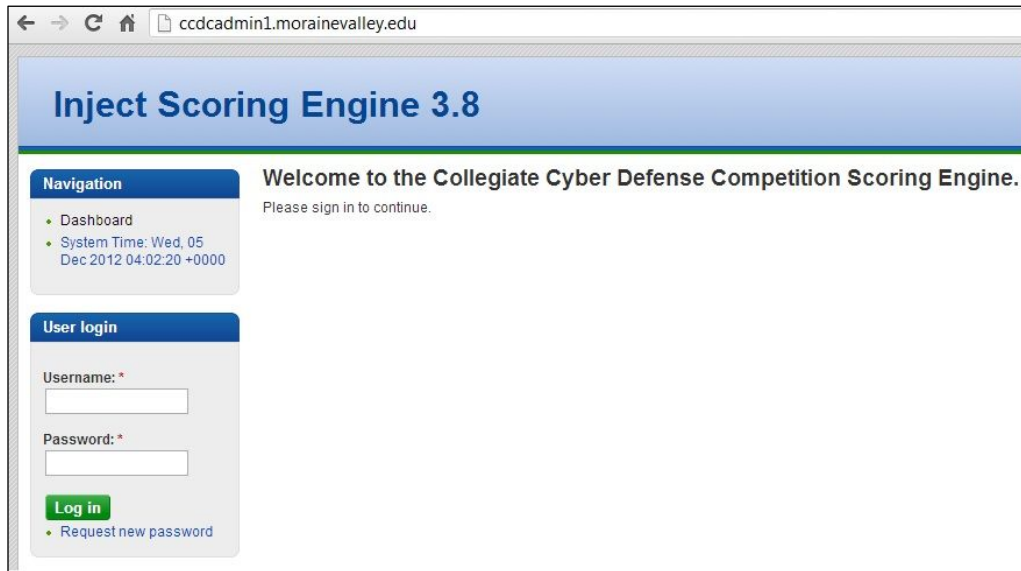
Using a NETLAB<sup>™</sup> VE-powered Cyber Stadium to compete is simple and straightforward. There are two separate systems that are used which interact to provide the services and communication necessary to meet the goals of the CCDC.

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:

<insert final URL here>



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' sidebar on the left with links to 'Dashboard' and 'System Time: Wed, 05 Dec 2012 04:02:20 +0000'. The main content area has a 'Welcome to the Collegiate Cyber Defense Competition Scoring Engine.' message and a 'Please sign in to continue.' prompt. Below this 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 will be distributed in the email the FINAL team packet was attached to. Team assignments are on page 4 above.**

When first connecting to the ISE, a member of the Blue 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 - URL subject to change**

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 Blue 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 Blue Teams initially only have access to the ISE/Team Portal.** Blue 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:

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

Each Blue 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.

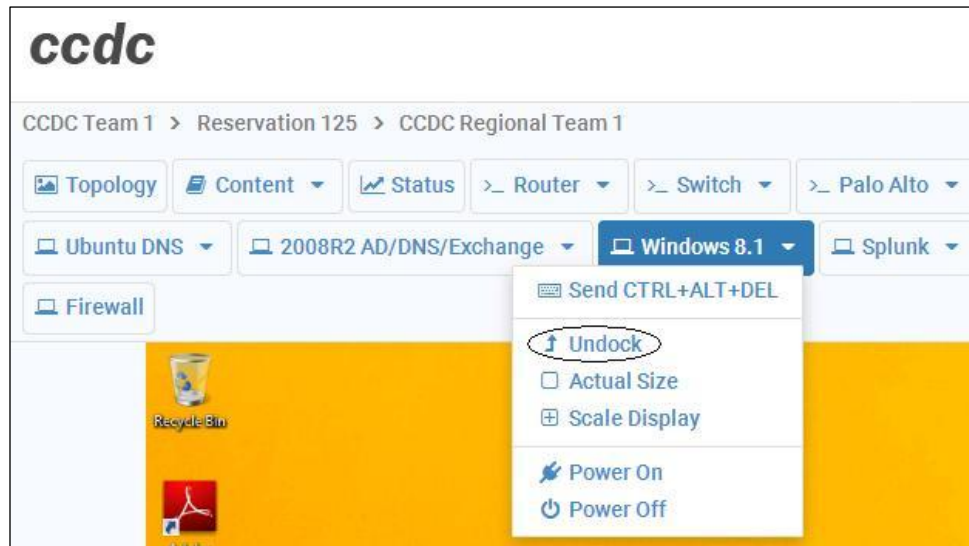

Home Pod

MyNETLAB > CCDC State Team 10 > Reservation 562 > Lab 0 (no VLANs) passwords

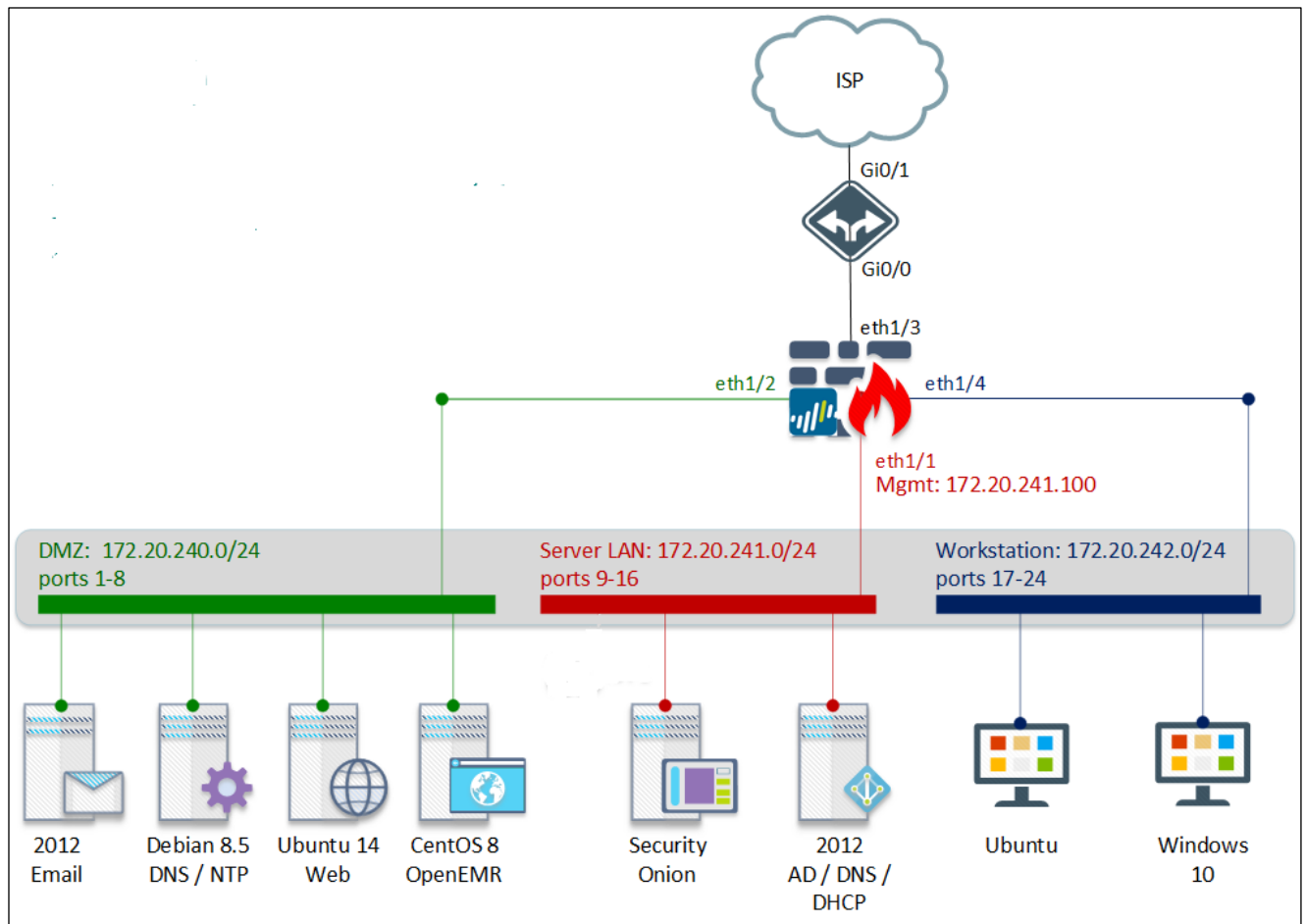
Topology
 Content
 Status
 > dummy
 Windows 10
 Phantom
 Debian
 Ubuntu
 2008 R2

Windows 8.1
 Splunk
 CentOS
 Fedora
 Palo Alto

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



## Competition Range Information



**Figure 1: 2020 MACCDC Regional Final Topology**

- The router and switch shown in Figure 1 are hardware devices as follows:
  - Cisco 2911 Router with IOS c2900-universalk9-mz.SPA.154-3.M5, Version 15.4(3)M5
  - Cisco 2960 Switch with C2960-LANBASEK9-M, Version 15.0(2)SE5
- You have direct access initially to the Cisco devices without login or privileged mode password.
- All servers and workstations are virtual machines under the management of NETLAB<sup>+</sup>.
- Each team has the following router internal address:
  - Router
  - g0/0 172.20.243.253

- Core IP addresses are the following (Team Assignments are on page 4 above):

Team	Router g0/1	Core connection to Router g0/1	"Public" IP pool
1	172.31.1.2/30	172.31.1.1	172.25.1.0/24
2	172.31.2.2/30	172.31.2.1	172.25.2.0/24
3	172.31.3.2/30	172.31.3.1	172.25.3.0/24
4	172.31.4.2/30	172.31.4.1	172.25.4.0/24
5	172.31.5.2/30	172.31.5.1	172.25.5.0/24
6	172.31.6.2/30	172.31.6.1	172.25.6.0/24
7	172.31.7.2/30	172.31.7.1	172.25.7.0/24
8	172.31.8.2/30	172.31.8.1	172.25.8.0/24
9	172.31.9.2/30	172.31.9.1	172.25.9.0/24
10	172.31.10.2/30	172.31.10.1	172.25.10.0/24

- The firewall is a Palo Alto firewall hardware device model 3050 running version 9.0.6 with the following addresses:
  - ethernet1/1 172.20.241.254
  - ethernet1/2 172.20.240.254
  - ethernet1/3 172.20.243.254
  - ethernet1/4 172.20.242.254
- The management IP is labeled on the topology:
  - 172.20.241.100
- Access to the Palo Alto is accessed with the account/password:
  - admin/Changeme123
- Switch port assignments within the topology are as follows:

VM Label	Switch Interface
2012 Email	f0/1
Debian 8.5	f0/2
Ubuntu 14	f0/3
CentOS 8	f0/4
PA eth1/2	f0/8
Security Onion	f0/9
2012 AD	f0/10
IOT1	f0/14
PA eth 1/1	f0/16
Ubuntu WS	f0/17
Windows 10	f0/18
PA eth 1/4	f0/24

- The delineation of local IP, major service, and administrative access credentials per VM are as follows:

	<i>Version</i>	<i>IP</i>	<i>Username</i>	<i>password</i>
<b>DMZ</b>				
Email	Srvr 2012 std	172.20.240.11/24	administrator (local)	!Changeme789
DNS/NTP Server	Debian 8.5.0	172.20.240.23/24	root / sysadmin	changeme
Web	Ubuntu 14.04.2	172.20.240.5/24	sysadmin	changeme
OpenEMR	Ubuntu 16.04.1	172.20.240.97/24	sysadmin	changeme

#### **Server LAN**

Security Onion	Ubuntu 16.04	172.20.241.3/24	sysadmin	changeme
AD /DNS/DHCP	Srvr 2012 std	172.20.241.27/24	administrator	!Password123

#### **Workstation LAN**

Ubuntu	Ubuntu Desktop 12.04	DHCP	sysadmin	changeme
Windows 10	Windows 10 N 64-bit	DHCP	Jane	changeme

Palo Alto	PAN OS 9.0.6	172.20.241.100	admin	Changeme123
-----------	--------------	----------------	-------	-------------

- 'Public' IP addresses are as follows:

VM	local IP	public' IP
2012 Email	172.20.240.11	172.25.team#.17
Debian 8.5	172.20.240.23	172.25.team#.9
Ubuntu 14	172.20.140.5	172.25.team#.34
CentOS 8	172.20.240.97	172.25.team#.29
Security Onion	172.20.241.3	172.25.team#.67
2012 AD	172.20.241.27	172.25.team#.83
IOT1	172.20.241.201	172.25.team#.97
Ubuntu		
Windows 10		

- Systems are loaded with various user accounts. Blue Teams are responsible to know which accounts are used for services. **Root, Administrator, Admin or Sysadmin will never be used for scoring.**

## 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.