Hello future CCDC members!

Thank you for your interest in CCDC! We hope you like it. Since training for CCDC is not as black and white as other competitions are… this document is used as a starting point. It will encompass the CCDC logistics, my recommendation for somebody who is just starting, and common things seen at the competition. For the interest and purpose of having you learn about things, this does not include how to spin up the service, etc. we want you to explore and discover it on your own. Figure out your niche and what you are comfortable with. Step out of your comfort zone and learn things that might make you uncomfortable. But just remember the captains apart of your team are here to help when you are confused or stuck. They might not be able to give you the final answer but can give you the guidance you might need.

But don't give up right away, CCDC is a fun time and even though it seems stressful. It's just a group of students having some fun and learning things about blue teaming.

CCDC Logistics:

You are a team hired by an organization to harden and protect the current network they have set up. You will also be tasked with creating and gathering information as requested throughout the competition. During this time "professional" hackers will be trying to infiltrate the network and cause more chaos to the event. Scoring is typically based on service uptime, inject competition, red team detection, resumes, and hidden gems removed in the OS (such has hidden credit card files, etc.)

Your team consists of 3 - 8 people, each person assigned to a service and one person as a scribe (in charge of the inject system, turning injects in, and putting injects out to the appropriate service). You are allowed up to 2 – 4 alternates to take a spot in the case that something happens to the main team member.

At state alt's participate in a non-scoring event, but are not allowed to join for later events at the physical competition

Before the competition itself there is an invitational that does not affect your chance in winning state. The purpose is to get to know the system used for the competition etc.

Following invitational, the week prior to the competition is the "practice" session. We are given full access to the environment and allowed to scrub and wipe it as many times. This is the time to get familiar with the setup, be able to harden within a 15-minute time window and discover all the things. So, you aren't completely blind-sided going into the competition.

At the competition you are given 15 minutes to harden your services. This is the time in which you should at least have completed the following:

CHANGE ALL PASSWORDS
ENFORCE FIREWALL RULES
TURN OFF UNECESSARY SERVICES/PROCESSES RUNNING
REVOKE ACCESS TO RANDOM USERS

Keep in mind this is the bare minimum of what should be done… you will obviously want to do more to make sure your service is harden to its fullest capacity (this can be tested during the week before the competition) and during your practice sessions to try out new things with the service you have spun up on a local VM or ESXI server (depends on how the captain wants to run practices). If you don't get through all the hardening within the first 15 don't worry, you still can harden… but the first 15 is just a guarantee that hackers won't do anything…

The competitions go as follows:

State -> wildcard placement (for those that win 2nd at state) -> regionals -> Nationals

Each increasing in difficulty as you progress further.

One thing to keep in mind is that you will not be allowed to bring your own technology in, but you can bring in binders, books, papers, etc. that might be useful for your time at the competition. You will have access to the internet so don't be too discouraged that you have to memorize everything.

In the case that your service is destroyed and there is no returning you are allowed to ask for a reset on that specific service… just know that you lose points to ask for a scrub. You also lose points if a hacker can successfully do something within their list of "techniques" (which we are unaware of… but think basic attacks (DDOS, DNS poison, Malicious files used for remote access, Generic passwords not changed, etc.)

Recommendation for beginners:

First start by spinning up a service listed below. Understand what it does and why it works the way it does. Once you can confidently do that, start work on hardening the service. Figure out what firewall rules might be useful to restrict outside access but still make the service run. Next, break your service. Intentionally change a setting or delete a config file. Then try to fix it. You want to make sure that in the case your services break during the competition you can try to fix it based on working knowledge. Once you are proficient find the hidden gems of the service… by this I mean find the settings that might be useful or things that might not useful. Try to use older OS's too… the competition doesn't do the latest and greatest software for the purpose of trying to make you use your knowledge to harden things that might have huge vulnerabilities compared to a new OS that's not as vulnerable.

If you really want a challenge… become the red teamer after you harden your service. See if you can hack it, learn from it and then redo it. REMEMBER TO BACKUP YOUR SERVICE BEFORE THIS POINT… you want to have a working service, so you don't have to spin it up from the ground up every time.

One thing to note. You will be overwhelmed, and you will not know what to expect and that's okay… take a deep breath and just focus. Nobody is expecting you to have the entire working knowledge of all of this. This is a learning experience for all. From a personal standpoint… I was an alt for the team in 2019-2020 and was dealing with some personal issues up until a couple weeks from the competition but got put as a primary spot and had to learn bind DNS in less than 2 weeks… and now I am captain ☺. I am not saying you should take this route. but it's possible. I knew nothing and now I know a ton, but not everything in the world. YOU. GOT. THIS.

-Lexie Nelson
Captain of CCDC 2020-2021

P.S. Once you are done and feel competent in one topic, switch to another. The more knowledge you know the more knowledge you know.

Linux services

1. Web service utilizing Apache, MySQL, and PHP (e-comm website)
2. Bind DNS 9 (used as a secondary DNS)
3. Dovecot Email service
4. Splunk/Phantom

Window Services

1. Window server AD
2. Window Server DNS (primary DNS)

Firewall / hardware services:

1. Iptables
   a. Make sure t look at stateful rules
2. Palo alto
3. Windows firewall
4. Cisco switches and routers (Regionals)
5. ESXI (Regionals)

Scribe duties (services)

1. Working knowledge of what tasks would be assigned to whom and
2. Inject system (you won't be able to see this system till invitational)
   a. YOU WILL BE BLIND SIDED. DO NOT FREAK OUT ☺
3. Understanding of NIST (following standards provided by NIST)
4. Organization and timing
5. Potential templates and verbiage made for turning in injects
6. Professionalism

Other services to note (appear in later competition stage)

1. Librenms
2. Pihole
3. Open-sourced malware scan services (for windows and linux)
4. NTP Server (on clients and host machine)
5. Logon Banner
6. Fail2ban

OS running:

1. Centos
2. Fedora
3. Debian
4. Ubuntu
5. Phantom OS
6. Pan OS
7. Windows 8/10/server 2008

Basic tools you should know how to use:

1. Vi, Vim, Nano
2. Wireshark
3. Linux commands
4. Windows working knowledge
5. Linux working knowledge
6. Know how to spin up your service that you are assigned to
    a. This would not be required at competition but it’s good to have a working knowledge

How to harden services (not applied to scribes)

1. Figure out what firewall rules should be utilized for your service
2. Turn off processes not needed
3. Find the “hidden gems” such as random credit card files, or user data
4. Make sure users or random accounts don’t have admin rights
5. See if there are vulnerabilities with your service
6. Run updates (if needed)
7. Turn off unnecessary settings for your service or lock it down better
    a. Just make sure it’s not to the extreme… otherwise your service will not work/be scored on
8. Research about your service
9. Golden ticket (windows), Iron skillet (palo alto)
10. MySQL hardening