Introduction to Cyber Defense Competition

Module 16

Objectives of the CDC

- Establish a safe and functional environment that:
  - Encourages students to discover the applied meaning of information/cyber security concepts
  - Facilitates the development of operational environments for which students design, implement and manage its security controls
  - Enhances mastery of security concepts, practices and skills by compressing the time between design and rigorous realistic security-threat based testing
    - Develops practical experiences that will inform future learning and decision making relevant to real operational environments

CDC Experience

- Defenders, the Blue Team:
  - Build and secure an IT environment
  - On attack day, defenders operate and defend their IT environment under nearly constant threat conditions
  - Attackers, the Red Team, penetrate defenses to acquire **flags** located on key systems in each Blue Team environment
  - Blue Teams compete by attempting to accumulate the most points

CDC Environment

- Two Environments
  - Virtual
    - VMWare-based platform hosts IT environments competitors will defend
    - ISEAGE residing on another VMWare platform emulates the entire Internet
  - Physical
    - All competitors assemble in their teams in a common space
    - Attackers, Red Team, will be located in another room

Competition Roles

- Four roles or teams
  - Blue Team – Competitors who defend their environments from attack
  - Red Team – Experienced penetration testers and ethical attackers
  - Green Team – Volunteers who behave as common users of the services provided by the Blue Team
  - White Team – Organizers, technical support and judges of the CDC

Role Objectives

- Blue Teams build and defend their IT environment
- Red Team attacks the Blue Teams in order for Blue Teams to take stock in their defensive skills and understanding
- Green Team performs the role of service users (Blue Teams' customers). Their activity gives purpose to Blue Team environments and source of background activity clutter in which the Red Team can hide
- White Team performs the functions of event coordination, judging and technology management

Rules

- Each role or team is governed by rules
- Training focus is on the rules that govern the Blue Team

CDC Rules for Blue Teams

- Must provide access to all scenario defined public services to all IP addresses and networks
- Must place specially crafted flag files in locations specified by the scenario
  - Flags are symbols that represent data commonly located in the specific locations
  - They may only be protected to the same level as other files within the directories they reside
  - These files must remain in the same form as provided and its file name must remain as specified in the scenario description
  - A flag found to be missing will be considered captured unless the Blue Team can prove otherwise

CDC Rules for Blue Teams

- Some scenario specified information provided by users, Green Team, is valued, and loss of this information to the attackers results in a loss of points
- User credentials (usernames and passwords) for public services will be provided and must be enabled
  - They will be used by the Green Team
  - Passwords may not be changed without permission from the Green Team leader

CDC Rules for Blue Team

- Prior to start of the competition each team must submit environment documentation that contains:
  - Network Diagram(s)
  - Operating System list
    - Versions and services hosted on these OSes
  - IP address lists
    - Documenting any NATed addresses
  - Description of the measures taken to secure the environment
  - Any other preparations you feel the White Team should consider while judging

CDC Rules for Blue Team

- User documentation is required
  - Provide user instructions on how to use the services provided
  - Provide a contact email that allows users to provide you potentially valuable feedback
- Both documents must be provided as a PDF and submitted before the competition
  - Professionalism is expected
  - Be clear and concise in your explanations

CDC Rules for Blue Team

- During the Attack Phase:
  - Facilitate communications between yourselves and the Green Team
    - Green team may communicate via email or in-person announcements
      - In-person announcements require one team member to leave the team to attend the announcement meeting
  - Green team flags will be placed by users on your systems
    - These flags represent valuable information and successful placement is a sign of the functionality and usability of the services your team is providing
    - Users will check periodically for those flags throughout the remainder of the competition – Be sure they can get to them
  - Response rules
    - Long-term blocking of specific IP addresses or IP address ranges is prohibited
    - Temporary port blocking and account lockout is permitted
      - Temporary security-policy violation based blocking must be documented in the environment documentation

CDC Rules for Blue Team

- During the Attack Phase (continued):
  - Service availability will be measured throughout the attack phase and will be scored
  - Intrusion Summary Reports
    - Reports are helpful for earning points for your team
    - Reports may be submitted every two hours or defined schedule
    - Reports summarize any identified intrusions, your team's assessment of their impact and your team's response to these intrusions in order to minimize their impact and risk
    - See the scoring section for details on point assignments
  - Blue Teams may not perform offensive actions towards fellow competitors or the CDC environment, such as the ISEAGE infrastructure
    - Penalties are loss of points or disqualification
  - Blue Teams may not receive help from anyone not a registered member of the team during the Attack Phase
  - Blue Team members may not contact Green Team or Red Team members without going through the Green Team or White Team leaders

Scoring

- Scoring is managed by an ISEAGE service called iScorE
  - Document submission is done via iScorE
- Scoring objectives breakdown by phases
  - Preparation
    - Focus is on design and documentation
  - Attack phase
    - Focus is on security operations: controls management, detection and response
    - Rewards given for documentation, service availability, service usability and user support

Scoring

Phase	Category	Weight	Description
Preparation	Green Team Documentation	5%	User documentation submitted to iScorE prior to Attack Phase
Preparation	White Team Documentation	5%	IT environment and controls design documentation submitted to iScorE prior to Attack Phase
Attack	Service Availability	15%	iScorE scans for service availability every 5 – 10 minutes
Attack	Intrusion Reports	5%	Summary of intrusion detection efforts and responses, submitted to iScorE
Attack	Red Team Evaluation	10%	Scoring based on categories: preparations, response, “additional” factors
Attack	Red and Blue Flags	30%	Penalties for losing Blue flags and Red Team’s ability to plant Red flags
Attack	Green Usability	15%	Scoring based on Green Team’s ability to use the functionality provided by the public services. Scenario compliance is also investigated
Attack	Green Team Anomalies	15%	Rewards for voluntarily servicing Green Team requests for support and accepting their challenges. They may be costly distractions or jeopardize your environment (e.g. permission changes)

Scoring – White Team Documentation

- Description of the implemented IT environment and security controls
- 5% contribution to final score
- Up to 100 points awarded
  - Detail (0-40 pts),
  - Professionalism (0-30 pts),
  - Supporting diagrams, figures and tables (0-20 pts),
  - Effectiveness of design (0-10 pts)

Scoring – Green Team Documentation

- User documentation that helps users use the services and environment you designed
- 5% contribution to final score
- Up to 100 points awarded
  - Detail (0-20 pts),
  - Professionalism (0-20 pts),
  - Supporting diagrams, figures and graphics (0-20 pts),
  - Clarity (0-40 pts)

Scoring – Service Availability

- Availability of public services during Attack Phase
- 15% contribution to final score
- Scans for service every 5-10 minutes
- 1 point awarded for every service running during the scan

Scoring – Intrusion Reports

- Describing any intrusions detected and the response actions taken
- 5% contribution to final score
- Reports are submitted on a set schedule.
  - Reports may not be submitted more frequently
- Up to 25 points per report will be awarded as follows:
  - Detail (0-7 pts),
  - Insightful analysis (0-5 pts),
  - Supporting evidence (0-5 pts),
  - Mitigating actions (0-8 pts)

Scoring – Red Team Evaluation

- Red Team's assessment of your team's performance
- 10% contribution to final score
- Assessment over three categories
  - Up to 100 points awarded on Blue Team's security preparations based on the criteria of whether they would be acceptable in real-world environments in terms of technical appropriateness and political/business acceptability
  - Up to 100 points awarded on Blue Team's responses to attacks based on criterion of whether the responses would have been acceptable in a real-world setting
  - Up to 50 points for a Blue Team's performance regarding: physical security, social engineering, professionalism and factors judges may consider noteworthy

Scoring – Red and Blue Flags

- A measure of compromise… Lost “blue” flags represent data theft and planting of flags, “red” flags, represent host integrity compromise
- 30% contribution to final score
- Loss of any the assigned "blue" flags results in 50 points **lost** per flag.
- "Red" flags are planted by the Red Team and each time they are successful the Blue Team **loses** 50 points.
- As many as 25 points can be **earned back** by documenting
  - Your understanding of the attack,
  - The weaknesses that resulted in the successful capture or planting of a flag
  - How the team would prevent the attack in the future.
  - The Red Team judges the documentation on the Blue Team's accuracy of understanding the attack.

Scoring – Green Usability

- A measure of the functional performance of your IT environment
- 15% contribution to final score
- Green Team will perform 2-4 full service usability checks, using the provided user documentation, over the period of the Attack Phase.
  - Full service usability involves users using services to achieve scenario oriented objectives
- Green Team verifies the environment complies with requirements specified in the competition scenario.
  - Many listed requirements under a host description within the scenario description are assigned a point value
    - Compliance to a scored requirement will result in receiving points
    - Not all requirements are assigned a point value, be sure to comply with the scenario to ensure receiving all the points possible

Scoring – Green Usability

- Shell Server Scenario Requirements:
  - Users should be allowed at least 1GB of storage on this server (even though they may not use that much).
  - File sizes must be able to grow to 250MB, as some users need to store large amounts of data on this system.
  - Users should be able to have at least 25 processes.
  - SSH/SFTP should be running on standard port 22
  - SSH/SFTP should be offered via the DNS name shell.siteN.cdc.com
  - Users must be able to compile and execute C, C++, Java, and Python code
  - Administrators (ben and nolan) must be able to use sudo to run commands as root
  - User files must be backed up

Scoring – Green Team Anomalies

- Introduced distractions both from a technical operational and human interaction perspectives
- 15% contribution to final score
- Green team will generate a series of user-oriented requests or security challenges that are common in operational environments.
- Points are awarded for servicing these "anomalies", but servicing them is voluntary.
  - Partial points will be awarded for some of the anomalies that allow for meaningful partial completion
- Be aware that Green Team requests may come at a price.
  - Request may ultimately reduce the security posture of a service or host
  - Request may distract team members from response activities

Scoring – Penalties

- Blue flag loss and Red flag planting results in a 50 point per flag penalty
- Late White and Green Team documentation,
  - Documents due prior to the start of the Attack Phase,
  - Results in a penalty of 25% document-score reduction for each document that is late
    - Additional 25% document-score reductions will occur after each subsequent 30 minute period past the deadline
- Restore image penalty of 75 points
  - In the event a VM image must be reinstalled by the White Team
  - Manage the provided VM's so that you can restore a CDC relevant image to its original state using copies and snapshots
- Offensive action towards fellow competitors and ISEAGE infrastructure
  - Number of points lost is not specified, but disqualification is a possible penalty.
- Penalty of 500 points for receiving external help during the Attack Phase
  - Only registered team members and advisers and mentors may contribute to a team's efforts
- Penalty for inconsiderate or irresponsible use of the CDC environment
  - Unacceptable attributable activity that comes to the attention of the White Team
  - The size of the penalties is not specified allowing for the White Team to pick the appropriate size of penalty

Challenge Scenario

- Technology, rules, roles and scoring objectives provide the CDC framework
- The challenge scenario operates within the framework and changes from one CDC to the next
- Challenge scenario provides:
  - Design and operating context
    - Useful for interpreting priorities
    - Useful for interpreting observed activities
    - Useful for assessing response actions
    - Useful for determining the value of information assets
  - Scenario specific rules, scoring and penalties, if necessary