2023 Midwest Collegiate Cyber Defense Competition Qualifier

Team Packet

Table of Contents

Contents

Midwest CCDC Mission and Objectives

The Midwest 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) 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 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.

Qualification Overview

The Midwest Collegiate Cyber Defence Competition Qualifier (MWCCDCQ) is managed by the MWCCDC Consortium, LLC. 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 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.

Qualifying teams from the 2023 MWCCDQC will have the opportunity to participate in the 2023 Erich J. Spengler Midwest Regional CCDC, March 17-18, 2023. This year the Regional CCDC will be hosted at Moraine Valley Community College. Teams travel to the Midwest Regional at their own expense.

A team qualifies to compete in the Erich J. Spengler Midwest Regional CCDC if they win their respective MW State CCDC Qualification competition, as long as there are at least two teams competing from their state. Multistate qualification CCDC competitions pick first place teams per state for regional eligibility regardless of actual placement. The Erich J. Spengler Midwest Regional CCDC can support up to ten teams, so there is room for the addition of two wildcard teams. A MW Wildcard CCDC event on March 4, 2023 will occur comprised of all second and third place teams, together with any single state participants. Winners of the MW Wildcard CCDC will be selected in order to obtain ten teams for the Erich J. Spengler MW regional CCDC.

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 Competition Manager. 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 Competition Manager.

- Members and adviser sign a participation safety agreement if teams compete anywhere other than their academic institution
- Members and adviser 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

- **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 Team** – Representatives from industry who serve as competition judges. 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. Black/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:**
  - Member of the Black Team that 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

- **Black/White Team:**

  The Black/White Team is comprised of Remote Site Judges. Each team competing remotely from their academic institution must have a remote site judge on site, present during most active times of the competition. Teams competing remotely from each other must also have a Remote Site Judge that may also be remote from other team members.

  Eligibility, Remote Site Judge qualifications, as well as the management of remote sites is documented in the separate policy document MWCCDC Remote Terms and Conditions.

- **Gold Team** – Comprised of the Competition Manager, 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 Black/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.

Communications & Remote Site Requirements

The nature of CCDC competitions has changed over time from its inception where teams met at a hosting site and student teams participated exclusively from competition rooms. Some state CCDC qualification events still retain this model, but with the added burden of Covid restrictions as well as budgetary restraints, provision has been made for teams to compete from remote sites, usually at their respective educational institutions. Further provision allows for teams to compete at locations remote from each other. This is especially for schools that have a significant online presence with students enrolled from locations at a great distance.

Teams competing remotely at their institutions of higher learning, or competing remotely from each other must have a remote site judge or judges to assure compliance with CCDC rules.

A web conference meeting (Zoom, WebEx, Microsoft Teams, &c.) will be used during the competition to facilitate communications and assure compliance. Details for Remote Site Judge and remote management of teams are documented in the policy document, MWCCDC Remote Terms and Conditions.

Initial Connection & the Start Flag

Using a NETLAB$^{+™}$ VE powered Cyber Stadium to compete is simple and straightforward. There are two separate systems that are used which interact to provide the services and communication necessary to meet the goals of the CCDC.

System 1 - 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 general notifications to all teams, 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 competition.

Students should login to the NISE first. There are nine accounts per team that may be used to connect to the NISE where multiple logins using the same account is permissible. The accounts for team1 are,

team01a, team01b, team01c, …, team01h, team01i

For team2 the accounts are

team02a, team02b, …, team02i

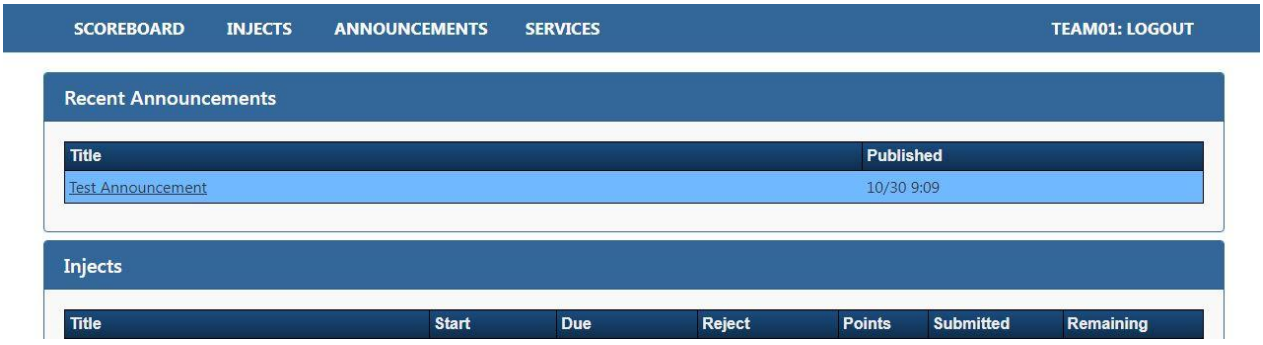
It's always two digits for the team number so team10 accounts are,

team10a, ….

Each team account has its own unique password. Nine accounts are provided to accommodate eight team members plus a room or remote judge.

The passwords for the NISE team accounts required to access the NISE are distributed, along with team assignment, by a competition manager prior to the scheduled start of the competition. Passwords for accounts ending in "i" may be distributed separately to the respective judges. Multiple logins using the same account are allowed.

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. **Times displayed on the NISE platform are set to CST.** Teams competing in the EST time zone should make note of this.

Responses to inject tasks must be in the form of an attached PDF file unless directed to do otherwise. It is possible to attach files with other formats, such as text files, but these cannot be read within the NISE platform. Such files must be downloaded and handled separately.

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 Black/Black/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. 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. For teams competing from remote locations, it is the responsibility of each student team member to assure 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. Teams cannot access the competition environment until the drop flag has been issued.

Team assignments are issued prior to the event so the proper accounts are known. In addition to team assignment, teams will receive the following information:

- Notice of which NISE platform they will be using, either,
  - ccdcadmin1.morainevalley.edu, or
  - ccdcadmin3.morainevalley.edu
- The NISE team account names and passwords
- The single initial password needed to access the competition stadium

At the drop flag the initial password needed to access the competition stadium will become valid.

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.

Schedule - Times are CST!

February 4, 2023	Minnesota, Indiana CCDC Qualifier
9am	Teams arrive at their competition rooms, or Teams competing remotely from each other assigned to a virtual meeting breakout room Welcome Inject Released; teams login to the NISE & respond to Welcome inject
10am	Drop Flag – competition stadium access notification released
10am-5pm	Active Scoring
5pm-6pm	Closing Dialogue & Wrap-up

February 18, 2023	Illinois, Missouri, Wisconsin CCDC Qualifier
9am	Teams arrive at their competition rooms, or Teams competing remotely from each other assigned to a virtual meeting breakout room Welcome Inject Released; teams login to the NISE & respond to Welcome inject
10am	Drop Flag – competition stadium access notification released
10am-5pm	Active Scoring
5pm-6pm	Closing Dialogue & Wrap-up

February 25, 2023	Ohio, Michigan, Kentucky, Iowa CCDC Qualifier
8am	Teams arrive at their competition rooms, or Teams competing remotely from each other assigned to a virtual meeting breakout room Welcome Inject Released; teams login to the NISE & respond to Welcome inject
9am	Drop Flag – competition stadium access notification released
9am-5pm	Active Scoring
5pm-6pm	Closing Dialogue & Wrap-up

For combined state events, teams should be careful to take note of time zone differences.

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 Black/Black/White Team members will occasionally need access to a team's systems for scoring, troubleshooting, etc. Teams must allow Green Team and Black/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 cold boot from within the administration console of the remote system. This will not reset any system to its initial starting configuration. Teams do not have the ability to revert/snapshot/scrub a VM, nor will Tech Support scrub a device. **There are no scrubs for the Qualification CCDC.**
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. Servers and networking equipment may be re-tasked or reconfigured as needed.

Competition Rules: Acknowledgement & Agreement

Competition rules are applicable to all participants of the Midwest Qualification 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 advisers and all student participants are expected to know and follow all CCDC rules and guidelines. Access to the competition stadium environment implies their acknowledgement of competition rules and their commitment to abide by them.

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

Competition Rules: Student Teams

1. Each team will consist of between four and eight members. All team advisers have been informed of and will adhere to all national rules. See www.nationalccdc.org
2. Each team may have no more than two graduate students as team members.
3. Each team may have one adviser 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 Competition Manager. Team advisers and faculty representatives may not assist or advise the team during the competition. Team advisers and faculty representatives may not be involved in any scoring or decisions that involve a participating institution or Blue Team.

4. All team members, the team adviser, and all faculty representatives 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, or competing remotely at different sites, and at all preparation meetings.
2. Host site/ local site policies and rules apply throughout the competition.
3. All Cyber Defense Competitions are alcohol free events. No drinking is permitted at any time during the competition.
4. Activities such as swearing, consumption of alcohol or illegal drugs, disrespect, unruly behavior, sexual harassment, improper physical contact, becoming argumentative, or willful physical damage have no place at the competition.
5. In the event of unprofessional conduct, student team members and their adviser will meet with Gold Team members upon request. The consequence of unprofessional conduct will be determined by the Site Administrator or Competition Director 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 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, room, or competition network. 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 Black/Black/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 advisers and sponsors. All private communications (calls, emails, chat, directed emails, forum postings, conversations, requests for assistance, etc.) with non-team members are forbidden and are grounds for disqualification.
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 Black/Black/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, Black/White Team members, other competitors, etc. outside of competition hours.
10. Only Blue Team, Black/White Team or Gold Team members will be allowed in any Blue Team competition room. On occasion, Black/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. Black, 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 Black/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 Black/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 Black/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 Black/White Team guidelines. It is the responsibility of the Blue Team to understand how scoring may be impacted by changing passwords. No admin, administrator, sysadmin, or root accounts are uses for scoring so passwords for these accounts may be changed freely and without notification to the Black/White Team.
14. Blue Team members should maintain ICMP on all competition devices and systems, except the Core port of the Palo Alto 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 Black/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 Black/White Team, and will not be shared with Blue Team members. Faculty advisers 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. A Web Proxy will be in place to limit internet access via the competition system to essential sites as defined by the NCCDC. Internet activity will be monitored.
2. Internet activity from the workstation used by a team member must follow local school policies. Internet access during the competition is expected to be appropriate to the event. 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 Black/White Team immediately.
3. Internet resources allowed by the Web Proxy are still subject to the following restriction: no fee must be 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.
4. Teams have been allowed to build a Github repository with appropriate resources according to published policy. Provided that the respective team Github repository specific url is provided to your respective State Director prior to the event, access to the repository will be included in the Web Proxy.
5. All network activity that takes place on the competition network may be logged and is subject to release. Competition officials are not responsible for the security of any personal information, including login credentials that competitors place on the competition network.

Competition Rules: Scoring

1. Scoring will be based on keeping required services up, controlling/preventing 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 Black/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 Black/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 Black/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 Black/White Team will assess scores for incident report submission based on clarity, thoroughness, and accuracy. The Black/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.

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.

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.

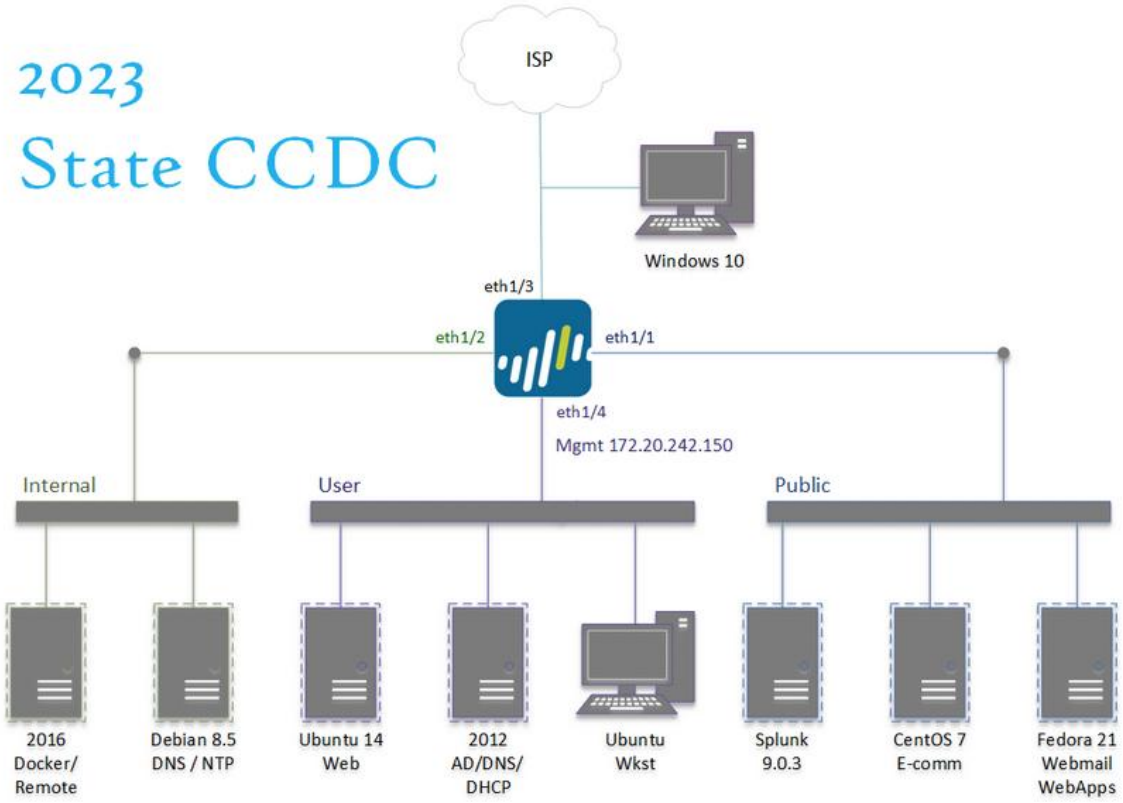
Aftermath

Members of the MWCCDC Consortium, Gold, Black, White, Red, and Green Teams strive to make the CCDC Qualifier 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/mwccdc. 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 CCDC Qualifier, and may also enumerate participating teams and winners.

Competition Topology



- Teams have access to 10 VMs – 7 serves, 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.
- Splunk has been updated to version 9.0.3, which requires an up to date browser to connect. **The initial topology may not have a browser suitable for this version of Splunk.**
- The firewall shown in the topology is a Palo Alto VM, version 10.0.0, which is licensed by Palo Alto.

  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
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
17	172.31.37.2/29	172.31.37.1	172.25.37.0/24
18	172.31.38.2/29	172.31.38.1	172.25.38.0/24
19	172.31.39.2/29	172.31.39.1	172.25.39.0/24
20	172.31.40.2/29	172.31.40.1	172.25.40.0/24

- VM data are as follows:

	Version	*IP*	*Username*	*Password*
INTERNAL				
2016 Docker/Remote	Srvr 2016 Std	172.20.240.10	administrator	!Changeme123
Debian 8.5 DNS/NTP	Debian 8.5	172.20.240.20	root sysadmin	changeme changeme
USER				
Ubuntu 14 Web	Ubuntu 14.04.2	172.20.242.10	sysadmin	changeme
2012 AD/DNS/DHCP	Srvr 2012 Std	172.20.242.200	administrator	!Password123
Ubuntu Wkst	Ubuntu Desktop 12.04	DHCP	sysadmin	changeme
PUBLIC				
Splunk	9.0.3	172.20.241.20	root admin (Web UI)	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 10.0.0	172.20.242.150	admin	Changeme123
Windows 10	Windows 10	172.31.xx.5	minion	kingbob

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

Specific NAT translations are as follows:

INTERNAL	Local IP	'Public' IP
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
2012 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/ISE.
- 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.**

Sponsors:

	Department of Homeland Security, http://www.dhs.gov/
	Raytheon Technologies Corporation www.raytheon.com
	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