Northeast Collegiate Cyber Defense Competition

Andrew Boutin, Nicolas Grande, David Harrigan, Justin Mansfield & Daniel McGuire

The Northeast Collegiate Cyber Defense Competition (NECCDC) is an annual cyber-security competition that aims to test the skills of the competing college teams in terms of their operational proficiency as IT workers. Students must attempt to secure a mock business network while defending their services against a team of professional hackers. The teams are scored on whether or not they have their services operational and on how well they complete their assigned tasks. The team with the most points at the end of the competition is deemed the winner.

Overview

The 2014 Northeast Collegiate Cyber Defense Competition was held at the University of New Hampshire during March 14 - 16, 2014.

10 schools competed to qualify for the national competition:

- UNH
- WPI
- Alfred
- SUNYIT
- RIT
- Northeastern
- UMaine
- Champlain
- Syracuse
- UMass

Each team was:

- Responsible for managing the IT portion of a simulated busineess environment.
- Placed in a specified room with two judges
- Given an identical set of hardware and software
- Located on a dedicated “commercial” network and had to operate administrative and protective duties
- Scored based on their ability to detect and respond to outside threats and maintain availability of existing services (checked with service scoring engine)
- Provided with the same business objectives and tasks (given and scored by the inject scoring engine)

Team Photo

Information Technology

The role of the IT group in the NECCDC event was to research, build, and support the 11 competitor environments for the competition.

Research: Determined which operating systems and software packages would effectively allow the teams to manage, run, and secure their services.

Build: Installed the operating systems and required software onto individual machines. Thoroughly tested proper compatibility and functionality to ensure the selected packages would work as intended. When confident with the choices, made a clone of each system to deploy to every team.

Support: Assisted the competitors if they requested technical support. Helped package hardware and clean rooms after the competition.

Computer Science

The role of the CS group in the NECCDC event was to ensure the functionality of the service scoring engine, inject scoring engine, and scoreboard along with implementing a network traffic capture.

There were existing versions of both the service scoring and inject scoring engines at the beginning of this project. They needed to be modified and tested to ensure that they met all specifications for the 2014 competition. This project required collaboration with UNH CS IT Support and volunteer competition administrators to complete all requirements.

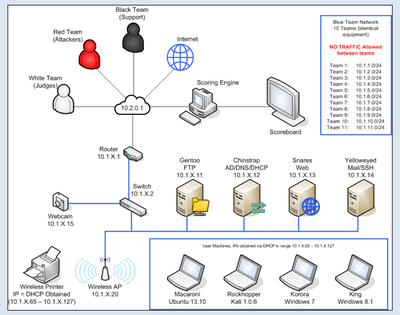
The project was broken up into two sections. The first section consisted of design and research which was completed during the first half of the year. The second section consisted of implementation and testing which was completed before the competition in March 2014. Online project management software was utilized to keep track of and distribute tasks to team members.

Acknowledgements

We would like to express our thanks to the following:
Ken Graf (Event Organizer), Gina Desmarais, Gerry Pregent, Scott Kitterman (Network Support), Carolyn Kirkpatrick, Collette Powers, Radim Bartos, CS Department (Event Assistance).

Network

The competition network was organized so that each competing team configured in the exact same way (with only the IP addresses changing between teams). Each team had four servers connected via Ethernet cables to their switch, a wireless access point connected to their switch, and four user machines connected to their access point. The teams also had a printer connected to the wireless access point and a camera connected to their switch. Their switch connected to their team router, and all the team routers were connected to an upstream router which linked each team to the judges, attackers, scoring engine, and internet.



Competition Network Diagram

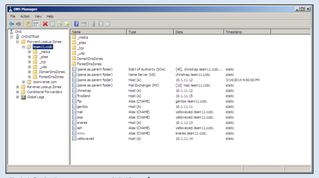
Servers

Active Directory/DNS/DHCP Server
Responsible for managing user accounts and passwords, user privileges, name resolution, and dynamic IP assignment. Ran on Windows Server 2008.

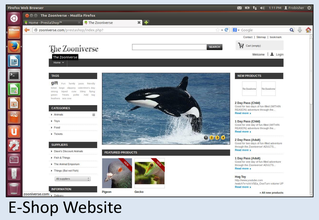
FTP Server
Allowed for teams to transfer files to and from the server, acting as a central file repository. Ran on Mint Linux.

Mail/SSH Server
Provided e-mail service for each team and allowed users to remotely connect to the server. Ran on Debian Linux.

Web Server
Hosted a team website with an e-shop feature that allowed customers to browse and purchase items. Ran on Ubuntu Linux.



DNS Manager Window



E-Shop Website

User Machines

Each team had four user machines separate from the servers. They were connected to the network via Wi-Fi and had no additional services installed on them beyond what was required for normal operations. They represented business users in the environment. Each of the four user machines had a different operating system from the list below

Operating Systems

- Ubuntu Linux 13.10
- Kali Linux 1.0.6
- Windows 7 Ultimate N Service Pack 1
- Windows 8.1

Each user machine was assigned an IP address by the DHCP server from the pool of 10.1.X.65-127, X being the designated team number.

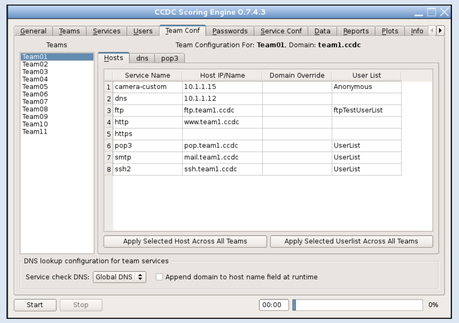
Two user machines required additional services to be fully operational. The Kali Linux user machine needed the Dell Wireless WLAN 1501 Driver to connect to the network. The Windows 7 user needed Internet Explorer 9 installed to interface with the network camera and the Axis Web Plugin to manage the camera.

Service Scoring Engine

About:
The CCDC Service Scoring Engine is a GUI-based program written primarily in Python with a MySQL database backend for storage of configuration and results data. It is used to check the services for the teams, allocate points, and update the scoreboard.

Tasks Completed:

- Validation tests for service checks
- Backup/failover system
- Configured engine for service checks and competition environment
- Monitored system during competition and made required changes



GUI screenshot of Scoring Engine

Inject Scoring Engine

About:
The CCDC Inject Scoring Engine is a web application developed for the following:

- Scoring Reports
- Point Adjustments
- Teams
- User Accounts
- Injects
- Submissions
- Incident Reports
- Exploit Reports

Tasks Completed:

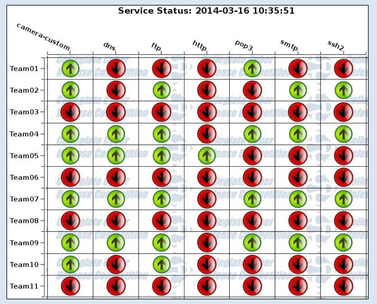
- Set up secure web server to make engine available over UNH network
- Backup/failover system
- Configured synchronization with service scoring engine to display scoring reports
- Created user and admin accounts
- Entered injects
- Defined competition and team information

Scoreboard

About:
The scoreboard showed each school’s team and the status of all of their services. It was made accessible over the UNH network and was displayed on a monitor in the competition break room.

Tasks Completed:

- Set up web server to host web page
- Created cron job to send scoreboard image from inject scoring engine to scoreboard web server
- Wrote script to update scoreboard image on web page



Screenshot of Scoreboard

Traffic Capture

About:
A traffic capture was implemented to capture all network activity during the competition. The information captured was used to verify that the teams weren’t attacking other teams, competition officials, or accessing prohibited websites.

Tasks Completed:

- Intercepted all competition network activity with TCPDump
- Analyzed collected traffic using Wireshark© to verify that teams were following competition guidelines
- Captured over 200GB of data each day