2016 Minnesota Collegiate Cyber Defense Competition

(Qualifier for the 2016 Erich J. Spengler Midwest Regional CCDC)

Team Packet

Table of Contents

Contents

Midwest CCDC Mission and Objectives

The 2016 Minnesota Collegiate Cyber Defense Competition (CCDC) is one of the Midwest Qualifying CCDCs and 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 Minnesota 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

All Midwest Collegiate Cyber Defence Qualification Competitions are managed by CSSIA, the Center for Systems Security and Information Assurance. The competition is designed to test each student team's ability to secure a networked computer system while maintaining standard business functionality. The scenario involves team members simulating a group of employees from an IT service company that will initiate administration of an IT infrastructure. The teams are expected to manage the computer network, keep it operational, and prevent unauthorized access. Each team will be expected to maintain and provide public services: a web site, a secure web site, an email server, a database server, an online curriculum server, and workstations used by simulated sales, marketing, and research staff as per company policy and mission. Each team will start the competition with a set of identically configured systems.

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

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

Qualifying teams from the 2016 Minnesota CCDC will have the opportunity to participate in the 2016 Erich J. Spengler Midwest Regional CCDC, April 1-2, 2016 at Moraine Valley Comm. College.

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

- **Red Team** – Professional network penetration testers from industry approved by the competition director and industry representatives
  - Scan and map the network of each competition team
  - Attempt to penetrate the defensive capabilities of each Blue Team network and modify any acquired environment
  - Assess the security of each Blue Team network
  - Attempt to capture specific files on targeted devices of each Blue Team network
  - Attempt to leave specific files on targeted devices of each Blue Team network
  - Follow rules of engagement for the competition

- **White Team** – Representatives from industry who serve as competition judges, remote site judges, room monitors and security enforcement in the various competition rooms.

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

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

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

- **Gold Team** – Comprised of the 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 White Team approves the Chief Judge
  - Has the authority to dismiss any team, team member, or visitor for violation of competition rules, inappropriate or unprofessional conduct
  - Makes provision for awards and recognition
  - Manages debrief to teams subsequent to the conclusion of the competition
  - If teams travel to another site, the Gold Team manages activities such as:
    - Greet people
    - Organize food
    - Assist in setting up the competition
    - Assist with hotel / travel arrangements

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

Initial Connection & the Start Flag

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

System 1 - ISE (Inject Scoring System)/Team Portal - This system is totally separate from the competition environment and is used by Blue Teams to display current services, as viewed by the indigenous scoring engine, communicate to the White Team, and receive inject tasks and notifications.

This system is accessed via a browser,

ccdcadmin1.morainevalley.edu

Note that CSSIA supports additional ISE/Team Portals,

ccdcadmin2.morainevalley.edu
ccdcadmin3.morainevalley.edu
ccdcadmin4.morainevalley.edu

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

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

team1, team2, team3, ……

The team password required to access the ISE is distributed, along with team assignment, by a competition manager prior to the scheduled start of the competition. When first connecting to the ISE, a member of the team should check for an initial inject task, usually identified as "Welcome" or something similar. The task simply requests a response back to the competition judges, signaling that access to the ISE has been successful, and that the responding team is ready to compete.

Once the competition judges have verified that all teams are ready to compete, or have provided ample time to respond, the competition judges will release a second inject, providing the team password (applicable to all accounts for a particular team) required to access,

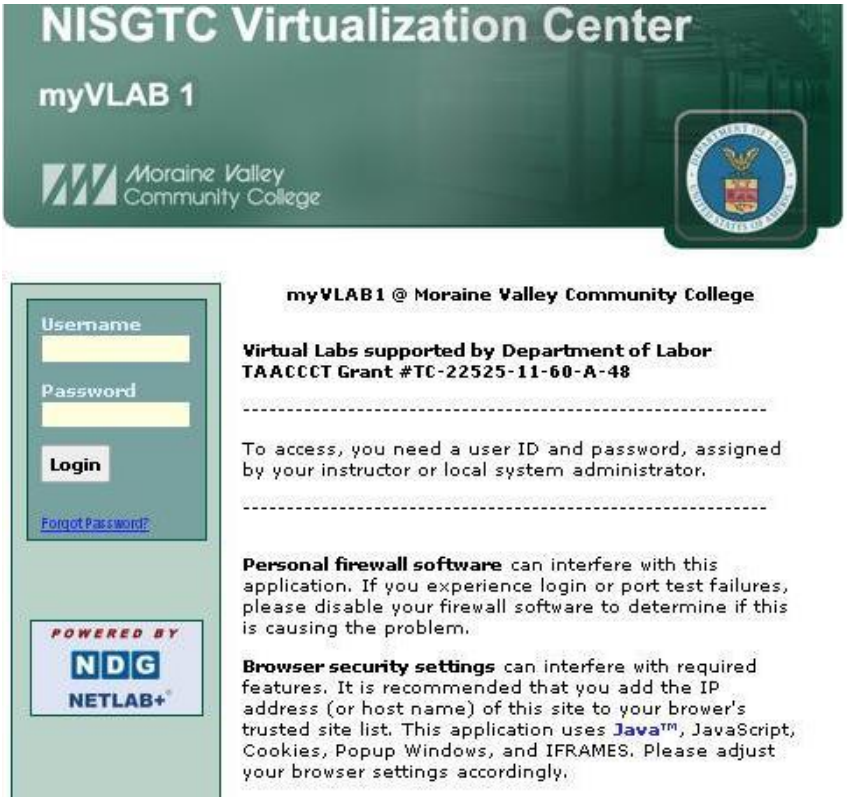
System 2 - The NETLAB+™ / myVLAB Competition Stadium system used to access and manage the competition network. This too is accessed via a browser,

myvlab1.morainevalley.edu

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

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

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



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

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

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

v1u1, v1u2, v1u3, …., v1u8

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

v2u1, ….

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

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

Network & Team Site Description

- Each competition network will be located remotely from the competition site and will be logically isolated from all other competing Blue Teams. All Teams will access the competition network via a browser connection.
- Each competition network will therefore be physically and logically isolated from the hosting organization's network.
- Each competing Blue Team will be provided a set of workstations at a host site that are logically and physically isolated from other Blue Teams in order to access respective remote competition networks via the internet. Alternatively, Blue Teams may compete from their own institution, in which case their institution must provide workstations in conformance with aforementioned requirements. Blue Teams competing from their own institution must do so from a dedicated, secure location where all team members are collocated **together with the local site judge**. Classrooms or conference rooms are considered ideal locations. The secure location is to have restricted access to only Blue Team members, remote site judges, local administrators and technical support. Competition workstations and servers are able to access the internet.
- The White Team and each respective Blue Team will communicate with each other via a trouble ticket and response application, the ISE/Team Portal, residing at Moraine Valley Community College.
- Red Team activity may be either externally or internally sourced with respect to the remote competition network. At no time will the Red Team have access outside the remote NETLAB+™ environment.
- Each Blue Team network will be monitored by a scoring system operating within the remote network. An indication of services, as viewed by the indigenous scoring engine, will be made available to each Blue Team via the ISE/Team Portal.

- A logical diagram of the team logical network is contained within this Team Packet. However, it is subject to change and /or modification as decided by the Competition Manager.

Schedule

February 20, 2016	Illinois CCDC Qualifier
March 5, 2016	Minnesota CCDC Qualifier
March 12, 2016	Iowa, Michigan, Missouri, Wisconsin CCDC Qualifier
March 19, 2016	Indiana, Kentucky, Ohio CCDC Qualifier

Specific time schedules will be deployed by respective CCDC State Directors. 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 White Team members will occasionally need access to a team's systems for scoring, troubleshooting, etc. Teams must allow Green Team and White Team member access when requested.
6. Network traffic generators may be used throughout the competition to generate traffic on each team's network. Traffic generators may generate typical user traffic as well as suspicious or potentially malicious traffic from random source IP addresses throughout the competition.
7. Teams must maintain specific services on the "public" IP addresses assigned to their team and stipulated by this document. Moving services from one public IP to another is not permitted unless directed to do so by an inject. Likewise, teams are not permitted to change the internal addressing or VLAN scheme of the competition network unless directed to do so by an inject.
8. Teams may re-task servers, moving a service from one server to another as long as the outside "public" IP address of the service remains the same. It is the responsibility of the team to understand all the particulars of scoring a service when doing so.
9. Teams are not permitted to alter the system names or IP address of their assigned systems unless directed by an inject; this may affect the results of the scoring mechanism.
10. In the event of system lock or failure, teams will be able to perform a complete restoration from within the administration console of the remote system. This will reset any system to its initial starting configuration. The number of system restorations will be tracked and negatively impact scores at the discretion of the White Team. Teams should also consider that system restoration will take time.

11. Systems designated as user workstations within the competition network are to be treated as user workstations and may not be re-tasked for any other purpose by teams.
12. Teams may not modify the hardware configurations of workstations used to access the competition network.
13. Servers and networking equipment may be re-tasked or reconfigured as needed.

Competition Rules: Acknowledgement & Agreement

Competition rules are applicable to all participants of the NECCDQC. They provide structure for the makeup of student teams, permitted actions during competition play, guidelines for scoring, and contingencies for handling disputes. They also document expectations for appropriate conduct during the entire time participants are guests at a host site, or are competing from their academic institution. Team advisors and all student participants are expected to know and follow all CCDC rules and guidelines. Access to the myVLAB competition environment implies their acknowledgement of competition rules and their commitment to abide by them.

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

Competition Rules: Student Teams

1. Each team will consist of up to no more than eight members. All team advisors have been informed of and will adhere to all national rules. See www.nationalccdc.org
2. Each team may have no more than two graduate students as team members.
3. Each team may have one advisor present during the entire competition – this may be a faculty/staff member or an administrator. Institutions may also send additional faculty representatives with the approval of the Competition Manager. Team advisors and faculty representatives may not assist or advise the team during the competition. Team advisors and faculty representatives may not be involved in any scoring or decisions that involve a participating institution or Blue Team.
4. All team members, the team advisor, and all faculty representatives may be issued badges identifying team affiliation. If issued, they must be worn at all times during competition hours.
5. Each team will designate a Team Captain for the duration of the competition to act as the team liaison between the competition staff and the teams before and during the competition.
6. If the member of a qualifying team is unable to attend the national competition, that team may substitute another student in their place from the submitted roster.

Competition Rules: Professional Conduct

1. All participants are expected to behave professionally at all times they are visiting the host site, or competing from a remote site, and at all preparation meetings.
2. Host site/ local site policies and rules apply throughout the competition.

3. All Cyber Defense Competitions are alcohol free events. No drinking is permitted at any time during the competition.
4. Activities such as swearing, consumption of alcohol or illegal drugs, disrespect, unruly behavior, sexual harassment, improper physical contact, becoming argumentative, or willful physical damage have no place at the competition.
5. In the event of unprofessional conduct, student team members and their advisor will meet with Gold Team members upon request. The consequence of unprofessional conduct will be determined by the Site Administrator with the recommendation of the Gold Team. This may be a warning, point penalty, disqualification, or expulsion from the campus.
6. The Site Administrator or a Gold Team member from CSSIA reserves the right to disqualify an offender from participation in future competitions.

Competition Rules: Competition Play

1. During the competition team members are forbidden from entering or attempting to enter another team's competition workspace or room. They are also forbidden from accessing another Team network, either through their competition network, or by remote access to another team.
2. All requests for items such as software, service checks, system resets, and service requests must be submitted to the White Team. Requests must clearly show the requesting team (do not identify your institution) , action or item requested, and date/time requested. Remote site judges may facilitate this function, or requests may be made via the ISE/Team Portal.
3. Teams must compete without outside assistance from non-team members which includes team advisors and sponsors. All private communications (calls, emails, chat, directed emails, forum postings, conversations, requests for assistance, etc.) with non-team members are forbidden and are grounds for disqualification.
4. No PDAs, memory sticks, CD-ROMs, electronic media, or other similar electronic devices are allowed in the room during the competition unless specifically authorized by the White Team in advance. All cellular calls must be made and received outside of team rooms. Any violation of these rules will result in disqualification of the team member and a penalty assigned to the appropriate team.
5. Teams may not bring any computer, tablets, PDA, or wireless device into the competition area. MP3 players with headphones will be allowed in the competition area provided they are not connected to any system or computer in the competition area.
6. Printed reference materials (books, magazines, checklists) are permitted in competition areas and teams may bring printed reference materials to the competition.
7. Team sponsors and observers are not competitors and are prohibited from directly assisting any competitor through direct advice, suggestions, or hands-on assistance. Any team sponsor or observers found assisting a team will be asked to leave the competition area for the duration of the competition and a point penalty will be assessed against the team.
8. An unbiased Red Team will probe, scan, and attempt to penetrate or disrupt each team's operations throughout the competition.

9. Team members will not initiate any contact with members of the Red Team during the hours of live competition. Team members are free to contact Red Team members, White Team members, other competitors, etc. outside of competition hours.
10. Only Blue Team, White Team or Gold Team members will be allowed in any Blue Team competition room. On occasion, White Team or Gold Team members may escort individuals (VIPs, press, etc.) through the competition area including team rooms. Guest visits must be approved by the Competition Director and are not encouraged as it may distract the Blue Team members during their activities.
11. White, Gold, or Green Team members will be allowed in competition areas outside of competition hours.
12. Teams are free to examine their own systems but no offensive activity against other teams, the White Team, or the Red Team will be tolerated. This includes port scans, unauthorized connection attempts, vulnerability scans, etc. Any team performing offensive activity against other teams, the White Team, the Red Team, or any global asset will be immediately disqualified from the competition. If there are any questions or concerns during the competition about whether or not specific actions can be considered offensive in nature contact the White Team before performing those actions.
13. Blue Team members may change passwords for administrator and user level accounts. Changes to passwords must be communicated according to the White Team guidelines. It is the responsibility of the Blue Team to understand how scoring may be impacted by changing passwords.
14. Blue Team members should maintain ICMP on all competition devices and systems, except the 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 White Team is responsible for implementing the scenario events, refereeing, team scoring and tabulation.
18. Scoring will be based on keeping required services up, controlling/preventing un-authorized access, and completing business tasks in timely manner that will be provided throughout the competition
19. Scores for inject completion and incident reports will be maintained by the White Team, and will not be shared with Blue Team members. Faculty advisors may receive debriefing at the end of the competition. Running totals and comparisons to others teams will not be provided during the competition.
20. If a scenario or event arises that may negatively impact the integrity or fairness of any aspect of the competition that was not previously anticipated, it is the final decision and discretion of the Chief Judge to make adjustments in scores, or deploy new policies.

Competition Rules: Internet Usage

1. Competition systems will have access to the Internet for the purposes of research and downloading patches. Internet activity will be monitored and any team member viewing inappropriate or unauthorized content will be immediately disqualified from the competition. This includes direct contact with outside sources through AIM/chat/email or any other non-public services. For the purposes of this competition inappropriate content includes pornography or explicit materials, pirated media files or software, sites containing key generators and pirated software, etc. If there are any questions or concerns during the competition about whether or not specific materials are unauthorized contact the White Team immediately.
2. Internet resources such as FAQs, how-to's, existing forums and responses, and company websites are completely valid for competition use provided there is no fee required to access those resources and access to those resources has not been granted based on a previous purchase or fee. Only resources that could reasonably be available to all teams are permitted. Teams may not use any external, private electronic staging area or FTP site for patches, software, etc. during the competition. All Internet resources used during the competition must be freely available to all other teams.
3. Public sites such as Security Focus or Packetstorm are acceptable. Only public resources that every team could access if they chose to are permitted. No peer to peer or distributed file sharing clients or servers are permitted on competition networks.
4. All network activity that takes place on the competition network may be logged and is subject to release. Competition officials are not responsible for the security of any personal information, including login credentials that competitors place on the competition network.

Competition Rules: Scoring

1. Scoring will be based on keeping required services up, controlling/preventing un-authorized access, mitigating vulnerabilities, and completing business tasks that will be provided throughout the competition. Teams accumulate points by successfully completing injects, maintaining services, and by submitting incident reports. Teams lose points by violating service level agreements, usage of recovery services, and successful penetrations by the Red Team.
2. Scores will be maintained by the White Team. Individual tracking of services will be available to respective teams during the competition. Blue Team members should use available service tracking reports and internal testing to assess the integrity of their network. Blue Team members should refrain from making direct requests to the White Team for routine service verification.
3. Any team action that interrupts the scoring system is exclusively the fault of that team and will result in a lower score. Should any question arise about specific scripts or how they are functioning, the Team Captain should immediately contact the competition officials to address the issue.
4. Any team that tampers with or interferes with the scoring or operations of another team's systems will be disqualified.
5. Teams are required to provide incident reports for each Red Team incident they detect. Incident reports can be completed as needed throughout the competition and

submitted to the White Team. Incident reports must contain a description of what occurred (including source and destination IP addresses, timelines of activity, passwords cracked, etc), a discussion of what was affected, and a remediation plan. The White Team will assess scores for incident report submission based on clarity, thoroughness, and accuracy. The White Team may also, at their discretion, assess negative scores for frivolous, unnecessary, or excessive communication.

6. The winner will be based on the highest score obtained during the competition. Point values are broken down as follows:

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

Precise percentage breakdown will be determined by the White Team.

Functional Services

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

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

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

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

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

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

Business Tasks

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

Questions and Disputes

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

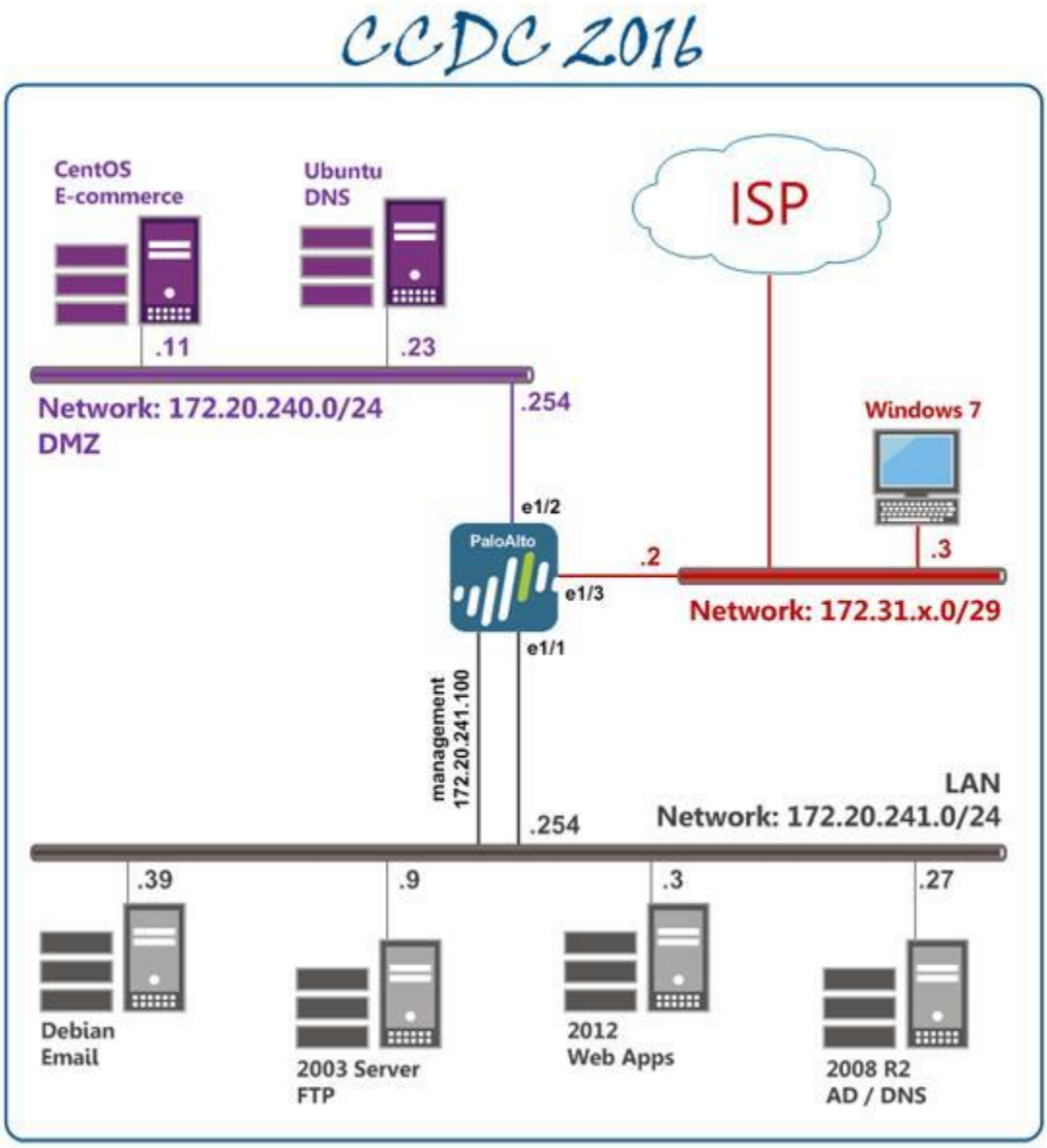
Aftermath

Members of CSSIA, Gold, White, Red, and Green Teams strive to make the NECCDQC 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. 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 NECCDQC, and may also enumerate participating teams and winners.

Competition Topology



- Teams have access to 8 VMs – 6 serves, 1 workstation, and the Palo Alto firewall.
- All servers, workstations, and Palo Alto firewall are virtual machines under the management of NETLAB+™.
- Teams do not have access to the underlying layer 2 switch.
- The firewall shown in the topology is a Palo Alto VM, version 6.0.7, which is licensed by Palo Alto.

  You can access the Palo Alto VM either directly, which yields a command window, or via a browser 172.20.241.100 from any of the LAN VMs.

admin/changeme

Note that this is different from the default username/password that you may have used in an MSEC+ pod.

- Each team has the following Palo Alto internal addresses:

  LAN, e1/1 172.20.241.254/24
  DMZ, e1/2 172.20.240.254/24

- 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

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

VM Label	Major Service	Internal IP	Public IP or pool	Account	initial pwd
CentOS E-Commerce	HTTP/S; FTP	172.20.240.11	172.25.20+team#.11	root	changeme
Ubuntu DNS	DNS	172.20.240.23	172.25.20+team#.23	root	changeme
2003 Server FTP	SQL	172.20.241.9	172.25.20+team#.9	administrator	changeme
Debian Email	Email	172.20.241.39	172.25.20+team#.39	administrator	changeme
2012 Web Apps	Web Apps	172.20.241.3	172.25.team#.3	administrator local	!changeme01
2008 R2 AD/ DNS	AD/DNS	172.20.241.27	172.25.20+team#.27	administrator	changeme
Palo Alto		172.20.241.100	172.25.20+team#.100	admin	changeme
Windows 7 Workstation		172.31.20+team#.3/29	NA	administrator	changeme

This table, minus the ‘public’ translations is accessible on the topology tab of NETLAB+™, via the “Show Lab Content” on the lower right.

Sponsors:

	Department of Homeland Security, http://www.dhs.gov/
	SecureWorks, http://www.secureworks.com
	Palo Alto Networks, https://www.paloaltonetworks.com/
	CSSIA, http://www.cssia.org/

Appendix - Addressing Access Problems to NETLAB+™ Systems

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

Generally the client requirements are easily met with simple browser and java plug-in.

Some browsers will simply download the script upon granting permission. The script then needs to be executed.

The bandwidth requirement likewise seems very reasonable at 256 kb/s up and down. Ports 80, 2201 must be allowed outbound.

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

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

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

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

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

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

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

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

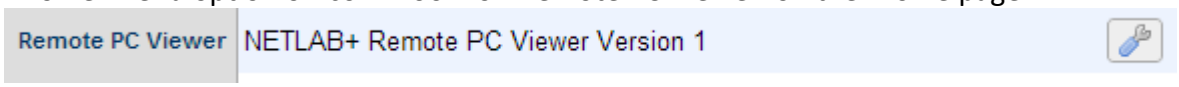
Note that this test may be performed without authenticating into the stadium as long as the url is active. Care should be taken when performing a pathping test to make sure the command completes, which may take several minutes. Experience has shown that connections with more than a few percent loss will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

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

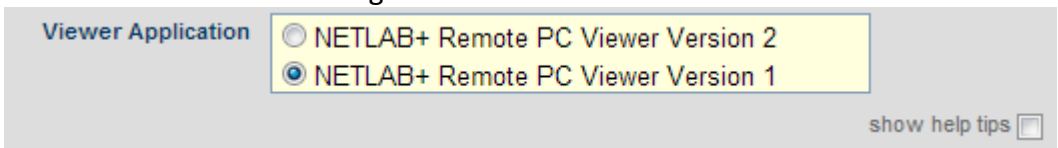
There may be a need for special provisioning at local institutions, even bypassing filters and firewalls for dedicated traffic to the stadium(s). Towards this end it is helpful to note the level of trust and the benign nature of traffic coming from the stadium(s). Though malicious traffic may be present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

Rarely, a remote site will experience difficulty due to packet loss somewhere in route in the big white cloud, and is not a result of faults either at the local site or MVCC. Institutions must contact their ISP to address such difficulties.
Even with excellent connectivity, there may still be problems with using the NETLAB+™ platform. The NETLAB+™ viewer has been programmed using java, and is sensitive to the specific combination of OS/browser/java version being used. With each update of java, the NETLAB+™ viewer may be affected.

Better response is often obtained simply by changing to a different browser. If this is unsuccessful, users may revert back to Viewer 1 instead of the default Viewer 2.
To change to Viewer 1, from the MyNETLAB page on the NETLAB+™ system, click on 'Profile' menu option or icon. Look for 'Remote PC Viewer' on the Profile page.



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



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