2017 Michigan Collegiate Cyber Defense Qualifier

Michigan Collegiate Cyber Defense Network

Team Packet for

February 2017 CCDN Qualifier

SUBJECT TO CHANGE OR REVISION

Table of Contents

Contents

State Qualifier Mission and Objectives

The 2017 Michigan Collegiate Cyber Defense Qualifier provides an opportunity for qualified educational institutions in the state of Michigan to demonstrate skills under a competitive environment while having those skills assessed by industry professionals. Qualified educational institutions include those with networking security curricula and a demonstrated commitment to their student population. The Michigan Collegiate Cyber Defense is designed to provide a controlled, measured and observed environment that will permit each participating institution to determine their students' depth of understanding and operational competency in managing the challenges inherent in protecting an enterprise network infrastructure from cyber-attack.

Overview

The qualifiers are 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, which may require configuration, installing and maintaining systems and services. Each student team is expected to manage the computer network, keep it operational, prevent unauthorized access, and accurately identify compromises and compromise attempts. Each team will be expected to maintain and provide public services, including but not limited to: a web site, a secure web site, an email server, a database server, firewalls, monitoring and recovery capabilities, and a workstation used by simulated sales, marketing, and research staff as per provided fictitious company policy and mission. Each team will start the qualifier with a set of identically configured environments.

This is not just a technical qualifier, but also one built upon the foundation of defensive response under a concept of business operations, policy, procedures and a variety of unknown circumstances and events that mimic occurrences likely to be experienced in industry. Student teams will be scored on the basis of their ability to detect and respond to both external and internal 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. Michigan CCDN qualifiers and competitive events are predesigned and turned over to industry professionals and volunteers for delivery, scoring, judging and execution. They have a vital interest in identifying the most effective student teams so that academic and professional quality can be maintained and encouraged in academic environments.

The first place team will have the opportunity to be invited to participate in the 2017 Midwest Regional CCDC, tentatively scheduled for March 17th and 18th at Moraine Valley Community College, Palos Hills, Illinois. Teams must travel to the 2017 Midwest Regional CCDC at MVCC at their own expense.

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 from among the entire mid-west region may also be selected for the regional, at the discretion of the CSSIA management team. CSSIA rules apply.

Qualifier 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 industry professionals
5. To have industry recognition, participation and acceptance of each competition
6. To rate the effectiveness of each competing team against industry expectations
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

Team Identifications

Blue Team - student team representing a specific academic institution participating in this qualifier; each team must submit a roster of up to no more than 12 student qualifiers to the State CCDN Director. Each qualifier 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 qualifying team cannot compete. Substitution in the qualifier requires approval from the State CCDN Director. Each team must:

- Members and advisor sign and submit the Participation Safety Agreement
- Representative from the participating institution sign and submit the Team Packet Acceptance
- Have completed a minimum of one semester in the participating institution's networking or security curriculum
- Students should maintain a minimum of half-time status at the time the qualifier is conducted.
- National rules apply to the mid-west regional competition; www.nationalccdc.org
- Further information regarding mid-west regional events is available at www.mwccdc.org the main website for Midwest Cyber Defense Competitions.
- Further state information on collegiate cyber defense activities, qualifiers and team assessments is available at www.michiganccdn.com

Red Team – Professional network penetration testers from industry approved by the Chief Judge, State CCDN representative and the administration team:

- Scan and map the network of each qualifier 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 guidelines of engagement for the qualifier

- **White Team** – Representatives from industry who serve as qualifier and assessment support, remote site judges, room monitors and security enforcement in the various event rooms. Under direction of the qualifier director, assistant director and / or chief judge, the white team will assess each blue 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 participating 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 other reported issues. Each student team may be monitored electronically using webcams or local host security systems.

- **Chief Judge:**
    - Serves as the final authority on scoring decisions or issues relating to equity or fairness of events or activities
    - Cannot be employed by any institution that has a participating Blue team or have any interest in any team outcome
    - Is a representative from industry or law enforcement
    - Final authority of all judging decisions, including assessment and determination of final scores and, blue team placements resulting from the qualifier
    - Is a member of the administration team

- **Administration Team** – May be comprised of the State CCDC Director, the State CCDN Director, the host sites event director, assistant director, the Chief Judge, as well as other representatives approved by the CCDN state director, who make up the administration team both in planning and during the exercises. Responsibilities include, but are not limited to,
    - Locating administration and staffing for the event
    - Works with industry partners to orchestrate establishing the event
    - Approves the Chief Judge
    - Has the authority to dismiss any team, team member, or visitor for violation of event rules, inappropriate or unprofessional conduct, or any manner of activity considered disruptive to the event
    - Approves the network topology

- **Compliance Monitor –** Approved by the regional authority (CSSIA), to monitor and maintain compliance for adhering to regional rules of play and competition. Has no authority over outcomes or administration decisions but rules on compliance to event rules.

- **Green Team** – Tech support and hospitality – assists with any technical needs necessary to maintain the integrity of the event. Assists with ancillary functions – greeters, food service, local directions.

Event Scenario

You have just been hired to take over a network for a company that specializes in software development. The company network has been the target of attacks from unknown sources. You and your team have been hired to perform an emergency assessment and maintenance of a local IT infrastructure that will maintain services and protect the network while adapting to varying business needs. The system has been under attack and previous attempts to defend it have been mixed by the previous IT team. You are not permitted to hack back, interfere with or alter any other team's services or systems unless specifically instructed to do so by the administration. Your team is completely responsible for the functionality, defense, adaptation, support and operation of your team network.

Initial Connection and Scoring

The start time of the scoring will be announced. Red team assaults may not be announced. Announcements will be either via email, personal runner or other electronic means and will be identified during the initial stages of the event.

Network & Team Site Description

- Each qualifier network may be logically isolated from the hosting organization's network.
- The 2017 Michigan CCDN Qualifier will be based on a localized VM build hosted by student systems in an academic setting.
- Each participating Blue Team will be provided an initial image or configuration information to import or configure into localized VMs from which they will initiate the build and / or configuration of the rest of their local VM network. From this initial build each team may be asked to connect to a local closed system FTP site and download additional images for completion or enhancement of their network.
- The method and mechanisms by which the White Team and each respective Blue Team will communicate will be presented at the start of the event and may be modified during the event as may be deemed necessary.
- Red Team activity may be either externally or internally sourced with respect to the network. Blue teams cannot physically disconnect red team access to their network.
- Each Blue Team network will be monitored by a scoring system operating within the network. An indication of services, as viewed by the indigenous scoring engine, will be made available to the White Team.
- A logical diagram of the team logical network is attached to this Team Packet. However, it is subject to change and /or modification as decided and / or approved by the Chief Judge, or the State CCDN Director.

Schedule Saturday February 25th, –APPROXIMATE – All Times are EST

8:30 – 9:00 AM	Arrive and Register at Davenport University, Sneden Center
9:00 AM	Introduction to the day's activities, materials disbursement, qualifier rules, business scenario and room assignments
10:00 AM	Teams go to rooms, start of Qualifier Activities
12:00 PM	Operational Pause for Lunch, Presentation by TekSystems and Cyber Security Forum Initiative.
1:00 PM	Teams Return to Room
5:15 PM	Qualifier activities end, scoring stops, teams clean up rooms
5:30 PM	Davenport University hosted dinner
6:15 PM	All Teams Return to Sneden Center. Review of days' activities, presentations from Cyber Defense Training Systems, E-Netsecurity of Curitiba Brazil, debrief from Red & White Team, announcement of 1st, 2nd and 3rd place positions by Chief Judge

Inclement weather or unforeseen circumstances: Should weather or other unforeseen circumstance be determined to impact or delay the Michigan 2017 CCDN Qualifier, two possible alternatives exist and will be determined by the industry representatives executing the event. These alternatives are: 1. The event may be delayed to one of the two subsequent weekends and will be conducted as originally planned as an onsite event. 2. The event may be rescheduled as a remote event with each blue team participating from their respective institutions.

Systems

1. Each team will start the event with identically configured systems.
2. Teams may not add or remove any host computer, printer, or networking device from the designated Blue Team area.
3. Teams will be provided the overall system architecture, network configuration, and initial set-up in this team packet.
4. Blue Teams should not assume any participating qualifying system is properly functioning or secure. If one system fails, it is the blue teams' responsibility to resolve the issue either by resolution or accurate identification. In the event of a hardware failure, the impacted blue team will be accommodated in both equipment and scoring.
5. Throughout the qualifier, White Team and Administration Team members will occasionally need access to a team's systems for scoring, troubleshooting, etc. Blue Teams must allow Green Team, White Team and Administration Team member access when requested and validated. Teams may use discretion for admitting non-recognized or non-validated individuals.
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 – for example if a team's web service is provided to the "world" on 10.10.10.2, the web service must remain available at that IP address throughout the event. A list will be provided. Moving services from one public IP to another is not permitted unless directed to do so by an inject request. Likewise, teams are not permitted to change the internal addressing or VLAN scheme of the qualifier network unless directed to do so by an inject request.

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, Blue teams will be able to perform a complete operating system restoration. The number of system restorations and recoveries must be identified and reported to the event administration. Teams should also consider that system restoration will take time.
11. Systems designated as user workstations within the qualifier 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 qualifier network.
13. Equipment is not to be opened by any Blue Team member. This includes computers, routers, switches, servers, cameras or any device associated with this event.
14. Teams are responsible to for the services identified on the topology are configured and running.

Qualifier Rules: Acknowledgement & Agreement

Each student team that participates in the Michigan 2017 Collegiate Cyber Defense Qualifier must:

1. Be supported and attended by a full time faculty member of their institution.
2. Agree to follow all the written, verbal or otherwise stated rules.
3. Not participate in hack back, system compromise or vulnerability assessment activities of any network outside of the student network for which they are assigned, unless specifically instructed to do so by the Chief Judge.
4. No faculty member from any institution can participate in the operational aspects of this event. They are present to represent their institution and their students.

Qualifier rules are applicable to all participants of the Michigan 2017 State Qualifier. They provide structure for the makeup of student teams, permitted actions during the event, guidelines for scoring, and contingencies for handling disputes. They also document expectations for appropriate conduct during the entire time participants are guests at the host site. Team advisors and team captains are required to sign where indicated, signifying their acknowledgement of event rules and their commitment to abide by them.

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

Qualifier Rules: Entry Fee Payment

A support participation fee per team is required for each participating institution that has requested to participate in this activity. Fees are collected within each state under the direction of the State CCDC or CCDN Director. It is required that all institutions satisfy the support fee requirement by payment prior to the start of the event. Failure to pay the support fee prior to the event will result in disqualification.

Teams wishing to drop out of the State Qualifier must notify the State Director no later than fifteen days prior to the scheduled event. A Team that drops out less than Fifteen days of the event, or is ‘no show’ at the event is expected to pay the support participation fee. Failure to pay the support fee in such a case will result in disqualification from State Qualifier the following year.

Qualifier Rules: Student Teams

1. Each team will consist of up to no more than active eight members with two observers. All team advisors will review and adhere to all national rules. See www.nationalccdc.org. The Michigan CCDN Qualifier reserves the right to impose additional rules for student play; including blue team members. For clarification or ruling please contact the state director.
2. Each team may have no more than two graduate students as team members.
3. Each team must have one full time faculty advisor present or immediately available during the entire event.
4. Team advisors and faculty representatives may not assist or advise the team during the event in any technical matter.
5. Team advisors and faculty representatives may not be involved in any scoring or decisions that involves participating institution or Blue Team.
6. 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.
7. Each team will designate a Team Captain for the duration of the event activities to act as the team liaison between the qualifier staff and the teams before and during the qualifier. Individual blue team members are not to communicate with the admin team unless directed to do so by their respective blue team captain.
8. If the member of a qualifying team is unable to attend the regional competition, that team may substitute another student in their place from the submitted roster.
9. Participating student team members must be enrolled for a minimum of 6 credits (half time) at the institution they represent. Any variance to this must be approved by the state CCDN director.
10. For the 2017 state qualifier, student team members may be employed full-time in a computer technology role in industry, including networking, security, programming or other related positions. They are not permitted to be an instructor or professor at any institution.
11. Students may create professional appearing incident report forms before the event; email them to themselves for downloading and use at the event. Assessment points are awarded by the administration team for efficient and professional incident reports.
12. Each team is expected to bring at least one unopened USB thumb drive and a spool of CDs or DVDs for use in their rooms as they may deem necessary.
13. Each blue team is to bring one web cam for configuration in room monitoring during the event. Configuration instructions will be provided at the start of the event.

Qualifier Rules: Professional Conduct

1. All participants are expected to behave professionally at all times they are visiting the host site, at all preparation meetings, and in all dealings with the organizers, host or supporters of this event.
2. Host site/ local site policies and rules apply throughout the event.
3. This event is alcohol free. No alcohol is permitted at any time.

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 this or other related state events.
5. The consequence of unprofessional conduct will be determined by the Chief Judge with the recommendation of the Administration Team. This may be a warning, point penalty, disqualification, or expulsion from the campus.
6. The Host Site Administrator reserves the right to disqualify an offender from participation in future events at their site.
7. The State CCDC or CCDN Director reserves the right to disqualify an offender from participation in future qualifier activities.

Qualifier Rules: Qualifier Play

1. During the qualifier, team members are forbidden from entering or attempting to enter another Blue Team's workspace or room. They are also forbidden from accessing another Team network, either through their network, or by remote access to another team, unless specifically directed to do so by an inject. Injects are issued by the admin team under the direction of the event director.
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, action or item requested, and date/time requested. The method of communication will be determined at the time of the event.
3. Teams must not solicit or accept outside assistance from non-team members which includes team advisors, sponsors or technical support help desks, work associates, etc.
4. System scrubs and resets are counted as point deductions. The amount of each deduction is entirely at the discretion and assessment of the industry representative / chief judge.
5. 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.
6. Each team is to bring at least one unopened flash or thumb drive and several CD-ROMs for use during their event. Other electronic media such as cell phones, PDAs or other similar electronic devices are not allowed to be used in the room during the qualifier unless specifically authorized by the Administration Team in advance. Teams may not bring any computer, tablets, PDA, or wireless device into the Blue Team room. MP3 players with headphones will be allowed provided they are not connected to any system or computer.
7. 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.
8. The team faculty advisor should be the emergency contact for their respective Blue Team participants during the event.
9. Printed reference materials (books, magazines, checklists) are permitted and teams may bring printed reference materials to their respective rooms.
10. Team sponsors and observers are not student qualifiers or competitors and are prohibited from directly assisting any participant through direct advice, suggestions, or hands-on assistance. Any team sponsor or observers found assisting a team will be asked to leave the event for the duration of the event and a point penalty will be assessed against the team.
11. An unbiased Red Team will probe, scan, and attempt to penetrate or disrupt each team's operations throughout the event.

12. Team members will not initiate any contact with members of the Red Team during the hours of live play.
13. Only validated personnel will be allowed in any Blue Team room. On occasion, White Team or Administration Team members may escort individuals (press, etc.) through the qualifying area including team rooms. Guest visits must be approved by the event director and are not encouraged as it may distract the Blue Team members during their activities.
14. It must be understood that these events and activities are not spectator sports. The performance of an institutions team under controlled conditions are being qualified for performance and placement. Past experience has demonstrated that excessive or unnecessary distractions may impact these results and are not tolerated.
15. White, Administration, or Green Team members will be allowed in all event areas outside of event hours.
16. 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, and does not impact the scoring engine. Failure to preserve pre-existing data during a service migration will result in a point penalty as deemed appropriate by the Chief Judge for each user and service affected. Teams may not move services from one OS System to another, unless specifically directed to do so via a business inject.
17. Teams are free to examine their own systems but no offensive activity against other teams during Saturday defensive operations, 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, without administration approval, or any global asset will be immediately disqualified from the event. If there are any questions or concerns during the event about whether or not specific actions can be considered offensive in nature contact the White Team before performing those actions.
18. Blue Team members may change passwords for administrator and user level accounts. Changes to passwords must be communicated to the White Team. Teams are required to provide modified passwords in the electronic format specified. Teams may not change usernames/passwords for access to services unless requested to do so.
19. Blue Team members should maintain ICMP on all qualifier devices and systems, including the router. 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.
20. Each Blue Team will be provided with the same objectives and tasks.
21. Each Blue Team will be given the same inject scenario at the same time during the course of the qualifier.
22. References to Blue Teams will be by random selection of a number. The Administration Team or the Red Team will not be informed of which student teams from which institution are assigned to which qualifier rooms.
23. The Administration and White Team is responsible for administering scenario events, scoring required business processes, and submitting team challenges

24. 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 event
25. 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 an initial debriefing meeting at the end of the event. This may be in the form of question and answer period, individual discussion, or other means as deemed appropriate by the Chief Judge
26. If a scenario or event arises that may negatively impact the integrity or fairness of any aspect of the qualifier 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.
27. Running totals will not be provided during the qualifier. A system service check resource may be available depending on the current phase and activities of the event.
28. Student teams are expected to provide an incident response form identifying each incident created on their systems or network as the result of an attack or self inflicted event.
29. Development, planning, deployment and administration of this qualifier require the efforts of numerous personnel and many hundreds of hours. It also involves significant expense. All configurations, images, files associated with this event are the intellectual property of Cyber Defense Training Systems, LLC, or individual red team members as developed. Copies of files, images or any types of software provided during this event are strictly prohibited. Any team copying such will be disqualified from the next year's event and their academic administration notified of the breach of security and legal action may be taken.

Resumes – Michigan and CSSIA Regional

Although the Michigan CCDN is specifically designed to provide participants an experience that is challenging while simulating real network scenarios, it will not require resumes for the 2017 qualifier. However, sponsors of the Mid-west Regional are particularly interested in students that are mature in their field of study and any team attending the EJS Regional CCDC event in Palos Hills Illinois will be required to have professional resumes prepared. The following information is from CSSIA for teams participating in the EJS Regional CCDC event scheduled for March 17th and 18th, 2017. It is presented here for preparation purposes for that event only. Resumes for the mid-west regional should include the following areas:

Education – It is assumed that most students have little work experience, so education must be stressed. You should list IT specific courses you have completed.
Experience –If you have IT related experience, highlight it, explaining what you have done, and especially any unique accomplishments. If you have work experience, but it is not IT related, make a very brief reference to it. Receipt of resumes without any significant work experience in the IT is to be expected. No penalty whatsoever will be assessed for the absence of IT experience.
Activities – This is probably a more important area of the resume than realized. Your interests and hobbies, whether related to IT or not, tell a lot about who you are, and how well you might fit in an organization.
Achievements –Be sure to note any special achievements you have received. These will oftentimes be recognition of academic achievement, such as honor role, grade point average, as well as certifications, &c. Again, no penalty will be assessed for relative lack of achievements,

but students are advised to include them. Students should certainly include expected degree award and date.

Strengths and Abilities – A description of your skills to date with some indication of the level of expertise should be included. A balance of presentation should be made here between being overly general, and not too detailed. We know you can use ping/traceroute, but if you state familiarity with OS, you need to be more specific.

Format – Clearly this will be a significant contribution to adjudicated scores. There are no set requirements as to format. Moreover, it is difficult to convey professionalism in appearance. Suffice to say that adjudicators will surely recognize a professional looking resume when they see one. Some items that are important here are organization, clarity of expression, accuracy, use of active constructs, and consistency of format and layout. Some things to watch for are awkward statements, poor grammar, passive constructs (such as 'responsible for…'), and of course misspelling.

Qualifier Rules: Internet Usage

1. Qualifier rooms may have access to the Internet for the purposes of research. Internet activity may be monitored and any team member caught viewing inappropriate or unauthorized content will be immediately disqualified from the qualifier. This includes direct contact with outside sources through AIM/chat/email or any other non-public services. For the purposes of this qualifier 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 qualifier 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 qualifier use provided there is no fee required to access those resources and access to those resources has not been granted based on a previous purchase or fee. Only resources that could reasonably be available to all teams are permitted. For example, accessing Cisco resources through a CCO account would not be permitted but searching a public Cisco support forum would be permitted.
3. Teams may not use any external, private electronic staging area or FTP site for patches, software, etc. during the qualifier. All Internet resources used during the qualifier must be freely available to all other teams.
4. Public sites such as Security Focus or Packetstorm are acceptable. Only public resources that every team could access if they chose to are permitted. No peer to peer or distributed file sharing clients or servers are permitted on qualifier networks.
5. All network activity that takes place on the qualifier network may be logged and is subject to release. Qualifier and host officials are not responsible for the security of any personal information, including login credentials that participants place on the qualifier network.

Qualifier 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. Blue Team members should refrain from making direct requests to the White Team for routine service verification. A status check

link of last services polled per team may be provided depending upon current stress load and conditions. It is not guaranteed.

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 qualifier 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 are to be completed as needed throughout the qualifier 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. Each team member must understand and accept that the network they are working in is dynamic and designed to accommodate both legitimate and malicious network traffic. Unknown circumstances, network failures, Internet interruptions are a part of this environment, whether intentional, non-intentional or maliciously caused by another team or actor. In the occurrence of such an event, student teams must adapt to the changing environment just as in a real-world situation. Out of band file and traffic passing may be necessary to accommodate such interruptions.
7. The first place position will be based on the highest score obtained during the qualifier. Exact point weights are not provided prior to the event. This is to discourage students from playing the point system against other categories. For example, a team that has 100% in electronic scoring may have 20% in inject management skills. It is desired that all skill categories be effectively addressed so that one or two areas are not focused on over others. Point categories are identified as follows:

Electronic Scoring: of functional services uptime as measured by scoring engine
Inject Management &Success: Successful completion of inject scenarios (Business Tasks) will result in varying points, depending upon the importance or complexity of the inject scenario
Incident Response: Correct incident response, reporting and Red Team assessment
Other Assessment Category: -On-line Assessment; - Overall defensive capabilities, timely responses, professionalism, etc.

Functional Services

Certain services are expected to be operational at all times or as specified throughout the qualifier. In addition to being up and accepting connections, the services must be functional and serve the intended business purpose. Certain services will be tested for function and content where appropriate, including, but not limited to:

HTTP

A request for a specific web page will be made. Once the request is made, the result may 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.

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

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

Additional services required to be operational and scored during the hours of the event qualifier include, but are not limited to, SMB, LDAP, RDP, TELNET, ICMP. Addition of scored services will be identified to the blue team at the time they are required. The Administration and Red Team will determine which services are injected into the qualifier.

Business Tasks

Throughout the qualifier, 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 and may be electronically scored.

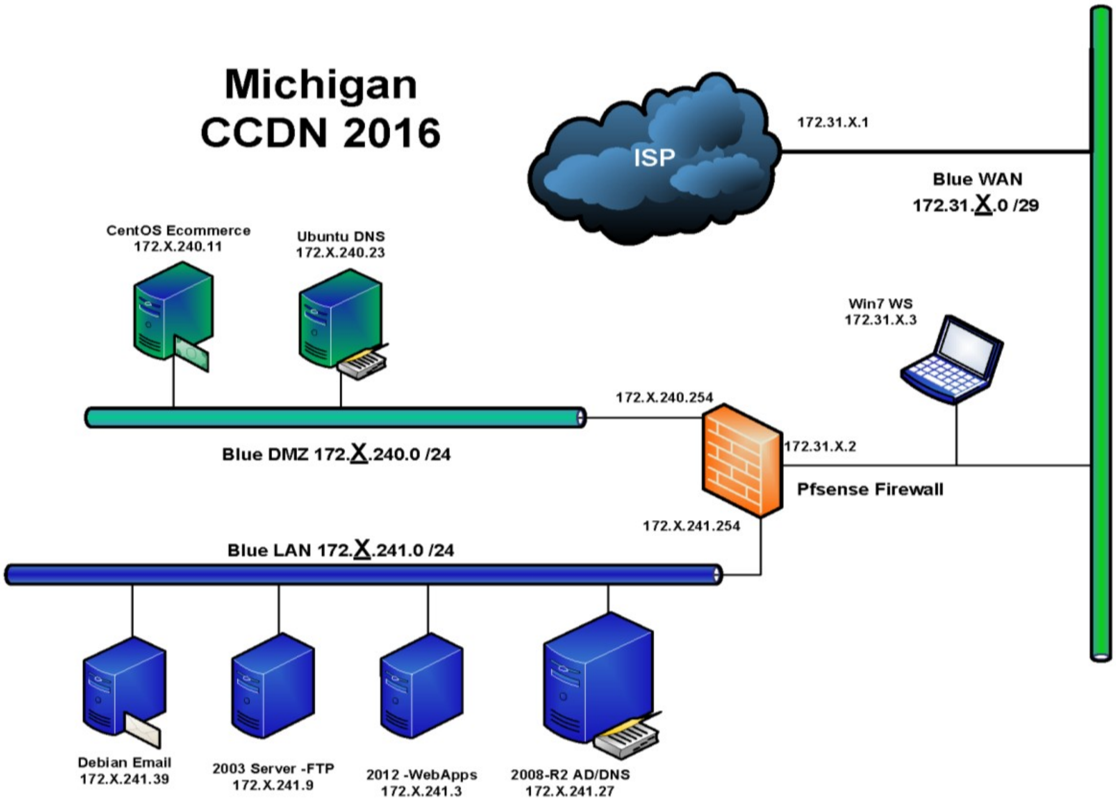
Questions and Disputes

1. Team captains are encouraged to work with the local site judge and staff to resolve any questions or disputes regarding the rules of the event or scoring methods before the activities begins. Administration Team officials will be the final arbitrators for any protests or questions arising before, during, or after the event and rulings by the Chief Judge are final.
2. In the event of an individual disqualification, that team member must leave the event area immediately upon notification of disqualification and must not re-enter the area at any time.
3. In the event of a notified team disqualification, the entire team must leave the event area immediately upon notice of disqualification and is ineligible for any individual or team award.

After Event

Participants and representatives of the respective institution are forbidden from publishing, posting on the internet, or publicly communicating details of the qualifier other than what is available at www. mwccdc.org or www.michiganccdn.com. They are also forbidden from publishing, posting on the internet, or publicly communicating assessments of the State Qualifier, 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 qualifiers.

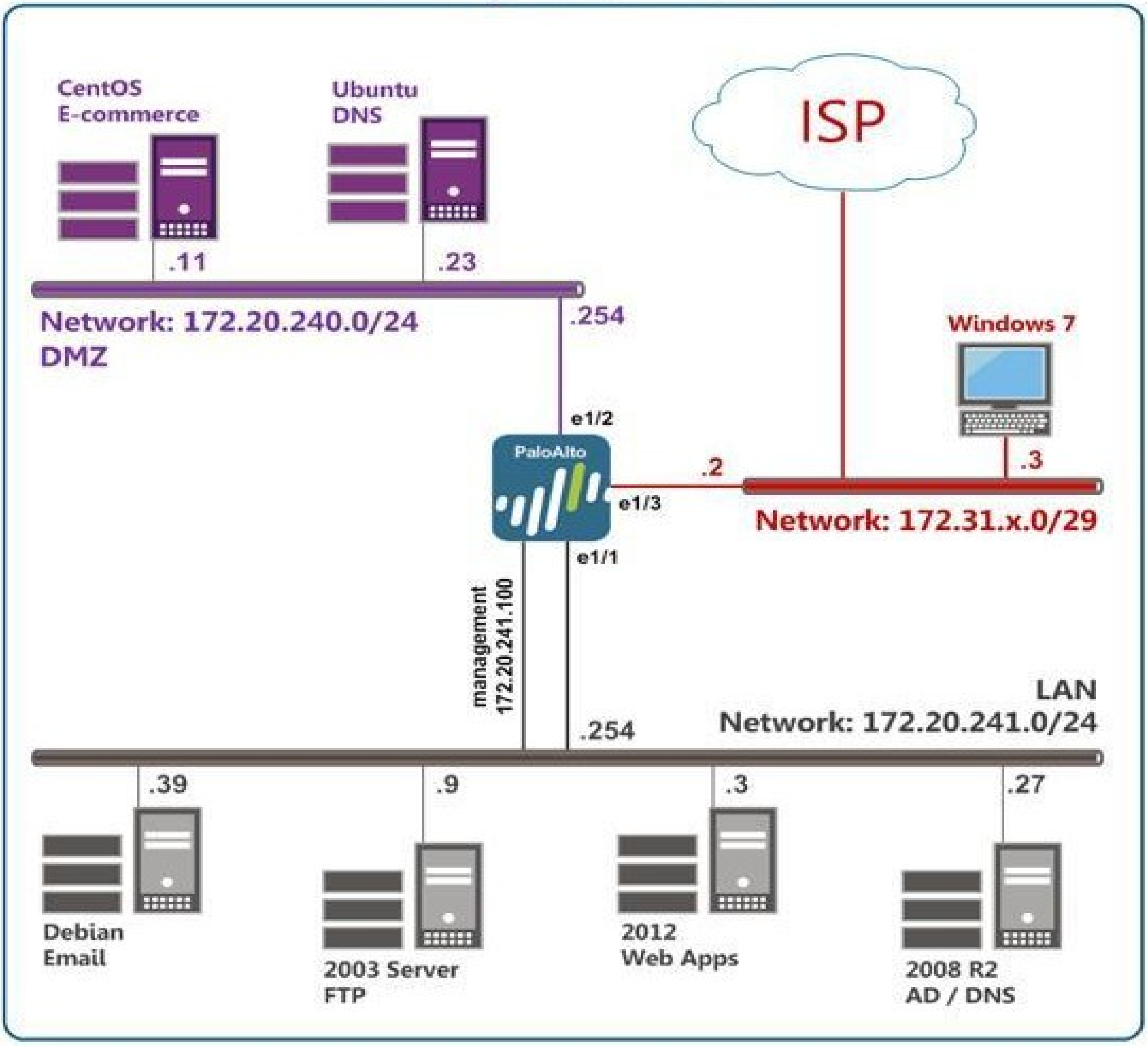
Michigan 2017 Qualifier Topology <u>(SUBJECT TO CHANGE)</u>



The Michigan CCDN attempts to provide an identical topology as the CSSIA CCDC network. However, this is not always possible due to service availability and configuration management requirements, industry input, capability of remote service providers and may change as necessary before or during the event. Both the Michigan and CSSIA topologies are included in this team packet for preparation purposes.

<u>NOTE: All teams should prepare for the injection of a Palo Alto VM to replace the PfSense Firewall.</u>

CSSIA 2017 Regional Qualifier Topology (SUBJECT TO CHANGE)



Subject to Change

Any information, topology or rules in this team packet are subject to revision, modification or change as may be deemed necessary by the chief judge or state director before or during the qualifier to ensure adaptability and equity in all aspects of this event.

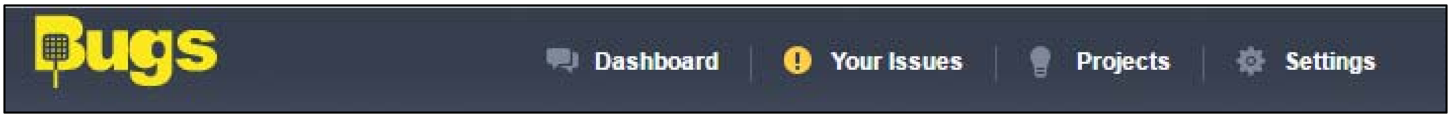
Sponsors

`MichiganCCDN	**Michigan Collegiate Cyber Defense Network** http://www.michiganccdn.com/
TEKsystems Our people make IT possible.	**TEK Systems** https://www.teksystems.com/en
DAVENPORT UNIVERSITY	**Davenport Univeristy** www.davenport.edu
Cyber Defense Training Systems, LLC	**Cyber Defense Training Systems** http://cyberdefensetrainingsystems.com
paloalto NETWORKS	**Palo Alto Networks** https://www.paloaltonetworks.com/
e-net security	**e-net security** http://www.e-netsecurity.com.br
THE CYBER SECURITY FORUM INITIATIVE	**Cyber Security Forum Initiative** **www.csfi.us**

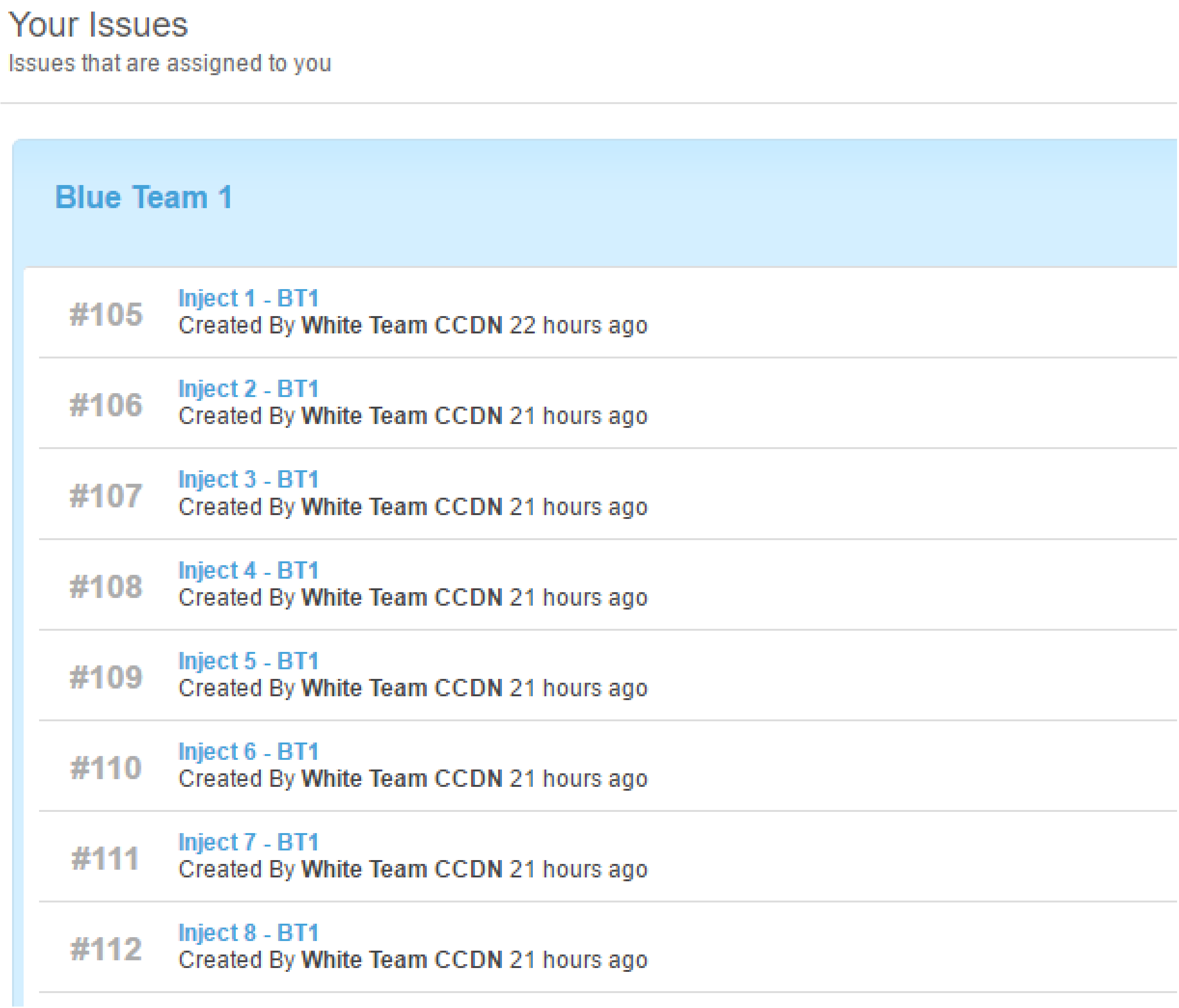
Bugs

“Bugs” FAQ

How do I receive my Injects?



Newly assigned Injects will appear automatically under the “Your Issues” screen. This screen automatically refreshes every 10 seconds.



Your Issues

Issues that are assigned to you

Blue Team 1

#105 Inject 1 - BT1
Created By **White Team CCDN** 22 hours ago

#106 Inject 2 - BT1
Created By **White Team CCDN** 21 hours ago

#107 Inject 3 - BT1
Created By **White Team CCDN** 21 hours ago

#108 Inject 4 - BT1
Created By **White Team CCDN** 21 hours ago

#109 Inject 5 - BT1
Created By **White Team CCDN** 21 hours ago

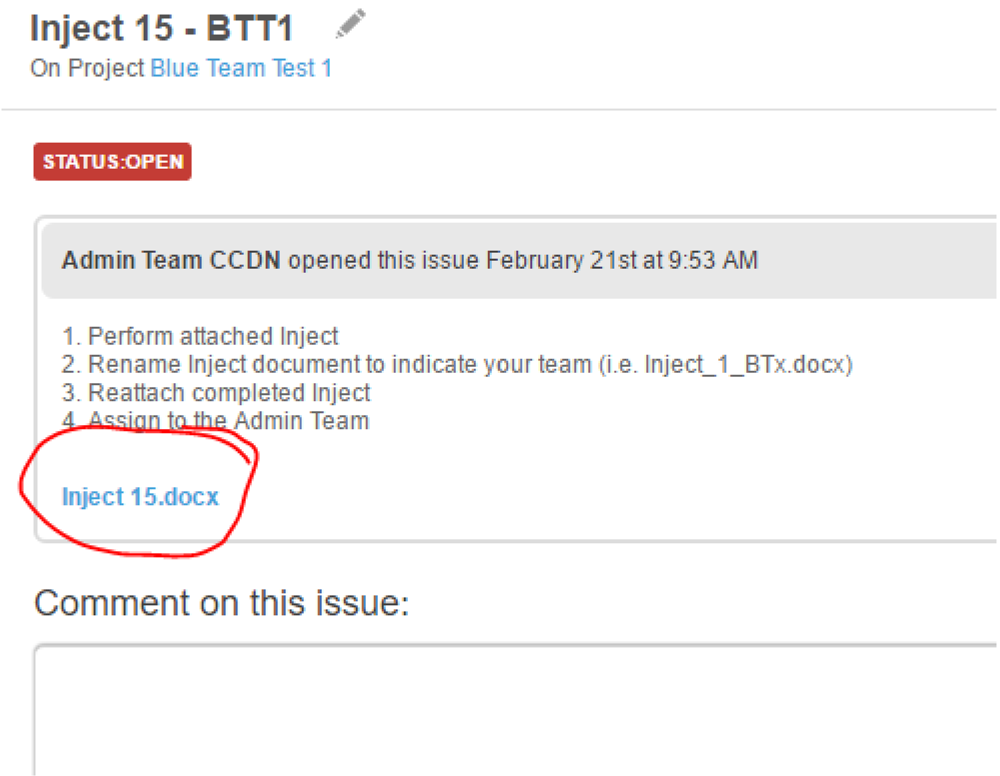
#110 Inject 6 - BT1
Created By **White Team CCDN** 21 hours ago

#111 Inject 7 - BT1
Created By **White Team CCDN** 21 hours ago

#112 Inject 8 - BT1
Created By **White Team CCDN** 21 hours ago

How do I process an Inject?

Inject documents will be attached to an “Issue”. Download the attachment and complete the Inject. Rename the inject to indicate which team it belongs to (i.e. Inject_1_BTx.docx), reattach the document to the Issue, and assign it back to the Admin team. To attach a file, you will have to make some kind of comment in the comment box.



Inject 15 - BTT1

On Project Blue Team Test 1

STATUS:OPEN

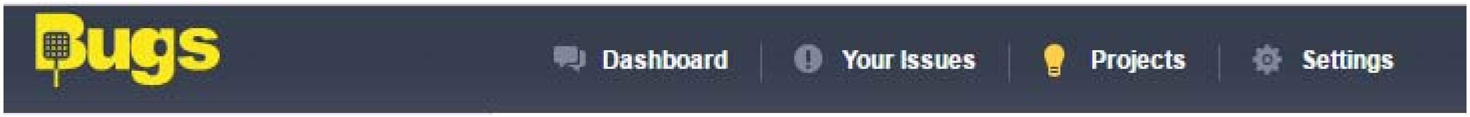
Admin Team CCDN opened this issue February 21st at 9:53 AM

1. Perform attached Inject
2. Rename Inject document to indicate your team (i.e. Inject_1_BTx.docx)
3. Reattach completed Inject
4. Assign to the Admin Team

Inject 15.docx

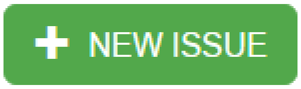
Comment on this issue:

How do I report problems and incidents?



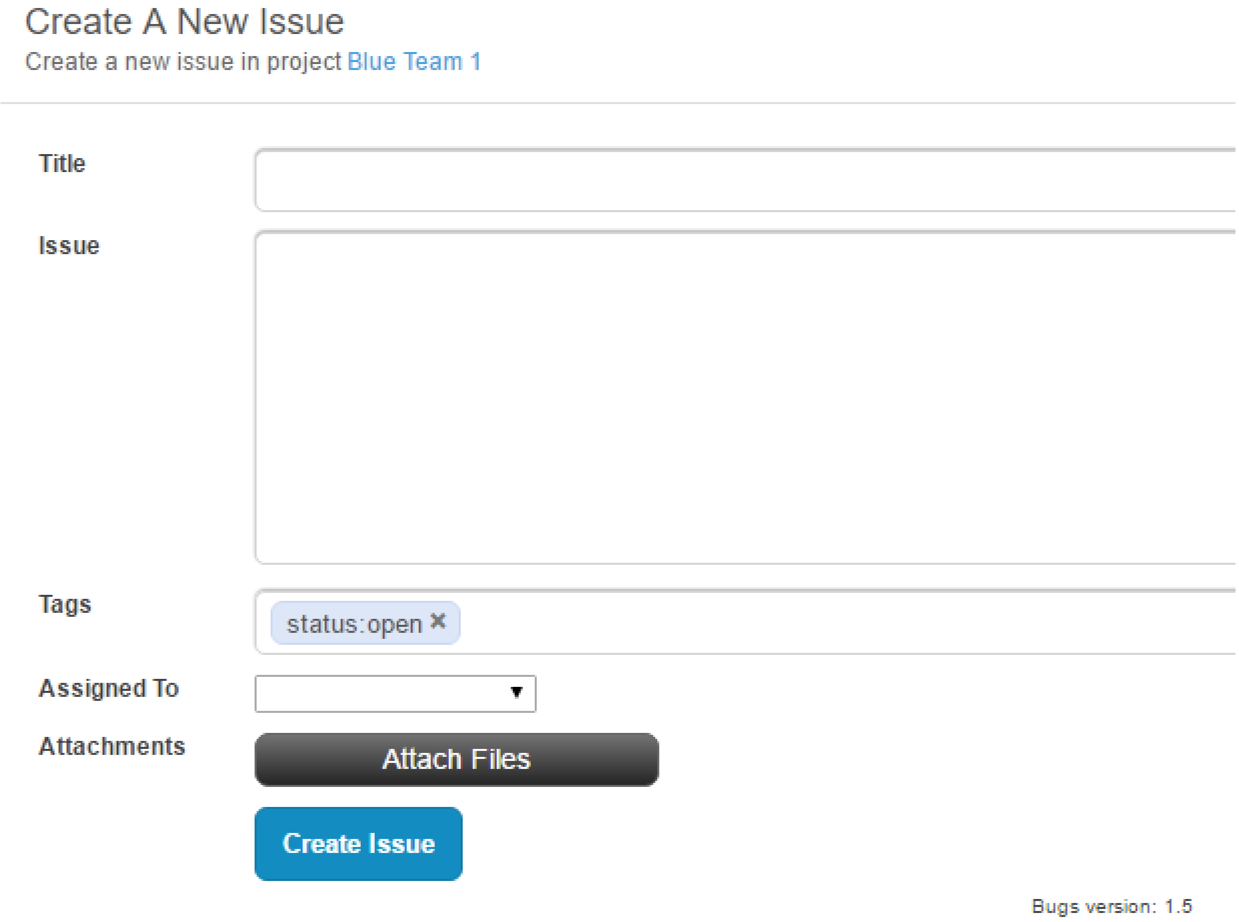
When you experience a system issue or need to report a security incident, select “Projects” from the main navigation menu at the top of the screen.

Click the “New Issue” Button.



In the New Issue screen, you can give your issue a title, description, attach files and assign it to the appropriate team.

After you complete the fields, assign to the Admin team (inject questions / ”Bugs” issues) or the White Team (VM / Network / Hardware Issues). If you are unsure who to assign it to, assign the issue to the admin and they will handle it.



Create A New Issue

Create a new issue in project Blue Team 1

Title

Issue

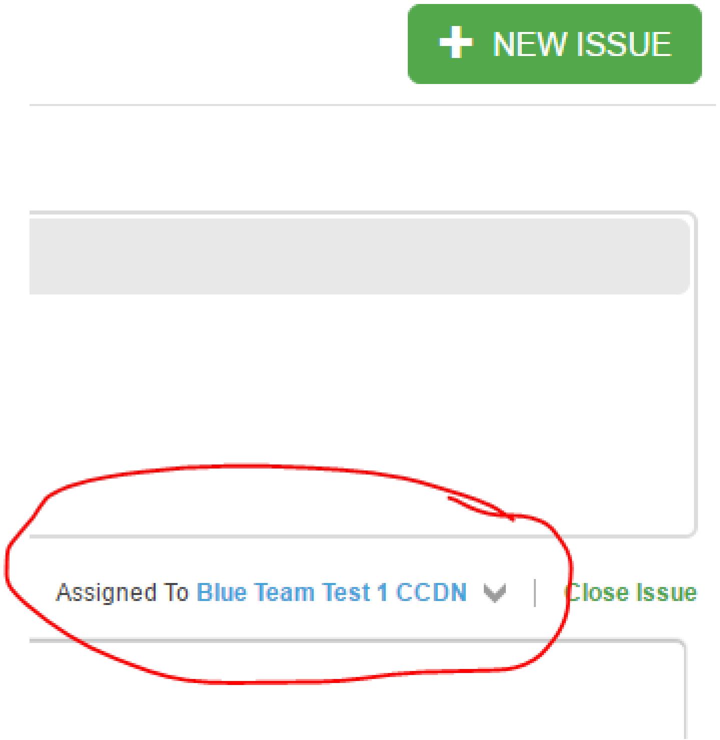
Tags: status:open

Assigned To

Attachments

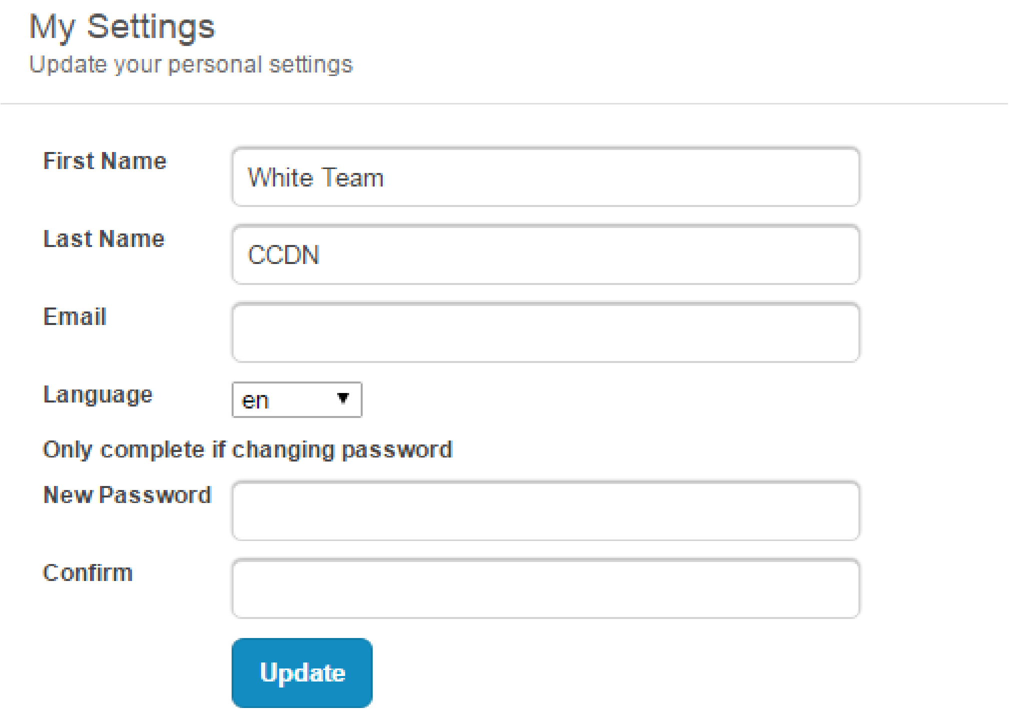
How to I assign an issue to another team?

On the right hand side of the Issue screen is a drop down menu to select which team the issue is assigned to. Just select the team. No further action is required.



How do I change my password?

Click “Welcome, Blue Team X” in the upper right hand corner of the navigation menu and it will take you to the settings screen. Here you can change your password.



My Settings

Update your personal settings

First Name: White Team

Last Name: CCDN

Email:

Language: en

Only complete if changing password

New Password:

Confirm:

Important items

1. Students must use Chrome. Firefox has multiple issues with this system and should not be used.
2. Students must allow Flash to work on this site or they will not be able to upload files. There should be an icon at the end of your browser's address bar to enable this option when creating an issue.
3. Students must change their password ASAP. Passwords can be reset by the White Team.
4. When attaching files, please limit your file types to
    a. .doc
    b. .docx
    c. .xls
    d. .xlsx
    e. .pdf
    f. .txt
    g. .jpg
    h. .jpeg
    i. .png