San Diego Mayor's Cyber Cup

User's Manual and Rules

November 2015

TABLE OF CONTENTS

9 November 2015

From the Organizers:

San Diego recognizes the need for a work force grounded in the scientific and engineering disciplines, capable of supporting the high technology industrial base that has been essential to the nation's military and, accordingly, the local economy. Beginning in 2009, the San Diego Chapter of the National Defense Industrial Association (NDIA), the Securing our eCITY (SOeC) Foundation, SAIC, and the University of California, San Diego partnered to host a regional competition cyber defense competition for middle and high school students. Now in its seventh year, the San Diego Mayors' Cup* has grown into an annual event where young people with an interest in computer science can compete as network administrators in the important area of cyber security. UCSD, National University and SOeC will coordinate school participation and act as the independent judge to ensure the fairness of this competition. LEIDOS (formerly SAIC) will conduct the competitions using their patent-pending trainer CyberNEXS™ cyber defense system that provides training, exercising, competitions and certification.

To augment our education system and keep pace with the high demand for a cyber- trained "high tech" work force, and equal or surpass other nations, we believe can be addressed by public policy, educators, and corporate America working together. Developing a response that will improve the ability of American students to compete for jobs calling for skills in math science, and engineering requires a partnership of these stakeholders. As representatives of the defense, information technology and education industries of San Diego, we are committed to fostering this partnership and playing an active role in improving the performance of our local students in science, technology, engineering and mathematics (STEM). Additionally, we are committed to encouraging local students to pursue a career in the engineering and scientific fields.

The San Diego Mayors' Cyber Cup computer security competition provides one avenue for attracting and retaining young engineers and scientists. LEIDOS's CyberNEXS™ provides an environment in which students of all levels of knowledge can learn and practically apply their knowledge of computer network operations and their skills at protecting vital computer systems. Through this competition, we hope to increase the level of excitement for learning technology in a stimulating, environment that provides immediate feedback.

Lillian Maestas STEM Lead, San Diego Chapter National Defense Industrial Association	Liz Fraumann Executive Director, Securing our eCITY Foundation	Craig Hardin Securing Our eCITY Youth Program Manager	Chris Simpson Professor, National University	Susan Crowe Training Director, Leidos Cybersecurity

* We take our name from the generous support and encouragement we received from the former Mayor of San Diego, the Honorable Jerry Sanders.

Competition Schedule, 2016 San Diego Mayor's Cyber Cup

September-December (2015): Mentor assignments and training

Monday, January 4 – Friday, January 8: Coach/Mentor WebEx information sessions

Tuesday, January 19 (8 am) – Friday, January 22 (6 pm): Practice Round (6 consecutive hours anytime during that window) - Remote

Monday, February 8 (8 am) – Thursday, February 11 (6 pm): Practice Round (6 consecutive hours anytime during that window) - Remote

Friday, February 26 (8 am) – Saturday, February 27 (6 pm): Qualification Round I (6 consecutive hours anytime during that window) - Remote

Friday, March 4 (8 am) – Saturday, March 5 (6 pm): Qualification Round II (6 consecurive hours anytime during that window) - Remote

Saturday, April 2 (10 am – 5 pm): Finals Round, San Diego Supercomputer Center Auditorium at UCSD

Saturday, April 2 (5:30 – 8:00 pm): Awards Dinner, UCSD Faculty Club Dining Room

History of the Event

In the fall of 2007, the National Defense Industrial Association (NDIA) San Diego Chapter selected cyber security competitions as one of their key Science, Technological, Engineering and Mathematics (STEM) initiatives for 2007-2008. The University of California San Diego (UCSD) Physical Sciences Department and SAIC's Intelligence and Information Systems Business Unit teamed to deliver the NDIA Cyber Defense Competition. In the spring of 2008, five San Diego-based High Schools participated in this proof-of-concept competition. Each school met at the SAIC Campus Point facility, where SAIC provided baseline instruction on Windows Security in the morning, followed by pizza for lunch and then the competition in the afternoon. San Diego Mayor, Jerry Sanders, attended the final event. After the five individual training and exercising events, UCSD hosted a Banquet to announce the winners and present the awards; everyone expressed great interest in when the next competition of this kind could be conducted.

Leidos has developed a third generation competition system called the Cyber Network Exercise System (CyberNEXS™), which provides a highly scalable training, exercising, competition and certification system. This technology and the procedures have been tested and validated during the Air Force Association Cyber Patriot I-VII National High School Cyber Defense competition series, which included several qualification rounds that were run via the Internet. The San Diego Mayor's Office agreed to institutionalize this important STEM outreach activity and, thus, the San Diego Mayors' Cyber Cup (SD MCC) was born. We thank the many businesses, academic institutions and people who have helped evolve this competition to what it is today – a proving ground for youth to engage, explore and find a path towards becoming our future cyber leaders and helping to protect our nation from cyber threats.

NDIA is sponsoring the competition as part of its STEM outreach program. Securing Our eCITY (SOeC) Foundation is again providing scholarships for the top teams. UCSD and SOeC are coordinating the registration of teams. The San Diego Supercomputer Center at UCSD is hosting the Finals Round of the competition. Leidos is providing the competition engine and the labor to conduct this three-phase program. National University is assigning and coordinating mentors for each team along with Red, White and Green Team support. All organizations are providing this support in-kind.

Mission and Objectives

Mission

To encourage and retain students in the degree and certification programs of Science, Technology, Engineering and Mathematics (STEM) disciplines.

Objectives

- Encourage students to learn about information assurance and computer security;
- Provide an educational venue in which students are able to apply the theory and practical skills they have learned;
- Foster a spirit of teamwork, ethical behavior, and effective communication both within and across teams;
- Create interest and awareness among participating schools and students; and,
- Encourage students to consider information assurance and computer security as a possible career path and/or as a possible course of study to pursue in higher education.

Overview of Competition

The San Diego Mayors' Cyber Cup invites all San Diego High Schools and Middle Schools to participate in this three phase cyber defense competition series (discussed in detail below). The first two rounds will be using the distributed competition mode, such that all San Diego County Middle and High Schools can train and then compete simultaneously via the Internet. The eight winners of the qualification round will then participate in a head-to-head comprehensive centralized competition, wherein all teams have individual CyberNEXS™ environments. This environment provides for 8 Blue (Contestant) Teams, Red (Hacker), White (Referee) and Green (Support) Team resources and the scoring system (ScoreBot).

During the final competition, contestants will be scored on their ability to administer the following five essential skills:

1) removing vulnerabilities and hardening systems;
2) maintenance of critical services
3) Length of maintaining system health
4) thwarting and removing hacker activities
5) decoding, decrypting and file carving forensic challenges

The procedures for the 2016 Mayors' Cyber Cup competition are outlined in this document. The finals will be conducted at the UCSD Campus, with eight teams competing head-to-head in a very challenging environment complete with Linux and Windows OS servers and workstations, as well as network and security devices. Each team will be individually scored on a minute-by-minute basis, such that at the end of the day, a winner is declared and then recognized at an Awards Banquet.

Description of Rounds

Practice Rounds

Overview

Practice Rounds – Two practice rounds are offered. These rounds are optional but are highly recommended for new teams unfamiliar with the competition. The practice rounds serve two primary purposes: (1) provide opportunities to validate hardware and network configurations for the qualification rounds, and (2) provide contestants with experiences that will be similar to those presented in the qualification rounds. Contestants will be provided vulnerable targets (i.e. Windows and/or UNIX operating systems as VMware images) that are downloaded to the contestants' personal computers. At the beginning of the Practice Round, they are provided with the password that will unlock the Target contents. Once unlocked, the contestant will register their system via a GUI interface, which will confirm their successful registration. Once that registration is complete they can verify their individual score via a web page linked on their machine. They will then begin to remove all vulnerabilities (harden) prior to end of the Practice Round. During that time, as their score improves, their Scorebot will be automatically updated. The goal is to fix the most vulnerabilities in the fastest time. Additionally contestants will be presented forensics challenges where they decrypt, decode and file carve the downloaded files. Part of forensics is discovering hidden data. Some suspects will try to obfuscate their stolen data. By understanding different encoding and encryption schemes it allows you to find this hidden/obfuscated data. There are tools out there that can decode and decrypt a majority of the challenges. However, you will need to find the tool without our help. Try searching for decoding tools, decrypting tools and file carving tools. You do not need to use Windows exclusively and may be able to use Live Linux CDs/DVDs.

Practice rounds will be timed sessions. Once a team register's their system they will have 6 continuous hours to practice within the environment. Once registered, the timer does not stop, or pause until the 6 hours is completed. You do not have to practice for 6 hours, but this is your limited time frame once you begin. You will not be permitted to create a second account to conduct multiple practice rounds within the same practice window. Only one practice round per team, per practice round.

Rules

1) Student (Blue) Teams

1. While there is no limit to the number of students on a team for the practice and qualification rounds, we recommend teams of 5-8 members since the Finals Round requires teams to consist of 5-8 students.
2. Each team may have one coach/mentor (aka advisor) present during the practice round. The advisor may assist and/or advise the team during the Practice Round Only.

3. Each team will designate a Team Captain for the duration of the competition to act as the team liaison.
4. Contestants may use any computer and any tool, including the Internet, during the conduct of the Practice Round.

2) Practice Systems

1. Each team will use their own computer and begin the competition with identically mis-configured VMware images(s)**.
2. Teams should not assume any competition system is properly functioning or secure; they should act as recently hired administrators who are now assuming responsibility for each of their systems.
3. All teams will be connected to the CyberNEXS™ scoring system, and will have near real-time feedback on their status of completion.
4. If a Team's system is not successfully registered with the CyberNEXS™ server, they will receive no score. Once registered, the Team will receive the score documented by the CyberNEXS™ server when the Team system was last connected.

3) System Requirements for Distributed Competition Contestants

Hardware Requirements are as follows:

a. 1 GHz Intel compatible processor (AMD processors have had issues with VMware and are not recommended);
b. 2 GB RAM;
c. 10 GB of free disk space;
d. Keyboard & Mouse;
e. 1024x768 or higher display;
f. (Optional) It is recommended to use a projector or large display to share the screen output with the rest of the team, but not required; and,
g. Network connection from computer(s) to Internet.

Software Requirements are as follows:

A. Operating System (Windows 2000 or newer, recent VMware supported Linux, or Macintosh 10.4.11 or later);
B. Web Browser;
C. SSH Client;
D. VPN Client; and,
E. VMware Player.

Internet Connectivity Requirements are as follows:

A. Minimum of 256kb uplink/downlink; and,
B. Network firewalls and/or Web Proxies should permit un-filtered TCP port 80 out-bound from your network from each of the computer(s) involved in the competition to the LEIDOS CyberNEXS™ server.

NOTE: VMware image – Using virtualization technology, an entire operating system and resources can be captured as a file, and then replayed (using VMware Player) on a Windows operating systems. In other words, one can run a completely different computer system in a container, within the host operating system, that is on the competitor's computer. **When playing

the Competition, make sure you are taking the appropriate action within the VMware image.

4) Practice Play

The Practice Round will include the following two events:

A) Initial Download– The students will be given a link to download one VMware image 24 to 48 hours prior to the start of the event. The download files will be locked and cannot be opened until 15 minutes prior to the start of the event. Approximately 15 minutes prior to the start of the exercise timeline, an email will be distributed with a password to unlock each of the zip files containing all the exercise materials. These images are hundreds of megabytes in size; therefore, they should be downloaded at the earliest opportunity using the fastest connections available, verified against their published MD5 checksums, and then brought to the computer that will be used for the competition. The Practice Round registration will not be active until STARTEX.

B) Practice Round – The purpose of the Practice Round is to provide Teams with an opportunity to validate that their hardware and network configurations are suitable for the actual competition, as well as provide time to learn about VMware images and how to successfully work and score on them. By successfully registering, the students will know that they are ready to compete by viewing their individual web status page. Once registered, each Team is permitted to "play the competition" and will receive their score via the Feedback page.

IMPORTANT!!! STEPS TO COMPLETE REGISTRATION FOR DISTRIBUTED/FORENSICS ROUND- The practice round will consist of concurrent forensics and distributed competitions. You will need to register your team with the CyberNEXS website in order to submit forensics tickets. The forensics challenges will **not** require a VMware image and will be provided to the contestants in a 7zip file. These are the steps that you need to accomplish in the specified order to successfully register your VMware image with CyberNEXS™:

1. Download Utility Programs

a) Download and install VMware Player: http://www.vmware.com/products/player/
b) Download and install 7-zip: http://www.7-zip.org/
c) Download an MD5 checksum utility: http://www.nullriver.com/products/winmd5sum

2. Download VMware Images and Instructions; Verify MD5 hash:

A link to the target and MD5 hash will be emailed prior to the exercise. The instructions will be made available at the start of the exercise.

a) Download the Practice and Qualification Round Instructions
b) Download the Practice Round Image Zip File [NOTE: MD5 checksum will be listed at time of download, (an example of an MD5 checksum is: fb5bc4b8142d3010a8e7ed0bdef2d195).
c) Download the Qualification Round Image Zip File [NOTE: MD5 checksum will be listed at time of download].

d) Verify the MD5 checksum(s) for both ZIP files, if the numbers don't match, then the down load is corrupt and must be re-downloaded,

3. Verify MD5, Unpack Images and Validate Internet Access

a) Unpack the Practice Round Image Zip File using the password in the instructions document provided at the start of the exercise.
b) Start VMWare Player, and open the Practice Round Virtual Machine (VM).
c) Once the Practice Round VM, has opened inside the VM window - open a web browser.
d) Verify that your Practice Round VM can get to any Internet site (www.google.com, www.cnn.com). (If not then consult with your local IT department for steps to enable.)

4. Registering for Competition

a) Once the Practice Round VM boots, a registration page appears after login. In this registration window select your school from the drop-down menu, enter your team nickname and system name**. IMPORTANT, the nicknames and system names can be anything you want, but all three must be completed and submitted before you can compete. All actions are not scored until you are successfully registered.**
b) Once the Practice Round VM is completely registered a "Get My Status" link will appear in the "C:\" path on the VM. Open this link by double clicking, to show your Status.
c) As you remove vulnerabilities in the Practice VM that were pre-configured for the competition, you should receive notification via this Web Status Page.

5. Play the Competition. You are now done with registration; proceed with getting comfortable with
the competition; your score will tell you how well you are removing vulnerabilities.

Forensics Challenge Instructions

When the exercise begins:

1. Open up http://cybernexs.leidos.com/cndx/ in a web browser.
2. Click on "Login Registrations".
3. Enter your Team Name as your ANALYST Name: **Please only create 1 Account for your team and share the account information with your team members.**
4. Enter a password: **Do not loose the password. If you do you will need to create a new login and you will loose access to all of the previously submitted tickets.**
5. Enter your Team's location.
6. Enter the same Team Name you entered in the ANALYST Name field.

What you need to do is analyze the files in each challenge and report your findings. If you find a "key" in a file then you should submit the whole line for that key in **ALL UPPERCASE LETTERS.**

After you have registered you will need to submit the answers that were found in each of the challenges. This can be done by:

1. Clicking on: Trouble Ticket Interface.
2. Clicking on: Create a New Trouble Ticket.

3. Select Trouble Ticket Type as Other.
4. Enter the deciphered text into the ticket area and then click on Create Ticket.

After you have submitted your ticket you can go to the analyst info page found at: http://cybernexs.leidos.com/cndx/analyst_info.php.

Qualification Rounds

Overview

Qualification Rounds – Two qualification rounds are scheduled. Both rounds are identical in format as described below. Teams **MUST** compete in both qualification rounds, and their **Average** score from both rounds will be used to determine which eight teams are invited to the Finals round.

The format of the qualification rounds is similar to the practice rounds. Contestant teams will be provided vulnerable targets (BOTH Windows and Linux operating systems as VMware images) that are downloaded to the contestants' computers. At the beginning of the Qualification Round, they are provided with the password that will unlock the Target file contents. Once unlocked, the contestant will register their system via a GUI interface, which will confirm their successful registration. Once that registration is complete they can verify their individual score via a web page linked on their machine. They will then begin to remove all vulnerabilities (harden the system) prior to end of the Qualification Round. During that time, as their score improves, their Scorebot will be automatically updated. The goal is to fix the most vulnerabilities in the fastest time. Additionally contestants will be presented forensics challenges where they decrypt, decode and file carve the downloaded files. Contestants will be provided a 7zip file at STARTEX. Answer the forensics questions via the CyberNEXS Web Interface at http://cybernexs.leidos.com/cndx/. The login and registration will be the same as in the Practice Round.

Qualification rounds will be timed sessions. Once a team register's their system they will have 6 continuous hours to repair services and vulnerabilities within the environment. Once registered, the timer does not stop, or pause until the 6 hours is completed. The Forensics Qualification Round is treated as a separate challenge, and has its own 6 hour timer. You may run the challenges consecutively or one after another. You are able to conduct your own schedule to best support your availability. You do not have to run the exercise for 6 hours, but this is your limited time frame once you begin. The Qualification Rounds are scored, so the longer you stay connected and maintain the health of your VMs, the higher your score will climb. You will not be permitted to create a second account to conduct multiple Qualification rounds within the same Qualification window.

Rules

1) Student (Blue) Teams

a) Each team will consist of five (5) to eight (8) student members.

b) Each team may have one advisor present at the competition. The advisor may not assist nor advise the team during the actual qualification round competition.
c) Each team will designate a Team Captain for the duration of the competition to act as the team liaison.
d) Contestants may use any computer and any tool, including the Internet, during the conduct of the competition.
e) Pre-developed scripts are not permitted for competition play. All scripts, and tools must be scripted or initialized onsite for every scored event.
f) The use of staged sites is not permitted. This refers to sites that provide personal storage or the ability to download pre-developed scripts or tools uploaded for later access.
g) Books, magazines, printed materials including notes and blank paper are permitted.
h) The judges' decisions on any subject will be final.

2) Competition Systems

a) Each team will use their own computer and begin the competition with identically mis-configured VMware images(s)**.
b) Teams should not assume any competition system is properly functioning or secure; they should act as recently hired administrators who are now assuming responsibility for each of their systems.
c) All teams will be connected to the CyberNEXS™ scoring system, and will have near real-time feedback on their status of completion.
d) If a Team's system is not successfully registered with the CyberNEXS™ server, they will receive no score. Once registered, the Team will receive the score documented by the CyberNEXS™ server when the Team system was last connected.

**NOTE: VMware image – Using virtualization technology, an entire operating system and resources can be captured as a file, and then replayed (using VMware Player) on a Windows operating systems. In other words, one can run a completely different computer system in a container, within the host operating system, that is on the competitor's computer.

3) Competition Play

This competition series will be conducted using Windows and Linux targets and will include the following Events:

a) Qualification Rounds: The students will be given a link to download one VMware image 24 to 48 hours prior to the start of the event. The download files will be locked and cannot be opened until 15 minutes prior to the start of the event. Approximately 15 minutes prior to the start of the exercise timeline, an email will be distributed with a password to unlock each of the zip files containing all the exercise materials. These images are hundreds of megabytes in size; therefore, they should be downloaded at the earliest opportunity using the fastest connections available, verified against their published MD5 checksums, and then brought to the computer that will be used for the competition. The Practice Round registration will not be active until STARTEX.

4) Scoring

a) The score provided by CyberNEXS for a client system is composed of four component calculations:

- removing vulnerabilities and hardening systems;
- maintenance of critical services
- Length of maintaining system health
- decoding, decrypting and file carving forensic challenges

Note: Red Team activities will not be engaged or scored during the Qualification Rounds, only during the Finals Event.

a) The CyberNEXS Server gathers information to make these calculations in the following ways:
   - Messages communicated from Client to Server reporting the number of vulnerabilities found and fixed on the client system
   - Messages communicated from Client to Server reporting the status of critical services on the Client system
   - Messages communicated from Client to Server reporting intent to reboot
   - Messages communicated from Client to Server reporting ongoing health and availability of the Client System

b) Winners

Winners that will proceed to the finals will be selected as those eight (8) teams that achieve the highest Average scores at the completion of both qualification rounds. Teams MUST compete in both qualification rounds. NDIA will announce the eight finalists within 48 hours, and their names will be listed on the Leidos site: https://www.leidos.com/commercialcyber/cybernexs

If there are two or more teams competing from a single school or group, only one team will be allowed to compete in the finals. For example, if Hometown High School registers two teams and both are among the top eight of the teams ion the qualification rounds, one team from Hometown High will advance to the finals. It will be up to the coach of Hometown High to pick the actual members of his or her team between the two teams for the finals.

1. System Requirements for Distributed Competition Contestants

Hardware Requirements are as follows:

A. 1 GHz Intel compatible processor (AMD processors are not recommended)
B. 2 GB RAM
C. 10 GB of free disk space
D. Keyboard & Mouse
E. 1024x768 or higher display
F. (Optional) It is recommended to use a projector or large display to share the screen output with the rest of the team, but not required
G. Network connection from computer(s) to Internet

Software Requirements are as follows:

A. Operating System (Windows 2000 or newer, recent VMware supported Linux, or Macintosh 10.4.11 or later);
B. Web Browser;
C. SSH Client;
D. VPN Client; and,
E. VMware Player.

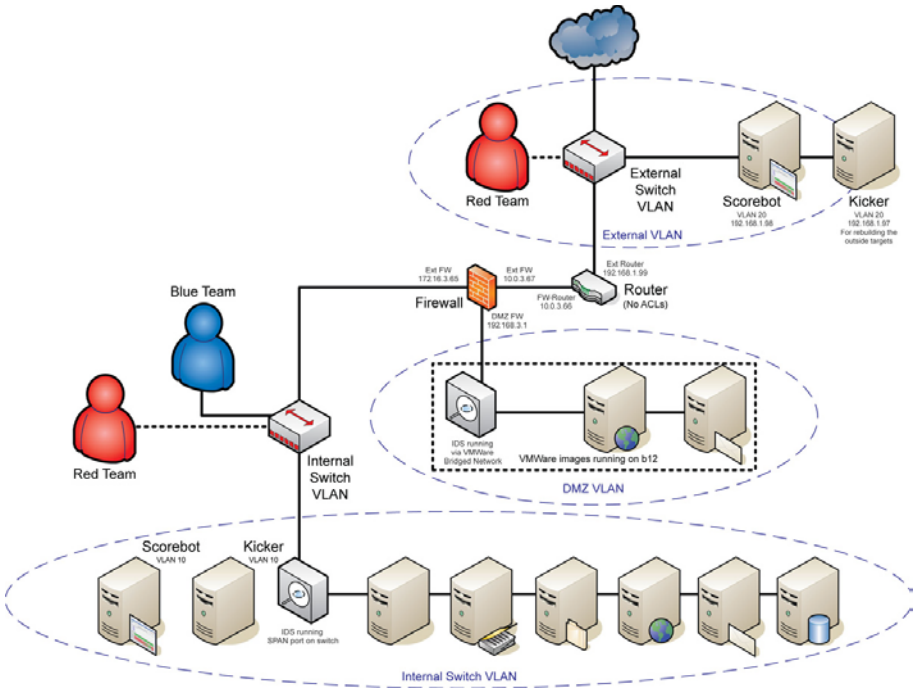
Internet Connectivity Requirements are as follows:

A. Minimum of 256kb uplink/downlink; and,
B. Network firewalls and/or Web Proxies should permit un-filtered TCP port 80 out-bound from your network from each of the computer(s) involved in the competition to the LEIDOS CyberNEXS™ server.

Finals Round

Overview

Finals Round – The finals round of the Mayor's Cyber Cup will be conducted with eight teams going head-to-head in the Leidos CyberNEXS™ centralized competition. This competition provides contestants with their own complete CyberNEXS™ environment, including Windows and Linux operating systems, switches and router, firewalls and intrusion detection devices. At the beginning of the competition, the contestants will log into CyberNEXS™, assume control of their "Blue" (exercise) systems, and begin to harden them as quickly as possible. Sometime later, the "Red" team (hackers) will begin to attack their systems. During all of this activity, contestants are expected to submit trouble tickets to request support. Contestants will also need to solve Forensic Challenges as they did in the Qualification Rounds.



Finals Round Sample Architecture

Rules

1) **Student (Blue) Teams**
   - **a)** Each team will consist of five (5) to eight (8) members. Each team member must be a full-time student of the school or community group/organization they represent.
   - **b)** Each team may have one advisor (coach) present at the competition – this may be a faculty/staff member of the school or a unit sponsor. The advisor may not assist or advise the team at all during the Finals Round. Advisors/coaches will likely be separated from their teams.
   - **c)** All team members will wear badges identifying team affiliation at all times during the competition.
   - **d)** Each team will designate a Team Captain for the duration of the competition to act as the team liaison between the competition staff and their team before and during the competition.
   - **e)** No offensive activity against the competition equipment, the Red Team, or the other teams is allowed. Any activity of this nature will result in the disqualification of the Blue Team conducting it.
   - **f)** The student teams are responsible for:
     i) maintaining the target systems and network defenses;
     ii) reviewing initial system configurations to verify that machines are properly configured and patched against vulnerabilities;
     iii) managing network and host-based systems to thwart any active threat (Red team activity);
     iv) reporting computer misuse to operational staff;

v) NOT modifying in any way users named "CNDXAdmin", "CNDXUser", "CNDXAdm", "CyberNEXS™Admin", "CyberNEXS™User", and "CyberNEXS™Adm". These accounts are used for administration purposes and are not used to gain red team access to your systems;

vi) allowing ICMP (ping) within the internal network and to external devices, other than the firewall; and

vii) following the guidelines set forth in your appropriate network security policy for securing your network.

g) Use of automated patching tools (i.e. Up2date, Windows "Automatic Updates" service, etc.) is not allowed except for identified client machines.

h) Network priorities are availability and security. Basically, do what needs to be done to secure the network without denying services to legitimate users.

i) Pre-created scripts are not allowed to be used for the competition.

j) The use of staged sites is not permitted. This refers to sites that provide personal storage or the ability to download pre-developed scripts or tools uploaded for later access.

k) Printed materials are allowed to be used including notes, paper for taking notes, books, etc.

2) Competition Systems

a) Each team will start the competition with identically configured networked systems.

b) Teams may not remove any computer, printer, or networking device from the competition area.

c) Teams should not assume any competition system is properly functioning or secure; they are assuming recently hired administrator positions and are assuming responsibility for each of their systems.

d) All teams will be connected to a central scoring system.

e) Throughout the competition, White Team members will be responsible for maintaining the competition equipment and can troubleshoot systems that malfunction when this malfunction is not part of the competition itself. White Team members are also responsible for judging functions during the competition.

f) Teams must not connect any outside devices or peripherals to the competition network.

g) Teams are not permitted to remove or alter any labels/stickers that are present on their assigned systems.

h) Teams may not modify the hardware configurations of competition systems. Teams must not open the case of any server, printer, PC, monitor, KVM, router, switch, firewall, or any other piece of equipment used during the competition. All hardware related questions and issues should be referred to the White Team.

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

1) Enumeration, discovery, and port scanning using RFC-compliant ICMP packets and TCP and UDP connections
2) Attempted logins using guessed and discovered account names and passwords
3) Network sniffing, traffic monitoring, and traffic analysis
4) Use of exploit code for leveraging discovered vulnerabilities
5) Password cracking via capture and scanning of authentication databases
6) Spoofing or deceiving servers regarding network traffic
7) Alteration of running system configuration except where denial of service would result
8) Denial of service attacks, directed, distributed, or otherwise
9) Scanning of user file content
10) Introduction of viruses, worms, Trojan horses, or other malicious code
11) Alteration of system configuration stored on disk
12) Changing passwords or adding user accounts
13) Spoofing or deceiving servers via dynamic routing updates or name service (DNS)

3) Competition Play

a. The competition will be conducted over a seven-hour period (one hour for lunch).
b. Operating Systems: Windows and Linux
Other devices: Firewalls, Intrusion Detection System (IDS), Switches and Routers, Network Management System and a Trouble Ticketing System.
c. The number of "Blue" Targets: Eight
d. The competition will be conducted for six hours (10AM-5PM) and the competition play will freeze for one hour during lunch.
e. During the competition team members are forbidden from entering or attempting to enter another team's competition workspace.
f. Teams must compete without "outside assistance" from non-team members, which includes team advisors (coach/mentor) and sponsors. All private communications (calls, emails, chat, directed emails, forum postings, conversations, requests for assistance, etc.) with non-team members, including team sponsors that would help the team gain an unfair advantage, are not allowed and are grounds for disqualification.
g. No PDAs, memory sticks, CDROMs, 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 competition area. Any violation of these rules will result in disqualification of the team member and a penalty assigned to the member's team.
h. Teams may not bring any computer, tablets, PDA, or other wireless devices into the competition area. Laptop computers (Windows XP), intrusion detection systems (Snort) and an on-line library of software resources will be provided for the student's use.
i. Printed reference materials (books, magazines, checklists) are permitted in competition areas and teams may bring printed reference materials to the competition.
j. 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.

k. Team members will not initiate any contact with members of the Red Team during the hours of live competition. Team members are free to talk to Red Team members, White Team members, other competitors, etc. outside of competition hours.
l. On occasion, White Team members may escort individuals (VIPs, press, etc.) through the competition area.
m. Only White Team members will be allowed in competition areas outside of competition hours.
n. Teams are free to examine their own systems but no offensive activity against the White Team, other teams, 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 or the Red Team 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.
o. Teams that are the most successful are those who proactively collaborate among their teammates.

4) Scoring

a) There will be one champion declared at the completion of the competition; the 2016 Mayors' Cyber Cup Champion will be the team with the highest overall score.
b) Scores will be monitored by the White Team, but will not be shared until the end of the competition day.
c) Any team that tampers with or interferes with the scoring system (ScoreBot) or with another team will be disqualified.
d) Students will be evaluated in five skill areas:

- removing vulnerabilities and hardening systems;
- maintenance of critical services
- Length of maintaining system health
- thwarting and removing hacker activities
- decoding, decrypting and file carving forensic challenges

e) Scoring will be weighted in the following way to determine the Final score for the Finals Event:

- Forensics -- 20%
- Windows Vulnerabilities -- 17.5%
- Windows Critical Services -- 12.5%
- Windows System Health (length of maintaining each healthy system) -- 10%
- Linux Vulnerabilities -- 17.5%
- Linux Critical Services -- 12.5%
- Linux System Health (length of maintaining each healthy system) -- 10%

5) Questions and Disputes

a. Team captains are encouraged to work with the competition officials to resolve any questions or disputes regarding the rules of the competition or scoring methods before the competition begins.
b. Protests by any team will be presented by the Team Captain to the competition officials as soon as possible. The competition 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.
c. In the event of an individual disqualification, that team member must leave the competition area immediately and must not re-enter the competition area at any time. Disqualified individuals are ineligible for any awards.
d. In the event of a team disqualification, the entire team must leave the competition area immediately and is ineligible for any individual or team award.

Scoring Described

The score provided by CyberNEXS for a client system is composed of five component calculations:

1) Removing vulnerabilities and hardening systems;
2) Maintenance of critical services
3) Length of maintaining system health
4) Thwarting and removing hacker activities
5) Decoding, decrypting and file carving forensic challenges

The CyberNEXS Server gathers information to make these calculations in the following ways:

- Messages communicated from Client to Server reporting the number of vulnerabilities found and fixed on the client system
- Messages communicated from Client to Server reporting the status of critical services on the Client system
- Messages communicated from Client to Server reporting intent to reboot
- Messages communicated from Client to Server reporting ongoing health and availability of the Client System

What Happens During an Exercise

When a Client registers with the CyberNEXS Server, the client receives profiles from the Server which describe the vulnerabilities that the Client should look for, and the critical services that should be maintained. When the exercise begins, the Server begins to process reports from Clients about the status of vulnerabilities and services. Points for each Client are calculated at a regular interval based on the reports, and these points are used in the calculation of scores.

The CyberNEXS Server expects to receive periodic Health Messages from registered Clients at an interval specified at the time of registration. The HealthMessage indicates that the Client system is up. The HealthMessage also contains information about the Client system's CPU, memory and disk usage. If the Server fails to receive a Health Message from a Client within the specified interval, that Client is marked as "down".

During an exercise, the Red Team will attempt to penetrate and manipulate a target system within a team's network. If the Red Team successfully gains access into a target system and is able to alter one of the vulnerabilities or services being scored on, the team will no longer gain points for the repaired vulnerability. If the team is unable to kick the red team out of the target, they will continue to alter repaired vulnerabilities affecting the team's ability to continue to gain points. It is up to the team to protect their systems from intrusion and repair any damages done by any successful intrusions.

Scoring Results

The CyberNEXS Team reviews the status of scores for all registered clients participating in an exercise. Each team is represented with an individual status and score of each Client as well as a comparison of all Clients. The CyberNEXS Team monitors a timeline of system and service uptimes, as well as the fixed or unfixed state of vulnerabilities identified on the Client systems. The CyberNEXS scoring server monitors scores in multiple capacities:

The CyberNEXS scoring server uses an algorithm to calculate a numbered score based on the performance from each recorded client based on the 5 categories listed at the top of this section. Once calculated, the score is output for a final tally of points earned for the exercise.

Stability of the CyberNEXS™ Scoring System

CyberNEXS is designed to ensure that any information communicated between Clients and the Server is reliably delivered. Queuing and re-transmission of messages on both Client and Server systems mitigates loss of network connectivity or downtime at either end of the communications link. When messages are successfully delivered to the Server, they are processed, and the information is stored in a database. Thus, the CyberNEXS Server is able to score Clients based on the most complete information available.

Ethical and Legal Considerations

During the competition students will learn to use a variety of tools to defend networks and computer systems. Participants are reminded that these tools should never be used to probe, scan or gain access to a system without proper authorization by the system owner. In many cases use of these tools in an unauthorized manner may be a violation of Federal or State law

Description of CyberNEXS ™

CyberNEXS™ Overview

In today's increasing hostile communications environment, a strong computer network defense (CND) program is the key to an organization maintaining maximum availability and security of their data networks. To most effectively prepare an IT organization, the "Security Team" needs to routinely train, as they would operate in their everyday environment. They need to not only rehearse against realistic attack scenarios but they must also train on IT systems that mirror their own infrastructure. Finally, training as a Team is critical to ensure that they can administer and coordinate the many functions of computer network defense, which include: secure system configuration, intrusion detection, incident analysis, forensics, misuse data collection and incident mitigation. In response to this need, LEIDOS developed the Cyber Network EXercise System (CyberNEXS™), which assists the organization's Chief Information Office (CIO) in the training and evaluation of their CND team's ability to detect network attacks/intrusions and defend their critical information resources from those attacks. It provides near-real time feedback in a realistic environment where new network defense tactics, techniques and procedures (TTP) can be developed, tested and integrated.

The LEIDOS CyberNEXS™ system was selected as the competition platform because of its scalability, real world IT systems, and scoring system that produces high fidelity, credible feedback of contestant's progress. The CyberNEXS™ service is performed in a controlled training environment, emulating real-world systems and threat activity. The training environment should include representative network, server and workstation systems that the students are expected to configure and maintain in the highest state of readiness. Additionally, an evaluation system has been implemented that will automatically sample system configurations to ensure that the students have installed the most up-to-date vulnerability fixes. It will also determine whether or not a system has been successfully attacked and whether critical services are being interrupted.