

# Collegiate Cyber Competition Toolkit



A Guide for Managers

## Contents

Overview.....	3
Plan & Manage Competition Process .....	4
Execute Competition Process .....	5
Judging Goals & Guidelines .....	6
Injects and Business Analysis.....	8
Remote/ Team Site Judging and Compliance .....	9
Scoring Management - Goals & Guidelines .....	10
Topology, Scenario and Team Packet .....	11
Penetration Activities (Red Team).....	13
Administration .....	15
Site Management / Hospitality.....	16
Appendix - Sample Team Pack.....	17
State CCDC Mission and Objectives .....	19
Overview.....	19
Competition Goals .....	20
Competition Team Identification .....	20
Initial Connection & the Start Flag .....	22
Network & Team Site Description.....	27
Schedule - Times are CST .....	27
Systems.....	28
Competition Rules: Acknowledgement & Agreement.....	28
Competition Rules: Entry Fee Payment.....	29
Competition Rules: Student Teams.....	29
Competition Rules: Professional Conduct .....	30
Competition Rules: Competition Play .....	30
Competition Rules: Internet Usage .....	32
Competition Rules: Scoring.....	32
Functional Services .....	33
Business Tasks .....	34
Questions and Disputes.....	35
Aftermath .....	35
Competition Topology .....	36
Sponsors:.....	38
Appendix - Addressing Access Problems to NETLAB+™ Systems .....	39

## Overview

Cyber competitions for collegiate students have been shown to enhance student learning and rapid acquisition of skills. Information technology is a challenging area for educators, and is quite different from traditional subjects like mathematics and the humanities. Managing information systems is not just a theoretical endeavor. Real systems and software run 'out there' someplace in ethereal space, making it difficult to visualize, discover, and administer. Such systems are becoming so diverse, and are changing so rapidly it is difficult to remain current while striving towards a comprehensive approach.

Students much endure numerous training sessions that focus on minute details or vignettes of information technology in order to even begin to function successfully in the field. What is oftentimes lacking is a comprehensive, integrative activity that will tie all their previous study together. This is the goal of a cyber-competition.

Because of the success of cyber competitions in meeting the educational needs of students and providing substantial preparation for the workspace, several types and styles of cyber competitions are being initiated throughout the country. CSSIA has managed the Collegiate Cyber Defense Competition (CCDC) since 2006, and serves as the basis for this document. Nevertheless, attention has been given to document concerns that are common to all types of cyber competitions.

Successful execution of a cyber-competition involves the coordination of a team of managers and information technology professionals. This document delineates the various organization of teams with guidelines and policies. The initial process diagrams specifically document visually the sub-processes and teams towards management and execution of the CCDC in the Midwest under the guidance of the Competition Industrial Advisory Board (CIAB), which has provided invaluable oversight for this publication.

It is hoped that this document will be instrumental in providing managers guidance towards design and management of future cyber competitions.

David Durkee  
CSSIA Competition Manger

# Plan & Manage Competition Process

## Process: Plan & Manage CCDC (Collegiate Cyber Defense Competitions)

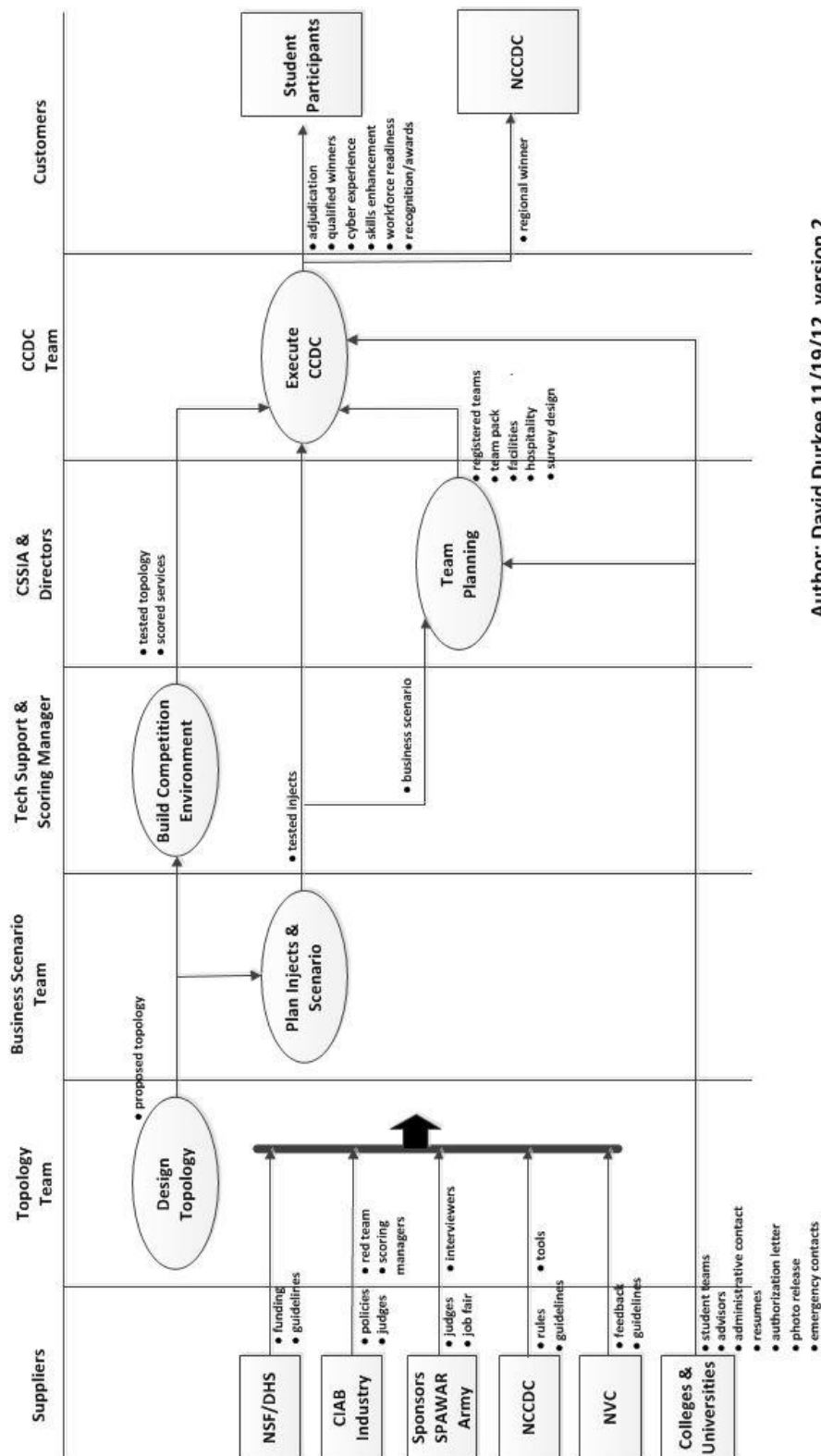
Process Owner: Erich Spengler

Process Goal: Provide Cyber Security & IT Management Training to Collegiate Students

Primary Customers: Collegiate Students enrolled in Cyber Security Curricula

### Guiding Principles

- Professional Conduct
- Educational for All Teams
- Judged by Industry
- Fair and Equitable
- Anonymous Judging
- NCCDC Compliance
- Competitiveness



Author: David Durkee 11/19/12, version 2

# Execute Competition Process

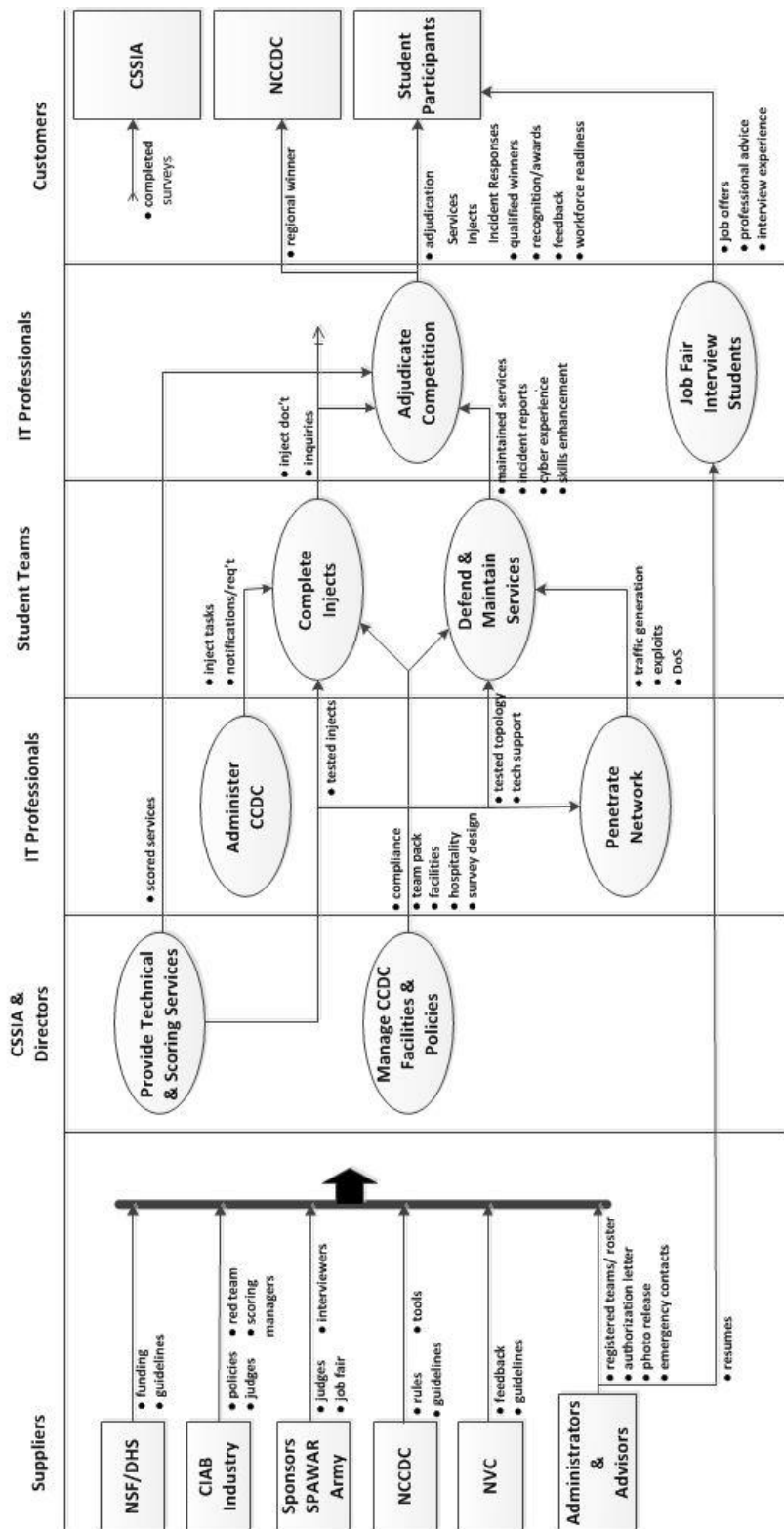
## Process: Execute CCDC (Collegiate Cyber Defense Competitions)

Process Owner: Erich Spengler

Process Goal: Provide Cyber Security & IT Management Training to Collegiate Students

Primary Customers: Collegiate Students enrolled in Cyber Security Curricula

- Guiding Principles**
- Professional Conduct
  - Educational for All Teams
  - Judged by Industry
  - Fair and Equitable
  - Anonymous Judging
  - NCCDC Compliance
  - Competitiveness



Author: David Durkee 12/31/12, version 1

## Judging Goals & Guidelines

The major task of the judging team is to provide to the competition accurate, objective judging and scoring. Tasks and issues include,

1. Identify chief judge
2. Define how subcommittee score will be tabulated and propose to CIAB
3. Select and secure competition judging staff / team
4. Recommend process and procedure for overall judging processes
5. Ensure guidelines and rules of competition are being followed as set by CIAB
6. Monitor all scoring processes (red team, injects, services, other) during given competition
7. Establish team / judging communication mechanisms
8. Validate and confirm final scores
9. Judge all inject as provided by inject team
10. Manage all conflict resolution
11. Address adhoc injects
12. How would the judging team handle the following: How points are awarded for injects completion? Timing, all or none.

### Judging Policies

#### Eligibility for Event Judge(s) & Compliance Monitor

Event judges may be selected from business, government agencies, or academia, but preferably from business. Judges should have extensive experience in information technology and security management, with oversight including but not limited to infrastructure and facilities planning, providing and maintaining services, policy generation and compliance, access controls, reporting, penetration testing, intrusion detection, quality management, risk assessment, and business recovery. Preferred judges have had experience managing direct reports and budget, with a broad view of organizational dynamics and information technology.

Judges from academia should also exhibit the foregoing qualifications, and must not be associated with competing institutions.

A representative of CSSIA is expected to be present at all Midwest Competition events, and will serve as a Compliance Monitor. The role of the Compliance Monitor is to apprise all teams of event policies and guidelines as needed.

Selection of judges may be made by the Competition Event Manager, or any member of the CIAB Judging Subcommittee, or the Midwest Competition Steering Committee. There shall be a minimum of three judges for any Competition event. Credentials of selected judges will be reviewed and approved by the CIAB Judging Subcommittee one week before any competition. The Process Manager reserves the right to reject selection of judgeship.

### Responsibility & Chief Judge

The role of Competition judge is crucial for the overall success and integrity of the event. As a team the judges are responsible for and have oversight of the cadence and direction of event

activities. As a group, the judges fulfill the role of management over the individual teams as part of the simulated environment. Judges do not have responsibility for site management.

All event judges should become familiar with the Midwest Competition Policy Guidelines as well as the specific event Team Packet distributed to participants prior to the event. Judges may also be requested to participate in pre-event “dry run” exercises.

The Chief Judge will be determined prior to the competition and will act as a final arbiter for all actions with collaboration of the judging team. The Chief Judge shall not be the CSSIA Compliance Monitor. The Chief Judge may, at their discretion, delegate their role of Chief Judge to another member of the team to maintain the role during extended event duration. The decisions of the Chief Judge or delegated Chief Judge are final and cannot be revoked. This includes the role of CSSIA Compliance Monitor, who can only advise as to Midwest Competition Policy.

As a team, the judges are responsible to,

- Announce the initiation of the event
- Direct and communicate with the Scoring Team as to all scoring times and services
- Decide and distribute injects to all team participants based on team performance
- Direct and communicate with the Red Team to sequence their activities – packet generation, reconnaissance, system compromise, denial of service
- Make decisions on behalf of teams needing management direction or clarification
- Delegate help to specific teams when requested
- Communicate with site management as to core network and services faults
- Adjudicate completion of inject requests based on timeliness and quality
- Adjudicate penalties or adjustments when teams have received outside assistance
- Maintain a master electronic compilation of adjudication results of inject and assistance requests by team
- Announce event cessation, whether temporary, scheduled, unscheduled, or final

### Scoring Criteria and Guidelines

During the event, each judge will score the teams using the scoring criteria and the competitions judging forms. Each Judge will individually score each task/inject according to the guidelines provided by respective scoring instructions. The Chief Judge will be responsible for collecting the scores from the judges and tally them on to one reporting form. All other Judge decisions will be by majority vote and will be final with regard to adherence to rules, disputes, team eligibility, disqualifications, and other competition conduct. At no time should a participating judge visit any of the competing team room.

### Communication to Teams

During the event, a means for the Judging Team to communicate to Student Teams needs to be determined consistent with the hosting facilities. Communication may be via hand written instructions, internal or external email, instant messaging service or internal or external telephone. The method of communication will be specified by the Judging Team on the first day of the event.

### Incident Reports

During the event, all Incident reports will be directed to the Judging Team and communicated to the appropriate personnel for action. Incident reports should be submitted on the formal Incident Report form. An electronic copy of the form will be distributed to each team on the first day of the event.

### Grievances

During the event, all grievances will be submitted to the Judging Team and communicated to the appropriate personnel for action. A grievance needs be submitted on the formal Grievance Report form, include all supporting documentation, and initialed by the team captain. The Judging Team is responsible for grievance resolution, and will communicate its decision in a timely manner to the submitting team. The Judging Team may also deploy policy or rule clarifications to student teams as needed, or request changes to scoring engine procedures. In the absence of Judging Team consensus, the Chief Judge, or delegated Chief Judge, will make the final decision regarding grievance resolution.

### Disqualification

By entering the competition, each student and advisor agrees to abide by all the competition rules. Failure to follow any of the rules will constitute grounds for disqualification of the entry. All participants must be supervised by a faculty advisor or instructor. The faculty member is responsible for insuring that each competing student adheres to the rules set by the competition. At anytime if a member of a competing school attempts to compromise another competing school system, the offending team will be automatically disqualified and excluded from the competition.

### Resolution of Winner(s)

The competition winner(s) will be determined through a collective effort between the Judges scores, the scoring engine team and the red teams' scores. The Chief Judge will add their scores to the overall competition scoring form and tallied to determine a winner to the competition. In the event there is a tie, the Chief Judge will review the information with the members of the scoring engine team, red team leaders and the participating competition board members to determine the winner.

### Announcement of Winners & Postmortem

Prior to making any announcement as to the winners of the competition, the Chief Judge will provide a brief discussion of how the competition resulted. The Chief Judge will then announce first, second, and third place winners.

## **Injects and Business Analysis**

Judges have the responsibility to establish inject tasks and anomalies for student teams to complete during the course of the competition. These will assess the skills and individual responses for each team. Tasks and issues include,

1. Create inject and anomaly template
2. Develop regional injects and anomalies with the following scope:



- a. Administrative
- b. Service changes
- c. Testing
- d. Upgrades
- e. Assessment
- f. Technical plans
- g. Infrastructure changes
- h. New or improved security measures
- i. Applications
- j. Reporting and incident response
3. Design state competition inject database to assist state
4. Establish scoring criteria for priority, difficulty and time assessment of each inject or anomaly
5. Ensure judging team is educated on inject scoring metrics
6. Recommend processes and procedures for overall inject development
7. Ensure all injects reflect topology and equipment availability
8. Publish final inject book for CIAB review prior to competition
9. Coordinate injects with red team for planted or inserted vulnerabilities
10. Red/ penetration team may request injects from inject team

## **Remote/ Team Site Judging and Compliance**

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

Remote teams are required to compete from a location with controlled access, i.e., a separate room or a portion of a room that is dedicated for the Competition. Workstations and internet access must comply with published requirements.

One or more Remote Site Judge(s) must be assigned to the team site, and be present at the remote site for the duration of the event in order to facilitate the execution of the Competition. The qualifications of Remote Site Judge are the same as Event Judge. The responsibilities of the Remote Site Judge are,

- 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 all Event Judges and provide status when requested
- Provide technical assistance to remote teams regarding use of the remote system
- Assure that the Team Captain has communicated to the Event Judges approval of initial system integrity and remote system functionality
- Assist Event Judges in the resolution of grievances and disciplinary action, including possible disqualification, where needed
- Report excessive misconduct to local security or police

- Assess completion of various injects based on timeliness and quality when requested by Event Judges
- Act as a liaison to site personnel responsible for core networking and internet connectivity
- Provide direct technical assistance to teams when requested by Event Judges
- Provide feedback to students subsequent to the completion of the Competition event

A recommendation for Remote Site Judge(s) is expected to be given from the administration or team advisor of the participating institution to the Competition Event Manager. Remote Site Judge(s) must not be employed or otherwise affiliated with the participating institution, other than membership on an advisory board. Competition Event Managers should also be apprised of a contact from the participating institution responsible for core networking and internet connectivity that will be present during the Competition event.

## Scoring Management - Goals & Guidelines

The task of scoring management is to manage scoring mechanisms and procedures for services with integrity and effectiveness throughout competition. Tasks include,

1. Identify chief scorer
2. Define how subcommittee score will be tabulated and propose to management team
3. Select and secure competition scoring staff / team
4. Recommend processes and procedures for overall service scoring and logging
5. Implement all scoring software and equipment for regional competition
6. Design architecture and process for redundant scoring systems
7. Provide training course for state competition scoring technicians
8. Create scoring toolkit with resources necessary to score competition (software, videos, instructions...)
9. Ensure guidelines and rules of competition are being followed as set by CIAB
10. Monitor all scoring processes (services, application, manual checks) during given competition
11. Establish scoring / judging communication mechanisms
12. Validate and confirm final scores within subcommittee

### Scoring Policies and Procedures

Scoring responsibility is to provide concrete data on the status of each team's network services, system services and any/all injects that impact services as they occur during the competition. To this end, service scoring must match requirements of the competition network, topology design, and documentation provided to teams. It is also the responsibility of the main scoring manager to present that material in a fashion that allows for comparison to the judging officials.

To this end the scoring management team must utilize an automated service check application that polls services and service integrity on an ongoing basis. A number of platforms are available which will accomplish this - Nagios, What's Up Gold, and the Scoring Engine used by the National Competition which is preferred. Team scores should be maintained in a scoring

database so that they are retained in the event of system failure. Preferred is to have redundant scoring engines and databases.

Scoring managers must configure and test the scoring engine platform prior to the competition to assure that all teams are scoring in an identical fashion. Generally the scoring engine is reset just prior to the start of the competition.

During the competition, scoring managers must maintain oversight of the scoring process on a continuing basis,

- Assure memory and processor utilization are within acceptable bounds
- Respond to judging and team requests as to why certain services are down
- Modify the scoring engine configuration per request of judges or teams within the allowable scope determined by judges, e.g., password changes
- Modify the scoring engine configuration to be consistent with the issuance of inject tasks
- Provide final service scores to competition judges in a timely manner at the conclusion of the event
- Backup all scoring data for post analysis and in the event of any grievances

## **Topology, Scenario and Team Packet**

The major goal of topology design is, working with the host site manager, design competition topology including hardware, software, and service selection including recovery processes. Write event scenario and publish team packet for management team approval and distribution. Tasks include,

1. Assist host site manager with topology implementation
2. Recommend processes and procedures for overall service scoring and logging
3. Design core architecture
4. Explore new technologies to be included in the competition network
5. Ensure guidelines and rules of competition are being followed as set by the management team
6. Methodology for white (judging and scoring), red (threats), blue (student teams), gold (chief judge and event operators), green (hospitality), other organizers interaction and connectivity
7. Design IP address scheme and naming conventions
8. Design central infrastructure and select central services
9. Create topology document
10. Develop event scenario
11. Publish team packet

### **Topology Design Policies and Procedures**

Competition Topology is intended to provide a simulated environment allowing Student/ Blue Teams the opportunity to manage and secure IT services as well as provisions to facilitate scoring, judging, and overall sight management. The topology should also provide flexibility for the Judging Team to facilitate injects during the event. All competition topologies should be approved by the management team. Cyber competition design, like the industry, is in a state of flux and development, so the specific areas delineated here under topology should be viewed

as representative rather than fixed. Nevertheless, cyber competition design will need to address the foregoing considerations.

## Topology Definition

Competition Topology should include the following:

A core network to allow interconnection to Student Teams, Scoring, Red Team, and Judging  
A competition team network comprising of servers, workstations, peripherals, and networking apparatus necessary to simulate remote access to the public internet; specific operating systems should be identified, as well as any virtual machines;

Provision for centralized, isolated access to the core network for White Team activity, including redundant scoring engines, and workstations for judges, accessible to all Student Team networks

Network access to Student Team networks for the Red Team to provide packet generation and allow substantive entry and opportunities to compromise Student Team services; multiple points of network access may be provided

Provision for network traffic monitoring throughout the competition

A separate workstation should be provided for internet access

In addition, the following guidelines should be followed for Competition Topology:

Each Student Team network will be logically and physically isolated from all other competing teams.

Each Student Team network will be physically and logically isolated from the hosting organization's network.

Each Student Team network will be physically and logically isolated from the Internet

Each Blue Team will be provided with a standalone PC with Internet access that may be used for research, software downloads, etc. At no time will Internet access be permitted to the competition networks.

The Competition Topology should be clearly defined via a logical diagram together with the documentation of all operating systems, IP addresses or ranges, DNS names, user names and password.

## Delineation of Student Services

The precise type and number of student services must be clearly identified by the Topology Team, as well as the initial underlying operating system providing the service. Though the set of services may vary from each event, the following services/protocols are expected to be provided by Student Teams: HTTP, HTTPS, FTP, SMTP, DNS, and Active Directory.

## Central Services

Managed central services need to be provided throughout the competition. In addition to the services needed for network monitoring, White and Red Teams, other centralized services may be provided. These would include centralized DNS, email, or call manager.

## Acceptable Software

All operating system software will be provided to Student Teams. The Competition Topology will document specific operating system software and revision level. Provision for older operating systems should be included in the topology in order to simulate real enterprises, and to provide opportunities for Red Team activity. Student Teams will be required to patch operating systems during the competition through use of the Internet access workstation.

Many of the services required at the competition are expected to be provided by the indigenous operating systems. Other services will be provided by using lower level devices such as routers and switches. All other software used during the event shall be open source only; no purchase software or trials may be used.

### Monitoring and Compliance

Workstation monitor(s) will be provided and operable throughout the event. As a critical element of topology, redundant monitors should be provisioned. Monitors should specifically log traffic to detect if one team attempts to connect to another team network, violating event rules. Preferred is the monitoring of each individual team, but a centralized monitor is acceptable.

### Movement of Services

The Topology Team should provide guidelines for specific placement of services during the event. The process of scoring may be able to footprint the platform providing a particular service, and thereby enforce a specific event policy. Conversely, Student Teams may be given the flexibility to move services to whatever platform they wish, including virtual machines.

### Communication to Student Teams

Student Teams need to be apprised of Topology requirement both prior and during the Competition. The Competition Topology diagram and delineation of services will be included in the Team Packet giving Student Teams advance notice. Detailed IP scheme and naming conventions should be withheld until the actual event.

During the event, a means for the Judging Team to communicate to Student Teams needs to be provided. Communication may be via hand written instructions, internal or external email, or internal or external telephone. The method of communication will be specified by the Judging Team, and the topology must include provisions accordingly.

## Penetration Activities (Red Team)

Provide competition with threats to CIA. The Red team will create threats and evaluate responses to create a more “real-world” competition environment. Task include,

1. Identify chief red team lead
2. Define how subcommittee score will be tabulated and propose to the management team
3. Select and secure competition red team staff and members
4. Recommend processes and procedures for all red team activity
5. Identify core red team toolset to include sponsor tools (not limited)
6. Acquire licenses to competition only use (ex Core Impact)

7. Work with site team to plant OS pre-competition vulnerabilities
8. Work with inject team prior to competition to create red team injects
9. Ensure guidelines and rules of competition are being followed as set by CIAB
10. Monitor all scoring processes (red team, injects, services, other) during given competition
11. Establish team / judging communication mechanisms
12. Validate and confirm final scores
13. Verify all activity meets agenda guidelines and propose a schedule of escalation

#### Penetration Team Guidelines

Commercial networks are typically subject to the relentless presence of traffic outside the bounds of normal communications. This may take the form of benign patterns intended to detect services, the presence of hosts, and above all vulnerabilities or interesting targets of opportunity. Unfortunately, traffic patterns may also include oddly crafted sequences and payloads designed to disrupt normal processing and ultimately gain access outside of normal channels.

A Red Team will emulate the hacker threat that exists on networks today. The type of network activity conducted by the Red Team may include:

- 1) Generation of random network traffic through each competition network.
- 2) Enumeration, discovery, and port scanning using RFC-compliant ICMP packets and TCP and UDP connections
- 3) Attempted logins using guessed and discovered account names and passwords
- 4) Network sniffing, traffic monitoring, and traffic analysis
- 5) Use of exploit code for leveraging discovered vulnerabilities
- 6) Password cracking via capture and scanning of authentication databases
- 7) Spoofing or deceiving servers regarding network traffic
- 8) Alteration of running system configuration except where denial of service would result
- 9) Scanning of user file content
- 10) Introduction of viruses, worms, Trojan horses, or other malicious code
- 11) Alteration of system configuration stored on disk
- 12) Changing passwords or adding user accounts
- 13) Spoofing or deceiving servers via dynamic routing updates or name service (DNS)
- 14) Attempt to penetrate the defensive capabilities of each Blue Team network and modify any acquired environment
- 15) Assess the security of each Blue Team network
- 16) Attempt to capture specific files on targeted devices of each Blue Team network
- 17) Attempt to leave specific files on targeted devices of each Blue Team network
- 18) Follow rules of engagement for the competition

Clearly, Red Team members should have extensive experience with penetration testing and vulnerability assessment.

The presence of a professional Red Team is an essential element for the series of Cyber Defense Competitions by adding an element of danger that seeks to imitate the real world. Red Team activity subjects students to the real-world dilemma of implementing security to best-practices, balanced with the need to offer services in a timely and efficient manner.

Ample time should be afforded teams to acclimate to the competition environment, and to mitigate obvious vulnerabilities that have been configured in the initial network, before any penetration and rogue access. Bringing down services en masse early in the competition frustrates the students getting into the game and the successful completion of early injects. Even while the Red Team merely generates traffic and scans team systems, students frequently believe they are being attacked.

Care should be taken in the process of penetration, rogue access, and compromise of systems. Red Team members should, in general, avoid extensive alterations to compromised student systems. Better that the Red Team initially perform subtle actions towards maintaining and increasing access.

Based on findings, the Red Team can escalate the attack to gain access to student team resources. The Holy Grail is acquisition of an administrative command line. Once again, the Red Team has a wide plethora of tools from which to choose in order to take advantage of discovered vulnerabilities. The Red Team host includes a number of penetration tools, especially Metasploit, for this purpose.

Note that in general DoS attacks are not included in Red Team activity. With the use of SAIC/CyberNEXS as the competition engine using remote connections, deploying DoS may also have unpredictable results.

Timing is also an issue. With automated scoring, ideal is to perform attacks on student teams synchronously. It should be noted that attacks that are conducted in the last half of the competition, will have lesser impact from a scoring standpoint, than those conducted earlier in the game. Red Team members may choose to elevate the severity of actions directed to compromised systems during the final hour of competition. This may include the installation of root kits, web page defacement, database deletion, etc.

It is important for the Red Team to document findings and actions during the competition in order to provide feedback to student teams, and to assist White Team Judges to adjudicate event winners. The Red Team should plan a method of regular communication to the White Team, giving Judges the opportunity to incorporate Red Team findings and activity into managing the competition.

## Administration

Coordinate all activities between all organizations including financial systems. Individual areas of attention will include final event agenda, financial issues, website, communications, event sponsorship and other administrative requirements and management team communications. Tasks include,

1. Final event agenda and schedule
2. Finance and budgets
3. Expense guidelines
4. Website management
  - a. Information sharing
  - b. News
  - c. Share point for resources

- d. WiKi
- e. Public and Private
- 5. Communications
- 6. Coordinate event sponsorships
  - a. Identify coordinators for each competition
  - b. Sponsorship canvas and coordination
  - c. Centralize sponsorship for big ticket sponsors together
  - d. Establish invoicing procedures
  - e. Create sponsorship marketing materials
- 7. Establish repository of documents and secure access
- 8. Ensure each competition site establishes a budget for approval
- 9. Ensure each site has a main contact and points of contact for billing
- 10. Other admin tasks as defined

## **Site Management / Hospitality**

An administrative team must support the function of any competition to assure facilities are managed and all hospitality is coordinated. Tasks include,

- 1. Create “greeter package” for each team and check-in processes for teams
- 2. Coordinate hotel needs for competition staff
- 3. Coordinate all food service activities to event agenda
- 4. Gifts and giveaways
- 5. Name tags
- 6. Trophies
- 7. Create and execute event surveys and feedback
- 8. Photos
- 9. Onsite help
- 10. Signage
- 11. Presentation equipment
- 12. Team invitation and travel information
- 13. Team packet distribution and management
- 14. Main team communication contact
- 15. Human resource issues and emergency contacts
- 16. Local site administrative liaison
- 17. Support local technology
- 18. Room assignments (teams, faculty, white room, red room, physical security, physical access, power distribution, troubleshooting and maintenance, breakout rooms, rest room
- 19. Core network access and wiring closet access
- 20. Local network administration
- 21. Provide detailed cable and implementation plan to topology team
- 22. Notify local security staff



# **2013 State Collegiate Cyber Defense Competition**

**[State specific graphic]**

**Team Packet**

**February [], 2013**

## Table of Contents

### Contents

State CCDC Mission and Objectives .....	3
Overview .....	3
Competition Goals.....	4
Competition Team Identification .....	4
Initial Connection & the Start Flag .....	6
Network & Team Site Description .....	9
Schedule .....	9
Systems.....	10
Competition Rules: Acknowledgement & Agreement.....	10
Competition Rules: Entry Fee Payment .....	11
Competition Rules: Student Teams.....	11
Competition Rules: Professional Conduct.....	11
Competition Rules: Competition Play.....	12
Competition Rules: Internet Usage .....	13
Competition Rules: Scoring .....	14
Functional Services .....	15
Business Tasks.....	16
Questions and Disputes .....	16
Aftermath.....	16
Competition Topology.....	17
Sponsors: .....	19
Appendix - Addressing Access Problems to NETLAB+™ Systems.....	20

## State CCDC Mission and Objectives

The Midwest State Collegiate Cyber Defense Competition (CCDC) provides an opportunity for qualified educational institutions in the Midwest to compete, and is part of a national organization (see [www.nationalccdc.org](http://www.nationalccdc.org)) to provide a unified approach across nine regions of the country. Qualified educational institutions include those with information assurance or computer security curricula. The Midwest State 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.

## Overview

Midwest Collegiate Cyber Defence Competitions are managed by CSSIA, the 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 scenario involves team members simulating a group of employees from an IT service company that will initiate administration of an IT infrastructure. The teams are expected to manage the computer network, keep it operational, and prevent unauthorized access. Each team will be expected to maintain and provide public services: a web site, a secure web site, an email server, a database server, an online curriculum server, and workstations used by simulated sales, marketing, and research staff as per company policy and mission. Each team will start the competition with a set of identically configured systems.

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

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

First place teams from each 2013 Midwest State CCDC will have the opportunity to participate in the 2013 Midwest Regional CCDC, March 22-23, 2013, at Moraine Valley Community College (MVCC), Palos

Hills, Illinois. Teams must travel to the 2013 Midwest Regional CCDC at MVCC at their own expense. A travel stipend may be forthcoming.

In the event that the first place team is unable to attend the Regional CCDC, invitation will be extended to the second, and then third place team. A wildcard team may also be selected for the regional, at the discretion of the CSSIA management team.

### Competition Goals

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

### Competition Team Identification

**Blue Team** - student team representing a specific academic institution or major campus competing in this competition; Each team must submit a roster of up to 12 competitors to the State CCDC Director. 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 State CCDC Director.

- Members and advisor sign a participation safety agreement if teams compete anywhere other than their academic institution
- Members and advisor sign a photo release document where applicable
- have completed a minimum of one semester in the participating institution's networking or security curriculum
- Students should maintain a full time status at the time the competition is conducted.

- 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, room monitors and security enforcement in the various competition rooms.

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

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

- **Chief Judge:**
  - Serves as the final authority on scoring decisions or issues relating to equity or fairness of events or activities
  - Cannot be from any institution that has a competing Blue team or have any interest in any team outcome
  - Ideally, should be a representative from industry or law enforcement
  - Final authority of all judging decisions, including assessment of final scores and winners of the competition
- **Gold Team** – Comprised of the State CCDC 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
  - Makes provision for awards and recognition
  - Manages debrief to teams subsequent to the conclusion of the competition
  - If teams travel to another site, the Gold Team manages activities such as:
    - Greet people
    - Organize food
    - Assist in setting up the competition
    - Assist with hotel / travel arrangements
- **Green Team** – Tech support and hospitality – assists with any technical needs necessary to maintain the integrity of the competition. Assists with ancillary functions – greeters, food service, local directions.

## Initial Connection & the Start Flag

Using a NETLAB<sup>+</sup>™ 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.

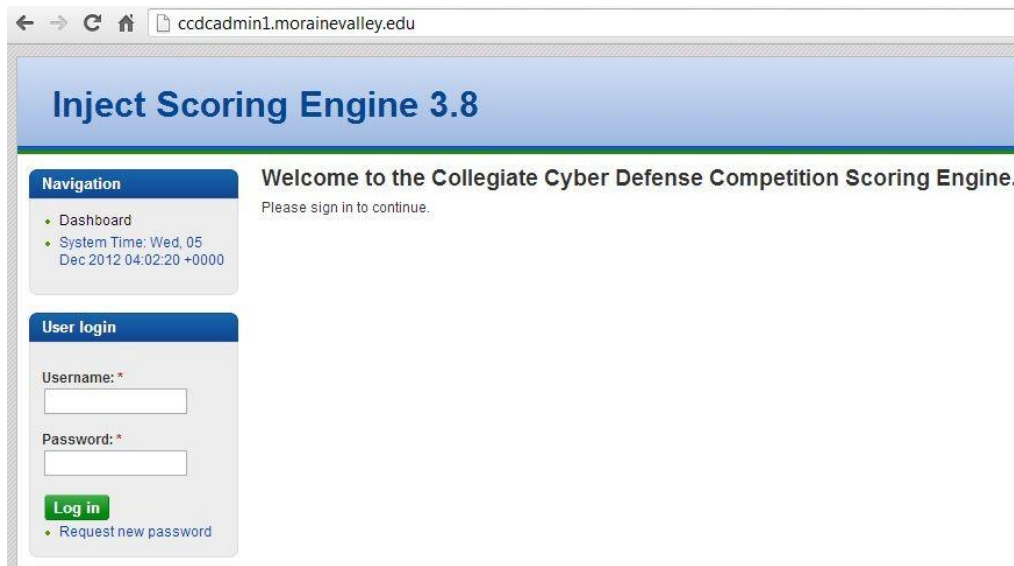
This system is accessed via a browser,

**`ccdcadmin1.morainevalley.edu`**

Note that the url for the ISE is also accessible on the [www.cssia.org](http://www.cssia.org) site.

[www.cssia.org/ccdc](http://www.cssia.org/ccdc)

click on Team Portal on the right = ISE



**Students should login to the ISE first to initiate communication with the competition judges.** There is one account per team that may be used to connect to the ISE where multiple logins using the same account is permissible. The accounts are,

team1, team2, team3, .....

The team password required to access the ISE is distributed, along with team assignment, by a competition manager prior to the scheduled start of the competition. When first connecting to the ISE, a member of the team should check for an initial inject task, usually identified as “Welcome” or something similar. The task simply requests a response back 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> / myVLAB Competition Stadium system used to access and manage the competition network. This too is accessed via a browser,


**myvlab1.morainevalley.edu**

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


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

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





Moraine Valley  
Community College



The National Information, Security & Geospatial Technologies Consortium

myVLAB


**Username**

**Password**

**Login**

[Forgot Password?](#)

POWERED BY



**NETLAB+**

**myVLAB1 @ Moraine Valley Community College**

**Virtual Labs supported by Department of Labor  
TAACCCT Grant #TC-22525-11-60-A-48**

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

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

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

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

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

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


There are eight accounts per team that may be used to connect to the 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, ....

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:


1488	<b>NOW</b> Sun Jan 27, 2013 8:00AM - Wed Jan 30, 2013 8:00PM <b>ENTER LAB</b>	 Team J: vTeam 10 User 1, vTeam 10 User 2, vTeam 10 User 3, vTeam 10 User 4, vTeam 10 User 5, vTeam 10 User 6, vTeam 10 User 7, vTeam 10 User 8 Class: .CCDC State 2013 CCDC State Info	<b>CCDC 2013 Team 10</b> <b>CCDC Team Pod</b>
------	--	--	--


Each team member can click on 'ENTER LAB' for their respective lab/pod reservation to gain access to their competition network. The competition network topology, shown later in this document, should be clearly visible. Access individual VMs simply by clicking on them.

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



**Lab Access**

MyNETLAB Logout  ddurkee

**ALERTS**  CCDC 2013 Team 1 9273 minutes remaining **WE'RE DONE**

Topology

Action

Status

Connections

Exercise

CCDC 2013

## Network & Team Site Description

- Each competition network will be located remotely from the competition site and will be logically isolated from all other competing Blue Teams. All Teams will access the competition network via a browser connection.
- Each competition network will therefore be physically and logically isolated from the hosting organization's network.
- Each competing Blue Team will be provided a set of workstations at a host site that are logically and physically isolated from other Blue Teams in order to access respective remote competition networks via the internet. Alternatively, Blue Teams may compete from their own institution, in which case their institution must provide workstations in conformance with aforementioned requirements. Blue Teams competing from their own institution must do so from a dedicated, secure location where all team members are collocated together with the local site judge. Classrooms or conference rooms are considered ideal locations. The secure location is to have restricted access to only Blue Team members, remote site judges, local administrators and technical support. The planning of remote vs. hosting sites will be managed and approved by the State Competition Director.
- 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 trouble ticket and response application, the ISE/Team Portal, residing at Moraine Valley Community College.
- 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 NETLAB+™ environment.
- Each Blue Team network will be monitored by a scoring system operating within the remote network. An indication of services, as viewed by the indigenous scoring engine, will be made available to each Blue Team via the ISE/Team Portal.
- A logical diagram of the team logical network is contained within this Team Packet. However, it is subject to change and /or modification as decided by the State Competition Director.

## Schedule - Times are CST

8:00am	Distribution of ISE/Team Portal passwords, and Room Assignment where applicable; Teams access remote system;
8:30am	Team access the ISE/Team Portal and respond to the Welcome inject
9:00am	Start of Competition; scoring begins
5:00pm	Competition ends/Scoring ends

Post competition announcement of final winners, and debriefing of the competition will be managed by the State Competition Director.

## Systems

1. Each team will start the competition with identically configured systems.
2. Teams may not add or remove any computer, printer, or networking device from the designated competition area.
3. This document provides the overall system architecture, network configuration, and initial set-up of the competition.
4. Teams should not assume any competition system is properly functioning or secure.
5. Throughout the competition, Green Team and White Team members will occasionally need access to a team's systems for scoring, troubleshooting, etc. Teams must allow Green Team and White Team member access when requested.
6. Network traffic generators may be used throughout the competition to generate traffic on each team's network. Traffic generators may generate typical user traffic as well as suspicious or potentially malicious traffic from random source IP addresses throughout the competition.
7. Teams must maintain specific services on the "public" IP addresses assigned to their team and stipulated by this document. Moving services from one public IP to another is not permitted unless directed to do so by an inject. Likewise, teams are not permitted to change the internal addressing or VLAN scheme of the competition network unless directed to do so by an inject.
8. Teams may re-task servers, moving a service from one server to another as long as the outside "public" IP address of the service remains the same. It is the responsibility of the team to understand all the particulars of scoring a service when doing so.
9. Teams are not permitted to alter the system names or IP address of their assigned systems unless directed by an inject; this may affect the results of the scoring mechanism.
10. In the event of system lock or failure, teams will be able to perform a 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.
11. Systems designated as user workstations within the competition network are to be treated as user workstations and may not be re-tasked for any other purpose by teams.
12. Teams may not modify the hardware configurations of workstations used to access the competition network.
13. Servers and networking equipment may be re-tasked or reconfigured as needed.

## Competition Rules: Acknowledgement & Agreement

Competition rules are applicable to all participants of the State 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 a host site, or are competing from their academic institution. Team advisors and all student participants are expected to know and follow all CCDC rules and guidelines. Access to the myVLAB competition environment implies their acknowledgement of competition rules and their commitment to abide by them.

Team advisors and team captains are responsible for deploying the competition rules to the remaining members of their team. Host sites reserve the right to stipulate additional rules conforming to local policies and guidelines.

### **Competition Rules: Entry Fee Payment**

A \$500 entry fee to the 2013 Midwest State CCDC is required for each participating institution that has been accepted through the application and acceptance process. Fees are collected within each state under the direction of the State CCDC Director.

It is required that all institutions satisfy the entry fee requirement by payment prior to the start of the competition. Failure to pay the entry fee prior to the competition will result in disqualification.

Teams wishing to drop out of the State CCDC must notify the State Director no later than one week prior to the competition. A Team that drops out within one week of the competition, or is 'no show' at the competition is expected to pay the \$500 entry fee. Failure to pay the entry fee in such a case will result in disqualification from State CCDC the following year.

### **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](http://www.nationalccdc.org)
2. Each team may have no more than two graduate students as team members.
3. Each team may have one advisor present during the entire competition – this may be a faculty/staff member or an administrator. Institutions may also send additional faculty representatives with the approval of the State Director. 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 may be issued badges identifying team affiliation. If issued, they 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.
6. If the member of a qualifying team is unable to attend the national competition, that team may substitute another student in their place from the submitted roster.

### **Competition Rules: Professional Conduct**

1. All participants are expected to behave professionally at all times they are visiting the host site, or competing from a remote 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 (do not identify your institution) , action or item requested, and date/time requested. Remote site judges may facilitate this function, or requests may be made via the ISE/Team Portal.
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. 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 contact 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 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.
12. 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.
13. Blue Team members may change passwords for administrator and user level accounts. Changes to passwords must be communicated according to the White Team guidelines. It is the responsibility of the Blue Team to understand how scoring may be impacted by changing passwords.
14. Blue Team members should maintain ICMP on all competition devices and systems, except the WAN port of the PFSense VM. 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.
15. Each Blue Team will be provided with the same objectives and tasks.
16. Each Blue Team will be given the same inject scenario at the same time during the course of the competition.
17. The White Team is responsible for implementing the scenario events, refereeing, team scoring and tabulation.

18. Scoring will be based on keeping required services up, controlling/preventing un-authorized access, and completing business tasks in timely manner that will be provided throughout the competition
19. Scores for inject completion and incident reports will be maintained by the White Team, and will not be shared with Blue Team members. Faculty advisors may receive debriefing at the end of the competition. Running totals and comparisons to others teams will not be provided during the competition.
20. 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 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. 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.
3. 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.
4. 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 un-authorized 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 tracking reports and internal testing to assess the integrity of their network. Blue Team members should refrain from making direct requests to the White Team for routine service verification.
3. Any team action that interrupts the scoring system is exclusively the fault of that team and will result in a lower score. Should any question arise about specific scripts or how they are functioning, the Team Captain should immediately contact the competition officials to address the issue.
4. Any team that tampers with or interferes with the scoring or operations of another team's systems will be disqualified.
5. Teams are required to provide incident reports for each Red Team incident they detect. Incident reports can be completed as needed throughout the competition and submitted to the White Team. Incident reports must contain a description of what occurred (including source and destination IP addresses, timelines of activity, passwords cracked, etc), a discussion of what was affected, and a remediation plan. The White Team will assess scores for incident report submission based on clarity, thoroughness, and accuracy. The White Team may also, at their discretion, assess negative scores for frivolous, unnecessary, or excessive communication.
6. The winner will be based on the highest score obtained during the competition. Point values are broken down as follows:

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

*Precise percentage breakdown will be determined by the White Team.*

## Functional Services

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

## **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 will be tested via the FTP protocol. Some indication of database integrity will also be examined.

## **DNS**

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

## **Business Tasks**

Throughout the competition, each team will be presented with identical business tasks. Points will be awarded based upon successful completion of each business task. Tasks will vary in nature and points will be weighted based upon the difficulty and time sensitivity of the assignment. Tasks may contain multiple parts with point values assigned to each specific part of the tasking. Each business task may have an indication of relative importance or value assigned and a specific time period in which the assignment must be completed. Business tasks may involve modification or addition of services.

## Questions and Disputes

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

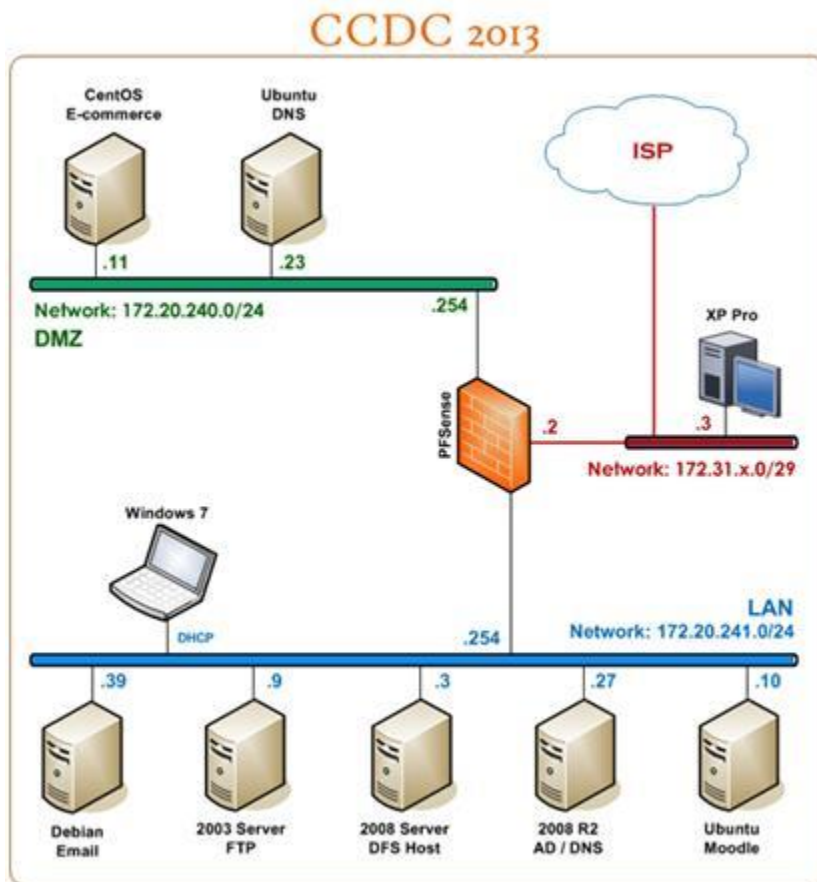
## Aftermath

Members of CSSIA, Gold, White, Red, and Green Teams strive to make State 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](http://www.cssia.org). They are also forbidden from publishing, posting on the internet, or publicly communicating assessments of the State CCDC, nor assessments of the performance of any team, nor speculations concerning different possible outcomes. Institutions that fail to adhere to this rule may be refused participation in future competitions.

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

## Competition Topology



- The numbers in the topology diagram associated with connections correspond to switch interface numbers.
- All servers, workstations, and PFSense are virtual machines under the management of NETLAB<sup>+</sup>.
- The firewall shown in the topology is a PFSense VM, version 2.0.1-RELEASE, which is a free, open source customized distribution of FreeBSD. See, [www.pfsense.org](http://www.pfsense.org).

Accessing the PFSense VM via NETLAB<sup>+</sup> brings you directly to a menu prompt without need for authentication. Access to the webConfigurator is made via a browser from another VM in the CCDC environment. It is recommended that you use the Windows 7 workstation for this purpose. The webConfigurator username/password is,

admin/password

Note that this is different from the default username/password that you may have used in an MSEC+ pod. For an introduction to PFSense, see the CCDC Boot Camp Series on the Illinois CCDC site: [ilccdc.wordpress.com](http://ilccdc.wordpress.com)

- Each team has the following PFSense internal addresses:

LAN, le0            172.20.241.254/24

DMZ, le1            172.20.240.254/24

- Core IP addresses are the following:

Team	PFSense WAN Outbound to Core	Core connection to PFSense WAN	"Public" IP pool
1	172.31.21.2/29	172.31.21.1	172.25.21.0/24
2	172.31.22.2/29	172.31.22.1	172.25.22.0/24
3	172.31.23.2/29	172.31.23.1	172.25.23.0/24
4	172.31.24.2/29	172.31.24.1	172.25.24.0/24
5	172.31.25.2/29	172.31.25.1	172.25.25.0/24
6	172.31.26.2/29	172.31.26.1	172.25.26.0/24
7	172.31.27.2/29	172.31.27.1	172.25.27.0/24
8	172.31.28.2/29	172.31.28.1	172.25.28.0/24
9	172.31.29.2/29	172.31.29.1	172.25.29.0/24
10	172.31.30.2/29	172.31.30.1	172.25.30.0/24
11	172.31.31.2/29	172.31.31.1	172.25.31.0/24
12	172.31.32.2/29	172.31.32.1	172.25.32.0/24
13	172.31.33.2/29	172.31.33.1	172.25.33.0/24
14	172.31.34.2/29	172.31.34.1	172.25.34.0/24
15	172.31.35.2/29	172.31.35.1	172.25.35.0/24
16	172.31.36.2/29	172.31.36.1	172.25.36.0/24

- 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 pwd
CentOS E-Commerce	HTTP/S; FTP	172.20.240.11	172.25.20+team#.11	administrator	changeme
Ubuntu DNS	DNS	172.20.240.23	172.25.20+team#.23	root	changeme
2003 Server FTP	SQL	172.20.241.9	172.25.20+team#.9	administrator	changeme
Debian Email	Email	172.20.241.39	172.25.20+team#.39	administrator	changeme
2008 Server DFS Host	DFS	172.20.241.3	172.25.20+team#.3	administrator	changeme
2008 R2 AD/ DNS	AD/DNS	172.20.241.27	172.25.20+team#.27	administrator	changeme
Ubuntu Moodle	Course Mgt	172.20.241.10	172.25.20+team#.10	root admin	changeme password
Windows 7 Workstation		DHCP 172.20.241.0/24	172.25.20+team#.2 overload	administrator	changeme
XP Pro Workstation		172.31.20+team#.3/29	N/A	administrator	

### Sponsors:

	National Science Foundation, <a href="http://www.nsf.gov/">http://www.nsf.gov/</a>
	SecureWorks, <a href="http://www.secureworks.com">http://www.secureworks.com</a>
	CSSIA, <a href="http://www.cssia.org/">http://www.cssia.org/</a>

## Appendix - Addressing Access Problems to NETLAB+™ Systems

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

Generally the client requirements are easily met with simple browser and java plug-in. The bandwidth requirement likewise seems very reasonable at 256 kb/s up and down. Ports 80, 2201 must be allowed outbound.

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

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

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

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

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

```
>pathping {cyber stadium url such as cyberlab.morainevalley.edu}
```

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

```
#mtr --report {cyber stadium url such as cyberlab.morainevalley.edu}
```

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

MVCC continues to monitor data center performance which has been provisioned to easily support hundreds of remote connections. The problem of network connectivity is usually at the local institution from which the connection is made. Though there may seem to be adequate bandwidth, local institutions must assure synchronous service without undue filtering.

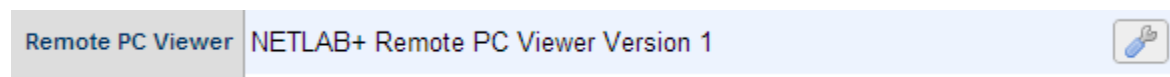
There may be a need for special provisioning at local institutions, even bypassing filters and firewalls for dedicated traffic to the stadium(s). Towards this end it is helpful to note the level of trust and the benign nature of traffic coming from the stadium(s). Though malicious traffic may be present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

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

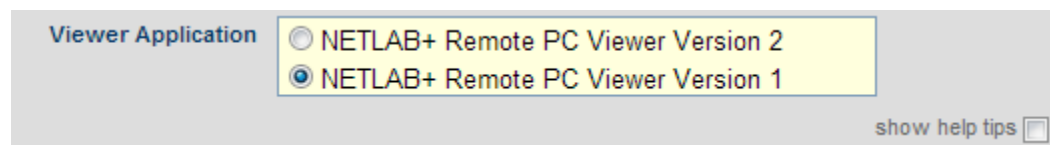
Even with excellent connectivity, there may still be problems with using the NETLAB+™ platform. The NETLAB+™ viewer has been programmed using java, and is sensitive to the specific combination of OS/browser/java version being used. With each update of java, the NETLAB+™ viewer may be affected.

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

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



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



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