Experiences During a Collegiate Cyber Defense Competition

By: Paul Sroufe, MS, Steve Tate, PhD., Ram Dantu, PhD, and Ebru Celikel Cankaya, PhD

P. Sroufe, S. R. Tate, R. Dantu, E. Celikel. "Experiences During a Collegiate Cyber Defense Competition," Journal of Applied Security Research, Vol. 5, No. 3, 2010, pp. 382–396.

Abstract:
The objective of this article is to encourage schools to participate in the Collegiate Cyber Defense Competition (CCDC) and to ease their entry by providing information about the event and describing the experiences of both the student participants and the educators. This article focuses mainly on the recent experience of a University of North Texas student team at the Southwest Regional CCDC 2008 hosted by Del Mar College in Corpus Christi, Texas. It describes the entire process of participating in the CCDC, including announcements, team formation, task assignments, preparations, and actual team experience during the competition and provides suggestions on strategies for future competitions.
Keywords: Cyber defense competition, servers, operating systems, network configurations

Article:

INTRODUCTION

The Collegiate Cyber Defense Competition (CCDC) is a 3-day defense-oriented competition in which the competitors provide and sustain the security of an enterprise network infrastructure, together with a well-maintained business information system, all while under attack from a "red team" put in place by the contest organizers.

The objectives of the CCDC are designed to meet the needs of both students and educators. For students, CCDC's objectives are to provide them a platform in which to apply computer and network-security-related concepts, encourage them to work harmoniously in teams (even under unexpected conditions), allow them to develop good communication skills among themselves and in a business environment, and teach them the value of ethical work under all circumstances. For educators, the CCDC's objective is to provide them a means of testing their course content and seeing how it helps students to solve real-world problems.

Because getting involved in this intense 3-day competition can be intimidating for schools that have not experienced CCDC before, the goal of this article is to share the experiences of the University of North Texas (UNT) so that interested schools know what to expect and can develop their teams and strategies to be competitive in the CCDC.

The contest and its evolution over the years are described in a series of papers by the contest creators (White & Williams, 2005; White & Dodge, 2006, 2007) and at the National CCDC website (2009). The contest has grown from the initial contest in April 2005 involving five teams from Texas to a coordinated set of seven regional contests and a total of 56 schools in 2008 sending regional winners to a final national competition in San Antonio, Texas. UNT has participated every year since the beginning of the contest, sending teams to compete each year and serving as the regional competition site and host in 2007. Although we describe experiences from our competing all 4 years and hosting a large regional competition, the most valuable information and primary focus in this article is based on the experiences and student reports from the latest regional competition, hosted by Del Mar College in Corpus Christi, Texas, from February 29 through March 2, 2008.

CONTEST OVERVIEW

This section gives a brief overview of the CCDC contest. Although there are variations between the different regional contests, there are some common components and a common set of goals as defined by the National CCDC organizers. The competition is based on a business scenario—student teams manage the information technology (IT) infrastructure of a company, which is already established at the beginning of the contest.

In the 2008 Southwest Region competition, hosted by Del Mar College, student teams worked for the fictional company "ValveX" and were given the company's business policy and other documents, such as a directory. The services required on this network were defined by the contest organizers, and certain information had to be maintained on the system. Throughout the contest, the organizers provided specific tasks, called "injects," that the teams had to perform (e.g., setting up a new service or adding new users). Points were awarded to teams for successful completion of the injects as well as for "uptime" of the required services as monitored by an automated scoring engine. During the contest, a "red team" of experienced penetration testers constantly tried to break into or disrupt the team networks, and points were deducted when the red team logged a successful exploit or retrieved sensitive information from a team's network. The teams were allowed to request certain recovery tasks but had to pay for them by giving up contest points.

The 2008 Southwest Region CCDC was an intense program spanning three days. Each day's competition ran from 8 a.m. to 8 p.m.; the half-day ran from 8 a.m. to 12 p.m. on Sunday. The participants and the organizers of the contest consisted of the following groups:

BLUE Teams: Each of the eight schools competing was designated as a BLUE Team; each competing team had up to eight members, including a team captain.

RED Team: Unbiased information security professionals from academic, commercial, military, and government organizations volunteered their skills to assist in the assessment of a team's ability to defend its network and services. This team periodically probed, scanned, and attempted to penetrate BLUE Team networks.

WHITE Team: This group served as room judges and referees in the various competition rooms. This group consisted of information security academics from the competing institutions and industry representatives. Each competing team was assigned a WHITE Team member on a rotational basis to assess the team's ability to maintain its networks and service availability based on a business inject and a scoring instrument.

GOLD Team: This team consisted of the competition administration of the contest hosts. For the 2008 Southwest Regional competition, the administration consisted of Del Mar College Computer Science/Information Technology faculty and industry professionals who conducted the exercise. This team was responsible for administering the competition from the master scenario event list, injecting business process events, and handling or mediating challenges.

TEAM INFORMATION

According to the rules set by the CCDC organizers, teams can have up to eight students, with no more than two graduate students. No team member can be working professionally in the area of computer security for more than 20 hours per week.

Announcing the CCDC event to attract students interested (as well as experienced to some degree) in the computer security field was the first step in team formation. We posted the announcement of the CCDC event on bulletin boards and let students know about it in related courses, such as Computer Security, Computer Networks, and Secure E-Commerce. The first two years of UNT's participation in the CCDC included students from the UNT College of Business Administration who were majoring in Business Computer Information Systems. Having business students on the team helped with the business organization aspects and added valuable breadth to the experience of our team members. However, in the past 2 years, we have not made this connection and the team has not had students with a business and management mindset. *For future competitions, we suggest having at least one team member who is studying business.* In addition to being

beneficial to the team, the business students provided our students an opportunity to meet others with similar interests but whom they would not normally meet in the course of their studies.

Recruiting student participation was difficult because the CCDC took place in the middle of the semester and students knew that it would require intense preparation. Still, some students were very enthusiastic about the CCDC and participated in the preparations and the whole process from the very beginning.

The CCDC rules allow teams to have alternates. We considered having alternates and let as many students as possible attend the initial meetings. Students who were not selected as team members helped in practice sessions by both giving advice and acting as stand-in red teams. In the end, we selected two students as alternates for the 2008 contest. One team member was selected Team Captain, and one student who had participated in a previous year but was ineligible to compete because of the restrictions on the number of hours of work in the security field was designated as "student sponsor."

TASK ASSIGNMENT AND PREPARATION

Distribution of Tasks

As part of preparations for the contest, we set up regular weekly meetings to discuss what types of tasks, servers, and security requirements would be needed for the competition and to assign tasks. We assigned a few (typically two or three) tasks per student, with the following distribution of tasks:

- Student 1: Virtual Private Network (VPN)/Firewalls
- Student 2: Web Servers, Database
- Student 3: File Transfer Protocol (FTP)/Secure Shell (SSH)/Syslog's
- Student 4: FTP/SSH/Syslog's
- Student 5: Active Directory, Internet Information Services (IIS), Windows
- Student 6: Active Directory, ITS, Windows
- Student 7: E-mail Servers, Domain Name System (DNS), FreeBSD Security, Web Servers
- Student 8: File Servers, Samba, Common Unix Printing System (CUPS), Linux System Administration

Task Preparation

In the Computer Security Laboratory, the team members tested and implemented security tools to be needed during actual competition. At this stage, the earlier experiences of the student sponsor were helpful. Based on the plan announced by Del Mar College and based on experiences in previous competitions, our team started preparations for the competition. Finding time for practice was not easy for students who were in the middle of the semester with their classes, assignments, and tests; but each student spent extra time and effort to prepare for the event.

Preparation Issues

The team captain was expected to take care of the business side of the competition. The captain was also assigned AD tasks but did not know how much time he could spend with the team while overseeing business. Another student thought that the competition in itself was a game and that it was interesting to play as long as it lasted. Team members had varying degrees of skills and interests. Some students were participating for the fourth time and some for the first time. Students did meet a few times, but a rehearsal with the whole team was needed.

NETWORK SETUP

The computer systems, networks, and security lab equipment provided during the competition are as follows (Figure 1). On the first day of the competition, the following systems and configurations were provided to the teams:

- Three 3COM switches (one of them had a connection to the Internet line, and the other two switches were used to bridge intra-network workstations or servers)

- A laptop for general testing and penetration testing

- A canary to keep track of the services' availability

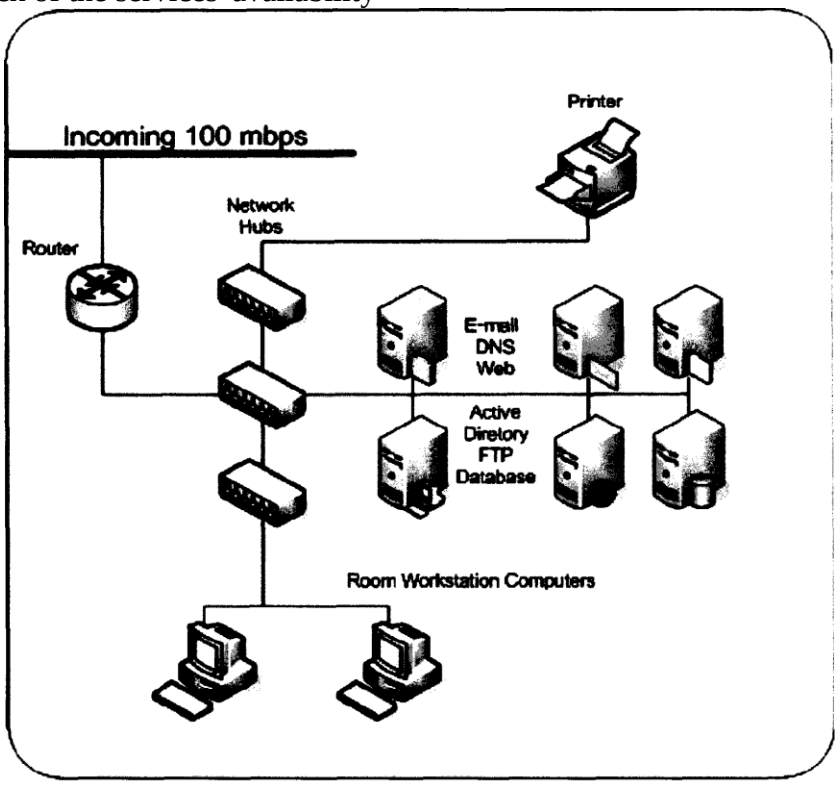

FIGURE 1 CCDC room layout.

- Six servers, two workstations, a telephone, a printer, universal serial bus (USB) backup hard drive with about 400 GB, 1 GB of flash memory, and a workstation from which we received notifications from the GOLD Team

- Supplies, including about 20 blank compact discs (CDs), removable self-stick notepads, markers for the white board and for boxes, regular writing notepads, operating system (OS) installation CDs (including FreeBSD, Fedora 8, Ubuntu 7, Windows 2000 Server, Windows 2003 server, and Windows XP), and some driver files provided by CCDC

On the second day of competition, in addition to the configurations listed above, a laptop with Internet access was provided to the teams. This laptop allowed the teams to download "free software" and shareware and to burn CDs, although teams were not permitted to use the USB flash drive with this system. On the last day of the competition, a Cisco ASA 5505 router and a Cisco x501 router with a Cisco PIX firewall were added to the systems in the BLUE Team rooms.

Day 1

All teams arrived at the competition location, registered, and received identity badges and other registration materials. After the orientation session, we learned that seven teams were competing this year, along with a "wildcard team" made up of students who were present but not part of an official team. The teams drew straws

to receive team numbers and were then taken into competition rooms assigned by number. After the teams were led to their rooms at the beginning of the contest, sponsors were no longer allowed to enter the competition room of their team. During the competition, the sponsors were working as WHITE Team members, observing teams other than their own (on a rotational basis) and communicating the GOLD Team's requests to the competing team (via their team captain). All communication between the competing team and the GOLD Team had to be done via formal memoranda and through the WHITE Team members. This requirement was part of the ValveX Corp. business plan that was used as the plot throughout the competition.

During the first day, the fictional contest scenario involved a hurricane striking the company's location, taking all of the servers and services down. Teams needed to back up their files and systems in order to protect themselves against this scenario hurricane.

Shortly after the introduction and presentation of the contest rules, the CCDC director received a phone call. This call started the competition as the director played a contrived weather reporter who suggested that a hurricane was coming to Corpus Christi, Texas, the site of the fictional team's company as well as the actual contest location. As the teams were ushered off to their rooms, they had 2 hours to work on their servers before lunch would be served. During this time, the team captain was called away for several meetings with the management (the contest GOLD team). The team captain would come back with suggestions of things to do; for example, backing up our services, users, and so on. The teams were told about the USB hard drive at orientation; but after opening the box of equipment, our UNT team found a USB stick of only 1 GB, which was not enough to contain all the data needed. Our team proceeded to back up some of the "essentials" onto it. However, our main backup plan, which was executed, was making and storing backups on every computer. With about 10 minutes remaining until lunch (and the hurricane), our team found the 120-GB USB hard drive behind one of our monitors. At this point, we did not have enough time to do anything with it.

At lunch, more of the hurricane update videos were played, and all the teams were then told, for the first time, that the hurricane had struck our data center and that we needed to have our backups with us. We were then going to proceed to our backup data center where we would have all the same equipment but would have to make a fresh start. Going back to the rooms, we had to prepare a disaster recovery plan, which we would present to the GOLD Team before we would be allowed to touch any of our equipment. As soon as we were allowed into the room again, to our surprise, nothing was in the servers and everything was erased. So, to start competing, we did not have any backups. If we had asked for the backups, then we would have gotten them at the cost of some contest points. We installed two FreeBSD servers and two GNU/Linux servers running Ubuntu. We quickly got the hypertext transfer protocol (HTTP), HTTP Secure (HTTPS), SSH, SSH file transfer protocol (SFTP), and MySQL Services running on those FreeBSD servers. A binder full of OS discs was used to reinstall our servers. Using FreeBSD and Windows server 2003, we started the long and arduous task of returning our servers to working condition. Even after bringing some of our services online, we had to buy back (using our competition points) our data that we should have had backed up, such as our database, Web pages, user accounts, and so on. This mistake was very costly, and we also lost a lot of uptime on our services. After presenting our backup plan, the GOLD Team turned the Internet on for 2 hours. We could only make effective use out of the Internet for about an hour because our servers had nothing on them, and we had to install the OSs first.

The first day of competition ended at 8 p.m.

Day 2

Day 2 started at 8 a.m. After the first day's warm-up session, our team made a lot of progress on day 2. The team members maintained good communication with each other and with the WHITE Team members.

Mid-Saturday, we finally got our services running, half of them at first (HTTP, HTTPS, FTP) and then a few hours later simple mail transfer protocol (SMTP), post office protocol version 3 (POP3), and DNS. After finally getting our services running, we started to focus on security concerns. Using FreeBSD's Internet protocol

firewall and a software Ethernet bridge, one of our team members custom-built a firewall script that enabled access only to the services we had running and specifically only on its IP address, such as HTTP on port 80 on the designated Web server (see Figure 2). Then we set up a network scanner that watched traffic over the Ethernet bridge. We were not allowed to block traffic from the RED Team's IP address block; so we watched as failed login, failed network scanners, and failed port access filled our log files. Meanwhile, our team worked diligently to migrate our services to multiple servers for fault tolerance.

Toward the end of the day, the GOLD Team distributed an inject that was very costly and would require a team effort to overcome. The GOLD Team informed each of the teams that there was a hardware vulnerability in the Dell Power series 2950s (the Dell 2950s were by far the most powerful servers that the teams were provided with). Each team would need to have the servers ready for pickup by the end of the day. "Ready" meant that we had to back up and power down those servers. For our team, however, the main portion of our services resided on other server machines; so we overcame this problem easily. It is worth mentioning that the GOLD team appreciated creativity from a business standpoint. Knowing this fact, our team developed a scenario in which we researched the hardware's vulnerability, had an expert hardware technician onsite, and repaired the vulnerability before the end of the day. We then wrote a design document, schematics, Dell online support, and outlines on how we fixed the issue. We turned in this document to the GOLD Team before the end of second day. Our team was able to keep the use of these servers throughout the next day.

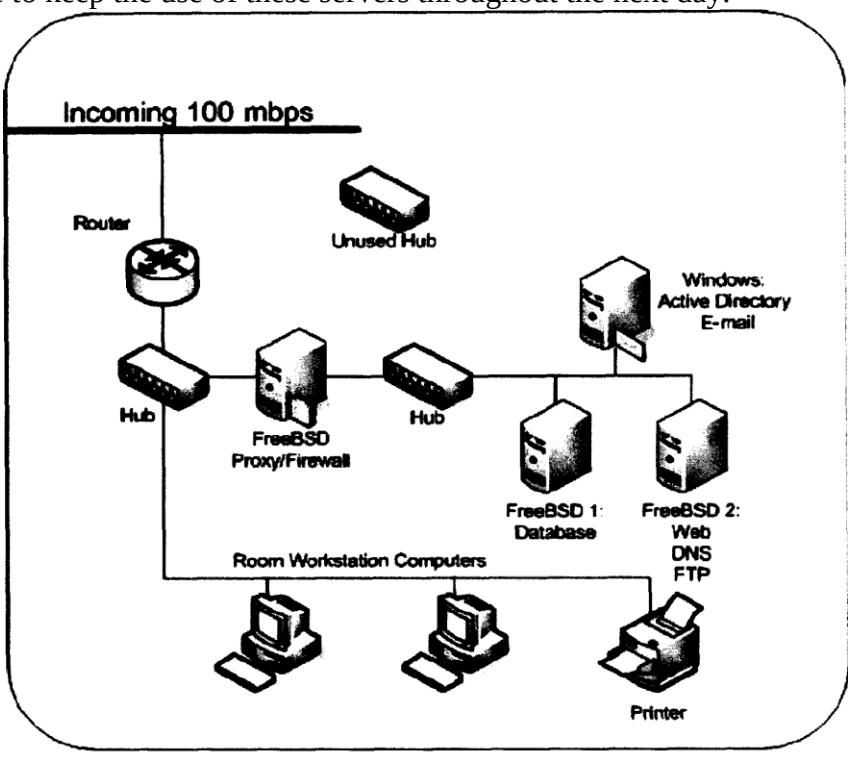

FIGURE 2 Room layout—Post hurricane (Day 2).

On the second day, a WHITE Team member came in and delivered a router but with the wrong cable. When the team tried to set up and configure the router, it could not communicate to the router through "HyperTerminal." The team needed an adapter with a serial port or a crossover cable to be able to do that, but the team was provided a regular local area network (LAN) cable.

Day 3

Day 3 again started at 8 a.m. but ended at 12 p.m. The teams were asked to keep satisfying business injects while the RED Team continued with different attacks.

As Sunday began, we received a Cisco ASA router, which we were allowed to use in any way that we wished. Our team was unfamiliar with the Cisco Internetwork Operating System (I0S); and as a result, we spent a lot of our focus working to configure our Cisco device. Paralleling our time with the Cisco router was our final set of

injects given by ValveX management (the GOLD team). At this point, we had our network running as well as possible given our current experience, and we rode out the rest of the day staying on top of RED team access attempts, Cisco configuration, and the remaining injects.

At the end of the competition, there was an award ceremony in which the winners were announced. Texas A&M University (TAMU) at College Station won first place, and the University of Louisiana was the runner-up. Through informal feedback, we learned that our team was in a block of teams that were very close in points for 3rd through 5th places. The official results have not been announced yet.

CCDC 2009 UPDATE

This section briefly covers the participant side of the Southwest CCDC 2009 competition hosted by Texas A&M University (TAMU) at College Station, Texas. The TAMU CCDC competition was significantly more difficult than that of the CCDC 2008 at Del Mar. The initial setup was very similar: Unix server and Windows implementations running multiple Web sites, e-mail, DNS, and file sharing.

The initial setup stage was also more difficult. An expert knowledge of systems administration was necessary, both in Unix and Windows. Some of the more difficult initial tasks were to gain access to a FreeBSD server that had its keyboard set to another language and correctly defend a very out-of-date Windows box.

During the 2009 competition, TAMU added features to the events. One added feature was an online store whereby contestants were awarded money for completing contracts (injects) that could be spent to buy computers, routers, and other equipment. This year, TAMU also added voice over Internet protocol (VoIP) to the mix and in one contract required the teams to configure a VoIP telephone to a central private branch exchange (PBX). Some contracts, if applicable, would add a service to your scoreboard. Some service contracts would lead to more service contracts, creating a tree-like structure of possible services. Missing a contract early on would be very costly to the total possible point accumulation.

Preparation for a CCDC competition of this magnitude should begin at least 6 months ahead of time and should include several team members with significant experience in Windows and Unix administration. If some of your participants are new to the field and wish to learn by example, they will find themselves left behind with nothing to do.

ISSUES AND LESSONS LEARNED FOR PARTICIPANTS

This section is based on student feedback. The RED Team members gave a quick overview of what they saw during the course of the 3 days. One of the first things that the RED Team mentioned was that they had obtained root/admin access to six out of the eight teams and all the user names and passwords. In hindsight, the team believes that the best strategy might have been to remove the team from the network until everything was secured and ready to be deployed. However, after asking the RED Team about our team after the hurricane, they had only one thing to say: "We saw you had an extra service running, which was SSH; and although it didn't have any immediate vulnerabilities, it would have been the first place I would have started, if this weren't a competition."

The second thing we learned almost from the start was that, even in a short contest like this one, it is vital to have a solid contingency plan and to back up, back up, back up. Even if there is not a hurricane staring you down, you should always have a recent backup of your work.

Third, this event was a competition, and the scoring engine was running. We should have quickly deployed all solutions on one server to start gaining points (hopefully before the other teams) and then from there expand the complexity of our network using different servers and several firewalls.

Fourth, even if you are a diehard Unix/Linux user, you should not underestimate the ease that a Windows server can provide you. We were so focused on our Unix servers that we neglected the fact that the Windows server

can deploy an e-mail, POPS, and DNS server with the click of a few buttons. This action would have been invaluable for gaining points early on. Although some would argue that the Windows server is less secure, it does not matter because during the time that it would take the RED Team to compromise your server, you could have designed and deployed a secure Postfix e-mail server. We should never forget that we are getting points based on running services and not from how fancy the Unix/Linux e-mail solution is.

Fifth, practice before you go to the competition. We knew we were not going to have access to the Internet while we were at Del Mar College, but we did not know how badly it would affect us. Practice on your own time with your favorite OS installed without using the Internet and with getting all the described services running. Find a good team leader who has some experience and knowledge to lead the team in showing them how to do everything (starting from scratch on your own can be painstaking).

Last, the most valuable experience we gained was going and participating in an exceptional competition. Students found the competition to be a very useful activity, and the ongoing CCDC annual contests add a valuable piece to the students' educational experience.

We had students with diverse technical backgrounds on the team; so the team was good at securing systems, given enough time. For most systems, there was almost always a person or two who knew about the subject at hand. However, sometimes our team was weak at following procedures. Brushing off things like equipment checks, backups, and visitor credential checks cost us many points in this competition. We need to emphasize the importance of backing up systems. In the competition, we were able to sacrifice some points to use their data restore disks; but in the real world, if we do not back up the data, there would not be any way to bring back lost data. We also need to figure out a better way to divide labor. Two team members were not able to do too much during the competition because the computers they were using did not have many services.

RUNNING A REGIONAL CONTEST

The previous sections have described the CCDC contest in general and given some information on what teams wanting to participate can expect. In this section, we give information for schools considering hosting a CCDC contest, based on our experience hosting the 2007 Southwest Regional CCDC.

Hosting CCDC is an intense event that cannot be taken lightly. In our case, the 2007 Southwest Regional competition was one of the largest ever held, with 10 teams of 8 students each. This activity required full use of 14 rooms, around 100 computers with a diverse set of operating systems and applications, and approximately 100 people at the contest. Because of the large facility requirements, the contest had to be scheduled when it would not conflict with other university classes or activities; so like many other regional contest hosts, we chose to schedule the contest during Spring break in March. Preparations began in earnest several months before the contest, with the formation of the contest advisory board consisting of faculty who had organized or participated in past CCDC events. Input from previous contest organizers was absolutely vital, for there are thousands of man-hours of contest experience that can and should be tapped into by any school wishing to host such a contest.

The next task was to create the scenario, complete with a company "story" and company policy, and design the team network architecture. The technical task of creating the contest infrastructure was handled by a team of one faculty member and three graduate students at UNT, who built a full team network and simulated contest infrastructure in a security research lab. During this time, students who were part of the UNT competition team were not allowed to use this particular lab (which had been used in previous years for team practices) in order to prevent the UNT team from inadvertently discovering any information about the contest. Since our facilities required the teams to be distributed throughout a large building, we chose to use existing network infrastructure rather than run separate dedicated wiring, as had been done in several other contests. In order to use the existing infrastructure, we tunneled all contest network traffic over the existing university network, with a tunneling router in each contest room and a centralized router handling all the tunnels in the contest control room (from

which the GOLD team operated). This setup worked extremely well during the contest, with no network infrastructure issues.

While the contest network was being designed and tested, the injects to be used during the contest were being created. During the design phase, we made changes to the network architecture to accommodate ideas for injects, and we had new ideas for injects based on our experience of putting the systems together. It is vital that people involved in these two phases of the contest design talk regularly and exchange ideas.

When the network design was stable on our test machines, we started working on the machines to be used during the contest. With 7 machines used by each of the 10 teams, it is obviously not a trivial matter to come up with 70 machines that can be moved and re-tasked for the contest. Our solution was to use several large labs of machines used by our introductory programming classes and set up a separate partition on the hard drives for the contest setup. This way, we could install and configure systems on the partition in the weeks leading up to the contest; and during class times, the original partition would remain hidden to students in classes, who would continue working with the standard lab configuration.

In the days leading up to the contest (over Spring break when the labs were not in use), we reset all systems to boot to the contest configuration; but since the contest configuration was already present and "hiding" on the disk, we could reset all the machines to the contest configuration in a matter of hours.

In the initial contest announcements, we described the machine setup and asked that teams avoid the standard lab setup partition if possible so that resetting the machines to the student lab setup would be easy after the contest. Many teams, however, wanted to do clean operating system installations during the contest, and they accepted the default disk layouts, which destroyed the partition we were trying to save. In the end, around one-third of the machines had to be re-imaged to the student lab setup after the contest, but it was much better than having to re-image all 70 machines.

Given to size of the contest, the operations went remarkably smoothly. The most serious problem that arose was that in the last minute of moving machines from the security lab into the rooms used in the contest and reconfiguring machines, the machine that we had used in the lab for our test-scoring engine was inadvertently reinstalled and the entire scoring engine was wiped out. This problem was only discovered shortly before the contest, and the first few hours of the contest went without a scoring engine as we rebuilt pieces from backups and reconstructed pieces on the fly. Ironically, this problem would have been avoided if we had followed the advice better that we drilled into our students: back up, back up, back up. The other problem we encountered was that several faculty members and graduate students who were initially supposed to help with the contest could not be at the contest. This "personnel shortage" was overcome with help from other faculty and volunteers during the contest, but our advice for teams hosting a contest is to make sure that they have enough fault-tolerance in personnel as well as equipment to handle unexpected events.

CONCLUSIONS

The CCDC was a defense-based competition. Each team defended its systems against the RED Team's security attacks, such as stopping Internet services; attacking the Web server, DNS server, and mail server; attacking root passwords; and so on. Every communication needed to be done through a business model. So, the teams prepared every request and response in a formal memorandum format. This preparation was particularly important in providing students with a means of testing themselves in a real-world scenario.

Interaction with GOLD Team members, WHITE Team members, and other team members helped build new communications among the participants. Our team (as well as the other teams) were very enthusiastic, hard-working, and interacted harmoniously with each other. This competition gave us the opportunity to be in a real-world environment to test what we know and how we can apply that knowledge. The team took lessons well and was willing to do better to recover. This was a very good experience for each participant. All of the students

involved reported that they learned a lot during the competition and would recommend it to other students interested in information assurance.

We also had a chance to meet with colleagues and students who share the same interests. CCDC 2008 was a good opportunity for the upcoming years' competitions. We believe that more students will be attracted to the competition in future years. The CCDC 2008 event was helpful and didactic in every sense for our team. Each member learned a lot; this knowledge will be helpful for the upcoming years' competitions. For the next time, our team plans to announce the event not only in the Department of Computer Science and Engineering but also in the Department of Business Computer Information Systems to form a more heterogeneous team.

Overall, hosting CCDC is an extremely satisfying but exhausting and intense experience. Schools interested in hosting such a contest are advised to start planning early, to have a way to set systems up as far in advance of the contest as possible, and to over-design in both equipment and human supplies to be prepared for unexpected events.

REFERENCES

National CCDC. (2009). Retrieved June 2009, from http://www.nationalccdc.org/

White, G. B., & Dodge, R. C. (2006). The National Collegiate Cyber Defense Competition. *10th Colloquium on Information Systems Security Education* (pp. 68-74).

White, G. B., & Dodge, R. C. (2007). The National Collegiate Cyber Defense Competition: What are the Next Steps. *11th Colloquium on Information Systems Security Education* (pp. 117-122).

White, G. B., & Williams, D. (2005). The Collegiate Cyber Defense Competition. *9th Colloquium on Information Systems Security Education.*