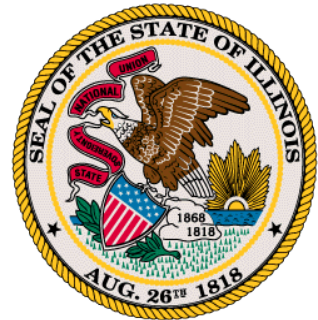


# 2019 Erich J. Spengler Midwest Regional Collegiate Cyber Defense Competition Team Packet



**March 15-16, 2019**

© CSSIA 2019

## Table of Contents

### Contents

Midwest Regional CCDC Mission and Objectives .....	3
Overview .....	3
Business Scenario .....	4
Midwest Regional Competition Goals.....	4
Institutional Requirements for Participation .....	5
Competition Team Identification .....	5
NDG NETLAB <sup>+</sup> ™ VE System Access.....	7
Competition Topology .....	8
Network Description .....	8
Functional Services .....	12
Schedule – all times CST .....	13
Systems .....	13
Competition Rules: Acknowledgement & Agreement .....	14
Competition Rules: Student Teams .....	15
Competition Rules: Professional Conduct .....	15
Competition Rules: Competition Play .....	15
Competition Rules: Internet Usage .....	17
Competition Rules: Scoring.....	18
Business Tasks .....	19
Questions and Disputes.....	19
Aftermath .....	20
Sponsors:.....	21

## Midwest Regional CCDC Mission and Objectives

The 2019 Erich J. Spengler Midwest Regional Collegiate Cyber Defense Competition (CCDC) provides a competitive opportunity for collegiate teams who have proven themselves in 2019 Midwest State CCDC Qualification or Wildcard events. The Midwest Regional Collegiate Cyber Defense Competition is designed to provide a controlled competitive environment that will permit each participating institution to assess their students' depth of understanding and operational competency in managing the challenges inherent in protecting an enterprise network infrastructure and business information systems. The winner of the 2019 Erich J. Spengler Midwest Regional CCDC is eligible to move on to the 2019 National CCDC in San Antonio, Texas, April 23-25, 2019.

## Overview

Midwest Collegiate Cyber Defence Competitions are managed by CSSIA, the National Resource Center for Systems Security and Information Assurance. The competition is designed to test each student team's ability to secure a networked computer system while maintaining standard business functionality. The teams are expected to manage the computer network, keep it operational, and prevent unauthorized access. Each team will be expected to maintain and provide public services per company policy and mission. Each team will start the competition with a set of identically configured systems.

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

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

There are ten teams competing in the 2019 Erich J. Spengler Regional CCDC comprising eight winners of respective state qualification CCDC plus two wildcard teams. The eight teams that have won their state qualifier are, in alphabetic order,

DePaul University	Illinois
Eastern Michigan University	Michigan
Indiana Institute of Technology	Indiana
Lakeland Community College	Ohio
Milwaukee School of Engineering	Wisconsin
Northern Kentucky University	Kentucky
Saint Cloud State University	Minnesota
Southeast Missouri State University	Missouri

First and second place teams from the 2019 Midwest Wildcard CCDC are,

Baldwin Wallace University     Ohio  
Metropolitan State University     Minnesota

### **Business Scenario**

Your organization is a manufacturer who produces a number of components for the US Department of Defense (DoD). As a DoD contractor, you are required to be compliant with the NIST 800-171 Cyber Security Controls. These are a subset of the well-known NIST 800-53 control framework. These controls are focused on two issues:

- Following industry best practices in Cyber Security.
- Protecting DoD supplied information from unauthorized disclosure.

You will be given a score which outlines the specific controls that we will be concerned with. The areas of NIST 800-171 that controls will be taken from are:

- 3.1 Access Controls
- 3.2 Awareness & Training
- 3.3 Audit & Accountability
- 3.4 Configuration Management
- 3.5 Identification & Authentication
- 3.6 Incident Response
- 3.7 Maintenance
- 3.10 Physical Security
- 3.11 Risk Assessment
- 3.12 Security Assessment
- 3.13 System & Communications Protection
- 3.14 System & Information Integrity

Expect to be asked to maintain an ongoing accounting of the alignment of the measures you put into place (either from direct injects or on your own volition) with the 171 framework.

### **Midwest Regional 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
10. To select an educational team to represent the Midwest at the National CCDC.

### **Institutional Requirements for Participation**

In order to compete at the regional, teams must satisfy the following requirements:

1. Submit paperwork from their institution authorizing their team to participate in the regional as an official school event; this authorization must include an explicit list of all student participants, and be signed by a school administrator. Schools should use their own authorization forms. This may also be an authorization letter on school letterhead. Teams may bring the authorization document to the event.
2. Have all student participants and alternates as well as all team advisers sign and submit MVCC Waiver forms. Emergency contact information is required.
3. All student participants must submit a resume in electronic form. Team advisers should collect these and email to the CSSIA Competition Director and Competition Administrator in a single compressed file.
4. All students and team advisers sign a MVCC photo release form; may submit at the event
5. Team Captain must sign this 2019 Erich J. Spengler Midwest Regional Team Packet; may sign at the event

### **Competition Team Identification**

- **Blue Team** - student team representing a specific academic institution competing in this competition; Each team consists of up to 12 competitors, submitted to the respective State CCDC Director for respective Midwest State CCDC. 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. Each competitor is expected to be a full time student at the school from which they compete. An exception is a part time student that expects to graduate in the current term. Such a student may compete if they were a full time student during the previous term. Substitution in the competition team requires approval from the CSSIA Competition Director or a CSSIA Compliance Monitor present at the competition.

Further guidelines for Blue Team participation have been documented in respective 2019 Midwest State CCDC Team Packets.

- National rules apply; [www.nationalccdc.org](http://www.nationalccdc.org)
- Further information is available at [www.cssia.org/ccdc](http://www.cssia.org/ccdc), the main website for Midwest Cyber Defense Competitions.

- **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, scoring management, room monitors and security enforcement in the various competition rooms. Judges will assess the competition team's ability to maintain their network and service availability based upon a business inject and a scoring instrument, delivering inject scenarios, scoring of injects, creating log entries, securing log files, issuing or controlling the timing of injects, etc. Each competing Blue Team may have a White Team member present in their room that will assist judges by observing teams, confirming proper inject completion as well as reported issues.
  
- **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 CSSIA Competition Director, 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
  - Manage event activities and events such as:
    - Greet people
    - Organize food, awards
    - Assist in setting up the competition
    - Assist with hotel / travel arrangements
  
- **Orange Team** – Student workers who assist the competition by accessing team services. Orange team members act like typical users, and may come from extraneous IP addresses. The Orange Team is expected to keep track of the accessibility of services and report to the White Team their results. The white team may use results of Orange Team activity as a part of scoring.

- **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.

### NDG NETLAB<sup>+</sup>™ VE System Access

- The competition network will be hosted via the Cyber Stadium located at Moraine Valley Community College. Each competition network will be located remotely from any competition room and will be logically isolated from all other competing Blue Teams. The access point is to an NDG NETLAB<sup>+</sup>™ VE system located at,

ccdc.cit.morainevalley.edu

The NDG NETLAB<sup>+</sup>™ VE is accessible via a web browser. Access accounts and initial passwords will be distributed at the start of the competition. Accounts will be,

t1u1, t1u2, ..., t1u8  
t2u1, t2u2, ...,  
....  
t10u1, ...

**ccdc**

[Home](#) [Pod](#) [Reservation](#)

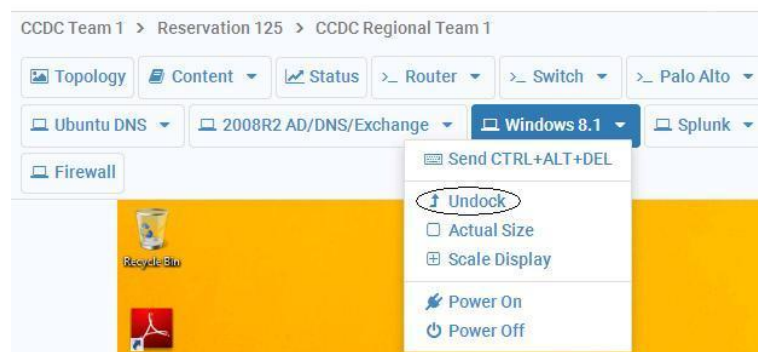
MyNETLAB > Master CCDC Regional > Reservation 971 > CCDC Team 1



Note that NDG has fixed the annoying WE'RE DONE button, which would end a team reservation, thankfully no longer appears on the topology page. However, a team may still end their reservation via the Reservation drop down, so teams are advised to avoid this during the competition.

Users can still access VMs by clicking on the topology diagram, but they can also click on the appropriate button at the top of the screen shown in the image. The VM access will then replace the topology image instead of a separate window as with a PE system. Users might wish to work on a VM in a separate window which they can do by the 'Undock' feature.

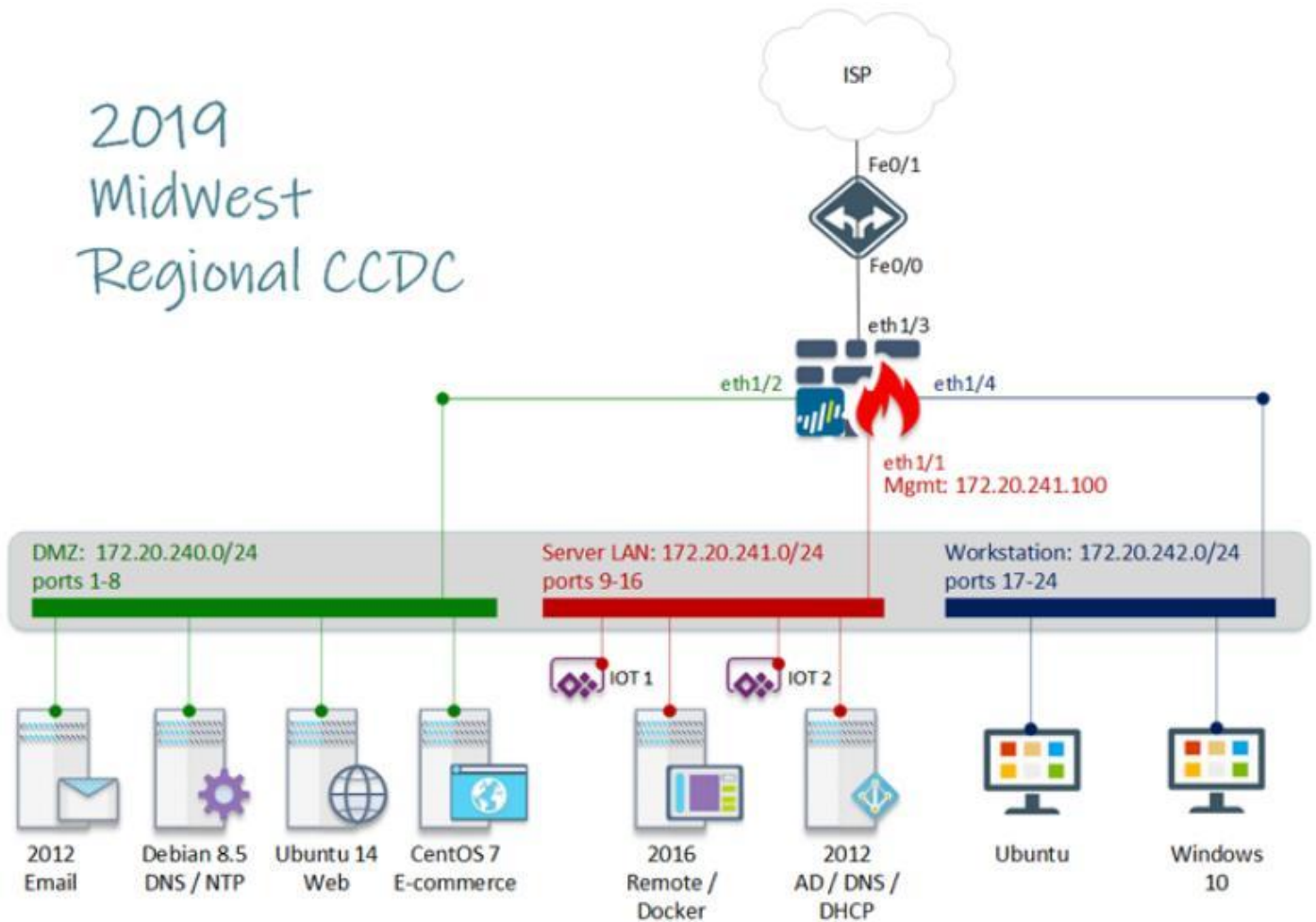
**ccdc**





## Competition Topology

2019  
Midwest  
Regional CCDC



## Network Description

- The router, and switch shown in the topology are hardware devices as follows:

Cisco 2811 Router with IOS c2800nm-adviservicesk9-mz.151.M10, Version 15.1(4)M1

Cisco 2960 Switch with C2960-LANBASEK9-M, Version 15.0(2)SE4

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  
f0/0 172.20.243.253



- Core IP addresses are the following:

Team	Router f0/1	Core connection to Router f0/1	"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 VM, version 7.1.13 with the following addresses:

```

ethernet1/1      172.20.241.254
ethernet1/2      172.20.240.254
ethernet1/3      172.20.243.254
ehternet1/4      172.20.242.254

```

The management IP is labeled on the topology:

172.20.241.100

The Palo Alto is intended to be managed from the 2016 Remote/ Docker via a secure browser session where the default account/password is:

admin:changeme

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 7	f0/4
PA eth1/2	f0/8
2016 Remote	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
E-commerce	CentOS 7	172.20.240.97/24	root / sysadmin	changeme

#### **Server LAN**

Remote / Docker	Srvr 2016 std	172.20.241.3/24	administrator	!Changeme123
AD / DNS/DHCP	Srvr 2012 std	172.20.241.27/24	administrator	!Password123
IOT		DHCP		

#### **Workstation LAN**

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

Palo Alto	PAN OS 8.0.0	172.20.241.100	admin	changeme
-----------	--------------	----------------	-------	----------

'Public' IP 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 7	172.20.240.97	172.25.team#.29
2016 Remote	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
IOT2		172.25.team#.98

- IOT1 & IOT2, internet of things, are physical devices attached to the competition network and are not directly accessible via NETLAB. IOT1 is a Raspberry Pi hardware appliance loaded with an Android OS. Access the Raspberry Pi via web, open access.
- IOT2 is expected to be an Arduino hardware appliance running http service to be scored. More information on IOT devices will be made available at the event.

- Systems are loaded with various user accounts. Teams are responsible to know which accounts are used for services. **Root, Administrator, Admin or Sysadmin will never be used for scoring.**
- As the hosting site, MVCC will adhere to client requirements for the Blue Team workstations in accordance with NDG guidelines. See, <https://www.netdevgroup.com/products/requirements/#client/>
- Each competition network will be physically and logically isolated from the hosting organization's network.
- Each competing Blue Team will be provided a set of workstations at the host site that are logically and physically isolated from other Blue Teams in order to access respective remote competition networks.
- The White Team and each respective Blue Team will communicate with each other via a Team Portal, a trouble ticket and response application (ISE – Inject Scoring Engine) residing within the remote network at Moraine Valley Community College. This system is accessible via a browser where the system is located at,

ccdcadmin1.morainevalley.edu

- Team accounts to the ISE are,

team1, team2,..., team10

The ISE permits multiple logins using the same account.

**Teams should login to the Team Portal/ISE first, using the team# account and password provided. Answer the Welcome inject signaling your readiness to compete. The drop flag is issued next, providing the initial password for all team accounts to the competition network at,**

ccdc.cit.morainevalley.edu

- Teams should be attentive to monitor inject requests and notifications via the Team Portal/ISE. A Welcome Inject will be issued ahead of the start of scoring. Response to this initial inject confirms team communication with the White Team. A Cyber Access inject will subsequently be issued containing the team password needed for initial access to the competition stadium.
- Red Team activity may be either externally or internally sourced with respect to the remote competition network. At no time will the Red Team have access outside the remote network perimeter. Neither will the Red Team be given direct access to any Team network directly via the NDG NETLAB<sup>+</sup>™ VE system.
- Each Blue Team network will be monitored by a scoring system operating within the remote network. An indication of services, as viewed by the indigenous scoring engine, will be made available to each Blue Team via the Team Portal/ISE.
- **While every effort is made to provide a stable and well defined competition topology, it is subject to change and /or modification as decided by the CCDC Competition Director.**

## **Functional Services**

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

### **HTTP**

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

### **HTTPS**

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

### **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.

### **DNS**

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

### **SSH**

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

## Schedule – all times CST

### **Friday, March 15, 2019**

- 12:00-1:30pm Check-in at Moraine Valley Community College, Technology Building  
Receive Competition Packets, Team and Room Assignment, ISE password  
Team captain signs off team packet  
Mingle with the Sponsors – light hors d’oeuvres
- 1:30pm Fogelson Auditorium  
David Durkee - Welcome & Introduction to the 2019 Regional CCDC  
Keynote Speakers:  
Kaitlynn Bestenheider  
Joe Wissler, Network Operator, NSA Red Team  
A Word from our Sponsors (5 minutes for each sponsor)  
George Meyer – White Team
- 3:00pm Speed Networking of Teams with the Sponsors
- 5:00-5:30pm Students return to competition room/ login to ISE/ respond to Welcome inject
- 5:30pm Start of Competition; scoring begins
- 6:00pm Dinner – T100 Area – Food will be delivered to the team rooms so teams do not have to leave their rooms.
- 10:00pm Competition ends/Scoring ends for the day

### **Saturday, March 16, 2019**

- 8:00-8:30am Continental Breakfast  
Student Teams arrive at Moraine Valley Community College  
Go straight to the competition room
- 8:30am Announcements via ISE
- 9:00am Start of Competition; scoring begins
- 12:30pm Lunch – Fogelson Foyer – teams filter through and return to their rooms
- 6:00pm Competition ends/Scoring ends  
Dinner – T100 Area & Fogelson Foyer
- 7:00pm Fogelson Theater - Presentations by Red & White Team representative(s)  
Announce final winners
- 7:30pm Competition Director meets with First Place Team

## 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. Teams must compete using the workstations provided. Competitors may not use their own laptops, workstations, tablet, &c.
3. Teams will be provided all access credentials on the morning of the competition.
4. Teams should not assume any competition system is properly functioning or secure.

5. Throughout the competition, Green, Orange, and White Team members will occasionally need access to a team's systems for scoring, troubleshooting, etc. Teams must allow Green, Orange, and White Team member access when requested. This includes access to the remote system. Teams reserve the right to refuse entry for those not wearing proper identification. Red Team members will not enter rooms.
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. 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 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.
9. **Teams are permitted to move services to another platform, provided that the same "public" IP address and DNS naming convention is maintained, along with other requirements of the service. Teams must also notify the White Team if services are moved to another platform, with a rationale for the change.**
10. Teams must maintain "public" services as available from all source IP addresses. Attempts to restrict or filter by IP source address may adversely affect scoring directly, and may also incur a penalty when detected.
11. In the event of system lock or failure, teams will be able to request a complete restoration (scrub/snapshot) via an inject released from the ISE. This will reset any system to its initial starting configuration. The number of system restorations will be tracked and negatively impact scores at the discretion of the White Team. Teams should also consider that system restoration will take time.
12. 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.
13. Teams may not modify the hardware configurations of workstations used to access the competition network.
14. Servers and networking equipment may be re-tasked or reconfigured as needed.

### **Competition Rules: Acknowledgement & Agreement**

Competition rules are applicable to all participants of the Midwest CCDC. 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 the host site. Team advisers and team captains are required to sign where indicated, signifying their acknowledgement of competition rules and their commitment to abide by them.

Team advisers 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.

### Competition Rules: Student Teams

1. Each team will consist of up to no more than eight members. All team advisers have been informed of and will adhere to all national rules. See [www.nationalccdc.org](http://www.nationalccdc.org)
2. Each team may have no more than two graduate students as team members.
3. Each team must have one adviser present during the entire competition – this may be a faculty/staff member or an administrator. Institutions may also send an additional faculty adviser. Team advisers and faculty representatives may not assist or advise the team during the competition. Team advisers and faculty representatives may not be involved in any scoring or decisions that involve a participating institution or Blue Team.
4. All team members, the team adviser, and all faculty representatives will be issued badges identifying team affiliation which must be worn at all times during competition hours.
5. 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. Team Captains should identify themselves to the White Team by team number, and not by institution.

### Competition Rules: Professional Conduct

1. All participants are expected to behave professionally at all times they are visiting the host site, and at all preparation meetings.
2. Host site/ local site policies and rules apply throughout the competition.
3. All Midwest Cyber Defense Competitions are alcohol free events. No drinking is permitted at any time during the competition.
4. Activities such as swearing, consumption of alcohol or illegal drugs, disrespect, unruly behavior, sexual harassment, improper physical contact, becoming argumentative, or willful physical damage have no place at the competition.
5. In the event of unprofessional conduct, student team members and their adviser will meet with Gold Team members upon request. The consequence of unprofessional conduct will be determined by the Site Administrator with the recommendation of the Gold Team. This may be a warning, point penalty, disqualification, or expulsion from the campus.
6. The Site Administrator or a Gold Team member from CSSIA reserves the right to disqualify an offender from participation in future competitions.

### Competition Rules: Competition Play

1. All teams will compete in a dedicated classroom with similar workstations, displays, overhead projector, and printer. Rooms are selected so that all teams may compete fairly. **Policy this year is that team room doors will be left open during the competition, and no window coverings will be allowed.**
2. During the competition team members are forbidden from entering or attempting to enter another team's competition workspace or room. They are also forbidden from accessing another Team network, either through their competition network, or by remote access to another team.



3. All requests for items such as software, service checks, system resets, and service requests must be submitted to the White Team. Requests must clearly show the requesting team by number, action or item requested, and date/time requested. **Teams should not identify the school they represent to the White Team.**
4. Teams must compete without outside assistance from non-team members which includes team advisers and sponsors. All private communications (calls, emails, chat, directed emails, forum postings, conversations, requests for assistance, etc.) with non-team members are forbidden and are grounds for disqualification.
5. No PDAs, memory sticks, CD-ROMs, electronic media, or other similar electronic devices, are allowed in the room during the competition unless specifically authorized by the White Team in advance. All cellular calls must be made and received outside of team rooms. Any violation of these rules will result in disqualification of the team member and a penalty assigned to the appropriate team.
6. Teams may not bring any computer, tablets, PDA, or wireless device into the competition area, including flash drives, Nook and Kindle. MP3 players with headphones will be allowed in the competition area provided they are not connected to any system or computer in the competition area.
7. Printed reference materials (books, magazines, checklists) are permitted in competition areas and teams may bring printed reference materials to the competition.
8. Team 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 a point penalty will be assessed against the team.
9. An unbiased Red Team will probe, scan, and attempt to penetrate or disrupt each team's operations throughout the competition.
10. 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, White Team members, other competitors, etc. outside of competition hours.
11. Only Blue Team, White Team or Gold Team members will be allowed in any Blue Team competition room. On occasion, White Team or Gold Team members may escort individuals (VIPs, press, etc.) through the competition area including team rooms. Guest visits must be approved by the CSSIA Competition Director and are not encouraged as it may distract the Blue Team members during their activities.
12. White, Gold, or Green Team members will be allowed in competition areas outside of competition hours. **The Red Team is never granted access to any Blue Team competition room, and is not granted access to the Cyber Stadium team networks outside of competition hours.**
13. All individuals involved with the competition will be issued badges which must be worn at all times during the competition.
14. Teams are permitted to replace applications and services provided they continue to provide the same content, data, and functionality of the original service. For example, one mail service may be replaced with another provided the new service still supports standard SMTP commands, supports the same user set, and preserves any pre-existing messages users may have stored in the original service. Failure to preserve pre-existing data during a service migration will result in a point penalty as deemed appropriate by the White Team for each user and service affected.

15. Teams are free to examine their own systems but no offensive activity against other teams, the White Team, or the Red Team will be tolerated. This includes port scans, unauthorized connection attempts, vulnerability scans, etc. Any team performing offensive activity against other teams, the White Team, the Red Team, or any global asset will be immediately disqualified from the competition. If there are any questions or concerns during the competition about whether or not specific actions can be considered offensive in nature contact the White Team before performing those actions.
16. Blue Team members may not change usernames within their respective environment, unless directed to do so by the White Team. Blue Team members may change passwords for administrator and user level accounts. **Changes to passwords affecting scored services must be communicated to the White Team via the password change request feature of the ISE. Look for a password change policy to be issued during the competition. Changes to administrator and root account passwords may be changed without notification, since these are not used for scoring services.** Competitors have the responsibility to determine how accounts relate to services.
17. 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.
18. Each Blue Team will be provided with the same objectives and tasks.
19. Each Blue Team will be given the same inject scenario at the same time during the course of the competition.
20. Blue Teams may request information from the White Team and Scoring Manager as to why a particular service is not scoring properly. Disclosure of information regarding non-scoring of services is at the discretion of the White Team. Nevertheless, if core system or scoring system faults are discovered, every effort will be made towards corrective action together with modification of scores to maintain equity and fairness.
21. The White Team is responsible for implementing the scenario events, refereeing, team scoring and tabulation.
22. Scoring will be based on keeping required services up, controlling/preventing unauthorized access, and completing business tasks in a timely manner that will be provided throughout the competition.
23. Scores for inject completion and incident reports will be maintained by the White Team, and will not be shared with Blue Team members. Running totals will not be provided during the competition. Some debriefing of a general nature is likely at the end of the competition.
24. If a scenario or event arises that may negatively impact the integrity or fairness of any aspect of the competition that was not previously anticipated, it is the final decision and discretion of the Chief Judge to make adjustments in scores, or deploy new policies.

#### **Competition Rules: Internet Usage**

1. Competition systems will have controlled access to the Internet for the purposes of research and downloading patches. **All internet access from the competition network will be through a web proxy.**

2. The web proxy will permit a predetermined set of common web sites including several used for software repositories. Per National CCDC practice, the complete list of accessible sites will not be published.
3. Teams have been solicited for up to 15 additional sites per team to be accessible from the competition network. Such sites will be assessed, added to the web proxy, and the complete list of added sites published to teams as part of the documentation received at check-in, or alternatively, available in the team rooms, or available within the competition environment.
4. Workstations located in competition rooms will have internet connectivity.
5. Although internet activity is restricted in the competition network, means to circumvent the intent of this limitation may be discovered. Thus internet activity will be monitored. Any team member caught viewing inappropriate or unauthorized content will be immediately disqualified from the competition. This includes direct contact with outside sources through AIM/chat/email or any other public or non-public services such as Facebook. For the purposes of this competition inappropriate content includes pornography or explicit materials, pirated media files or software, sites containing key generators and pirated software, etc. If there are any questions or concerns during the competition about whether or not specific materials are unauthorized contact the White Team immediately.
6. No peer to peer, distributed file sharing clients or servers are permitted on competition networks.
7. Additional software or tools must be either free or open source within the limits of pre-determined internet accessibility.
8. Teams may not use any external, private electronic staging area or FTP site for patches, software, etc. during the competition.
9. All network activity that takes place on the competition network may be logged and is subject to release. **Competition officials are not responsible for the security of any personal information, including login credentials that competitors place on the competition network.**

### Competition Rules: 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 violating service level agreements after services have been unavailable, usage of recovery services, and successful penetrations by the Red Team.
2. Scores will be maintained by the White Team. Individual tracking of services will be available to respective teams during the competition. Blue Team members should use available service 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 generally be completed as needed throughout the competition and submitted to the White Team. The White Team reserves the right to stipulate the times and manner in which incident reports may be submitted. 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.

### **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 CSSIA Competition Director, the White Team, 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, and Green Teams strive to make the Midwest CCDC 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/ccdc](http://www.cssia.org/ccdc). They are also forbidden from publishing, posting on the internet, or publicly communicating assessments of the Midwest 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 Midwest CCDC, and may also enumerate participating teams and winners.

**Sponsors:**

	<p>Department of Homeland Security,  <a href="http://www.dhs.gov/">http://www.dhs.gov/</a></p>
	<p>SecureWorks, <a href="http://www.secureworks.com">http://www.secureworks.com</a></p>
	<p>Raytheon Company, <a href="https://www.raytheon.com">https://www.raytheon.com</a></p>
	<p>Palo Alto Networks,  <a href="https://www.paloaltonetworks.com/">https://www.paloaltonetworks.com/</a></p>
	<p>Walmart Inc., <a href="https://www.walmart.com/">https://www.walmart.com/</a></p>
	<p>780th Military Intelligence Brigade, INSCOM,  <a href="https://www.inscom.army.mil/msc/780mib/">https://www.inscom.army.mil/msc/780mib/</a></p>
	<p>XR Trading LLC, <a href="http://www.xrtrading.com/">http://www.xrtrading.com/</a></p>
	<p>SPAWAR, <a href="https://www.public.navy.mil/spawar">https://www.public.navy.mil/spawar</a></p>
	<p>National Security Agency, <a href="https://www.nsa.gov/">https://www.nsa.gov/</a></p>

	<p>Air Force Civilian Service  <a href="https://www.afciviliancareers.com/">https://www.afciviliancareers.com/</a></p>
	<p>CSSIA, <a href="http://www.cssia.org/">http://www.cssia.org/</a></p>