Remote Qualifier Round
Team Packet
2019 Southwest Regional CCDC

https://southwestccdc.com/

February 11, 2019

Game Organization

The game is divided into several teams, each named with a color. Student competitors are on "blue" teams. Game officials are "gold" team. Gold team is not part of the scenario and perform all judging and game administration. The "white" team operates the simulated business and policy aspects of the game. A team of professional penetration testers and will compose "red" team, with the explicit goal of attacking your network. The "black" team handles network operations and game infrastructure.

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 rules. All team members will be expected to have read this document and the rules in their entirety. DO NOT JUST SKIM THEM.

NOTE: YOUR TEAM WILL BE REQUIRED TO SUBMIT RESUMES AND THE ROSTER SPREADSHEET OR WE CANNOT ALLOW YOU TO PARTICIPATE IN THE GAME. THIS IS A REQUIREMENT FROM NATIONAL CCDC.

Business Scenario: CrispyGen

Teams are tasked with operating the network for CrispyGen, a genetics startup. CrispyGen uses CRISPR gene-editing techniques to "upgrade" chicken DNA with dinosaur DNA. Using the dinosaur DNA, these chickens become bigger and tastier. CrispyGen plans to flood the chicken meat market with their patented super-chicken and destroy the current chicken market. Delicious! CrispyGen operates various internal network services, including a high-performance computing environment.

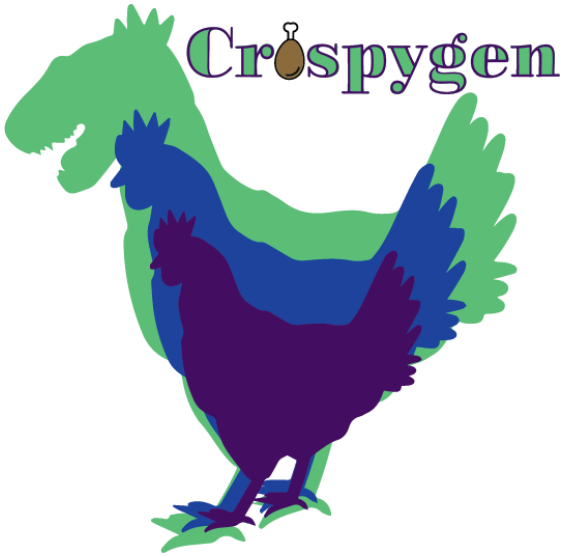

Figure 1: Bok, Bok, ROAR!

On-site Judge

Your team will be required to provide an on-site judge for the remote qualifier round. This judge serves as an impartial third-party and cannot be actively affiliated with your school in any way. The judge needs to have basic technology skills so they can enforce the rules of the game. Judges will also serve as a point of contact for the game organizers during the remote qualifier round. The best judges are former CCDC players and professionals in the security and/or technology fields. Alumni of your school are permitted, provided they are not currently working for or attending your school.

Competition Infrastructure

You will connect to the competition's simulated network environment using OpenNebula. Teams will be allowed to test their connections to the environment on Wednesday the 13th and/or Thursday the 14th when the test environment is ready. Teams will be notified via email when the test environment is ready. Credentials will be sent out via email. OpenNebula relies on VNC for its underlying connections. If you university or location blocks VNC with an application-level firewall, you will need to find a way around this.

For injects, policy, IR, and scoring teams will access portal.southwestccdc.com via a web browser. Your team's credentials for the portal were created when your team signed up for the competition. The SWCCDC Portal and the OpenNebula accounts will be different set of credentials.

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.

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.

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.

Red Team Engagement

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.

Post-Game

The top eight teams will advance to the on-site regional game in March. We will send out the list of teams advancing within a day or two of the qualifier. Teams will be provided with team-specific feedback from qualifiers within 1-2 weeks. There are typically around 20 teams participating in the qualifier and compiling feedback takes some time. Please be patient after the game for specific feedback.

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)
- Regionals Hints