Collegiate Cyber Defense Competition

5th Mid-Atlantic Regional CCDC
March 11-13, 2010
Columbia, MD

Team Packet
1st Draft

Table of Contents

Competition Schedule (Subject to Change)

Thursday, March 11th

9:00 AM-1:00 PM	Equipment load-in, network setup/test
1:00 PM	Teams arrive
1:15 PM	Announcements
1:30-4:00 PM	Team pre-competition prep
4:30-6:30 PM	Networking Reception/Job Fair
7:00 PM	Northrop Grumman CSOC site visit (tentative)

Friday, March 12th

11:00 AM	Volunteer check-in/debrief
11:30 AM	Teams check-in
12:00 PM	Opening announcements
12:30 PM	Guest Speaker: Larry Pesce, PaulDotCom
1:00 PM	Day one competition starts
5:00-5:30 PM	Guest Speaker: Marcus Ranum, Tenable Network Security
5:30-6:00 PM	Invited Guest Speaker TBD
5:00-6:00 PM	Dinner
7:00 PM	Day one competition ends
7:15 PM	Announcements
7:30 PM	Guest Speaker: Alan Greenberg, Boeing

Saturday, March 13th

9:00 AM	Volunteer check-in/debrief
9:30 AM	Announcements
9:45 AM	Day two competition starts
12:00-1:00 PM	Lunch (provided by CSC) and guest speaker: Randy Georgieff, Department of Defense Cyber Crime Center (DC3)
1:15 PM	Break Out Session: Alan Greenberg, Boeing
5:00-6:00 PM	Working dinner
7:00 PM	Day two competition ends/network teardown
7:45 PM	Debrief and awards ceremony

CCDC Mission and Event Objectives

Mission

"The goal of a Cyber Defense Competition is to provide hands-on application of information assurance skills; as such, they enhance students' understanding of both theory and practice. They provide students a laboratory in which to experiment, just as in other fields of science. They fulfill the same role as capstone projects in a traditional engineering program (i.e., projects that allow students to synthesize and integrate knowledge acquired through course work and other learning experiences into a project usually conducted in a workplace). The competition combines legal, ethical, forensics, and technical components while emphasizing a team approach. Such experiential education increases the knowledge and expertise of future professionals who may be in a position to contribute to the secure design and operation of critical information and its supporting infrastructure" (from *Exploring a National Cyber Security Exercise for Colleges and Universities*, Lance J. Hoffman and Daniel Ragsdale, 2004).

Event Objectives

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

Teams

Teams involved in this year's competition include:

•**Blue Teams**: student teams consisting of full-time, undergraduate and graduate, degree-seeking students, representing four year universities and community colleges from the Maryland, North Carolina, and Pennsylvania. This year's qualifying teams include:

1. Asheville-Buncombe Technical College, NC
2. Community College of Baltimore County, MD
3. Millersville University, PA
4. Towson University, MD
5. University of MD Baltimore County (UMBC), MD

•**Red Team (AKA Red Cell)**: a group of students and information security professionals from volunteer commercial organizations who have offered their skills to assess the abilities of the teams to defend their systems. The red team will conduct probes, scans and attempted penetrations of the blue teams.

•**White Team**: a group of professionals who will conduct the exercise, control the flow and timing of the events and injects, and who will serve as mediators for disputes and challenges.

•**Gold Team**: a group of volunteers that will help the White team run the competition. Each blue team will be assigned a gold team liaison. The liaison will periodically query the team as to their actions and score "injects" designed to challenge the teams' implementation. Blue teams are advised not to argue or question the gold team representative.

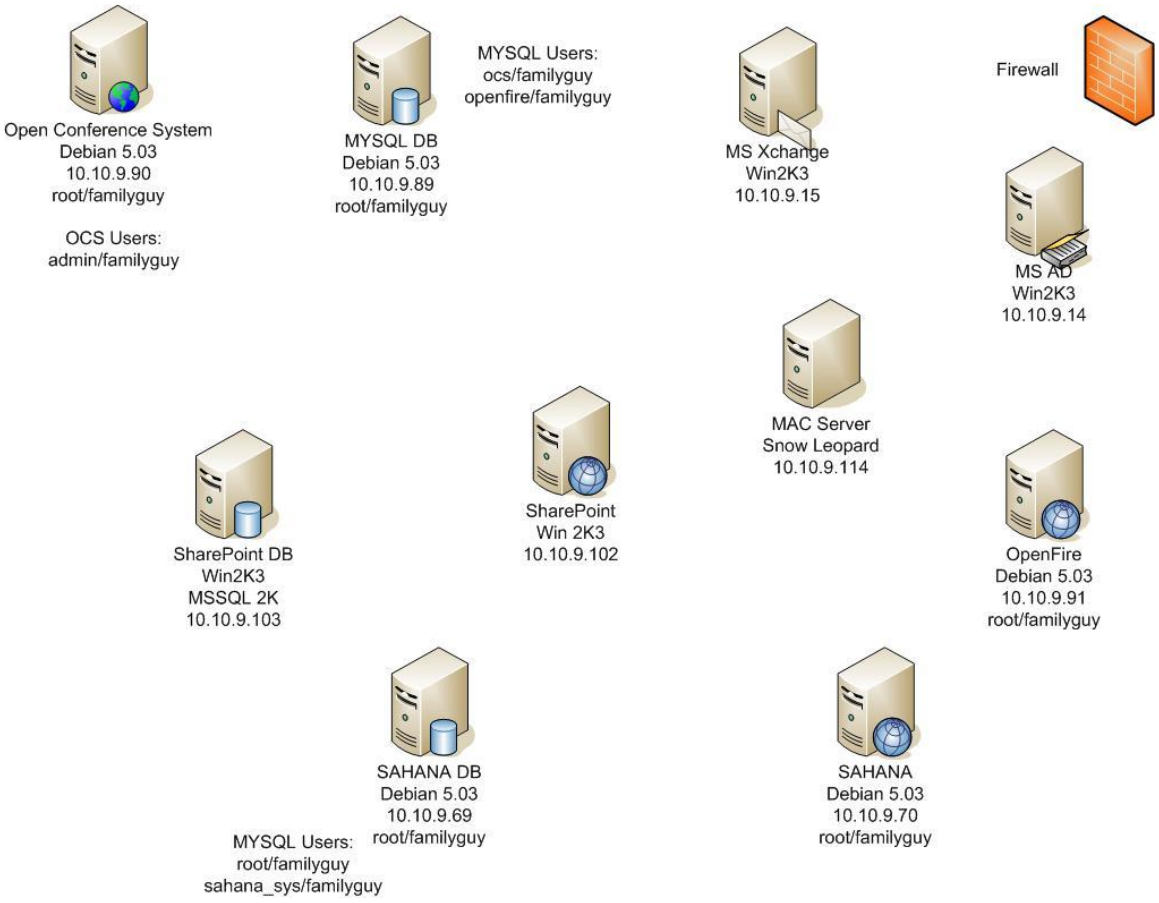
To create a fair and even playing field:

- Each team will consist of up to eight (8) members. Each team member must be a full-time student of the institution the team is representing. Team members must qualify as full-time students as defined by the institution they are attending - typically this means the team member must be enrolled in 12 or more semester credit hours for undergraduates and 9 or more semester credit hours for graduate students during the semester the competition is held.
- Each team may have no more than two (2) graduate students as team members.
- Each team may not have advisors present in the blue team competition room.
- All participants will wear badges identifying competition affiliation at all times during competition hours.

- Each team will designate a Team Captain for the duration of the competition to act as the team liaison between the white team and the gold team, before and during the competition.

Network Information

The competition network will be completely standalone with no external connectivity. Global servers, the red team network, the white team network, and each blue team network will be connected to a central connectivity device that will be maintained by the white team.



- Each blue team will be provided with a standalone PC and direct access to the Internet for the purposes of research, downloading patches, etc.
- Internet activity will be monitored and any team member caught viewing inappropriate or unauthorized content will be immediately disqualified from the competition. This includes direct contact with outside sources through AIM/chat/E-mail 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 a white team member immediately.
- Internet resources such as FAQs, how-to's, existing forums and responses, and company Web sites 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 blue 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.
- Blue 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 blue teams.
- No peer-to-peer or distributed file-sharing clients or servers are permitted on the competition networks.
- 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.
- Blue teams may not remove any computer, printer, or networking device from the competition area.
- Blue teams should not assume any competition system is properly functioning or secure; they are assuming responsibility for each of their systems.
- All teams will be connected to a central connectivity device and scoring system.
- Throughout the competition, white team members will occasionally need access to a team's system(s) for scoring, troubleshooting, etc. Blue teams must allow the white team members access when requested.
- Blue teams must maintain specific services on the "public" IP addresses assigned to their team (e.g., if a blue 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).
- Blue teams are not permitted to alter the system names of their assigned systems.

- Blue teams are not permitted to remove or alter any labels/stickers that are present on their assigned systems.

System Information: General

The following notes are provided to help assist in your understanding of the various systems, the roles they play, and how they are configured.

- Each system is running Windows XP SP3 as the Host OS. In most cases, the competition OSes/services are running within a virtual machine (VM) and viewed using VMware Player.
- **The Host OS username is either administrator or admin and the password is familyguy. You cannot change this username and password**.
- All systems are to be synchronized to the Eastern TimeZone (-5 hours off GMT) using **time.nist.gov**. This means that the Network Time Protocol (NTP) daemon on the Linux systems must remain running.

System Information: Firewall

The firewall is setup in a two-segment configuration (DMZ and outside). Network Address Translation (NAT) and traffic flow is very important.

All services/ports that must be allowed inbound must also be allowed outbound.

All systems are NAT'd through the firewall to:

- A-B Tech: 130.68.81.x
- CCBC: 202.11.82.x
- Millersville: 150.204.83.x
- Towson: 41.204.84.x
- UMBC: 69.178.85.x

All systems are NAT'd by changing their first three octets (10.10.9) with the first three of octets of their team space.

System Information: Outside Segment

- **Windows Server 2008 - Active Directory (AD)**: This is your primary domain controller and is responsible for managing user and system information across the enterprise. There are over 10,000 users with corresponding email accounts on the Exchange system (see below). The AD server is also your primary DNS server. As your primary DNS server, it must allow zone transfers and other inbound DNS requests. Email is sent using proper DNS MX record lookups. Failure to resolve DNS lookups from outside your network will result in email and other shutdowns. Your DNS server is setup to forward lookups to one of the Root DNS servers located at 198.41.0.4. This is essential for DNS to work.
- **Windows Server 2003 - Exchange**: Provides all email functionality for the enterprise. This system is a member of the Domain and must remain so in order to function. All users with an AD account must have a functional email account. Email must be available through all email protocols (POP3, SMTP, IMAP4, and HTTP).
- **Windows Server 2003 - SharePoint Portal**: This is your organization's web site to the outside world. It is there for collaboration and information dissemination. It is running Microsoft SharePoint 2003 and is using Microsoft SQL server as its database backend.
- **Windows Server 2003 – SharePoint Portal Database**: This is the Microsoft SQL database for your SharePoint portal. If it goes down, it will most likely take your web site with it.
- **Debian 5.03 Server - Open Conference System**: This is the web site supporting the 2010 World Convention. There are 1,000 users registered for the convention. The site is managed using the Open Conference System. Open Conference Systems (OCS) is a free Web publishing tool that will create a complete Web presence for your scholarly conference. OCS will allow you to:
  - create a conference web site
  - compose and send a call for papers
  - electronically accept paper and abstract submissions
  - allow paper submitters to edit their work
  - post conference proceedings and papers in a searchable format
  - post (if you wish) the original data sets
  - register participants
  - integrate post-conference online discussions
- **Debian 5.03 Server - OpenFire**: Openfire is a real-time collaboration (RTC) server licensed under the Open Source Gnu Public License (GPL). It uses the only widely adopted open protocol for instant messaging, XMPP (also called Jabber). Openfire is incredibly easy to setup and administer, but offers rock-solid security and performance.

- **Debian 5.03 Server - OpenFire Database:** This is the MySQL database backend for your OCS and OpenFire servers.
- **Debian 5.03 Server - SAHANA Server**: Sahana is a Free and Open Source Disaster Management System. It is a web-based collaboration tool that addresses the common coordination problems during a disaster from finding missing people, managing aid, managing volunteers, tracking camps effectively between Government groups, the civil society (NGOs), and the victims themselves.
- **Debian 5.03 Server - SAHANA Database**: This is the MySQL Database backend to the SAHANA server.
- **MAC Snow Leopard Server**: This server will be used to extend your organization's presence to include iChat, podcasting, and enhanced web services.

System Information: DMZ Segment

- **Debian 5.03 Nagios**: This system is beyond the boundaries of your network and can only be managed remotely. It is not configured for your team. It is up to you to do so.

Rules of Engagement

Overview

The competition is designed to test each blue team's ability to secure networked computer systems while maintaining standard business functionality. As newly hired IT staff of the City of Avalon, each blue team's primary job will be to ensure that the various systems stay up and responsive to customers' needs. In addition, blue teams are expected to manage the computer network, keep it operational, and control/prevent any unauthorized access. Each blue team will also be expected to maintain and provide certain services (i.e., SSH, IMAP).

The competition measures each blue team's ability to maintain secure 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 higher score, as will a business success that results in security weaknesses.

Competition Play

- During the competition, blue team members are forbidden from entering, or attempting to enter, another team's competition workspace.
- A laptop and VoIP phone have been provided to communicate with the white team. The laptop is preconfigured with Exchange and Microsoft Messenger. The VoIP phone has a directory (press the directories button then #5 for external directories) of all the extensions. These assets are not scored.

- All communications will be via E-mail, VoiP phones, and/or face-to-face with a designated gold team member.
- Requests to the white team can be submitted via E-mail to the **whitecell@cyber-exercise.com** account. Requests must clearly show the requesting blue team, action or item requested, and date/time requested.
- Blue teams must compete without outside assistance from non-team members during the competition, which includes team advisors and sponsors. All private communications (calls, E-mails, 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.
- Blue teams may not bring any computers, removable media, tablets, PDAs, or wireless devices 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.
- A 16GB thumb drive will be provided to you. This drive will be collected at the end of each competition day and wiped clean.
- Blue teams are not allowed to bring any software with them to the competition (this includes updates and patches to OSes).
- Printed reference materials (books, magazines, checklists) are permitted in competition areas and blue teams may bring printed reference materials to the competition.
- Blue teams are not allowed to bring electronic copies of configuration files (e.g., iptables) or scripts (e.g., script to change passwords) to the competition (hard copies are allowed however). These must be created during the competition.
- Observers are not competitors and are prohibited from directly assisting any competitor through direct advice, “suggestions”, or hands-on assistance. Any observer found assisting a blue team will be asked to leave the competition area for the duration of the competition and a 1,000-point penalty will be assessed against the blue team.
- Blue team members will not initiate any contact with members of the red team during the hours of live competition. However, blue team members are free to talk to red team members, white team members, other competitors, etc. outside of competition hours.
- On occasion, the white team members may escort individuals (VIPs, press, etc.) through the competition area.
- Blue teams are permitted to replace applications and services provided they continue to provide the same content, data, and functionality of the original service.

- Blue teams are free to examine their own systems, but no offensive activity against other blue teams, the white team, or the red team will be tolerated. This includes port scans, unauthorized connection attempts, vulnerability scans, etc. Any blue team performing offensive activities against other teams, 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.
- Each blue team may change passwords for any account. A web site on the OOB network will be provided for you to make password changes. As a failover, any password changes to scored user accounts (a list of these accounts is provided in the Scoring: Services section below) may be sent to the white team password account (**password@cyber-exercise.com**) immediately upon change (unless the password changes are part of a competition inject). Failure to notify the white team of password changes can result in service check failures. Please note that the white team will not error-check the provided password changes - they will simply upload the provided changes.
- Blue 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 blue 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 blue teams.
- The white team is responsible for monitoring the network, implementing scenario events, and refereeing.
- Protests by any blue team will be presented by the Team Captain to a gold team member as soon as possible. White team members will be the final arbitrators for any protests or questions arising before, during, or after the competition.
- Team Captains are encouraged to direct and resolve any questions or disputes regarding the rules of the competition or scoring methods before the competition begins. Queries should be sent to Casey O'Brien (cobrien@ccbcmd.edu).
- ICMP, IPv4, and IPv6 traffic must flow between all the teams.
- All systems on the network diagram must be reachable and respond to ICMPv4 and ICMPv6 pings.
- All services that are tested for must remain open and functional.
- Prior to the start of the exercise a zero round will be run on the scorebot. A zero round tests ALL the functionality of each blue team's infrastructure. Each blue team must receive a perfect score (0 points) during the zero round before the exercise starts. This means that all servers and systems are fully functional at the start of the exercise. It is your job to keep them so.

- Blue teams may block by single source IP, as long as an accompanying Incident Response form is submitted and approval by the white team is granted. To block by single source IP is to run the risk of blocking the scoring engine. If the scoring engine cannot reach the systems, blue teams will be penalized accordingly.
- Blue teams cannot block by IP range.
- A complete list of necessary ports/services is provided in the Scoring: Services section below.
- Free (as in Beer and Liberty) software for commercial organizations can be downloaded and used during the competition. Limited trial periods of commercial software is strictly prohibited. No consumer products are allowed without prior written approval of the white team. There will be periodic audits of the systems. For each copy of software that does NOT meet these guidelines, the blue team will be penalized 1,000 points (per violation) and the software must be removed within the time frame determined by the white team.

Scoring: General

Blue teams will not be rewarded with points for doing their job; that is, keeping functional services running and completing the business injects accurately and on time. However, blue teams can have points deducted from their score for identifying and reporting unauthorized accesses and compromises. All blue teams must complete at least two Incident Response forms and open two cases with the attendant Law Enforcement Agent, if in attendance. Incident Response forms can be downloaded from the following location: **www.midatlanticccdc.org/CCDC/wp-content/uploads/2010/02/Incident.Response.Form.pdf**.

Scoring will be based on three metrics:

1. Keeping required services up and running
2. Controlling/preventing unauthorized access and compromises
3. Completing business injects accurately and on time

Raw scores are used for these three metrics. However, at the end of each day's competition, blue teams are ranked using an ordinal scale, which is a measurement scale that assigns values to objects based on their ranking with respect to one another. For example, a first place finish at the end of day one in the service check metric warrants an ordinal score of 1; a second place finish warrants an ordinal score of 2; up to a fifth place finish warranting an ordinal score of 5. This process is repeated for the business injects and red team compromises (see Scoring: Red Team section below for more on the latter).

The ordinal scores from the three metrics are then totaled for each blue team, yielding a combined ordinal score for each day of competition, which is used to rank the blue teams from first through fifth place. **The winning blue team will be based on the lowest combined ordinal score obtained during the competition time**.

In addition:

- Scores will be maintained by the white team. Team standings will be provided at the beginning of day two, but without specific scores.
- Any blue team action that interrupts the scoring engine is exclusively the fault of that blue team and will result in a higher score. Should any question arise about specific scripts or how they are functioning, the blue team captain should immediately contact the gold team liaison to address the issue.
- Any blue team that tampers with or interferes with the scoring or operations of another team's system(s) will be disqualified.
- A thorough Incident Report that correctly identifies a successful red team attack will reduce the red team's penalty by up to 50 percent – no partial points will be given for incomplete or vague Incident Reports.
- Raw scores will be generated using a combination of automated tools and manual checking.
- Penalties will take the form of points being added to a blue team's overall score.

Scoring: Red Team

The red team will be attempting to find and exploit weaknesses in each blue team's environment. Points will be added to the appropriate blue team's score based on the severity and type of compromise. For certain categories of compromise, such as root access, points will be added for each *unique* method used by the red team to compromise the targeted systems. For example, if the red team is able to gain root access on a blue team's system using a buffer overflow and by brute forcing an administrator account, each compromise will be scored separately and points will be applied for each.

A root level compromise is proven through several means (e.g., red team phone home script is executed, documented proof, clear text version of root/administrator password, etc).

Blue teams have 500 points added to their score in the event of a successful root-level access, per round. Teams may obtain a portion of their points back based on conducting an investigation. If the officer running the investigation thinks they have enough evidence to obtain a search warrant, 150 points will be returned. If the officer running the investigation thinks they have enough evidence to obtain an arrest warrant, 250 points will be returned.

Scoring: Services

All systems are pinged before the service check is run. Therefore, all systems on the network diagram must be reachable and respond to ICMPv4 and ICMPv6 pings. If a system fails to respond to pings, it will be fined the total value of all services at Level 1 (see chart below). For example, a server has three services on it and each service is worth 1,000 points. If the server cannot be pinged, then the team will have 4,000 points added to its total (1,000 points for the failed pings and 1,000 x 3 for each down service).

NOTE: we will be scoring ICMPv6 as a service only. If a system fails the ICMPv6 ping, blue teams will only be penalized for the one service outage. If a system fails the ICMPv4 ping, we'll add up ALL the points.

If the external interface of the firewall cannot be pinged, then no subsequent tests will be run and the maximum penalty of all services scored at Level 1 will be added to the team.

TCP is scored at three levels:

- Level 1 is the three-way handshake. If the port is not open, or does not complete the three-way handshake, then the blue team is fined the number of points for that service as listed in the below table.
- Level 2 is the service request. If Level 1 is passed (the port is open and the three-way handshake is completed), then the scoring engine makes a service request (e.g., HTTP get index.html). If the request is not processed, then the blue team is fined one-half the number of Level 1 points.
- Level 3 is the integrity check. If Levels 1 and 2 are passed, then checks will be performed on the various flags to ensure their integrity has not changed since the start of the exercise. If the flag fails the integrity check, then the blue team is fined one-fourth the number of Level 1 points.

UDP is scored at two levels:

- Level 1 is the port check, to see if the port is open by issuing a service request to that port. If the port is unresponsive, then the blue team will be fined the number of points for that service as listed in the below table.
- Level 2 is the integrity check. If Level 1 is passed, then checks will be performed on the various flags to ensure their integrity has not changed since the start of the exercise. If the flag fails the integrity check, then the blue team is fined one-half the number of Level 1 points.

The following tables detail the services that will be scored during the competition. **NOTE: these are subject to change**. The services are organized by the Cisco ASA interface/network in which they reside. In addition to the system's IP address, the tables below detail the necessary ports and protocols to which the scoring engine needs access to. You will also find the required administrator/root passwords to the various systems.

Firewall			
-10.10.9.254 -Cisco ASA 5505 -Enable password: familyguy	ICMPv4		Ping
	ICMPv6		Ping
	TCP	22	SSH
	UDP	161	SNMP
	UDP	162	SNMP
	SNMP community string: scorebot		

DMZ Segment			
-10.10.9.14 -Windows Server 2008 -Active Directory -Username: Administrator -Password: chiapet	ICMPv4		Ping
	ICMPv6		Ping
	UDP	53	DNS (IPv4)
	UDP	53	DNS (IPv6)
	TCP	389	LDAP
	TCP	5666	NSClient++
	TCP	31300 (out)	Tenable LCE Client
-10.10.9.15 -Windows Server 2003 -Exchange -Username: Administrator -Password: chiapet	ICMPv4		Ping
	ICMPv6		Ping
	TCP	25	SMTP
	TCP	80	HTTP
	TCP	110	POP3
	TCP	143	IMAP
	TCP	5666	NSClient++
	TCP	31300 (out)	Tenable LCE Client
-10.10.9.69 -Debian 5.03 -SAHANA DB -Username: root -Password: familyguy	ICMPv4		Ping
	ICMPv6		Ping
	TCP	22	SSH
	TCP	3306	MySQL
	TCP	5666	NRPE Server
	TCP	31300 (out)	Tenable LCE Client

DMZ Segment			
-10.10.9.70 -Debian 5.03 -SAHANA Server -Username: root -Password: familyguy	ICMPv4		Ping
	ICMPv6		Ping
	TCP	20/21	FTP
	TCP	22	SSH
	TCP	80	HTTP
	TCP	5666	NRPE Server
	TCP	31300 (out)	Tenable LCE Client
-10.10.9.89 -Debian 5.03 -OpenFire/OCS DB -Username: root -Password: familyguy	ICMPv4		Ping
	ICMPv6		Ping
	TCP	22	SSH
	TCP	3306	MySQL
	TCP	5666	NRPE Server
	TCP	31300 (out)	Tenable LCE Client
-10.10.9.90 -Debian 5.03 -OCS Server -Username: root -Password: familyguy	ICMPv4		Ping
	ICMPv6		Ping
	TCP	20/21	FTP
	TCP	22	SSH
	TCP	80	HTTP
	TCP	5666	NRPE Server
	TCP	31300 (out)	Tenable LCE Client

DMZ Segment			
-10.10.9.91 -Debian 5.03 -OpenFire Server -Username: root -Password: familyguy	ICMPv4		Ping
	ICMPv6		Ping
	TCP	20/21	FTP
	TCP	22	SSH
	TCP	80	HTTP
	TCP	3478/3479	STUN Services
	TCP	5222	XMPP: Client-to-Server
	TCP	5223	XMPP: Client-to-Server (SSL)
	TCP	5666	NRPE Server
	TCP	7070	XMPP: HTTP Clients
	TCP	7777	XMPP: File Transfer
	TCP	9090	OpenFire Admin: http://IP_Address:9090 (admin/familyguy)
	TCP	9091	OpenFire Admin (SSL)
	TCP	31300 (out)	Tenable LCE Client
-10.10.9.102 -Windows Server 2003 -SharePoint Portal -Username: Administrator -Password: familyguy	ICMPv4		Ping
	ICMPv6		Ping
	TCP	80	HTTP
	TCP	5666	NSClient++
	TCP	31300 (out)	Tenable LCE Client
-10.10.9.103 -Windows Server 2003 -SharePoint Portal DB -Username: Administrator -Password: chiapet	ICMPv4		Ping
	ICMPv6		Ping
	TCP	1433	Microsoft SQL
	TCP	5666	NSClient++
	TCP	31300 (out)	Tenable LCE Client
-10.10.9.114 -MAC OS X (Snow Leopard Server) Services TBD -Username: -Password:	ICMPv4		Ping
	ICMPv6		Ping

Outside Segment	
x.x.x.253 -Debian 5.03 Nagios Username: root Password: familyguy	Not being scored

Scoring: Business Policy Manual

The City of Avalon *Business Policy Manual* is included in this team packet. As a new employee of the City of Avalon, it is your responsibility to familiarize yourself with this manual.

Any action violating a policy in the Business Policy Manual will result in a 1,000-point penalty, per violation.

Business Injects

Throughout the competition, each team will be presented with identical business injects. These injects will vary in nature and be weighted based upon the difficulty and time sensitivity of the tasking. Tasks may contain multiple parts. Some examples include: setting up an Intranet web server; performing a zone transfer between a secondary DNS server and the primary DNS server.

Injects will be delivered via E-mail, phone, and/or hard copy and will include the point values and time restrictions associated with the task (e.g., in the event an blue team doesn't complete the business inject, the blue team will know how many points will be added to their score). Blue teams can prioritize their efforts based on outstanding requests. Upon completion of the injects, a scoring sheet will be signed by the blue team captain and returned to the appropriate gold team judge, who will note the time that the event was/was not completed.