NATIONAL
COLLEGIATE
CYBER
DEFENSE
COMPETITION

2007 National Collegiate Cyber Defense Competition

April 13 – 15, 2007

San Antonio, TX

Team Packet

Hosted by the Center for Infrastructure Assurance and Security

Center for Infrastructure • Assurance and Security • UTSA

Table of Contents

Welcome Letter 3

Sponsors 4

Competition Schedule 5

Overview 6

CCDC Mission and Objectives 7

Competition Rules 7

Scoring 13

Logical Network Diagrams 15

Letter from Burnsodyne CIO 17

Burnsodyne Network Information 18

Burnsodyne Network Diagram 20

On behalf of the Center for Infrastructure Assurance and Security (CIAS) and The University of Texas at San Antonio (UTSA) I'd like to welcome each of you to the Second National Collegiate Cyber Defense Competition. You have all already participated in a regional competition and have shown that you are capable of maintaining the security of an operational network. We hope that you will find this national competition a challenging follow-on to your experience so far.

The CIAS and UTSA are excited to be able to host this event. We are also very thankful for our sponsors from industry as well as the Department of Homeland Security (DHS). Our staff, volunteers, and sponsors have tried to make this an interesting, exciting, and challenging competition. As most of you know, this three day event has grown from its modest beginnings to the point where we believe we are poised to have a significant impact on security programs around the nation. The competition is receiving increased attention from government and industry and we expect this attention to continue to grow. Our eventual goal is to have 8 to 10 regional competitions with the winner from each being invited to the national championship. We have already identified three potential schools to host competitions in parts of the country previously uncovered and we anticipate that more will follow. As we asked after the first national competition, we encourage you to provide comments and feedback to help us improve future events. While this is a competitive event, we also encourage you to take a few minutes to meet your fellow competitors, talk to the vendors present, and explore our wonderful city. We wish the very best of luck to each of you and your teams!

Gregory White, Ph.D.
Director
Center for Infrastructure Assurance and Security

NATIONAL
COLLEGIATE
CYBER
DEFENSE
COMPETITION

Event Sponsors

We would like to thank all the sponsors who have made this event possible through their generous donations of time, equipment and funds.

Special Thanks

This event is funded in part through a grant from
The Department of Homeland Security

Platinum Sponsor

Cisco Systems, Inc.

Gold Level Sponsors

CORE SECURITY TECHNOLOGIES

symantec.

ISSA™ Information Systems Security Association

rackspace® MANAGED HOSTING

TippingPoint a division of 3Com

Acronis Compute with confidence

coretrace®

Silver Level Sponsors

ThinkGeek

NORTHROP GRUMMAN

INFORMATION SECURITY

PEARSON Prentice Hall

CoDe .NET The Leading Independent Magazine for .NET Developers www.code-magazine.com

PEPSI

O'REILLY®

KFC

Pizza Hut

Competition Schedule

Friday – April 21

11:00 AM	Registration opens
12:30 PM	Opening announcements in the Lonestar Ballroom
1:30 PM	Competition Day 1 begins
5:00 PM – 6:00 PM	Dinner available in the Lonestar Ballroom
7:30 PM	Competition Day 1 complete

Saturday – April 22

8:45 AM	Day 2 Announcements in the Lonestar ballroom
9:00 AM	Competition Day 2 begins
12:00 PM – 1:00 PM	Lunch available in the Lonestar Ballroom
7:00 PM	Competition Day 2 complete
7:01 PM – 9:00 PM	Networking reception sponsored by Rackspace®

Sunday – April 23

8:45 AM	Day 3 Announcements in the Lonestar Ballroom
9:00 AM	Competition Day 3 begins
12:00 PM	Competition Day 3 complete
12:15 PM – 1:00 PM	Vendor feedback session in the Lonestar Ballroom
1:00 PM – 3:00 PM	Lunch in the Ballroom 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 help facilitate the development of a regular, national level cyber security exercise, the Center for Infrastructure Assurance and Security at the University of Texas at San Antonio agreed to host the first Collegiate Cyber Defense Competition (CCDC) for the Southwestern region. 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 "commercial" 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 operations. 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 or mentors during the competition.
- A non-biased red team will be used: A non-biased, volunteer, commercially experienced red team 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.

Competition Rules

Overview

The competition is designed to test each team's ability to secure and administer 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 chemical distributor. 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.

1. **Student Teams**
    - **a.** 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 and must not be currently employed in the IT industry (security operations, network administrator, system administrator, programmer, network operations, help desk, etc.) as a salaried employee or as an hourly employee for more than 20 hours per week. 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.
    - **b.** Each team may have no more than two (2) graduate students as team members.
    - **c.** Each team may have one advisor present at the competition – this may be a faculty/staff member of the institution or a team sponsor. The advisor may not assist or advise the team during the competition.
    - **d.** All team members will wear badges identifying team affiliation at all times during competition hours.
    - **e.** 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.
    - **f.** If the member of a qualifying team is unable to attend the national competition, that team may substitute another student in their place provided the substitute meets all stated eligibility requirements.
2. **Competition Systems**
    - **a.** Each team will start the competition with identically configured systems.
    - **b.** Teams may not remove any computer, printer, or networking device from the competition area.
    - **c.** Teams will be provided the overall system architecture, network configuration, and initial set-up prior to the event to permit planning but no detailed information, such as patch levels and application versions, will be provided ahead of time.
    - **d.** 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.
    - **e.** All teams will be connected to a central router and scoring system.
    - **f.** Throughout the competition, Operations and White Team members will occasionally need access to a team's system(s) for scoring, troubleshooting, etc. Teams must allow Operations and White Team members access when requested.
    - **g.** Teams must not connect any outside devices or peripherals to the competition network.
    - **h.** Network traffic generators will be used throughout the competition to generate traffic on each team's network. Traffic generators will generate typical user traffic as well as suspicious or potentially malicious traffic from random source IP addresses throughout the competition.

i. **i.** 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 however teams are free to NAT addresses inside their team networks.

j. Teams are not permitted to alter the system names of their assigned systems.

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

l. 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 Operations Team and will cost the team 50 points per system recovered.

m. Each 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.

n. Systems designated as “user workstations” are to be treated as user workstations and may not be re-tasked for any other purpose by teams. They must remain user workstations throughout the entire competition unless otherwise directed by an Operations or White Team member or indicated through competition injects. Teams may not change the operating system on user workstations but are free to patch and secure user workstations.

o. 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.

p. In addition to user workstations each network will have one “admin workstation”. Teams are free to modify the operating system and load tools, scripts, or applications on this workstation; however, this administrative workstation may not be used to provide critical services such as SMTP, FTP, HTTP, etc.

q. Servers and networking equipment may be re-tasked or reconfigured as needed.

3. Competition Play

a. The competition will run over a three day period (Friday April 13th to Sunday April 15th). Registration will occur on Friday April 13th and a mandatory meeting for all team members and faculty sponsors will be held prior to the start of the competition.

b. During the competition team members are forbidden from entering or attempting to enter another team’s competition workspace or room.

c. All requests for items such as software, score checks, system resets, and service requests must be submitted on paper (typed and printed) to the Operations Team. Requests must clearly show the requesting team, action or item requested, and date/time requested.

d. Teams must compete without “outside assistance” from non-team members which includes team advisors and sponsors. All private communications (calls, emails, chat, directed emails, forum postings, conversations, requests for assistance, etc) with non-team members including team sponsors that would help the team gain an unfair advantage are not allowed and are grounds for **<u>disqualification.</u>**

e. 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 Operations or White Team in advance. All cellular calls must be made and received outside of team rooms. Any violation of these rules will result in **<u>disqualification of the team member and a 200 point penalty assigned to the appropriate team</u>**.

f. Teams may not bring any computer, tablets, PDA, or wireless device into the competition area. MP3 players with headphones will be allowed in the competition area provided they are not connected to any system or computer in the competition area.

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

h. Team sponsors and observers are not competitors and are prohibited from directly assisting any competitor through direct advice, “suggestions”, or hands-on assistance. Any team sponsor or observers found assisting a team will be asked to leave the competition area for the duration of the competition and a 200 point penalty will be assessed against the team.

i. An unbiased Red Team will probe, scan, and attempt to penetrate or disrupt each team’s daily operations throughout the competition.

j. 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, Operations staff, White Team members, other competitors, etc. outside of competition hours.

k. On occasion, Operations Team members may escort individuals (VIPs, press, etc) through the competition area including team rooms.

l. Only Operations Team members will be allowed in competition areas outside of competition hours.

m. All individuals involved with the competition will be issued badges which must be worn at all times individuals are in the competition area.

n. 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 user and service affected.

o. 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.

p. Each 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 can 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.

q. 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.

r. The White Team will provide a mechanism to show teams the official status of their critical services during the last scored service check.

4. **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 White Team, but will not be shared until the end of the competition. There will be no running totals provided during the competition. Team standings will be provided at the beginning of day two and three but without specific scores.

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

d. Any team that tampers with or interferes with the scoring or operations of another team's systems will be **disqualified**.

e. 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, etc), 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 by up to 50 percent – no partial points will be given for incomplete or vague incident reports.

5. **Internet Usage**
    - **a.** Competition systems will have direct access to the Internet for the purposes of research and downloading patches. 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/email or any other non-public services. For the purposes of this competition inappropriate content includes pornography or explicit materials, pirated media files or software, sites containing key generators and pirated software, etc. If there are any questions or concerns during the competition about whether or not specific materials are unauthorized contact the Operations Team immediately.
    - **b.** Internet resources such as FAQs, how-to's, existing forums and responses, and company websites are completely valid for competition use provided there is no fee required to access those resources and access to those resources has not been granted based on a previous purchase or fee. Only resources that could reasonably be available to all teams are permitted. For example, accessing Cisco resources through a CCO account would not be permitted but searching a public Cisco support forum would be permitted.
    - **c.** Teams may not use any external, private electronic staging area or FTP site for patches, software, etc. during the competition. All Internet resources used during the competition must be freely available to all other teams.
    - **d.** Public sites such as Security Focus or Packetstorm are acceptable. Only public resources that every team could access if they chose to are permitted.
    - **e.** No peer to peer or distributed file sharing clients or servers are permitted on competition networks.
    - **f.** 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.
6. **Questions and Disputes**
    - **a.** Team captains are encouraged to work with the contest staff 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 upon notification of disqualification and must not

re-enter the competition area at any time. Disqualified individuals are also ineligible for individual awards or team trophies.

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.

Scoring

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): 2,592 possible points
- Successful completion of business tasks: Awarded points will vary by task for a possible total of 2,408 points

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 random 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. If the service is down for over two hours the team will be assessed a 40 point penalty. If the service is down for over 3 hours the team will be assessed a 50 point penalty for **each additional hour** 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:

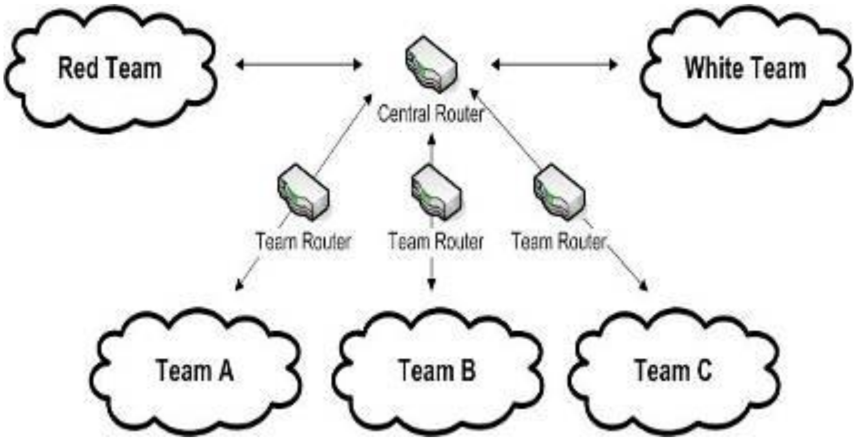
- Obtaining root/administrator level access to a team system: -100 points
- Obtaining user level access to a team system (shell access or equivalent): -25 points

- 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 **<u>per system</u>** and **<u>per method</u>** 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.

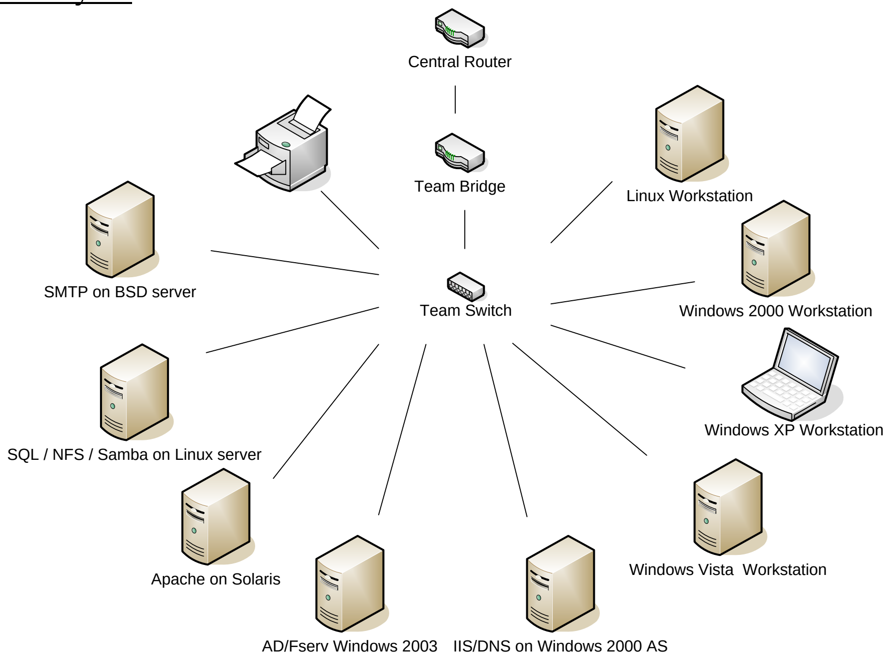
Logical Network Diagrams

<u>Overall Competition Network Layout</u>



All teams will have equal access to Internet resources as well as an internal patch server. All traffic is logged, reviewed, and subject to public release. Logging in to your bank account or personal email is highly discouraged as competition officials will not clean the logs before releasing them. 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 White Team.

Individual Team Layout



Each team network will be connected to the central router through provided networking equipment (switch, firewall, or router). No other equipment may be connected to the competition network at any time unless it is provided by the White Team as part of the competition.

No commercial security-related or network management hardware or software (networking monitoring, anti-virus, firewalls, IDS, IPS, etc.) will be permitted unless it has been provided by the White Team – this includes trial or shareware versions of commercial products. 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.

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

- Solaris
- BSD
- Linux
- Windows 2000 Server
- Windows 2003
- Windows XP
- Windows 2000 Professional
- Cisco IOS
- SQL
- MS-DNS
- SMTP
- IIS
- Apache

Letter from the Burnsodyne Chief Executive Officer

From: Adam Waverly

To: IT Staff

CC:

Subject: Welcome

Welcome to the Burnsodyne 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 ASA and a Cisco switch with a monitor port you can sniff traffic from. I'll try and dig up a few more things in the next couple of days if I can. I've also secured the Acronis software for backup and recovery use – 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 Burnsodyne – remember we rely on our network and public services a great deal so keep them running!

Thanks,

Adam

Burnsodyne Network Information from the CIO

The Burnsodyne network has quickly become a vital part of our business. Shop.burnsodyne.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:

Teams are assigned IP blocks as listed below:

Team A 10.10.10.0 – Burnsodyne.com
Team B 10.20.20.0 – Burnsodyne.net
Team C 10.30.30.0 – Burnsodyne.org
Team D 10.40.40.0 – Burnsodyne.biz

Subnet mask: 255.255.255.0
Default gateway: X.X.X.1

Cisco Catalyst:
Span Port: FA 0/12
Uplink Port: FA 0/1

Cisco ASA:
Uplink: Interface 0/0

HP LaserJet Printer:
Currently not functioning but a USB cable has been provided

Server Architecture:

Windows 2003
Roles: AD/Fileserver/IIS
Hostname: Nigel7
IP: X.X.X.15

Windows 2000 Advanced Server
Roles: DNS,Fileserver/IIS
Hostname: NylarIV
IP: X.X.X.10

Solaris X86
Roles: Ecommerce
Hostname: PersiVIII
IP: X.X.X.25

Ubuntu
Roles: Ecommerce Backend
Hostname: Spheron1
IP: X.X.X.26

FreeBSD
Roles: Mail
Hostname: Chapek9
IP: X.X.X.7

Sample Set of Supported Client Architectures:

Windows XP
Linux
Windows 2000

As far as we know 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:

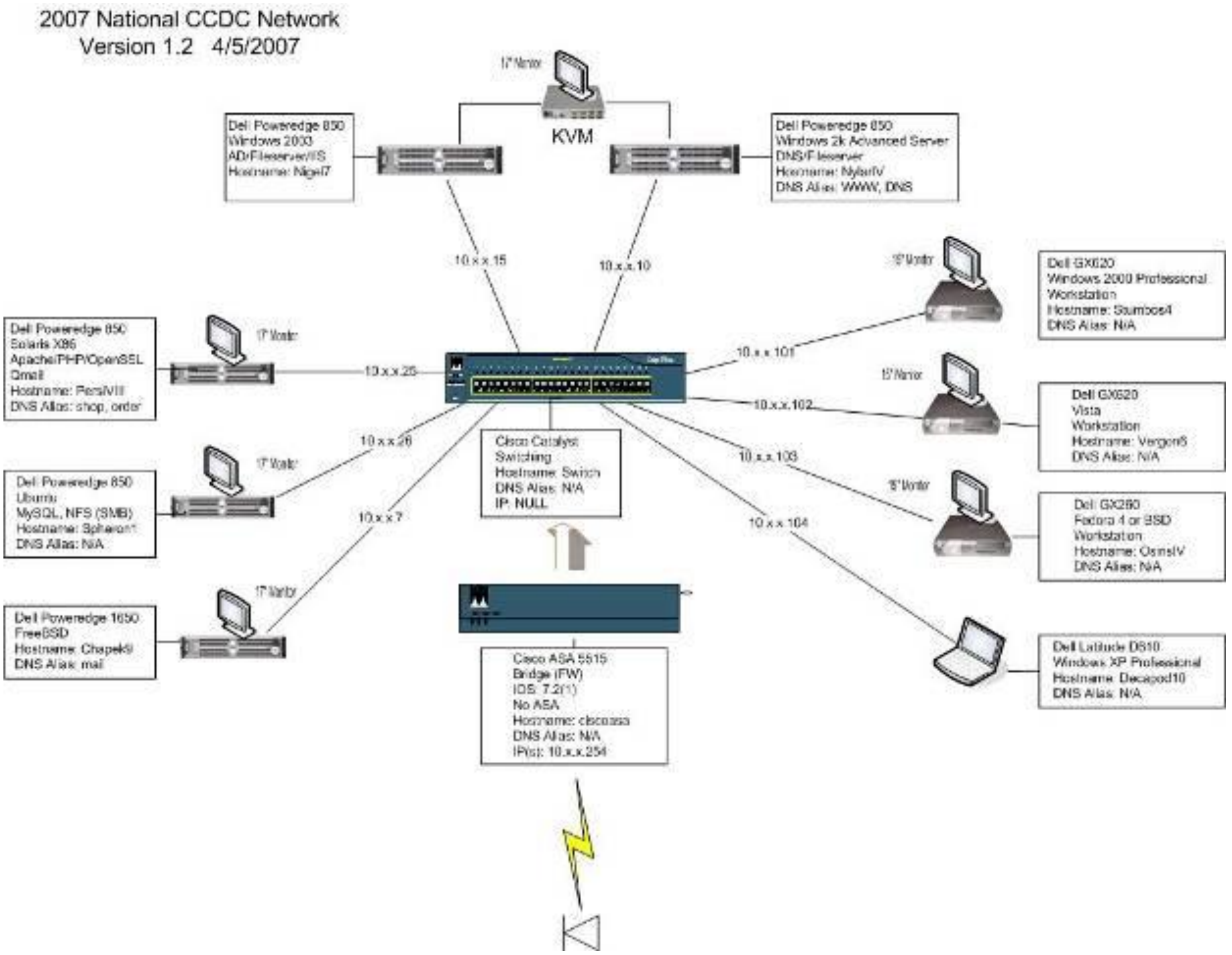
- Mail (POP, SMTP)
- Web (shop.burnsodyne.com, www.burnsodyne.com)
- DNS

Internally:

- File Servers
- Network Printers
- Clients
- Active Directory
- Network Monitoring
- Network Printing
- 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.

Burnsodyne Network Diagram


2007 National CCDC Network
Version 1.2 4/5/2007
17" Monitor
KVM
Dell Poweredge 850
Windows 2003
AD/Fileserver/IIS
Hostname: Nigel7
Dell Poweredge 850
Windows 2k Advanced Server
DNS/Fileserver
Hostname: NylarIV
DNS Alias: WWW, DNS
10.x.x.15
10.x.x.10
Dell Poweredge 850
Solaris X86
Apache/PHP/OpenSSL
Qmail
Hostname: PersiVIII
DNS Alias: shop, order
17" Monitor
10.x.x.25
Dell Poweredge 850
Ubuntu
MySQL, NFS (SMB)
Hostname: Spheron1
DNS Alias: N/A
17" Monitor
10.x.x.26
Dell Poweredge 1650
FreeBSD
Hostname: Chapek9
DNS Alias: mail
17" Monitor
10.x.x.7
Cisco Catalyst
Switching
Hostname: Switch
DNS Alias: N/A
IP: NULL
Cisco ASA 5515
Bridge (FW)
IOS: 7.2(1)
No ASA
Hostname: ciscoasa
DNS Alias: N/A
IP(s): 10.x.x.254
19" Monitor
Dell GX620
Windows 2000 Professional
Workstation
Hostname: Stumbos4
DNS Alias: N/A
10.x.x.101
15" Monitor
Dell GX620
Vista
Workstation
Hostname: Vergon6
DNS Alias: N/A
10.x.x.102
15" Monitor
Dell GX280
Fedora 4 or BSD
Workstation
Hostname: OsirisIV
DNS Alias: N/A
10.x.x.103
Dell Latitude D810
Windows XP Professional
Hostname: Decapod10
DNS Alias: N/A
10.x.x.104