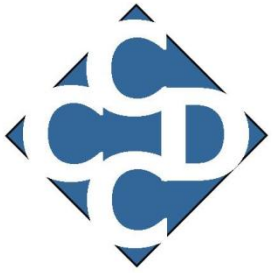
2024 Midwest Invitational CCDC Team Pack



Collegiate Cyber Defense Competition

November 9, 2024
November 16, 2024
December 7, 2024

Table of Contents

Contents

CCDC Mission and Objectives

The Collegiate Cyber Defense Competition (CCDC) 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

CCDC is managed on a national level by The Center for Infrastructure Assurance and Security (CIAS) which is part of the The University of Texas at San Antonio (UTSA). The CCDC is managed across nine regions of the country, where each region hosts a Regional CCDC and winners are eligible to compete in the National CCDC (see www.nationalccdc.org).

The competition is designed to test each student team's ability to secure a networked computer system while maintaining standard business functionality. The teams are expected to manage the computer network, keep it operational, and prevent unauthorized access. Each team will be expected to maintain and provide public services per company policy and mission. Each team will start the competition with a set of identically configured systems.

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

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

Invitational CCDC

The CCDC is a very challenging event, and can be daunting even for experienced teams. New teams can especially be disconcerted with the need to quickly assimilate to a completely new and different environment. It seems that teams need to participate in a CCDC to discover its nature, and be able to integrate their skills successfully.

An invitational CCDC is intended to give student teams a somewhat small-scale version of a real CCDC in order to provide the initial experience needed for first participants, and to enable experienced teams to hone their skills.

The Invitational CCDC is hosted via a Moraine Valley Community College (MVCC) Cyber Stadium powered by NETLAB+™ VE. Thus the Invitational also allows teams to acclimate to the MVCC Cyber Stadium environment.

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

Rules for participation in the Invitational CCDC are less stringent than those of a real CCDC event where national rules are followed. Participants are expected to be students registered at the same institution of higher learning. Schools with multiple campuses are expected to field a team from a single campus.

Many requests have been made to the Consortium to allow assistance to teams from their coach/adviser. During the invitational, coaches and team alumni are allowed to work with teams as a means of team preparation and guidance. Coaches and team alumni should refrain from performing tasks required of student participants. The invitational CCDC is not intended to be a contest between respective coaches.

There may or may not be room judges, and in their absence, the invitational works on an honor system. Students should be aware that the best Invitational experience is where students adhere to the rules like a real event.

Student teams should expect an invite to a Web Conference session that will engage all invitational CCDC participants, and can be used to facilitate all aspects of the event. Teams are advised to have a workstation equipped with mic, speakers, and overhead

video projector. While using the Web Conference audio keep in mind all teams can hear the audio.

Competition Team Identification

- Blue Team - student team representing a specific academic institution competing in this competition; each team is up to eight (8) members.

Teams may wish to anticipate future CCDC events by consulting national rules - www.nationalccdc.org

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 team before and during the competition. Team Captains should identify themselves to the White Team by team number, and not by institution.

- 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

- Black & White Teams – Representatives from industry who serve as competition judges (Black), remote site judges (White), and scoring management. Judges will assess the competition team's ability to maintain their network and service availability based upon a business inject and a scoring instrument, delivering inject scenarios, scoring of injects, creating log entries, securing log files, issuing or controlling the timing of injects, etc. Each competing Blue Team may have a White Team member present in their room that will assist judges by observing teams, confirming proper inject completion as well as reported issues.

- Chief Judge:
  - Serves as the final authority on scoring decisions or issues relating to equity or fairness of events or activities
  - Cannot be from any institution that has a competing Blue team or have any interest in any team outcome
  - Ideally, should be a representative from industry or law enforcement
  - Final authority of all judging decisions, including assessment of final scores and winners of the competition

- Gold Team – Comprised of the MWCCDC Consortium Competition Director, 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 invitational 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

- Green Team – Tech support– assists with any technical needs necessary to maintain the integrity of the competition.

Initial Connection & the Start Flag

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 - NISE (National Inject Scoring Engine)/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, receive inject tasks and notifications, and make submissions of completion for inject tasks.

This system is accessed via a browser,

ccdcadmin1.morainevalley.edu

Note that the MWCCDC Consortium supports an additional NISE/Team Portal,

ccdcadmin3.morainevalley.edu

Follow the instructions from your competition manager for the specific NISE/Team Portal that will be used for your CCDC Invitational.

Students should login to the NISE first. There is one account per each team member that may be used to connect to the NISE where multiple logins using the same account is permissible. The accounts are,

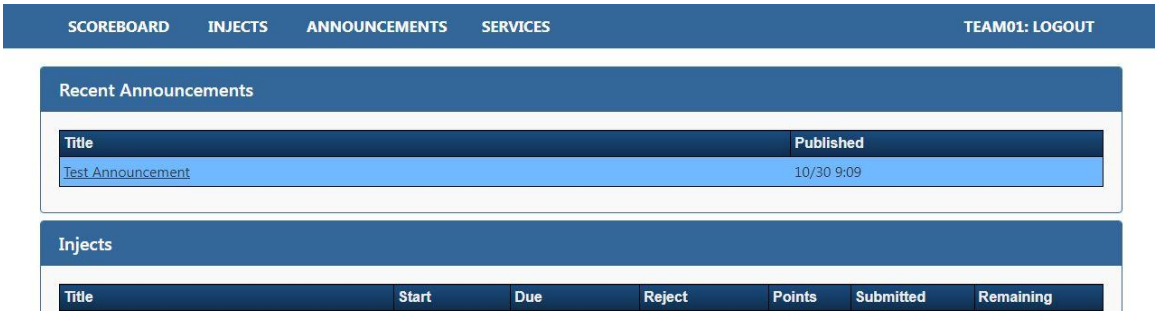
team01a,team01b, …,team01h
team02a,…., team2h
….
team10a,team10b,…,team10h
…..
team20a,…, team20h

There is also a ninth account per team that may be used for a room judge or for the invitational, a coach. These accounts are,

team01i
team02i
…
team20i

The passwords for each team account, required to access the NISE, are distributed, along with team assignment, by a competition manager prior to the scheduled start of the competition.

After logging in the main (Inject) page is displayed.



Using the NISE platform is straightforward and intuitive. Teams should explore the various features of the NISE during the event and be especially attentive to announcements and new inject tasks. Responses to inject tasks must be in the form of an attached PDF file. Any exceptions to this rule will be noted within inject instructions. Student teams should be attentive to submission requirements, as the judging team will likely reject responses that do not conform to requirements.

Students should note that NISE time is based on the Central Time Zone. Teams in other time zones must take this into account. Teams should avoid submitting inject responses in the last minute of validity. The NISE platform is intended to keep accurae time, but it's very common to have an inject submission rejected in the last minute.

After an inject submission has been submitted, and while the inject task is still open, both teams and judges may mark a submission invalid allowing the team to resubmit. There is a limit to how many times a team may resubmit, depending on White team policy.

When first connecting to the NISE, 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 NISE 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 notification indicating the drop flag has been issued and the competition has started.

System 2 - The NETLAB+™ VE Competition Stadium system used to access and manage the competition network. Using a NETLAB+™ VE powered Cyber Stadium to compete is simple and straightforward.

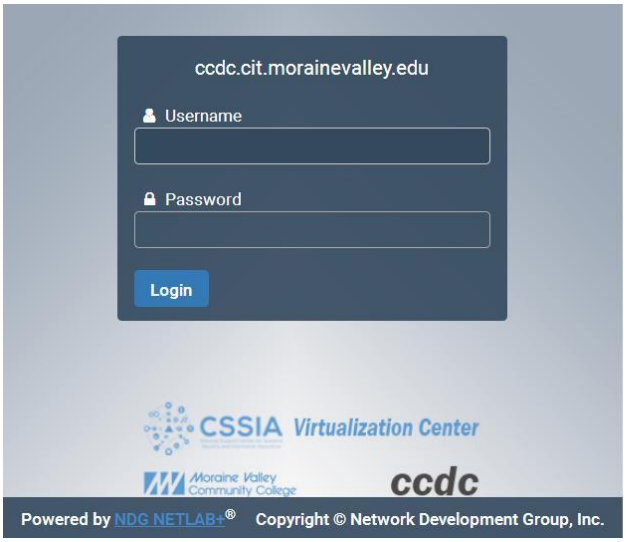
This too is accessed via a browser,

ccdc.cit.morainevalley.edu

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

Generally the client requirements are easily met with a simple browser. The bandwidth requirement is 256 kb/s up and down per client minimum. Ports 80, 443 must be allowed outbound. A 10 Mb/s minimum synchronous service is recommended. It is the responsibility of each participating school to assure that client requirements are met, and that proper internet service is provided.

The Competition Stadium login screen is shown below.



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

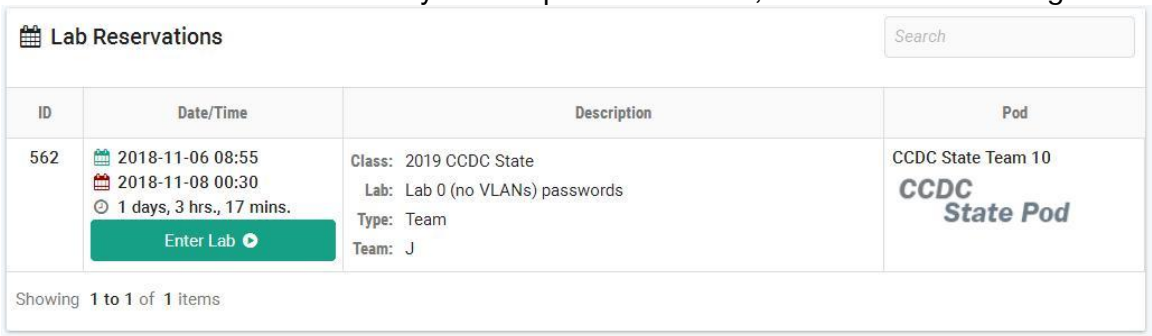
v1u1, v1u2, v1u3, …., v1u8

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

v2u1, ….

Note that teams initially only have access to the NISE/Team Portal. Team assignments are issued prior to the event so the proper accounts are known. The initial stadium password needed for all team accounts in order to access the Competition Stadium is also communicated to teams at the same time team assignments and NISE passwords are conveyed. Access to the stadium/ competition environment with the initial stadium password becomes valid at the time of the drop flag, which is indicated via a notification on the NISE.

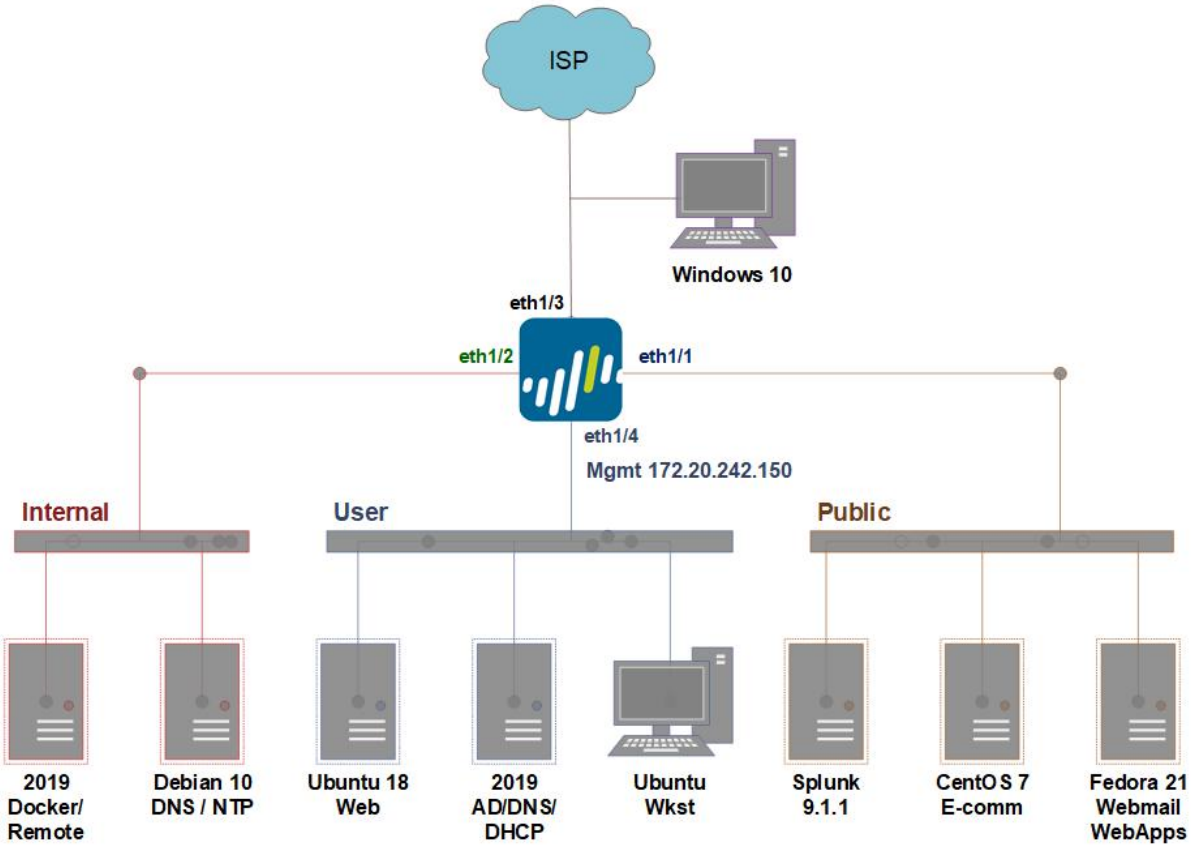
Once authenticated you will be asked to change your password and confirm a few details regarding your profile. Remember your new password! Subsequently you should see a lab reservation for your competition network, similar to the following:



Each team member can click on 'ENTER LAB' for their respective lab/pod reservation to gain access to their competition network. The competition network topology, shown later in this document, should be clearly visible. To access individual VMs simply click on the respective VM name at the top of the screen.

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

Competition Topology



- Teams have access to 10 VMs – 7 servers, 2 workstations, and the Palo Alto firewall.
- All servers, workstations, and Palo Alto firewall are virtual machines under the management of NETLAB+™ VE.
- Teams do not have access to the underlying layer 2 switch for the Virtual Network.
- The firewall shown in the topology is a Palo Alto VM, version 11.0.0, which is licensed by Palo Alto, and includes Threat Defense.
- There is connectivity between your Hardware and Virtual networks.
- You can access the Palo Alto VM either directly, which yields a command window, or via a browser 172.20.242.150 from any of the User LAN VMs. The PA user/password are,

  admin/Changeme123

- Each team has the following Palo Alto internal addresses:

  Internal, e1/2 172.20.240.254/24
  User, e1/4 172.20.242.254/24
  Public, e1/1 172.20.241.254/24

- Core IP addresses are the following:

Team	Palo Alto e1/3 Outbound to Core	Core connection to Palo Alto	"Public" IP pool
1	172.31.21.2/29	172.31.21.1	172.25.21.0/24
2	172.31.22.2/29	172.31.22.1	172.25.22.0/24
3	172.31.23.2/29	172.31.23.1	172.25.23.0/24
4	172.31.24.2/29	172.31.24.1	172.25.24.0/24
5	172.31.25.2/29	172.31.25.1	172.25.25.0/24
6	172.31.26.2/29	172.31.26.1	172.25.26.0/24
7	172.31.27.2/29	172.31.27.1	172.25.27.0/24
8	172.31.28.2/29	172.31.28.1	172.25.28.0/24
9	172.31.29.2/29	172.31.29.1	172.25.29.0/24
10	172.31.30.2/29	172.31.30.1	172.25.30.0/24
11	172.31.31.2/29	172.31.31.1	172.25.31.0/24

- VM data are as follows:

This table is accessible on the topology tab of NETLAB+™ VE, via the “Content” upper left.

	Version	*IP*	*Username*	*Password*
INTERNAL				
2019 Docker/Remote	Server 2019 Std	172.20.240.10	administrator	!Changeme123
Debian 10 DNS/NTP	Debian 10	172.20.240.20	root sysadmin	changeme changeme
USER				
Ubuntu 18 Web	Ubuntu Server 18.04	172.20.242.10	sysadmin	changeme
2019 AD/DNS/DHCP	Server 2019 Std	172.20.242.200	administrator	!Password123
Ubuntu Wkst	Ubuntu Desktop 20.04	DHCP	sysadmin	changeme
PUBLIC				
Splunk	9.1.1	172.20.241.20	root sysadmin admin (Web UI)	changemenow changemenow changeme
CentOS 7 E-comm	CentOS 7	172.20.241.30	root sysadmin	changeme changeme
Fedora 21 Webmail/WebApps	Fedora 21	172.20.241.40	root	!Password123
Palo Alto	PAN OS 11.0.0	172.20.242.150	admin	Changeme123
Windows 10	Windows 10	172.31.xx.5	minion	kingbob

Specific NAT translations are as follows:

INTERNAL	Local IP	'Public' IP
2019 Docker/Remote	172.20.240.10	172.25.20+team#.97
Debian 8.5 DNS/NTP	172.20.240.20	172.25.20+team#.20
USER		
Ubuntu 14 Web	172.20.242.10	172.25.20+team#.23
2019 AD/DNS/DHCP	172.20.242.200	172.25.20+team#.27
Ubuntu Wkst	dynamic	dynamic
PUBLIC		
Splunk	172.20.241.20	172.25.20+team#.9
CentOS 7 E-Comm	172.20.241.30	172.25.20+team#.11
Fedora 21 Webmail/WebApps	172.20.241.40	172.25.20+team#.39

- Teams should be attentive to monitor inject requests and notifications via the Team Portal/NISE.
- Red Team activity will be active throughout the event. At no time will the Red Team have access outside the Cyber Stadium perimeter. Neither will the Red Team be given direct access to any Team network directly via the NDG NETLAB+™ VE system.
- Each Blue Team network will be monitored by a scoring system operating within the remote network. An indication of services, as viewed by the indigenous scoring engine, will be made available to each Blue Team via the Team Portal/ISE.
- While every effort is made to provide a stable and well defined competition topology, it is subject to change and /or modification as decided by the 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. Precise services to be scored are configured by the scoring management team, but will be delineated via the ISE/Team Portal.

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

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

SMTP
Email will be sent and received through a valid email account via SMTP. This will simulate an employee in the field using their email. Each successful test of email functionality will be awarded points.

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

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

Schedule – All Times are CST!

Saturday, November 9, 2024

Morning Section

7am	Morning Section Participants join Zoom Web Conference
	Welcome Inject Released; teams login to ccdcadmin1.morainevalley.edu
7:30am-8am	Welcome & Opening Presentation
	Question & Answer from Teams
8am	Drop Flag – Cyber Stadium access inject released
8am-noon	Active Scoring
Noon-12:30pm	Closing Dialogue & Wrap-up

Saturday, November 16, 2024

Morning Section

7am	Morning Section Participants join Zoom Web Conference
	Welcome Inject Released; teams login to ccdcadmin1.morainevalley.edu
7:30am-8am	Welcome & Opening Presentation
	Question & Answer from Teams
8am	Drop Flag – Cyber Stadium access inject released
8am-noon	Active Scoring
Noon-12:30pm	Closing Dialogue & Wrap-up

Afternoon Section

12:30pm	Afternoon Section Participants join Zoom Web Conference Welcome Inject Released; teams login to ccdcadmin3.morainevalley.edu
12:30pm-1pm	Welcome & Opening Presentation Question & Answer from Teams
1pm	Drop Flag – Cyber Stadium access inject released
1pm-5pm	Active Scoring
5pm-5:30pm	Closing Dialogue & Wrap-up

Saturday, December 7, 2024

Morning Section

7am	Morning Section Participants join Zoom Web Conference Welcome Inject Released; teams login to ccdcadmin1.morainevalley.edu
7:30am-8am	Welcome & Opening Presentation Question & Answer from Teams
8am	Drop Flag – Cyber Stadium access inject released
8am-noon	Active Scoring
Noon-12:30pm	Closing Dialogue & Wrap-up

Afternoon Section

12:30pm	Afternoon Section Participants join Zoom Web Conference Welcome Inject Released; teams login to ccdcadmin3.morainevalley.edu
12:30pm-1pm	Welcome & Opening Presentation Question & Answer from Teams
1pm	Drop Flag – Cyber Stadium access inject released
1pm-5pm	Active Scoring
5pm-5:30pm	Closing Dialogue & Wrap-up

Note that each day has a single Zoom Web Conference meeting.

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 should not assume any competition system is properly functioning or secure.
4. Throughout the competition, Green Team and Black/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.
5. 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.

6. 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.
7. 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.
8. 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 Black/White Team if services are moved to another platform, with a rationale for the change.
9. Teams must maintain "public" services as available from all source IP addresses. Attempts to restrict or filter by IP source address may adversely affect scoring directly, and may also incur a penalty when detected.
10. In the event a VM locks or fails, teams will be able to power cycle the VM from their NETLAB+™ VE console. Note that the NETLAB+™ VE system does not support scrubbing a device as with the NETLAB+™ PE system. As such, teams will not have the ability to scrub or revert to snapshot a VM during the invitational. Tech Support will not support any snapshot/scrub of a particular VM. Teams may request starting over with a new lab reservation. Service scores up to that time will be retained.
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 Invitational 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. Participation in the Invitational CCDC is tacit agreement with the rules contained in this document.

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

Competition Rules: Professional Conduct

1. All participants are expected to behave professionally at all times including all preparation meetings.
2. Local site policies and rules apply throughout the competition.
3. All MWCCDC Consortium hosted 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 the MWCCDC Consortium reserves the right to disqualify an offender or team from participation in future competitions.
7.

Competition Rules: Competition Play

1. During the competition team members are 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 other than team coaches and alumni present with the team. 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. 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.
10. 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.
11. Teams may install software within the competition network as long as such software is either free or open source. No 'free trial' software is permitted.
12. 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.
13. 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.
14. Each Blue Team will be provided with the same objectives and tasks.
15. Each Blue Team will be given the same inject scenario at the same time during the course of the competition.
16. 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.
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 a timely manner that will be provided throughout the competition.
19. Scores for inject completion and incident reports will be maintained by the Black/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.
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. Team internet activity will be monitored.
2. Internet activity from team workstations is subject to local access policies. While for the invitational, proper controls are not put in place, teams are asked to adhere to local access rules. Teams should refrain from viewing inappropriate or unauthorized content. This includes direct contact with outside sources through AIM/chat/email or any other non-public services. 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.
3. 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.
4. 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.
5. 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, distributed file sharing clients or servers are permitted on competition networks.
6. 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.
7.

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 after services have been unavailable, usage of recovery services, and successful penetrations by the Red Team.
2. Scores will be maintained by the Black/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 Black/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 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 the MWCCDC Consortium, Gold, Black/White, and Green Teams strive to make the Invitational 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 Invitational 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 Invitational CCDC, and may also enumerate participating teams and winners.

Sponsors:

	Department of Homeland Security, http://www.dhs.gov/
	Palo Alto Networks, https://www.paloaltonetworks.com/
	Cisco Networkin Academy www.netacad.com
	Fortra, LLC www.fortra.com
	Battelle www.battelle.org
	SecureWorks, www.secureworks.com
	Center for Infrastructure Assurance and Security https://cias.utsa.edu
	National CCDC http://www.nationalccdc.org
	CSSIA, http://www.cssia.org/mwccdc