Getting Ready For The Cyber Defense Competition!

Competition Overview:

What to expect:

Cyber Defense Competitions (CDCs) are a hands-on educational experience that teaches students about defensive cybersecurity in a realistic setting. The CDC is a part of the IT-Olympics set up by Iowa State University and runs through ISEAGE. Students are faced with challenges such as securing payment websites, or securing a corporate network that interacts with a city's power grid. Clubs will receive access to their new playground a month in advance. This is normally around the end of March or beginning of April. The CDC will take place at the end of April. The access includes a description of the scenario, their new presetup virtual machines. Once the scenarios are sent out, clubs are then able to register their teams to be a part of the scoring system called IScorE. All material regarding the CDC will be sent out through the scoring system.. The CDC is composed of four different teams; Blue Teams, Red Team, Green team, and White team. Clubs will be working as Blue Teams during an eight hour competition held on a Saturday at Iowa State University. Their goal is to receive as many points as possible. Points can be earned through anomalies, and points will be lost if the red team gains access or the system is not running properly for the green team. Anomalies are random events that will happen every hour for teams to earn points. These events can include anything from scavenger hunts to puzzles. Each team will be working together under one laptop to help secure their systems and earn points in order to win the competition. Generally, the Red Team will always win because they are industry professionals, so Blue Teams need to try their best to gain as many points as possible protecting their network. However, it is not all about winning. The main goal of the CDC is to have FUN, learn, and gain experience.

Setup Phase:

- Roughly 1 month before the IT Olympics, students are given access to virtual machines.
    - This includes the username and password to a new virtual machine for each team and the given scenarios.
- The machines come insecure by default and must be fixed.

- Machines have a common theme, referred to as the scenario.
- During this phase, teams are to properly audit and fix security issues that they find in the provided scenario.
- Changes can also be made to the network and tests can be done to make it more secure.
- During this time, no attacks will be carried out by Red Team against Blue Team.
- The Blue Team may seek assistance from the White Team.
- Set up, secure, and configure changes, edit codes for websites

Attack Phase:

- Starting at 8am on Saturday of the competition weekend.
- During this phase, the Red Team will actively try to break into systems put up by the Blue Team.
- The Green Team will be actively testing to ensure that the systems are usable.
- At the beginning of the day, each Blue Team will start with full points. Points will be deducted for…
    - Green Team not be able to use the systems
    - Red Team gaining access to the system
- Extra points will be offered through Anomalies, tasks released throughout the competition day
- Ends at 4pm

Blue Team:

- Each team of competitors is classified as the Blue Team.
- These teams are the IT security teams
- Their job is to properly audit and remedy security issues found during the setup phase.
- Each high school will have 1 to 2 teams
- There will be about 8 students per team
- Tasked with defending systems during the attack phase by setting up and securing their provided systems.
- During the competition, teams must defend and monitor their systems and complete anomalies for additional points.

Red Team:

- These are information security professionals or experienced students
- Bad guys/hackers/malicious actors

- The Red Team will attempt to thwart protections put up by the Blue Team during the attack phase.
- Their goal is to break into the Blue Team's servers by any means necessary, and steal/place flags:
    - Steal "Blue" flags, which represent sensitive information (SSNs, credit card numbers, etc.)
    - Place "Red" flags, which represent compromise of integrity (i.e an attacker is able to modify and tamper with sensitive data or trigger specific action)

Green Team:

- These represent your end users/customers of your fictional company.
- Made up of volunteers
- They act as your customers to test if the actions put in place by the blue team do not make the system unusable.
- Check if the systems are working properly as they are said to.
- They will use your system during the attack phase to make sure it is working.
- Perform tasks like changing passwords

White Team:

- Authority of the competition
- Creates the scenario and all the virtual machines
- The white team is played by the staff of ISEAGE.
- They serve to help administer the competition and assist teams.

Competition Network:

- This is the competition's internet. Each of the Blue Teams will be required to have specific services exposed to the competition network.
- This is how the Green Team and Red Team will access the services by the Blue Team.

IScorE:

- The scoring application that will be used by all teams during the competition.
- For scoring, the Blue Teams will submit their documentation and intrusion reports to the White Team.

- Flags will be downloaded here in order to put on the Competition VMs that Red Teams will try to capture.
- Flags are also kept track of here.
- Anomalies will be done through IScorseE as well, where they can be viewed, downloaded, and submitted for grading.

vCenter:

- This is a VMware vCenter instance where the Blue Team will access their VMs during the setup phase for administration in order to prepare for the competition.

Flag:

- A flag is a part of the competition that serves as proof that a Red Team member was able to access a Team's VM.
- It can be a randomly generated string of characters that the Red Team will place on a machine or need from a restricted part of a machine.
- It can be an action to be done on a machine, such as running a command or accessing part of a custom application.

Anomalies:

- Random events that will happen every hour
- Allow teams to gain points
- These events can be from small tasks to scavenger hunt or puzzles.

Strategies:

- Don't be afraid to use other resources on the internet, just make sure they work for you version of OS/Software
- Take you time and read error messages if they pop up, they usually give you good insight to why something didn't work
- Make sure to always be monitoring your system to make sure there are no breach and everything is working properly
- Do not forget about the little things like physical security
- Ask for help from both your mentors and your peers
- Questions can be sent to cdc_support@iastate.edu, if outside of the setup phase please include [High School] in the subject line.

- For more information visit http://www.it-adventures.org/learning/cyber/ or contact IT-Adventures support staff at ita@iastate.edu.