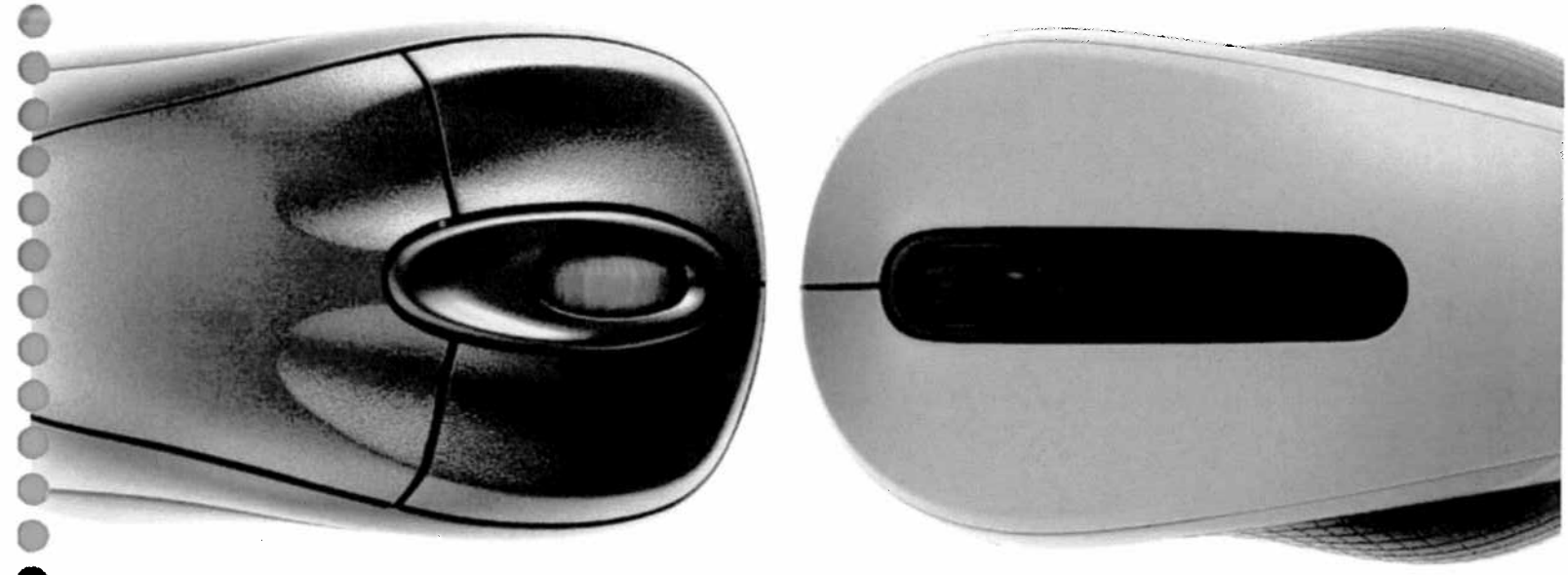
Deloitte.

NATIONAL
COLLEGIATE
CYBER
DEFENSE
COMPETITION

2011 National Championships

Presented by Deloitte



April 8–10, 2011
San Antonio, Texas

NATIONAL
COLLEGIATE
CYBER
DEFENSE
COMPETITION

2011 National Collegiate Cyber Defense Competition

April 8 – 10, 2011

San Antonio, TX

Team Packet

Hosted by the Center for Infrastructure Assurance and Security

Table of Contents

On behalf of the Institute for Cyber Security's 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 Sixth 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 Deloitte, our other industry partners, and 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 10 regional competitions with the winner from each being invited to the national championship. We are in the process of identifying additional host universities to reach this goal. As we asked after the previous national competitions, 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

2011 NCCDC Presented by:

Deloitte.

Platinum

Homeland Security

Gold

redlambda

CORE SECURITY TECHNOLOGIES

McAfee

Silver

splunk>

zynga

RAPID7

Trustwave
Security begins with Trust

NORTHROP GRUMMAN

Sponsors

SAIC
From Science to Solutions

OPSWAT

Microsoft

infosecurity
STRATEGY. INSIGHT. TECHNIQUE.

WOLFRAMRESEARCH
MAKERS OF MATHEMATICA AND WOLFRAM|ALPHA

DENIM GROUP

Supporters

Vic Helbling Consulting

ISSA
Information Systems Security Association
The Global Voice of Information Security

NATIONAL COLLEGIATE CYBER DEFENSE COMPETITION

CIAS CENTER FOR INFRASTRUCTURE ASSURANCE AND SECURITY

Competition Schedule

Please note that due to the nature of the competition, schedule changes may occur.

Thursday, April 7th
Teams arrive; no official events scheduled

Friday, April 8th

10:00 AM to 10:45 AM	Registration
11:00AM to 11:59 AM	Opening Ceremonies (Ballroom E)
12:00 PM	Competition Day One Starts
12:30 PM	Pizza lunch available (Ballroom E)
2:00 PM to 3:30 PM	Coaches Meeting (Lone Star Ballroom West)
6:15 PM	Competition Day One Ends
6:30 PM	Sponsor Dinner (Hilton restaurant)

Saturday, April 9th

8:45 AM	Morning announcements (Ballroom E)
9:00 AM	Competition Day Two Starts
12:00 PM	Pizza lunch available (Ballroom E)
5:00 PM	Competition Day Two Ends
5:15 PM to 6:00 PM	Guest speaker: Lee Kushner (Ballroom E)
6:30 PM to 9:00 PM	Recruiting Mixer (Lone Star Ballroom)

Sunday, April 10th

8:45 AM	Morning announcements (Ballroom E)
9:00 AM	Competition Day Three Starts
12:00 PM	Competition Day Three Ends
12:30 PM	Awards Lunch (Ballrooms B, C, and D)

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 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.

Throughout these rules, the following terms are used:

- Gold Team/Operations Team - competition officials that organize, run, and manage the competition.
- White Team - competition officials that observe team performance in their competition area and evaluate team performance and rule compliance.
- Red Team - penetration testing professionals simulating external hackers attempting to gain unauthorized access to competition teams' systems.
- Black Team - competition support members that provide technical support, pick-up and deliver communications, and provide overall administrative support to the competition.
- Blue Team/Competition Team - the institution competitive teams consisting of students competing in a CCDC event.
- Team Captain - a student member of the Blue Team identified as the primary liaison between the Blue Team and the White Team.
- Team Co-Captain - a student member of the Blue Team identified as the secondary or backup liaison between the Blue Team and the White Team, should the Team Captain be unavailable (i.e. not in the competition room).
- Team representatives - a faculty or staff representative of the Blue Team's host institution responsible for serving as a liaison between competition officials and the Blue Team's institution.

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

h. Team representatives, 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.

i. 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.

j. 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.

k. 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.

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

m. 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, Ops 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, Disputes, and Disclosures

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. Local Competition Rules

a. MP3 players may be brought into competition rooms and are permitted with headphone use only. Smart phones may be used as MP3 players.
b. Incident reports must be complete to receive any consideration for points. You may use the provided form or create your own but all incident reports must have team number, date, source IP, destination IP, date/time of activity, description of activity, and remediation/mitigation plans.
c. All operating system and application changes not specified by inject must be approved **prior** to implementation.
d. All use of virtualization not specified by inject or currently part of the competition network must be approved **prior** to implementation.
e. You must configure all SMTP servers to allow the scoring engine to connect to and send mail from a valid user at your organization to another valid user at your organization.
f. No food is allowed in competition rooms. Drinks may be brought into team rooms but **MUST** be placed on tables away from competition equipment.
g. Teams must not intentionally disconnect competition systems from the network unless moving cables from one system to another.

Scoring

The winner will be based on the highest cumulative score at the end of the competition. Accumulated point values are broken down as follows (some variance in points may occur due to the timing and randomization of scoring engine checks):

- Functional services account for roughly half of the possible points (based on a random polling interval of core services)
- Successful completion of business tasks account for roughly half of the possible points (awarded points will vary by task with a cumulative total of roughly half the possible 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 semi-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 any critical service. For example, if a critical service is down continuously for 6 service checks, the team will be assessed a 50 point penalty. After a service is down for 6 consecutive checks, **each additional 6 consecutive checks** a service is down will result in an additional 50 point penalty. The specific number of service checks used during the competition will be addressed by competition officials prior to the start of the event.

Business Tasks (Injects)
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 completion of any tasking will result in a team penalty and can 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:

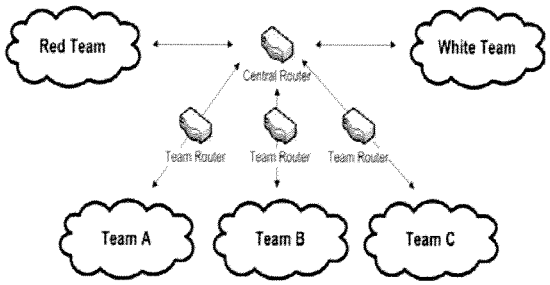
- Obtaining root/administrator level access to a team system: -100 points
- Obtaining user level access to a team system (shell access or equivalent): -25 points
- Recovery of userids and passwords from a team system (encrypted or unencrypted): -50 points
- Recovery of one or more sensitive files or 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
- Recovery of encrypted customer data or an encrypted database: -25 points

Red Team actions are cumulative. For example, a successful attack that yields root level access and allows the downloading of userids and passwords will 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.

Red Teams will also be allowed to perform malicious actions based on their access such as defacing websites, disabling or stopping services, removing or modifying files, etc.

Logical Network Diagrams

Overall Competition Network Layout

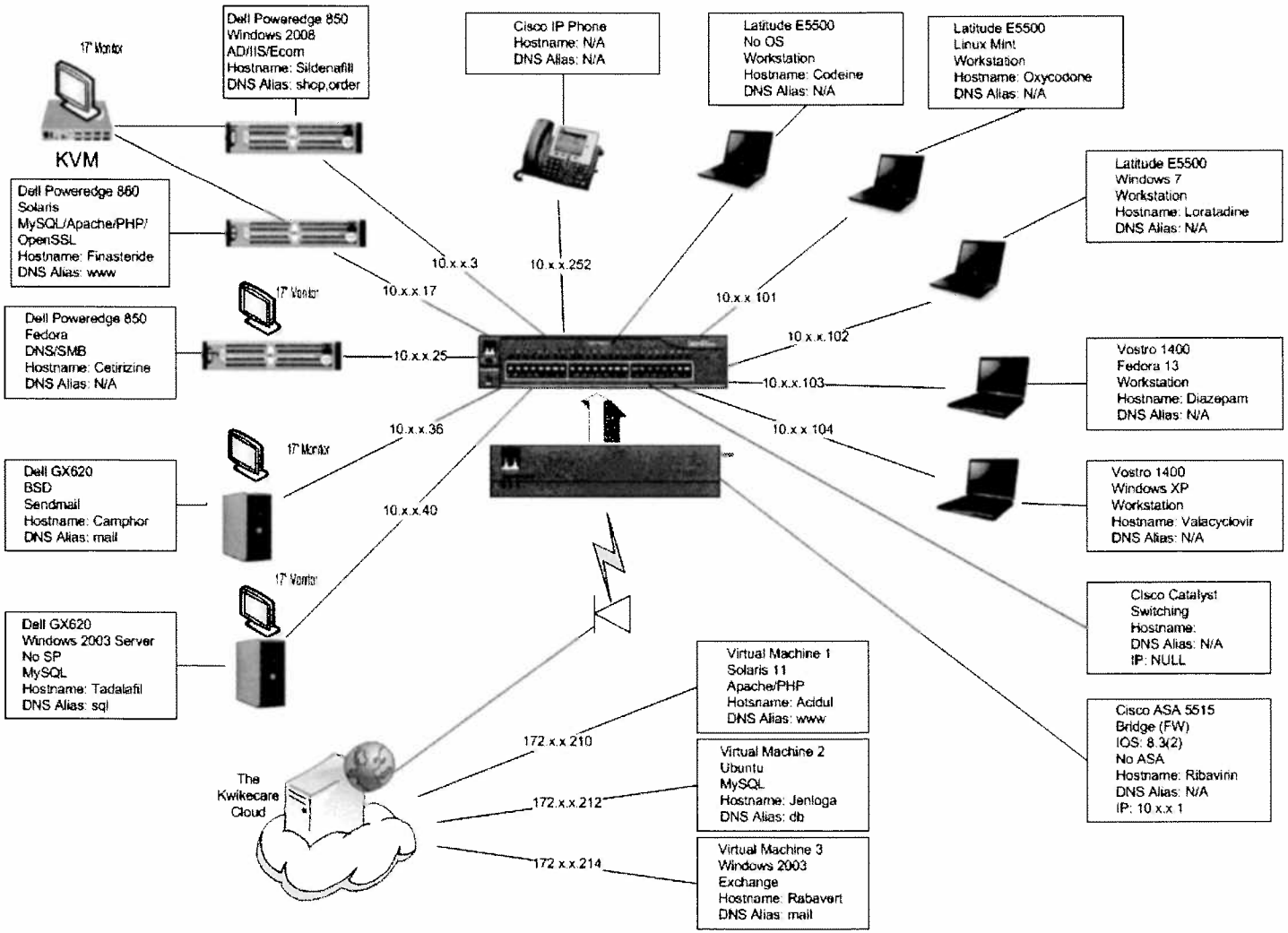


The Red Team network, the White Team network, and each team network will be connected to a central router that will be maintained by the White Team.

NATIONAL COLLEGIATE CYBER DEFENSE COMPETITION

CIAS CENTER FOR INFRASTRUCTURE ASSURANCE AND SECURITY

Team Network Diagram



NATIONAL COLLEGIATE CYBER DEFENSE COMPETITION

CIAS CENTER FOR INFRASTRUCTURE ASSURANCE AND SECURITY

Letter from KwikePills Director of IT

KwikePills

From: Philip Carson
To: IT Staff
Subject: Welcome

Welcome to the KwikePills team! We're thrilled to have you on board. As you know from your hiring briefings, we had to replace our entire group of system administrators and security personnel. And they were not happy about being fired. While everything "seems" to be working I'm quite sure we've got some major issues that need to be addressed on our network – and we're counting on you to do that for us.

You're now responsible for managing and maintaining our network. Patch and repair as you see fit, but before you go making any big changes like replacing applications or operating systems come see me for approval.

Our network really consists of two organizations. We have the main KwikePills network as well as our recently acquired subsidiary KwikeCare to maintain. KwikeCare's servers are hosted in a cloud environment off-site and we have no physical access to them.

Remember we rely on our network and public services a great deal so keep them running! You should be maintaining the following services at all times:

HTTP and HTTPS on 10.X.X.3
HTTP on 10.X.X.17
SMTP on 10.X.X.36
DNS on 10.X.X.25
HTTP on 172.16.X.210
SMTP on 172.16.X.214
SSH on 172.16.X.212

We may be adding to that list, but that's the initial list of critical services you need to have up, running, and accessible to the public at all times. BTW it looks as if the HTTPS service may not be configured quite right on the e-commerce site - that should be fixed ASAP. And some of the workstations appear to be missing software as well.

Thanks,

Philip

KwikePills Network Information from the Director of IT

The KwikePills network has quickly become a vital part of our business. shop.kwikepills 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 1 10.10.10.0 and 172.16.10.0 (.com)
Team 2 10.20.20.0 and 172.16.20.0 (.net)
Team 3 10.30.30.0 and 172.16.30.0 (.org)
Team 4 10.40.40.0 and 172.16.40.0 (.shop)
Team 5 10.50.50.0 and 172.16.50.0 (.biz)
Team 6 10.60.60.0 and 172.16.60.0 (.us)
Team 7 10.70.70.0 and 172.16.70.0 (.pro)
Team 8 10.80.80.0 and 172.16.80.0 (.int)
Team 9 10.90.90.0 and 172.16.90.0 (.med)

Subnet mask: 255.255.255.0
Default gateway: 10.X.X.1
NOTE: The .1 address belongs to the competition network and is your default gateway. Do not attempt to use the .1 address inside your team network.

Cisco switch:
Span Port: is normally the last port on the switch but you can change that
Uplink Port: 1

Cisco ASA:
10.X.X.2
Uplink: Interface 0

Laser printer:
Currently not functioning as a "network" printer

Server Architecture:

Windows 2008
- Roles: AD, IIS, E-com
- Hostname: Sildenafill
- IP: 10.X.X.3

Solaris x86
- Roles: Web Server
- Hostname: Finasteride
- IP: 10.X.X.17

Fedora
- Roles: DNS/SMB
- Hostname: Cetirizine
- IP: 10.X.X.25

Windows 2003
- Roles: Database
- Hostname: Tadalafil
- IP: X.X.X.40

BSD
- Roles: Mail
- Hostname: Camphor
- IP: X.X.X.36

Solaris x86
- Roles: Web Server
- Hostname: Acidul
- IP: 172.16.X.210

Ubuntu
- Roles: Database
- Hostname: Jenloga
- IP: 172.16.X.212

Windows 2003
- Roles: AD, SMTP
- Hostname: Rabavert
- IP: 172.16.X.214

Sample Set of Supported Client Architectures:

Windows XP
Linux
Windows 2000 Professional
Vista Business
Windows7

The previous administrators should have set all administrative level passwords to either "changeme", "changeme!", "password", 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 (SMTP) – must be available at the 10.X.X.36 and 172.16.X.214 addresses
HTTPS/HTTP

- HTTP must be available at the 10.X.X.17 and 172.16.X.210 addresses
- HTTP and HTTPS must be available at the 10.X.X.3 address

DNS – must be available at the 10.X.X.25 address
SSH – must be available at the 172.16.X.212

VoIP - Inside your network is a Cisco VoIP phone with an IP address of 10.X.X.252. You must allow it to communicate with the 10.120.0.X and 10.110.0.X network for your voice service to work. If you restrict the traffic to/from this phone you must determine the ports required for VoIP communications and allow those in and out of your network.

Internally:

File Servers
Network Printers
Client Workstations
Active Directory
Network Printing
Internet Access

Outbound Services:
Your user base will need unrestricted outbound access to common protocols such as HTTP, HTTPS, SSH, FTP, SFTP, POP3, DNS, update services, etc.

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.

Please note that systems identified as user workstations must remain user workstations – they cannot be re-tasked, reloaded, etc unless you are instructed to do so with an inject. You will have one system identified as an "admin workstation" – that system you may reload, change, or update in any way you like including replacing the entire operating system.

Networks available for internal NAT:
You may use any 10.X.X.0 network for internal NAT where the second octet matches your team network's second octet. For example Team 1 could use 10.10.20.0, Team 2 could use 10.20.90.0, Team 3 could use 10.30.20.0, and so on.