Remote Qualifier Round
Team Packet
2017 Southwest Regional CCDC

February 10, 2017

1 Game Organization

The game is divided into several teams, each with a color designators. Student competitors are on "blue" teams. All game officials will be on "white" team. The "white" team ensures the game runs as intended, and is not part of the scenario. A team of professional penetration testers and will compose "red" team, with the explicit goal of attacking your network. A group of simulated customers will be "orange" team. 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.

2 Competition Infrastructure

You will connect to the qualifier competition environment using an HTTP proxy. Teams will be allowed to test their connections to the environment on Wednesday, February 15th. We have tested the environment heavily with Chrome, so use of another browser is at your own risk.

The proxy requires a username and password that you will be provided. Teams will need to provide their source IP range for the proxy or the firewall will NOT allow you to connect. You will need to provide this no later than Tuesday, February 14th so we can have adequate time to alter the firewall rules before the connectivity testing session on Wednesday. All traffic, including searches and basic internet use will be required to be routed through the proxy throughout the competition. Judges will be instructed to monitor teams and ensure they are only using the browser connected to the game environment.

Once you are connected to the proxy, you will have access to a machine running VMware via a web interface. This is your only access to the machines for the qualifier.

The VMWare host is NOT part of the simulated network and not subject to red team activity. Shutting down or reconfiguring the VMware host will result in the team being disconnected from the environment. Given that the number of teams, we will likely not be able to help teams recover from these kind of self-inflicted wounds, so please only modify settings INSIDE the virtual machines you are provided. Snapshots of the virtual machines may be present, but may revert you to a non-functional or vulnerable state. Each machine has limited disk space of 500GB. If you create enough snapshots fill up the disk and cause the machine to become slow or unusable, this is outside the control of the competition organizers. Be EXTREMELY conservative with any changes to the VMWare environment.

3 Business Scenario

Teams are taking over the network of Crap-Router Industries (CRI), a second-rate router vendor that is bad at pretty much everything. CRI produces physical routers and writes software that runs on the devices. They operate their own support and customer service system for their devices. CRI's devices are known for having security vulnerabilities and being an overall burden to the customers who choose to use their products.

4 Services

Teams will access the scoring engine on an IP range 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. Continued failure of a service across multiple checks for a service that is critical to the success of the business will result in exponential penalties. 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. This is the biggest source of points for the game.

5 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 40-percent immediately before any subject-matter scoring is completed.

6 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 believe you have been attacked. 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. CRI's engineering documents and source code will need to be protected from corporate espionage. If Red Team acquires any these documents, points will be deducted. Access to critical business documents is scored separately from attacks.

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.

7 Network Resources

Teams will have access to the following resources on the network of CRI: