Team Packet
2019 Southwest Regional CCDC

https://southwestccdc.com/

March 13, 2019

Welcome

Welcome to the 2019 Southwest Regional CCDC. Congratulations on reaching the second round of the competition. This packet is your guide to rules and information for this year's competition. We update this every year so please read through this. The Regional competition is a lot more involved and intense than the qualification round. We wish everyone the best of luck!

This document serves as a supplement to the official National CCDC rules (http://nationalccdc.org/index.php/competition/competitors/rules). Reading this document is not a substitute for reading the National CCDC rules. All team members will be expected to have read this document and the rules in their entirety. DO NOT JUST SKIM THEM.

Game Organization

The game is divided into two days of competition. Between the end of day one and the start of day two the game is completely stopped. The scoring engine and all red team activity will stop during competition stops. The game is divided into several teams, each named with a color. Student competitors are on "blue" teams.

Gold Team

Gold Team members are the highest-level game and competition administrators and serve as the chief judges for scoring. A decision from Gold Team is final. Gold team is not part of the game scenario. Gold team members must be allowed in your rooms.

White Team

White Team members support the competition and ensure everything runs smoothly. White Team members are also responsible for delivering items from the store and grading injects. In order to score some injects, White Team members may need to enter your

room to grade an inject. Thus, refusing a White Team member entry into your room may negatively affect your score.

Black Team

As the network and game operations team, members of the Black Team members ensure that the network and systems are functioning as intended as part of the game. Black Team members must be allowed in your room.

Green Team

Sponsors and Observers are part of Green Team. Many sponsors choose CCDC as a way to meet emerging security talent with the hopes of potentially recruiting you in the future for internships and employment. Allowing them to observe the competition from the inside allows them to see team dynamics and to scout for talent. Green Team have been specifically asked to be remain quiet while in Blue Team rooms, however if you feel they are being too distracting you may ask them to leave. If you ask a green team member to leave, please notify white team so we can take preventative steps if continuous problems arise.

Purple Team

Purple Team, known as Orange team at nationals, simulates in-scenario characters. These can be inspectors, co-workers, customers, etc. Purple Team members are tasked with completing tasks for injects. For example, a person from Finance might come by and ask you to help setup email on their laptop. As the IT team it is your task to ensure employees have access to the services needed to keep this company running. If a Purple Team member is not able to complete the required task (either because the service was not available or you refusing to serve them) you will loose the points associated with the tasks.

As the company is a sizable enterprise, the CEO will not be able to confirm who is an employee and which employee needs access to which systems. Additionally, there will not be an inject associated with every request from the Purple Team. Users may drop in and need a password reset and you have to serve them. It is up to Blue Team to validate all requests.

Red Team

Your adversary. Members from the Red Team will attempt to bring your services down, infiltrate the company, and exfiltrate your data.

Blue Team

That's you, the student competitors. You are tasked with operating the network and business operations within the scenario.

Schedule

Thursday, March 21st

- Team Travel Day - teams arrive at hotels.

Friday, March 22nd

- 6:00AM - Breakfast available at Hotels
- 7:30AM - Registration Opens
- 9:00AM - Beginning Brief in Lecture Hall
- 9:50AM - Teams released to rooms
- 10:00AM - Approx Game Start
- 12:00PM - Lunch Available (game continues)
- 6:00PM - Game Stop for the day
- 6:10PM - End of Day Wrap-UP in Lecture Hall
- 6:30PM - Dinner Event in Great Hall (Allen Chapman Student Union)

Saturday, March 23rd

- 6:00AM - Breakfast available at Hotels
- 7:30 AM - Competition Building Open
- 9:00 AM - Morning Brief in Lecture Hall
- 9:15 AM - Game Start for the Day
- 12:00PM - Lunch Available (game continues)
- 6:00 PM - End of game
- 6:10PM - End of Day Wrap-UP in Lecture Hall
- 6:30 PM - Recruiting reception, food and free stuff

Sunday, March 24th

- 6:00AM - Breakfast available at Hotels
- 7:30 AM - Competition Building Open
- 9:00 AM - Morning Brief in Lecture Hall
- 10:00 AM - Teams sent to rooms for post-game analysis
- 10:00AM-12:00PM - Individual Debrief in Rooms (15 min each)
- 12:00 PM - Lunch Available
- 12:30 PM - Room Tear-down
- 2:00 PM - Red and Gold Team Presentation and Q&A
- 3:00 PM - Awards Ceremony and final remarks

Monday, March 25th

- Travel Day - Students must check out of provided hotel

Hotel Information

Teams that are traveling have been provided hotel rooms at the SpringHill Suites at Tulsa Hills located at 1521 West 80th Street, Tulsa, OK 74132. Teams may check-in Thursday, March 21st and must check out no later than Monday, March 25th. The rooms are fully paid but you might be asked to provide a card for incidentals.

Building Location and Parking

You can find a map of the University of Tulsa campus at the following link: UTulsa Campus Map. The competition will be held in Helmerich Hall, #17 on the map. Please park in the UMC parking lot just north-west of the building. You will not need a parking permit or pass.

2019 Business Scenario - Triassic Park

Blue Teams will be working for Triassic Park, a dinosaur theme park based on the island of Isla Fubar. Triassic park was made possible from advances in genetics technology. The park operates services for guests, the dinosaur livestock, and the island staff.

Competition Infrastructure

Blue teams will be provided with a room with a group of physical and virtual machines to manage. These machines will be provided an upstream Internet connection. This connection will be filtered and logged for any unauthorized access to prohibited resources. A NAS will be provided on the competition network with ISOs. All white/red/purple teams share a single mixed and rotating IP space. Blocking addresses from this range is extremely dangerous and will likely result in lost scoring points. Physical security of the team rooms overnight has been accounted for and red team will not have access to the rooms overnight. Do not connect any competition equipment to any wireless networks unless explicitly given permission to do so by an inject, or a black or gold team member.

Business Injects

Teams will be responsible for answering requests, memos and correspondence in a professional manner. Take care to understand what each request is asking for in detail. Do not provide a short memo when asked for a report and do not provide a report as a paragraph. All responses should include the team number, not a school name. Responses to injects and requests for policy related items are scored heavily and can influence the final outcome of the game. Late responses are penalized heavily once they are past the due date, which will be by the minute. A memo reply requested by 10:00 AM that is received at 10:01 will be penalized no less than 50-percent immediately before any subject-matter scoring is completed. All injects will be submitted through the portal (portal.southwestccdc.com). Additionally, all injects for day 1 are due at the end of day 1. No points will be awarded for day 1 inject submissions after the first day. The inject graders always grade the last submitted response of an inject. You are not allowed to reference previous responses. The portal is out of scope for red team.

Services

Teams will have access to the scoring engine to monitor the operational status of their network. Services are checked on random intervals every few minutes. Each of these service checks are worth points. If a service is down, it will not grant any points to the team. All services will be functional when you gain access to the network. It is the team's responsibility to secure them and ensure their continued operation. You will be provided a list of services you are operating along with the network diagram a few days before the competition. Services must remain on the same major version of the software operating the service, same major OS version and the same machine for the first day of the competition, unless otherwise indicated by an inject. For example, a machine running Windows 2008 R2 Server and IIS 7.x must continue to run that version combination for day one. On the second day of the competition, requests for modernization can be sent to the CEO/CIO for consideration. Submit these requests through the portal.

Scoring

Teams accumulate points through maintaining functional network services and by corresponding with the simulated business environment through documents called injects. Injects can be documented technical tasks or business and policy focused. Injects and Services each account for approximately half of the total points available to teams. Red Team activity deducts points accumulated from injects and services scores. Systems will be scored for functionality. For example, an email server must be able to send and receive emails.

User Support

Blue teams will be expected to support requests from simulated customers and users on Purple Team. These requests may come via the company phone, email, or in-person. Users may request password resets, help accessing services or other technical support inquiries. Customers may require help using things.

Team Spending Budget

Teams will be provided a "budget" with which they may buy things they find useful such as portable hard drives, networking equipment and extra cloud VMs and resources. Initially each team will be provided $TBD, available immediately at the start of the game. Large injects and game events may provide your team access to more money to spend. New items may be made available for purchase throughout the game.

Store Access

The store is available through the "Store" tab of the portal site. Your current balance and available items will be there. If you loose all Internet access during the competition and wish to purchase something from the store, you can chat with the store via the canary machine Slack instance. A store manager will be able to tell you your current balance and the status of ordered items.

Gold / Black team support

Through the slack canary you will be able to reach a white team representative who can direct your question to the correct person. If you believe something is severely wrong with the competition please request an escalation to gold or black team. If you call for gold/black team support and if gold/black team deems the issue to be blue or red team's fault the blue team may be penalized up to $500 from their budget, at the discretion of gold/black team. For example, if a laptop's Ethernet port stops working that is not blue team's fault and there will be no penalty. If the red team breaks into a router under blue team control and prevents traffic from being routed, that is blue/red team's fault and the

blue team will be penalized. The penalties only apply for teams who call for gold/black support. If you solve the issue on your own, you do not risk the penalty. However if you believe something is wrong, reach out to Black or Gold Team. This applies to scoring as well. If you believe a service is not being scored correctly, the same penalty applies if scoring is found to be working correctly. The purpose of this is to prevent unnecessary escalations and overloading gold/black team with "tech support".

Red Team

Red team engagement will occur as soon as the game begins. Red team will not have access to this document unless you leak it to them. Red team will document all attacks against your network, successful or not. You have the opportunity to submit an incident response memo whenever you have been compromised. A detailed description of what machine you believe was compromised, it's IP address, the time-frame you believe the attack occurred and what can be done to mitigate future similar attacks is requested. A memo that reads "someone scanned us" will likely be disregarded. Accurate incident responses can recover up to half of the points lost from Red-Team activity. If there was no documented attack or access by red team, you will not regain any points.

NOTE: Red team has been advised not to pursue "scorched-earth" style attacks. If your machine doesn't boot and the partition table is gone, it was likely a blue-team action.

At the regional competition, the red team is allowed to engage in social engineering tactics in a limited scope. We will not disclose all of the rules imposed on red team, however we will disclose the following.

- Red team members are not allowed to posses the following badge colors: Gold, White, Black, Green.
- Red team members must respect all reasonable rules imposed on team rooms, unless the rule conflicts with a competition rule.
- Red team members are not required to identify themselves as red team.

If you feel a red team member has violated a rules above, notify gold team immediately.

Canary

Teams will be provided a dedicated machine for checking scoring, scanning their network from the outside, and for communication needs. Teams will be able to communicate with White/Gold/Black team via a Slack instance provided on the Canary machine. Students are not allowed to share files or information to other blue teams. Students will not have root on the Canary. The Canaries are out of scope for the red team.

Post-Game

The winner of the Southwest Regional CCDC will advance to the National CCDC competition in April. Teams in first, second and third place will be awarded trophies for their achievement. Even if you don't win, we hope the competition will be an exhilarating learning experience.

Resource Links

- Full Game Rules @ National CCDC
- Mubix's How to win CCDC GitHub
- National CCDC Team Prep Guide
- SWCCDC - "What is CCDC video" on YouTube (15 min)
- Intro to CCDC and 2018 scenario review video on YouTube
- Intro to CCDC and 2018 scenario review slides (PDF)