NorthEast Regional
Collegiate
Cyber
Defense
Competition

2011 Northeast Regional Cyber Defense Competition

Hosted by Northeastern University

College of Computer and Information Science

March 4 – March 6, 2011

Team Packet

Table of Contents

NorthEast Regional
Collegiate
Cyber
Defense
Competition

Welcome Letter

On behalf of Northeastern University, College of Computer and Information Science, we would like to welcome you to the 2011 Northeast Collegiate Cyber Defense Competition (NECCDC). The NECCDC event has been an outstanding learning experience for the students. Many of the students have gained a great deal of experience, and even employment offers from industry sponsors, during these events. This training event will greatly benefit the students, their prospective employers and will address societal and national needs for increased cyber security.

We would also like to recognize our sponsors whose generous support has made this event possible:

- University of Texas at San Antonio, as the prime CCDC contractor for the Department of Homeland Security
- EMC Corporation for providing their Training Center in Franklin, MA, as the venue for the NECCDC competition, and many volunteers
- Microsoft Corporation for providing the software licenses used by the competing teams
- Many individuals on the White, Red and Black teams who have given their time and worked tirelessly to ensure the success of this event

We wish you best of luck for your preparation and for the competition. Each team that shows up with at least six team members and a faculty/staff coach will receive a $750 travel assistance grant. In addition the winner team will receive travel expenses to compete at the National Collegiate Cyber Defense Competition to be held April 8-10, 2011 in San Antonio, Texas.

Sincerely,

Themis A. Papageorge, Ph.D.
Director of Information Assurance
Associate Clinical Professor
College of Computer and Information Science
Northeastern University

Competition Schedule

Friday – March 4

11:00 AM	Registration opens
11:30 AM	Opening announcements and orientation
12:30 PM – 1:00 PM	Lunch Available
1:00 PM	Competition Day 1 begins
7:00 PM	Competition Day 1 complete

Saturday – March 5

8:15 AM – 8:45 AM	Continental Breakfast Available
8:45 AM	Day 2 Announcements
9:00 AM	Competition Day 2 begins
12:00 PM – 1:00 PM	Lunch available (No break in competition)
7:00 PM	Competition Day 2 complete
7:00 PM – 8:30 PM	Networking Event with Sponsors' hiring recruiters

Sunday – March 6

7:15 AM – 7:45 AM	Continental Breakfast Available
7:45 AM	Day 3 Announcements
8:00 AM	Competition Day 3 begins
11:00 PM	Competition Day 3 complete
1:00 PM – 3:00 PM	Luncheon and awards ceremony

Overview

On February 27 and 28, 2004, a group of educators, students, government and industry representatives gathered in San Antonio, Texas, to discuss the feasibility and desirability of establishing regular cyber security exercises with a uniform structure for post-secondary level students. During their discussions this group suggested the goals of creating a uniform structure for cyber security exercises might include the following:

1. Providing a template from which any educational institution can build a cyber security exercise
2. Providing enough structure to allow for competition among schools, regardless of size or resources
3. Motivating more educational institutions to offer students an opportunity to gain practical experience in information assurance

The group also identified concerns related to limiting participation to post-secondary students, creating a level playing field to eliminate possible advantages due to hardware and bandwidth differences, having a clear set of rules, implementing a fair and impartial scoring system, and addressing possible legal concerns.

In an effort to continue this new tradition of a regular, national level cyber security exercises, the Networking, Security and Systems Administration Department at the Rochester Institute of Technology agreed to host the first Regional Collegiate Cyber Defense Competition (CCDC) for the Northeastern region. This year marks the fourth annual Northeastern regional competition, which is hosted for the first time by Northeastern University. While similar to other cyber defense competitions in many aspects, the CCDC is unique in that it focuses on the operational aspect of managing and protecting an existing network infrastructure. While other exercises examine the abilities of a group of students to design, configure, and protect a network over the course of an entire semester, this competition is focused on the more operational task of assuming administrative and protective duties for an existing “enterprise” network. Teams will be scored based on their ability to detect and respond to outside threats, maintain availability of existing services such as mail servers and web servers, respond to business requests such as the addition or removal of additional services, and balance security needs against business needs. To create a fair and even playing field:

- Each team will begin with an identical set of hardware and software: Each team will be given a small, pre-configured, operational network they must secure and maintain. This eliminates any potential advantage for larger schools or organizations that may have better equipment or a larger budget.
- Each team will be located on a dedicated internal network: To remove the variables associated with VPNs and propagation delay each team’s network will be connected to a competition network allowing equal bandwidth and access for scoring and Red Team actions. This also allows tight control over competition traffic.

- Each team will be provided with the same objectives and tasks: Each team will be given the same set of business objectives and tasks at the same time during the course of the competition.
- Only team members and White Team members will be allowed inside their competition rooms: Each team will be assigned their own room during the competition and only the members of the student team will be allowed inside during the competition. This eliminates the potential influence of coaches during the competition.
- A non-biased Red Team will be used: A non-biased, volunteer, experienced Red Team consisting of IA professionals will be used during the competition.

CCDC Mission and Objectives

Mission

The Collegiate Cyber Defense Competition (CCDC) system provides institutions with an information assurance or computer security curriculum a controlled, competitive environment to assess their student's depth of understanding and operational competency in managing the challenges inherent in protecting a corporate network infrastructure and business information systems.

Event Objectives

- Build a meaningful mechanism by which institutions of higher education may evaluate their programs.
- Provide an educational venue in which students are able to apply the theory and practical skills they have learned in their course work.
- Foster a spirit of teamwork, ethical behavior, and effective communication both within and across teams.
- Create interest and awareness among participating institutions and students.

National CCDC Competition Rules

1. Competitor Eligibility

a. Competitors in CCDC events must be full-time students of the institution they are representing.

i. Team members must qualify as full-time students as defined by the institution they are attending.

ii. Individual competitors may participate in CCDC events for a maximum of five seasons. A CCDC season is defined as the period of time between the start of the first state event and the completion of the National CCDC event. Participation on a team in any CCDC event during a given season counts as participation for that entire season.

iii. A competitor in their final semester prior to graduation is exempt from the full-time student requirement and may compete in CCDC events as a part-time student provided the competitor has a demonstrated record of full-time attendance for the previous semester or quarter.

iv. If a team member competes in a qualifying, state, or regional CCDC event and graduates before the next CCDC event in the same season, that team member will be allowed to continue to compete at CCDC events during the same season should their team win and advance to the next round of competition.

b. Competitors may only be a member of one team per CCDC season.

2. Team Composition

a. Each team must submit a roster of up to 12 competitors to the competition director of the first CCDC event they participate in during a given CCDC competition season. Rosters must be submitted at least two weeks prior to the start of that event. All competitors on the roster must meet all stated eligibility requirements. No changes to the team roster will be permitted after the team competes in their first CCDC event. The competition team must be chosen from the submitted roster. A competition team is defined as the group of individuals competing in a CCDC event.

b. Each competition team may consist of up to eight (8) members chosen from the submitted roster.

c. Each competition team may have no more than two (2) graduate students as team members.

d. If the member of a competition team advancing to a qualifying, state, regional, or national competition is unable to attend that competition, that team may substitute another student from the roster in their place prior to the start of that competition.

e. Once a CCDC event has begun, substitutions or additions of team members are prohibited. A team must complete the competition with the team that started the competition.

f. 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. In the event of the Team Captain’s absence, teams must have an identified team liaison serving as the captain in the competition space at all times during competition hours.

g. An institution is only allowed to compete one team in any CCDC event or season.

3. Team Representatives

a. Each team must have at least one representative present at every CCDC event. The representative must be a faculty or staff member of the institution the team is representing.

b. Once a CCDC event has started, representatives may not coach, assist, or advise their team until the completion of that event (including overnight hours for multi-day competitions).

c. Representatives may not enter their team’s competition space during any CCDC event.

d. Representatives must not interfere with any other competing team.

e. Except in the event of an emergency, a representative must avoid contact with their team during CCDC competition hours and must not attempt to influence their team’s performance in any way.

4. Competition Conduct

a. Throughout the competition, Operations and White Team members will occasionally need access to a team’s system(s) for scoring, troubleshooting, etc. Teams must immediately allow Operations and White Team members’ access when requested.

b. Teams must not connect any devices or peripherals to the competition network unless specifically authorized to do so by Operations or White Team members.

c. 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.

d. Teams may not remove any item from the competition area unless specifically authorized to do so by Operations or White Team members including items brought into the team areas at the start of the competition.

e. Team members are forbidden from entering or attempting to enter another team’s competition workspace or room during CCDC events.

f. Teams must compete without “outside assistance” from non-team members including team representatives from the start of the competition to the end of the competition (including overnight hours for multi-day events). All private communications (calls, emails, chat, texting, directed emails, forum postings, conversations, requests for assistance, etc) with non-team members including team representatives that would help the team gain an unfair advantage are not allowed and are grounds for disqualification and/or a penalty assigned to the appropriate team.

g. No memory sticks, flash drives, removable drives, CDROMs, electronic media, or other similar electronic devices are allowed in the room during the competition unless specifically authorized by the Operations or White Team in advance. Any violation of these rules will result in disqualification of the team member and/or a penalty assigned to the appropriate team.

h. All cellular calls, texts, smart phone usage, and so on must be made and received/viewed outside of the team’s competition space and must not be used to receive outside assistance. Any violation of these rules will result in disqualification of the team member and/or a penalty assigned to the appropriate team.

i. Teams may not bring any computer, laptop, tablets, PDA, or wireless device into the competition area unless specifically authorized by the Operations or White Team in advance. Any violation of these rules will result in disqualification of the team member and/or a penalty assigned to the appropriate team.

j. Printed reference materials (books, magazines, checklists) are permitted in competition areas and teams may bring printed reference materials to the competition.

k. 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/or a penalty will be assigned to the appropriate team.

l. 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 during official competition events such as breakfasts, dinners, mixers, and receptions that occur outside of live competition hours.

m. Teams are free to examine their own systems but no offensive activity against other teams, the Operations Team, 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 Operations Team, 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 Operations Team before performing those actions.

n. 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.

o. All team members will wear badges identifying team affiliation at all times during competition hours.

p. Only Operations Team/White Team members will be allowed in competition areas outside of competition hours.

5. Internet Usage

a. 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 membership, 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. Public sites such as Security Focus or Packetstorm are acceptable. Only public resources that every team could access if they chose to are permitted.

b. Teams may not use any external, private electronic staging area or FTP site for patches, software, etc. during the competition. Teams are not allowed to access private Internet-accessible libraries, FTP sites, web sites, network storage, or shared drives during the competition. All Internet resources used during the competition must be freely available to all other teams. Accessing private staging areas is grounds for disqualification and/or a penalty assigned to the appropriate team.

c. No peer to peer or distributed file sharing clients or servers are permitted on competition networks unless specifically authorized by the competition officials.

d. Internet activity, where allowed, will be monitored and any team member caught viewing inappropriate or unauthorized content will be subject to disqualification and/or a penalty assigned to the appropriate team. This includes direct contact with outside sources through AIM/chat/email or any other public or non-public services including sites such as Facebook. For the purposes of this competition inappropriate content includes pornography or explicit materials, pirated media files, 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.

e. All network activity that takes place on the competition network may be logged and subject to release. Competition officials are not responsible for the security of any information, including login credentials, which competitors place on the competition network.

6. Permitted Materials

a. No memory sticks, flash drives, removable drives, CDROMs, electronic media, or other similar electronic devices are allowed in the room during the competition unless specifically authorized by the Operations or White Team in advance. Any violation of these rules will result in disqualification of the team member and/or a penalty assigned to the appropriate team.

b. Teams may not bring any type of computer, laptop, tablet, PDA, cell phone, smart phone, or wireless device into the competition area unless specifically authorized by the Operations or White Team in advance. Any violation of these rules will result in disqualification of the team member and/or a penalty assigned to the appropriate team.

c. Printed reference materials (books, magazines, checklists) are permitted in competition areas and teams may bring printed reference materials to the competition as specified by the competition officials.

7. Professional Conduct

a. All participants, including competitors, coaches, White Team, Red Team, Operations Team, and Gold Team members, are expected to behave professionally at all times during all CCDC events including preparation meetings, receptions, mixers, banquets, competitions and so on.

b. In addition to published CCDC rules, Host Site policies and rules apply throughout the competition and must be respected by all CCDC participants.

c. All CCDC events are alcohol free events. No drinking is permitted at any time during competition hours.

d. Activities such as swearing, consumption of alcohol or illegal drugs, disrespectful or unruly behavior, sexual harassment, improper physical contact, becoming argumentative, willful violence, or willful physical damage have no place at the competition and will not be tolerated.

e. Violations of the rules can be deemed unprofessional conduct if determined to be intentional or malicious by competition officials.

f. Competitors behaving in an unprofessional manner may receive a warning from the White Team, Gold Team, or Operations Team for their first offense. For egregious actions or for subsequent violations following a warning, competitors may have a penalty assessed against their team, be disqualified, and/or expelled from the competition site. Competitors expelled for unprofessional conduct will be banned from future CCDC competitions for a period of no less than 12 months from the date of their expulsion.

g. Individual(s), other than competitors, behaving in an unprofessional manner may be warned against such behavior by the White Team or asked to leave the competition entirely by the Competition Director, the Operations Team, or Gold Team.

8. Questions and Disputes, Disclosure

a. PRIOR TO THE COMPETITION: Team captains are encouraged to work with the Competition Director and their staff to resolve any questions regarding the rules of the competition or scoring methods before the competition begins.

b. DURING THE COMPETITION: Protests by any team must be presented in writing by the Team Captain to the White Team as soon as possible. The competition officials will be the final arbitrators for any protests or questions arising before, during, or after the competition. Rulings by the competition officials are final. All competition results are official and final as of the Closing Ceremony

c. 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 or team awards.

d. 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.

e. All competition materials including injects, scoring sheets, and team-generated reports and documents must remain in the competition area. Only materials brought into the competition area by the student teams may be removed after the competition concludes.

9. Scoring

a. Scoring will be based on keeping required services up, controlling/preventing un-authorized access, and completing business tasks that will be provided throughout the competition. Teams accumulate points by successfully completing injects and maintaining services. Teams lose points by violating service level agreements, usage of recovery services, and successful penetrations by the Red Team.

b. Scores will be maintained by the competition officials and may be shared at the end of the competition. There will be no running totals provided during the competition. Team rankings may be provided at the beginning of each competition day.

c. Any team action that interrupts the scoring system is exclusively the responsibility of that team and will result in a lower score. Should any question arise about scoring, the scoring engine, or how they function, the Team Captain should immediately contact the competition officials to address the issue.

d. Teams are strongly encouraged to provide incident reports for each Red Team incident they detect. Incident reports can be completed as needed throughout the competition and presented to the White Team for collection. Incident reports must contain a description of what occurred (including source and destination IP addresses, timelines of activity, passwords cracked, access obtained, damage done, etc), a discussion of what was affected, and a remediation plan. A thorough incident report that correctly identifies a successful Red Team attack may reduce the Red Team penalty for that event by up to 50 percent – no partial points will be given for incomplete or vague incident reports.

10. Regional Rules

a. No personal-only use or non-commercial trial software is allowed. Only commercial trials or free use software (e.g. Apache License, GPL) are allowed. Violations of EULA's is considered a severe offense and can be subject to any sanctions deemed necessary by the Competition Staff.

NECCDC Competition - Best Practices Competitors Need to Know

Overview

The competition is designed to test each student team's ability to secure networked computer systems while maintaining standard business functionality. The scenario involves team members simulating a group of new employees that have been brought in to manage and protect the IT infrastructure at a small to medium sized IT services company/reseller. The teams are expected to manage the computer network, keep it operational, and control/prevent any unauthorized access. Each team will be expected to maintain and provide public services: a web site, an email server, a database server, an application server, and workstations used by simulated sales, marketing, and research staff. Each team will start the competition with a set of identically configured systems.

The objective of the competition is to measure each 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. A technical success that impacts the business operation will result in a lower score as will a business success which results in security weaknesses. A detailed business scenario will be distributed along with technical specifications prior to the exercise to allow teams to develop their team and capabilities.

Systems

- Student teams will be given identical hardware and software installations to configure and support.
- Student teams will be provided the system architecture and initial set-up prior to the event to permit planning.
- Student teams should not assume any system is properly functioning or secure; they are assuming recently hired administrator positions and are assuming responsibility for each of their systems.
- All teams will be connected to a central router and scoring system.
- Network traffic generators will be used throughout the competition to generate traffic on each team's network.
- Teams are permitted to replace applications and services provided they continue to provide the same content, data, and functionality of the original service. For example, one mail service may be replaced with another provided the new service still supports standard SMTP commands, supports the same user set, and preserves any pre-existing messages users may have stored in the original service. Failure to

preserve pre-existing data during a service migration will result in a 50 point penalty for each service.

- All SMTP services using authorization must support AUTH LOGIN and base64 encoded userids and passwords.
- Teams are strongly encouraged to provide incident reports for each Red Team incident they detect. Incident reports can be completed as needed throughout the competition and presented to the White Team for collection. Incident reports must contain a description of what occurred, a discussion of what was affected, and a remediation plan. A thorough incident report that correctly identifies a successful Red Team attack will reduce the Red Team penalty for that attack by 50 percent.
- Each student team may change passwords for administrator level and user level accounts. Any password changes to user accounts must be provided to the White Team with a minimum of 15 minutes advance warning prior to the changes being implemented (unless the password changes are part of a competition tasking). Failure to notify the White Team of user level password changes could result in service check failures. Teams are required to provide modified passwords in the electronic format specified. Please note that the White Team will not error check the provided password changes – they will simply upload the provided changes.
- Student 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 competition. Moving services from one public IP to another is not permitted.
- Student teams are not permitted to alter the system names of their assigned systems.
- The White Team will provide a mechanism to show teams the official status of their critical services during the last scored service check.
- Teams will have access to a “Restore from Backup” capability that will reset any system to its initial starting configuration. This service will be performed by the White Team and will cost the team 50 points per system recovered.
- Each student team will be provided with a set of install disks for the operating systems and major applications used in the competition network. These may be used to reload systems, add/remove functionality, reinstall, etc.
- Systems designated as “workstations” are to be treated as user workstations and may not be re-tasked for any other purpose by student teams. They must remain user workstations throughout the entire competition unless otherwise directed by a White Team member. Other hardware platforms, such as servers and networking equipment, may be re-tasked or reconfigured as needed.

How the Winner is Determined – Scoring Methodology

The winner will be based on the highest cumulative score at the end of the competition. During this competition a team may accumulate a total maximum of 5,000 points. Accumulated point values are broken down as follows:

- Functional services (based on a random polling interval of core services): 2,448 possible points
- Successful completion of business tasks: Awarded points will vary by task for a possible total of 2,552

Successful Red Team actions will result in point deductions from a team's total score based on the level of access obtained, the sensitivity of information retrieved, etc.

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 5 minute intervals, certain services will be tested for function and content where appropriate. Each successfully served request will gain the team the specified number of points.

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 specific page 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. SMTP services must be able to support either unauthenticated sessions or sessions using AUTH LOGIN (base64) at all times.

SSH

An SSH session will 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.

SQL

An SQL request will be made to the database server. The result will be stored and compared against an expected result. Each successfully served SQL request will be awarded points.

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

The official list of required services will be provided at the start of the competition.

Each of the required services operates under a Service Level Agreement and teams will be assessed penalties for extended outages of critical services. For example, if a critical service is down continuously for over 1 hour, the team will be assessed a 20 point penalty **<u>for each hour</u>** the service is down.

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 tasking or part of a tasking. Tasks will vary in nature and points will be weighted based upon the difficulty and time sensitivity of the tasking. Tasks may contain multiple parts with point values assigned to each specific part of the tasking.

Some examples:

- Opening an FTP service for 2 hours given a specific user name and password: 200 points
- Closing the FTP after the 2 hours is up: 50 points
- Creating/enabling new user accounts: 100 points
- Installing new software package on CEO’s desktop within 30 minutes: 100 points

Every team must make an effort to complete each tasking. Failure to attempt any tasking will result in a team penalty and could result in a “firing” of team members.

Red Team Actions
Successful Red Team actions will result in penalties that reduce the affected team’s score. Red team actions include:

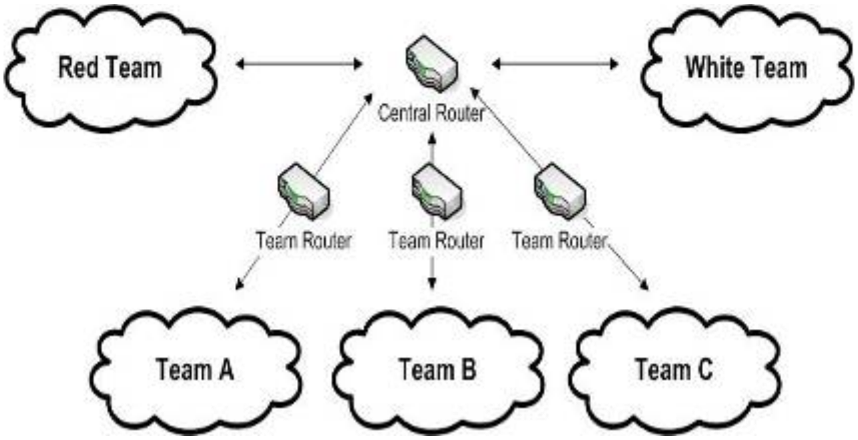
- Obtaining root/administrator level access to a team system: -100 points
- Obtaining user level access to a team system (shell access or equivalent): -25 points
- Recovery of userids and passwords from a team system (encrypted or unencrypted): -50 points
- Recovery of one or more sensitive files or pieces of information from a team system (configuration files, corporate data, etc.): -25 points

- Recovery of customer credit card numbers: -50 points
- Recovery of personally identifiable customer information (name, address, and credit card number): -200 points

Red team actions are cumulative. For example, a successful attack that yields root level access and allows the downloading of userids and passwords would result in a -150 point penalty. Red team actions are scored on a **per system** and **per method** basis – a buffer overflow attack that allows the Red Team to penetrate a team's system will only be scored once for that system; however, a different attack that allows the Red Team to penetrate the same system will also be scored. Only the highest level of account access will be scored per attack – for example, if the Red Team compromises a single user account and obtains root access in the same attack the penalty will be -100 points for root level access and not -125 points for root and user level access.

NECCDC Logical Network Diagrams

Overall Competition Network Layout



The competition network will be mostly standalone, with Internet access for obtaining patches and documentation, either by limited external connectivity through the competition network or as a separate “outside network” with its own node. The Red Team network, the White Team network, and each team network will be connected to a central router that will be maintained by the Operations Team.

Individual Team Layout

Each team network will be connected to the competition network through provided networking equipment (switch or router). No other equipment may be connected to the competition network at any time.

No commercial security-related or network management hardware or software (networking monitoring, anti-virus, firewalls, IDS, IPS, etc.) will be permitted unless the White Team has provided it. Completely free products from commercial companies, such as the Microsoft Baseline Security Analyzer, are permitted. Teams are not allowed to bring any equipment or media including laptops, servers, monitors, PDAs, tablets, MP3 players, flash drives, USB drives, floppies, CDs, or DVDs into the competition area. Teams may bring printed materials such as magazines, reference books, and checklists.

Each team will be provided with an email account to send files to be worked on after hours. This email address will be monitored. There is to be no deletion or personal use of this email account. If you have any questions about this email account, ask your White Team member.

The following operating systems and applications may be used in the competition network:

- Linux
- Windows Desktop and Server Operating Systems
- Solaris
- Cisco IOS
- MySQL
- BIND
- Sendmail
- IIS
- Apache

Letter from Go2Market CIO

Go2Market, Inc

ECommerce at its finest

From: Philip Carson

To: IT Staff

CC:

Subject: Welcome

Welcome to the Go2Market family! As you can see we had to essentially replace our entire IT staff in the last couple of days so we've brought you in to help us out. The last crew wasn't that great but you should find a couple of documents to help you get started – admin passwords, IP addresses, network maps, that sort of thing. If you don't see a password listed for a specific device, be sure to try a blank password (that's one of the reasons the old crew is gone).

We're a small company, we move pretty quickly, we've got a couple of major projects coming up, and we really depend on our IT infrastructure. So do your best to keep things up and running smoothly. To help you assess and secure the network I've managed to secure a few things – there's a Cisco Router, and a Cisco switch. I'll try and dig up a few more things in the next couple of days if I can. I'm not sure how stable some of this old gear is. Up until last week we had a contractor come in and do our weekly backups so I can probably convince them to come back and fix one system but anything beyond that we'll have to pay them by the hour.

So welcome again to Go2Market – remember we rely on our network and public services a great deal so keep them running!

Thanks,

Philip

Go2Market Network Information from the CIO

The Go2Market network has quickly become a vital part of our business. shop.go2market.com is now our leading point-of-sales method and therefore the integrity of our network is critical. As you are all new to our organization, the outline below details what little documentation the former administrative team provided us on the inner workings of our infrastructure. While the executive staff recognizes this information is spotty at best, it should at a minimum provide your team with enough details to get you started.

Overall Network Architecture:

Network Details:

Each team will be assigned a private autonomous system number (64512-65535), an IP block of the form 10.235.X.0/24, and an IPv4 default gateway of 10.235.X.1.

Server Architecture:

- CentOS
  - Roles: Central Authentication
  - Hostname: oak
  - IP: 10.235.X.130

- Debian
  - Roles: DNS
  - Hostname: elm
  - IP: 10.235.X.150

- Windows 2003
  - Roles: Ecommerce Site
  - Hostname: maple
  - IP: 10.235.X.170

- Ubuntu
  - Roles: Mail
  - Hostname: pine
  - IP: 10.235.X.190

Sample Set of Supported Client Architectures:

Windows XP
Linux
Windows 2003

The previous administrator set all administrative passwords to “changeme” or a blank password before their departure.

Critical Services:

In order for our business to function properly the following functionality must be available at all times.

Externally (IPv4):
- Mail (POP, SMTP)
- Web (Ecommerce and Corporate Website)
- DNS

Internally:
- File Servers
- Network Printers
- Clients
- Central Authentication
- Internet Access

As our business needs change so might the preceding list of necessary services shown above. The list provided above is merely a snapshot in time of what we currently need to properly function. Failure to provide any of these services for a prolonged amount time costs our company money and may ultimately cost you your job.