CCDC Team Preparation Guide

Version 1.0

NATIONAL COLLEGIATE CYBER DEFENSE COMPETITION

Collegiate Cyber Defense Competition

CCDC Team Preparation Guide
Table of Contents

Collegiate Cyber Defense Competition
Team Prep Guide

What this guide is:
This guide is designed to assist students in preparing a new or inexperienced team for competition in the Collegiate Cyber Defense Competition program (CCDC). This guide will cover basic topics such as how the competitions are organized, how points are scored, suggestions on team composition, sample injects, and so on. Much of the material presented in this guide was collected from highly successful CCDC teams.

What this guide is not:
This guide is not an exact "how to" or checklist for CCDC victory. There is no single "right" answer or team makeup that will guarantee victory at any CCDC event. This guide will provide you with the basic concepts and point you in the right direction, but the challenge of building and preparing your team is up to you.

What is CCDC:
CCDC is a tiered competition system (state, regional, nationals) that exercises both technical AND business skills. CCDC focuses on the operational aspects of managing and protecting an existing "commercial" network infrastructure. Your team will be securing, managing, and maintaining a small business network – responding to business tasks called injects, a live Red Team that is attempting to break into your systems, and maintaining a core group of "critical services" such as a mail server, e-commerce site, etc.

How CCDC is scored:
Teams are scored on three main areas:

- Critical Services: During each CCDC event, a set of critical services is identified that teams must manage and maintain at all times. Those services are checked for functionality and availability throughout the competition – you gain points each time one of your services is "up" or functioning properly when it is checked. If one or more of your services are down for an extended period of time your team will be assessed with a service level agreement violation and you will lose points.
- Injects: Injects are business tasks teams must address or respond to during the competition. Injects range from the very simple, such as resetting a user's password, to the complex, such as migrating web servers from IIS to Apache with zero down time. Many injects have a written portion, such as a report detailing actions taken by your team or the creation of a new business policy. Injects are weighted – more complex and lengthy injects are worth more points than simple injects.
- Red Team Activity: Teams lose points to successful Red Team activity based on the nature of the activity and the level of access obtained. User

level access costs a team fewer points than root/administrator level access which costs less than the Red Team downloading a team's entire client database with credit card numbers.

NOTE: You may find variations in scoring between CCDC events, please make sure you check the local rules for your event before making any plans or decisions based on scoring weights.

Team Composition:

Teams that do well at CCDC events possess strong organizational, writing, process, time management, and technical skills. As teams progress up the ladder in CCDC events, the balance between the skill sets becomes even more critical as the challenges increase. Past winners of the National CCDC have demonstrated that a well-organized, balanced team has a higher probability for success at CCDC events. Teams possessing the following skill sets tend to perform better at all CCDC events:

- Time Management: CCDC events tend to be hectic with many different activities needing to be accomplished at the same time – you may be patching systems, responding to injects, and fending off the Red Time while creating a new Social Media policy. Being able to rank order tasks, allocate the appropriate amount of time to them, and meet assigned deadlines is very important in CCDC events.
- Delegation: CCDC events are a team effort, but successful teams must be able to "divide and conquer". Teams must be able to identify what needs to be done and then assign the tasks to individuals or small groups. Delegation and division of duties can be extremely important at CCDC events.
- Writing: The ability to communicate your ideas clearly and effectively on paper is very important at CCDC events – just as it is in the business world. At CCDC events your team will see purely technical tasks AND tasks that involve written responses.
- Organizational: CCDC events can be stressful and it's far too easy for an entire team to get focused on what the Red Team is doing or why a particular service isn't functioning properly and start missing inject deadlines. An organized team approaches a CCDC event with a game-plan. They know which team members will be responsible for specific tasks, they know who will be keeping an eye on deadlines and deliverables, and they know who will proof-reading inject responses.
- Flexibility: No campaign plan survives first contact with the enemy and at CCDC events teams have to be willing and able to make changes to their approach. Have a team member that's a HP-UX expert but there's no HP-UX systems to play with? Be ready to re-assign that team member to other tasks. Have three injects that involve written responses? Be prepared to pull a team member off patching/backup duty for an hour to help catch up.

- Technical Skills: Technical skills are a fairly obvious requirement, but diversity of technical skills is something teams tend to overlook. Having a single "expert" for a given technology is great – until that person becomes overwhelmed or gets sick. Having a primary expert with one or more secondary experts can be very beneficial.
- Conceptual knowledge vs. Specific knowledge: You never know exactly what sort of environment you'll be walking into at a CCDC event. As each one is different, having a firm grasp of **concepts** is very beneficial. For example, if your team understands how a firewall works and has hands-on experience with one platform you are better able to adapt to a new firewall platform. It is much easier to learn the specific commands for a new firewall platform if you understand how access lists work.

The Team Captain:
At every CCDC event you will be required to identify a Team Captain – this individual is your team's primary interface to the White Team and other competition officials, should have a clear understanding of the rules, and be able to make decisions on your team's behalf. Whether or not your Team Captain is the individual "running" your team internally is up to you. While many teams have their Team Captain serve as their primary interface and team lead, other teams have found it advantageous to have a Team Captain that serves as the official team interface to those outside your team and a Team Lead that manages the team from an internal perspective.

Can anyone besides my Team Sponsor help us get ready to compete?
Absolutely. During your preparations, you are encouraged to seek assistance/guidance from past participants, faculty, members of the IT industry, and so on. A good source of expertise can be found in the local chapters of professional organizations such as ISSA (www.issa.org) or ISACA (www.isaca.org). Local companies and professional organizations are also good potential sources of sponsorships that help offset the costs of attending state or regional events.

Is writing that important to CCDC?
As they are in most business environments, writing skills are emphasized at CCDC. While no one expects you to produce perfect output in a stressful competition format, items such as formatting, spelling, use of complete sentences, and so on are taken into consideration with grading written responses. A poorly written response that looks like it was thrown together with little to no effort will receive a lower score than a similar response that is well formatted and well presented.

Inject Deadlines
Almost every inject you see at a CCDC event will have an associated deadline (complete this task in the next X hours/minutes). Meeting those inject deadlines is very important – your team has no chance at receiving full points for their inject responses unless you meet the associated deadlines. However, in some cases you may still receive some points for

turning in a response late. As many CCDC injects build upon each other it can still be very much worth your while to complete an inject even if you are unable to complete the inject on time.

Setting up a practice environment

A typical CCDC competition provides each team with a small business network. Network size, design, and composition will vary between events but a sample CCDC network might be composed of the following devices:

- 5 Servers
- 5 Workstations
- 1 Firewall
- 1 Switch
- 1 Printer

Operating systems that are used as server platforms include versions of Windows and UNIX, such as Windows 200x, Fedora, FreeBSD, and Solaris. Workstations are provided to the teams and may have any operating system running on them so prepare you team to handle both Windows and UNIX based desktops.

On servers, it will be in your best interest to include older operating systems in your preparations as well as older versions of application services like Apache, BIND, or Sendmail. It's best to become familiar with their vulnerabilities and learn how to quickly apply patches and updates, upgrade to newer versions while maintaining existing data, or even replace applications with alternates (such as migrating from IIS to Apache or vice versa).

CCDC Scoring engines check for the availability and integrity of services such as SMTP, DNS, POP3, HTTP/S, SSH, FTP and SQL. As you install operating systems in your test lab, make sure these services are installed, configured, and running as well.

After a working test environment has been established, the team can practice by having a coach provide injects that must be completed within a preset time duration, practice patching and securing servers, or even scrimmaging each other or other schools in a mock CCDC event. Success at the NCCDC will be based on how well a team prepares for the event. Winning teams have been known to practice from four to six hours per week.

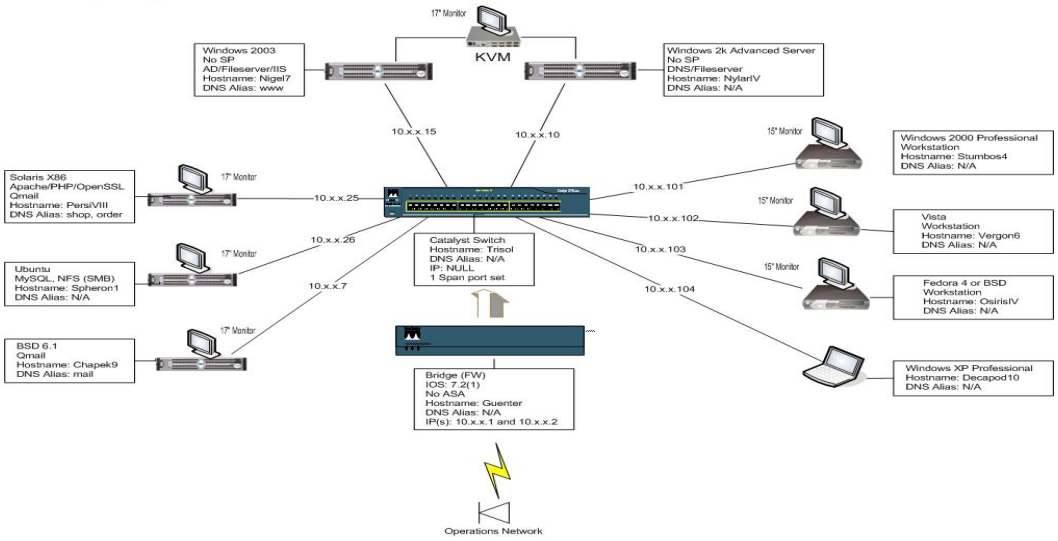

Figure 1: Example CCDC Network

Note: Every CCDC event has a different network structure, the above is merely an example of what a CCDC network might look like.

Concepts

Below is a list of the critical concepts to familiarize yourself and your team with while preparing to compete in a CCDC event. This is by no means a comprehensive list of everything each CCDC event will encompass; in fact some of these concepts may not be present at all or may not be emphasized during a particular event. However, having a thorough understanding of the following 10 concept areas will help your team be competitive with the other schools represented at the competition. For each of these core areas, you should be familiar with how the concept applies to securing a network, reacting to incidents, and so on. For example, with a core concept such as firewalls, your team should be familiar with how to use those types of products including deployment, configuration, using them to control traffic flow, analyzing log data from them, maintenance, and so on.

1. Perimeter Security – Network and Host based firewalls, how they work and how to configure them, as well as Intrusion Detection Systems, Virtual Private Networks, and DMZs.
2. Flashing/Patching – Both Hardware and Software Flashing/Patching
3. Networking – Traffic flow, switching, and routing.
4. UNIX – Multiple flavors of UNIX such as Fedora Core, Solaris, Gentoo, BSD, Ubuntu, etc.
5. Windows – NT, 2000, 2010, XP, 7
6. User Management – Adding and deleting users on multiple Operating Systems and managing those user accounts
7. Services and Applications – Email, DNS, HTTP, HTTPS, SQL, Web applications
8. Tools - Port Scanners, Vulnerability Scanners, MD5, and Software based firewalls and IDSs.
9. Authentication – Beyond just knowing how to change passwords in multiple environments also understanding other forms of authentication such as multi-factor, biometrics, and tokens
10. General - Performing admin duties such as installing, securing, updating, troubleshooting, and maintaining the functionality of computer systems on a network.

Web Resources

Below are lists of web sites that contain information that may prove useful during any given CCDC event or during your preparation. Please note that these pages are not being operated, managed, or maintained by CCDC affiliates. The sole purpose of this list of links is to provide teams with example web sites that may provide a useful concept or tool. **WARNING: Some of these sites are run by the hacker community and should be visited at your own risk.**

- Administration
  - http://www.technicalinfo.net
  - http://tldp.org/
  - http://onlamp.com/
  - http://technet.microsoft.com
  - http://www.rootsecure.net/
- Assessment
  - http://osvdb.org/
  - http://packetstormsecurity.org/
  - http://www.securityfocus.com/
  - http://sectools.org
  - http://www.insecure.org/
- Incident Response and Forensics
  - http://www.cert.org
  - http://www.first.org/
  - http://www.computerforensicsworld.com/
  - http://www.forensicfocus.com/
  - http://www.e-evidence.info/
  - http://blog.securitymonks.com/
- Malware
  - http://www.malwarehelp.org/
- Perimeter
  - http://www.networkworld.com/topics/security.html
  - http://www.owasp.org
- General
  - http://www.scmagazineus.com/
  - http://www.sans.org/security-resources.php
  - http://searchsecurity.techtarget.com/
  - http://csrc.nist.gov/
  - http://www.us-cert.gov/
  - http://www.itsecurity.com/
  - http://www.securitynewsportal.com/

Security and Administration Tools

Competitors should be familiar with running assessment, incident response, and network administration/troubleshooting tools on multiple platforms. As with the links in the previous section many of these tools are developed by the hacker community and should be **used with extreme caution** on a segregated network with no route(s) to other networks (ie. a closed loop practice network not connected to anything else). **Do not use these tools on any network where you do not have explicit permission to do so!!!**

- Assessment Tools:
  Backtrack, Codescout, Metasploit Framework, Microsoft Baseline Security Analyzer, Nessus, Netcat, Nikto, Nmap, Paros Proxy, Superscan

- Forensics Utilities:
  Coroners Toolkit

- DNS Utilities:
  Digg, Nslookup, Whois

- Packet Analysis:
  Ettercap, TCPDUMP, Wireshark

- Compression Utilities:
  Gzip, 7-Zip, Tar, Zip

- Perimeter Security:
  Iptables/TCP Wrappers, Snort

- Password Auditing:
  John the Ripper, L0pht Crack, Cain and Abel

- Miscellaneous Tools:
  GCC, Make MD5, Microsoft Update, Nagios, PGP, PHPMyAdmin Ping, Sysinternals, Traceroute, Tripwire

- Training:
  Hackme Bank, Books, Casino, Shipping, or Travel, WebGoat, WebMaven

Appendix A: Sample Injects

Injects are essentially business tasks ranging from the very simple to the very complex. Though you may see some similarities, each CCDC event uses a different set of injects and they may be delivered to your team in a slightly different way between competitions – some events may hand you a piece of paper, some events may email them to you, others post them on a website. Regardless of delivery method every inject will have tasks and objectives and the more complex an inject is, the more points it is probably worth. In this appendix we've provided two sample injects from past CCDC events.

Sample Inject #1

From: Philip Carson

To: IT Staff

CC: Stephen Gearheart, Milburn Lauffer, Jannine Paul

Subject: New Printer

We just received an HP 2300 network capable printer and we need it setup and working on the LAN in the next 45 minutes. Please set it up so that anyone in the company can print to it (all servers and workstations). You should have the printer in your area already.

Thanks,

Philip

Discussion of Sample Inject #1

This inject is asking you to take an HP2300 laser printer, set it up as your network printer, and then make sure that EVERY system in your team network can print to it in the next 45 minutes. To accomplish this task, your team would need connect the printer to your internal network, assign it an IP address, and then setup each server and workstation to print to that HP2300. When injects say things like "all servers and

workstations" they mean every single server and workstation regardless of operating system – don't assume if a server is Solaris or Linux based it won't need to print and neglect to set up printing capability on those systems. To get full points for this inject you need to make sure every system can print. When an inject like this is scored, White Team members will attempt to print from one of more systems in your team network – you may get partial points if 2 of 3 systems that were tested print or you may get no points at all as the inject required you to setup ALL systems. This type of inject is testing your team's ability to move quickly (you only have 45 minutes) and solve a technical issue.

Sample Inject #2

From: Philip Carson

To: IT Staff

CC: Stephen Gearhart, Adam Waverly, Jannine Paul

Subject: Public FTP Site Launch

Folks,

As part of our continuing mission to provide better IT services for our customers and our employees, Grand Chasm is launching a public/private FTP site. I need you to stand up an FTP service on Stingray with a public side (that allows anonymous access) and a private side (that only allows Grand Chasm employees to access it). Please place the files on the accompanying CD on the FTP site (there's a folder called public and one called private). Put the public files right at the top level of the FTP service so visitors can see them immediately when they login. Please create a DNS entry as well so users can access ftp.grandchasm.com as well as 10.X.X.10 and get to our FTP site. We will be placing some Grand Chasm files out there, so make sure all the employees can access the private side. I suspect most users will be using standard FTP clients to get to this site. Anyway, we need this up by start of business tomorrow and then it needs to remain up indefinitely (or until you hear otherwise).

Thanks,

Philip

Discussion of Sample Inject #2

This inject is asking you to setup an FTP site with a public side and a private side and indicates there is a CD containing files for both side of the FTP site. You are also being asked to create a DNS entry called ftp.grandchasm.com linked to a specific IP address in your team network. You should notice a few things about this inject:

1. The FTP service should be installed on a server called "Stingray". In some cases injects will specify what platforms you need to update/change/modify and in others you will be free to choose. When an inject specifies a server, as it does in this case, that's where you should be installing the new FTP service. If you've made changes to your network that make it difficult to complete the inject, it's your responsibility as a team to let the White Team know as soon as you get an inject like this – they may allow you to install the FTP service on a different system or may tell you to do the best you can given your current circumstances. But you need to speak up as soon as you get the inject! Don't wait until the inject is being scored or time is up.
2. It does not specify what FTP server application you should use. In this case you are free to choose a product that you are familiar with and will work on the operating system of the system where you install the FTP service.
3. There are files that need to be placed in specific locations – some on the top level of the public side and some on the private side.
4. The inject tells you that employees will be accessing the private side – they'll need userids and passwords to do this. If you have a single sign-on solution in place, you're all set – otherwise you'll need to make sure all the employees in your "company" have access to the FTP site.
5. Once established, the FTP service needs to stay up and running for the rest of the competition. This can indicate that the FTP service will become a critical service in the near future (scored by the scoring engine) or could indicate this inject will be scored more than once to ensure the service remains active.

When an inject like this is scored, it is typically done both internally and externally. In other words, White Team members inside your team room will score part of it (the employee access portion for example) and White Team members outside your room will score part of it (remote, public access).