Remote Qualifier Round
Team Packet
2022 Southwest Regional CCDC

https://southwestccdc.com/

February 4, 2022

Game Time

The 2022 Southwest CCDC Qualifier will be held from 2:00PM-6:00PM Central time on Saturday February 5th. We would suggest your team login to Discord and Portal to troubleshoot any issues well in advance.

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.

On-site Judge

Normally teams are required to provide an on-site judge for monitoring their team. For this year, all students should participate from home on their own machines for safety. While this may provide more freedom than in years past, please understand the limitation due to current circumstances and please do not abuse the situation. We will be monitoring the team networks for any suspicious behavior.

Competition Infrastructure

The competition is designed to simulate a work-from-home experience. Participants will compete using their own computers, which connect to the competition environment using a VPN, which will place them on a simulated "Internet" (the Competition "Internet" cloud in the provided network diagram). From there, the blue teams will be able to reach the competition environment over the network from their own computers (or from the optional virtual machine we've provided).

Blue teams should expect to do a significant amount of their competition work over this network, rather than virtual console access to the servers. In addition to the corporate office (bottom half of network diagram), your company operates a cloud environment (top half of the network diagram). The cloud environment is reachable over the network once you're on the competition VPN. It's also managed via the SWCCDC private cloud (running OpenNebula) at https://cloud.southwestccdc.com. You should think of cloud.southwestccdc.com as analogous to, for example, the AWS or Azure web console. Connecting to these instances over the network on the VPN, then, is analogous to connecting to public cloud instances over the Internet. SSHing directly over the VPN to these servers, or using other remote management tools to access them, is encouraged! VPN configuration files and instructions are located in this shared folder:
https://1drv.ms/u/s!AoFtBT9cDltHgdo0B5ctjEePpjFXBA?e=KRSO2E.

Please do not distribute outside of your blue team.

SWCCDC is also providing an optional virtual machine pre-configured with competition VPN access. It is tested to work in VirtualBox. Instructions are located in the readme file in the shared folder link above.

Credentials for the SWCCDC cloud will be sent in the Portal "Announcements" tab. You can test your connectivity to the cloud interface at any time. We'll also have a designated testing time period from noon to 1pm Central time on the day of the competition and we'll provide support for any issues then. Please refrain from creating or modifying any resources in the cloud environment prior to the competition start.

Business Scenario: florp.online, again!

The company for 2022 Qualifiers is similar to the one from 2021, although the IT environment and injects have changed. Florp is a social media video sharing platform that specializes in short videos, up to six seconds in length. Florp was acquired last year; however, due to a failure to successfully merge the business with its parent company, it has been spun back out into its own company again.

Figure 1: Who needs Tiks or Toks, when you can Florp it!

Scenario Network Info

This diagram was found on the floor in the office and may be incomplete or inaccurate, but it's what you have:

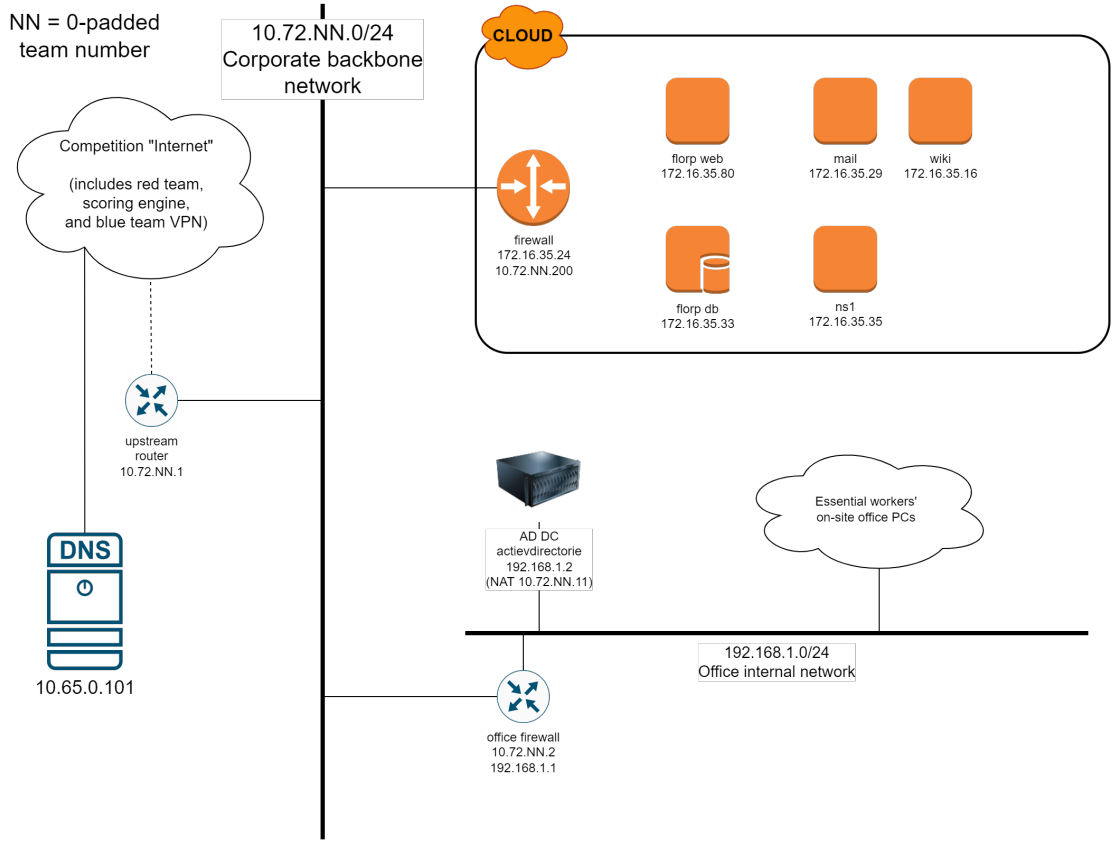

Figure 2: Florp Corporate Network

Team portal

For injects, policy, IR, and scoring teams will access portal.southwestccdc.com via a web browser. The SWCCDC Portal and the OpenNebula accounts will be different credentials. You may access the portal directly during the competition from your browser without going through the competition environment. From the portal, you will be able to see your team's service up/down status as seen from the scoring engine. The portal also includes a manual, which is accessible via the "manual" link in the menu and details how to use various features.

Ports and Firewall info

Students will need access to portal.southwestccdc.com, cloud.southwestccdc.com, our VPN and Discord for communication between the teams. Your computer will need to establish connections with the following destination ports or applications:

```
OpenVPN: 129.244.246.64 port 1195 udp
```

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.

NOTE: This qualification event we will be using DNS for scoring services. The scoring engine will use the IP your DNS servers provide for each scored service when preforming a check.

Services

Teams will be able to see service status 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.

Injects can be scored in a variety of ways. For example, if an inject asks you to enable a service on a host, the inject might be worth 0 points however the scoring can come through a scoring engine checking the new service. Don't assume that injects worth low or 0 points are not important.

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. Aside from gaining login access, the Red Team may also score points by gaining access to confidential data, such as trade secrets, personally identifiable employee or customer data, or other sensitive materials. 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 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.

NOTE: DO NOT REPORT PORT SCANS. SCANS ARE NOT A COMPROMISE.

Post-Game

The top eight teams will advance to the 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. Details about how and whether you will be able to access your qualifiers machines after the game ends will be shared with the room judges/monitors during the competition.

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)