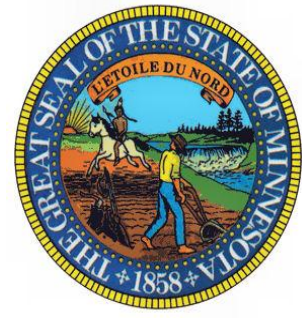


2012 Midwest Regional Collegiate Cyber Defense Competition Team Packet



March 16-17, 2012

© CSSIA 2012

Table of Contents

Contents

Midwest Regional CCDC Mission and Objectives	3
Overview	3
Business Scenario	3
Midwest Regional Competition Goals.....	4
Institutional Requirements for Participation	4
Competition Team Identification.....	4
Competition Topology	6
Network Description.....	6
Functional Services	9
Schedule	9
Systems	10
Competition Rules: Acknowledgement & Agreement	11
Competition Rules: Student Teams	11
Competition Rules: Professional Conduct	11
Competition Rules: Competition Play	12
Competition Rules: Internet Usage	14
Competition Rules: Scoring.....	14
Business Tasks	15
Questions and Disputes	16
Aftermath	16
Sponsors:.....	17

Midwest Regional CCDC Mission and Objectives

The 2012 Midwest Regional Collegiate Cyber Defense Competition (CCDC) provides a competitive opportunity for collegiate teams who have placed in 2012 Midwest State CCDC 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 2012 Midwest Regional CCDC is eligible to move on to the 2012 National CCDC in San Antonio, Texas, April 20-22, 2012.

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 servers and web servers, respond to business requests such as the addition or removal of additional services, and balance security against varying business needs.

Business Scenario

The IT staff and management of your company have just been dismissed due to continual failure to pass a SOX audit. You are the new staff. The new management is just starting to review and develop new policy and procedures to address the audit and other operational deficiencies. You will need to keep the infrastructure in a production status while implementing new requirements as they are developed. Your firm deals with health care services, and thus have requirements for HIPAA compliance as well as SOX, being a publicly traded company.

The company had just acquired another similar company and these two independent networks need to be operated by the new IT staff and the need to interconnect for data exchange has just been announced.

You have been given the current accounts and passwords a topology map, and existing running servers with their services.

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. Have all members fill out their respective State CCDC electronic based event survey
2. 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.
3. Have all student participants and alternates as well as all team advisors sign and submit MVCC Waiver forms. Emergency contact information is required.
4. All student participants (not alternates) must submit a resume in electronic form. Team advisors should collect these and email to the CSSIA Competition Director in a single compressed file.
5. All students and team advisors sign MVCC photo release form; may submit at the event
6. Team Captain must sign this 2012 Midwest Regional Team Packet; may sign at the event

Competition Team Identification

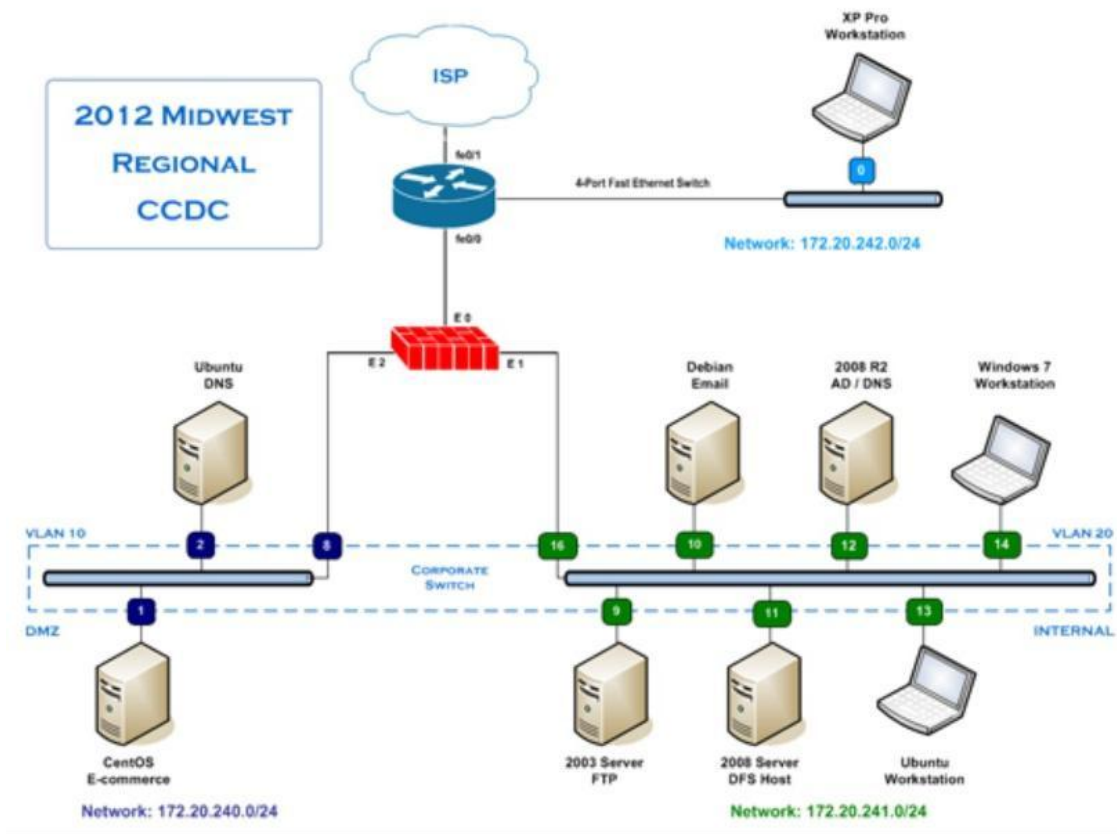
- **Blue Team** - student team representing a specific academic institution competing in this competition; Each team consists of up to 12 competitors, submitted to the respective State CCDC Director for respective Midwest State CCDC. Each competition team may consist of up to eight (8) members chosen from the submitted roster. The remainder of the roster is for substitution in the event a member of the active competition team cannot compete. Substitution in the competition team requires approval from the CSSIA CCDC Director or a CSSIA Compliance Monitor present at the competition.

Further guidelines for Blue Team participation have been documented in respective 2012 Midwest CCDC Team Packets.

- National rules apply; www.nationalccdc.org
- Further information is available at 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 who 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
- 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.

Competition Topology



Network Description

- 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⁺™ PE system located at,

cyberlab.morainevalley.edu

NDG NETLAB⁺™ PE is accessible via a web browser. Access accounts and initial passwords will be distributed at the start of the competition. Accounts are expected to be the same as used for respective 2012 Midwest State CCDC.

- The numbers in the topology diagram associated with connections correspond to switch interface numbers.
- The router, firewall, and switch shown in the topology are hardware devices as follows:

Cisco 2811 Router with IOS C2800NM-ADVIPSERVICESK9-M, Version 12.4(24)T1
 Cisco Pix 515E with Security Appliance Software Version 7.2(1); ASDM also loaded
 Cisco 2950 Switch with C2950-I6Q4L2-M, Version 12.1(14)EA1a

All servers and workstations are virtual machines under the management of NETLAB⁺™.

- Each team has the following router/ pix internal addresses:

Router
 f0/0 172.20.243.253
 Vlan30 172.20.242.254

Pix
 Ethernet0 172.20.243.254
 Ethernet1 172.20.241.254
 Ethernet2 172.20.240.254

- 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

- Services provided by the servers in the topology are expected to have the same last octet of the IP address for internal and external "Public".

VM Label	Major Service	Internal IP	Public' IP or pool	Account	initial password
CentOS E-Commerce	HTTP/S; FTP	172.20.240.11	172.25.team#.11	root	changeme
Ubuntu DNS	DNS	172.20.240.23	172.25.team#.23	root	changeme
2003 Server FTP	SQL	172.20.241.9	172.25.team#.9	administrator	changeme
Debian Email	Email	172.20.241.39	172.25.team#.39	root	changeme
2008 Server DFS Host	DFS	172.20.241.3	172.25.team#.3	administrator	changeme
2008 R2 AD/ DNS	AD/DNS	172.20.241.27	172.25.team#.27	administrator	changeme
Ubuntu Workstation		DHCP 172.20.241.0/24	172.25.team#.240-253	administrator	changeme
Windows 7 Workstation		DHCP 172.20.241.0/24	172.25.team#.240-253	administrator	changeme
XP Pro Workstation		DHCP 172.20.242.0/24	172.25.team#.140-150	administrator	changeme

- As the hosting site, MVCC will adhere to client requirements for the Blue Team workstations in accordance with NDG guidelines. See, www.netdevgroup.com/products/pe/requirements/
- 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.
- A workstation at the host site cannot access the competition network and the internet at the same time. Competition workstations and servers are able to access the internet.
- 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

- Access and accounts and passwords to the ISE are synchronized with the accounts and initial passwords to the NDG NETLAB⁺™ PE system.

Links to both the NDG NETLAB⁺™ PE system which accesses the Cyber Stadium, and the Team Portal are also at

www.cssia.org/ccdc

- Teams should be attentive to monitor inject requests and notifications via the Team Portal/ISE. A Welcome Inject will be issued soon after the start of scoring. Response to this initial inject confirms team communication with the White Team.
- 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.
- 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.

FTP

Successful access to a database and authentication will be tested via the FTP protocol. Some indication of database integrity will also be examined.

SSH

An SSH session will be initiated to simulate a vendor account logging in on a regular basis to check error logs. Each successful login and log check will be awarded points.

DNS

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

Schedule

Friday, March 16, 2012

12:00-1:30pm Check-in at Moraine Valley Community College, Technology Building

1:30pm Fogelson Auditorium

David Durkee - Welcome & Introduction to the 2012 Regional CCDC

Mike Davis of Savid Technologies – Keynote Speaker

Doug Huber of Loraine County Community College - Chief Judge

2:30pm	Materials Disbursement, Competition Packets, and Room Assignment where applicable; Teams access remote system; Team captain signs off confirmation for system ready
3:00pm	Start of Competition; scoring begins
5:00pm	Red Team Escalation
9:00pm	Competition ends/Scoring ends for the day
9:00pm-	Job Fair - food will be served

Saturday, March 17, 2012

8:00-8:30am	Student Teams arrive at Moraine Valley Community College
8:30am	Announcements
9:00am	Start of Competition; scoring begins
6:00pm	Competition ends/Scoring ends
7:00pm	Presentations by Red & White Team representative(s); announce final winners

Systems

1. Each team will start the competition with identically configured systems.
2. Teams may not add or remove any computer, printer, or networking device from the designated competition area.
3. Teams 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 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. This includes access to the remote system.
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 if detected.
11. In the event of system lock or failure, teams will be able to perform a complete restoration from within the administration console of the remote system. This will reset

- any system to its initial starting configuration. The number of system restorations will be tracked and negatively impact scores at the discretion of the White Team. Teams should also consider that system restoration will take time.
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 advisors and team captains are required to sign where indicated, signifying 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.

Competition Rules: Student Teams

1. Each team will consist of up to no more than eight members. All team advisors have been informed of and will adhere to all national rules. See www.nationalccdc.org
2. Each team may have no more than two graduate students as team members.
3. Each team must have one advisor present during the entire competition – this may be a faculty/staff member or an administrator. Institutions may also send an additional faculty advisor. Team advisors and faculty representatives may not assist or advise the team during the competition. Team advisors 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 advisor, 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 advisor 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. 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.
2. 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.**
3. Teams must compete without outside assistance from non-team members which includes team advisors 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.
4. 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.
5. Teams may not bring any computer, tablets, PDA, or wireless device into the competition area, including 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.
6. Printed reference materials (books, magazines, checklists) are permitted in competition areas and teams may bring printed reference materials to the competition.
7. 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.
8. An unbiased Red Team will probe, scan, and attempt to penetrate or disrupt each team's operations throughout the competition.
9. 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.

10. 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.
11. 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 outside of competition hours.
12. All individuals involved with the competition will be issued badges which must be worn at all times during the competition.
13. 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.
14. 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.
15. 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 must be communicated to the White Team, including administrator and root accounts using the Team Portal.** Competitors should bear in mind that changes to passwords may affect scoring on certain services.
16. Blue Team members should maintain ICMP on all competition devices and systems, including the router and pix, unless directed otherwise by the White Team. 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.
17. Each Blue Team will be provided with the same objectives and tasks.
18. Each Blue Team will be given the same inject scenario at the same time during the course of the competition.
19. 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.

20. The White Team is responsible for implementing the scenario events, refereeing, team scoring and tabulation.
21. 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.
22. 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.
23. 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 access to the Internet for the purposes of research and downloading patches. Internet activity will be monitored and 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 non-public services. For the purposes of this competition inappropriate content includes pornography or explicit materials, pirated media files or software, sites containing key generators and pirated software, etc. If there are any questions or concerns during the competition about whether or not specific materials are unauthorized contact the White Team immediately.
2. Internet resources such as FAQs, how-to's, existing forums and responses, and company websites are completely valid for competition use provided there is no fee required to access those resources and access to those resources has not been granted based on a previous purchase or fee. Only resources that could reasonably be available to all teams are permitted. For example, accessing Cisco resources through a CCO account would not be permitted but searching a public Cisco support forum would be permitted.
3. Teams may not use any external, private electronic staging area or FTP site for patches, software, etc. during the competition. All Internet resources used during the competition must be freely available to all other teams. Internet activity will be monitored for access to staged sites as well, and penalties levied for infractions.
4. Public sites such as Security Focus or Packetstorm are acceptable. Only public resources that every team could access if they chose to are permitted. No peer to peer or distributed file sharing clients or servers are permitted on competition networks.
5. 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, 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:

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

Precise percentage breakdown will be determined by the White Team.

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. 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:

	National Science Foundation, http://www.nsf.gov/
	Department of Homeland Security, http://www.dhs.gov
	Space and Naval Warfare Systems Command, www.public.navy.mil/spawar
	U.S. Army INSOM Cyber Bridgade, www.cyberspaceskills.com
	EC-Council, http://www.eccouncil.org
	SecureWorks, http://www.secureworks.com
	CSSIA, http://www.cssia.org/
	Deloitte, http://www.deloitte.com