Lockdown

Lockdown is a student-run Cybersecurity competition targeted for beginner Cybersecurity students. Students who attend Lockdown will leave after experiencing an active breach within a small corporate environment. They will also learn their strengths and weaknesses working with a team. Students should leave feeling accomplished but also with a drive to learn more!

Description

Lockdown is similar to Regional CCDC, except shorter and should be looked at as a stepping stone to CCDC. We offer a 1-day 7 hour competition with a mock corporate network that contains user infrastructure, cloud machines and general services to operate a company. Your job is to run the network and company during an active intrusion.

This competition is completely ran and developed by students, usually compromising of 10-12 developers of the competition, usually putting in 30-40 hours each. Totaling roughly 400 hours of time.

This is closer to a “real world” project. Not a school project.

Teams

There will be times there are not enough students for each role. Students will need to wear multiple “hats” in order to do Lockdown. People with multiple roles will need to know the scope of each role. This is to help with biased decisions when there is a conflict in roles.

Gold

Project Manager of Lockdown. Do not put someone here who does not have a good work ethic. This person has a holistic view of the competition from start (e.g. planning, role assignments, etc.) to finish (e.g. competition debrief, clean up, etc.).

Gold Team Leader's team consists of Gold Team, Red Team Leader, White Team Leader, and Black Team Leader. This is Lockdown's Leadership team. Each Team's Leader has defined roles and responsibilities; Gold Team needs to know them and know how the teams interact with one another. Gold Team Leader has final decision power for students (e.g. if other team leaders cannot come to a decision, the gold team leader should make the decision).

Gold Team Leaders who do not fulfill their role's responsibilities are noticed and cause ripples to the rest of Lockdown.

Leading indicator: How much are things planned out for each event, each sponsor, each team?

Lagging indicator: How much were you running around during the competition?

Roles and Responsibilities (Not every single one of these tasks will *always* be applicable. But it is important to have a definition of all possible tasks to make sure you are oriented for success.)

- Gold Team Leader
    - Project Manager
    - “CEO/CISO”
    - Reports to Advisers
- Management students recommended here, needs strong project management and people management skills
- Making sure interest Form goes out to past schools and Blue Teams
- Inventory
    - Registered Schools
    - Lockdown Organizers
- Administration!
- Planning/Logistics
    - Responsible for making a Google Calendar of dates and holding everyone accountable to those dates
    - Post competition dates and invitation to competition debrief in Town Square channel
    - Post team leads and invitation to volunteer in Town Square channel
- UB Policies (Newspaper, room assignments)
    - Responsible for making sure we treat and competitors treat UB property with respect
        - Inviting Partners and Schools
        - Project Management
            - Tasks, due dates, assignees, quality
        - Sponsors
            - Responsible for getting sponsors and deliverable they are owed
              * Size of 1 - 3 people

Black

Everyone is a member during design and development

Why?

Everyone needs to be familiar with the infrastructure of the competition, at the very least Blue Team infrastructures. Not knowing the infrastructure causes issues during the competition (e.g. White Team members now have to ask Black Team lead about how something works, Red Team doesn't know what to target and not to target, Black Team is bogged down with simple questions)

Everyone needs to know at a base level the machines and what services are on them and if they are cloud or not. No excuses.

Roles and Responsibilities (Not every single one of these tasks will *always* be applicable. But it is important to have a definition of all possible tasks to make sure you are oriented for success.)

- Black Team Leader

    - Reports to Gold Team Leader
    - In charge of Black Team responsibilities and acting as a project manager for Black Team with Gold Team
- Charge of the Network Infrastructure
    - Assigning tasks to Black Team members
    - Reports to Gold Team Leader
    - CSE students recommended here!
- vSphere
    - Network Infrastructure
- Topology, IP schema
- Design
- Development
- Operating Systems
- Creation of VMs Templates
- Snapshots
- Documentation
    - Make sure existing documentation is updated to current standards and operations
- Development
- Templates
    - Follow the template standard
        - Documentation is Key Factor
        - Services
        - Configuration
        - Documentation
        - Testing
        - PCAP of Competition
            - Not always necessary
        - Clone Teams from Templates
        - Change Settings of Services and IPs
        - Testing
            - Passwords on White Team password sheet
            - Laptops in the rooms with exception account

Red

Create what's in scope and not in scope document and share with white team. White team will have an easier time to know what red team will and will not be doing (e.g. Not changing passwords, not deleting user accounts, etc.)

Currently, we partner with RIT students to do Red Team. Red Team Leader needs to coordinate with RIT's point of contact to discuss strategy and timeline of the competition.

Roles and Responsibilities (Not every single one of these tasks will *always* be applicable. But it is important to have a definition of all possible tasks to make sure you are oriented for success.)

- Red Team Leader
    - Handling duties of red team
    - organizing attacks that won't break systems but more towards for educational exercises
    - Assigning tasks to red team members
    - Reports to Gold Team Leader

- CSE students are recommended here
- Understand the configuration of services
- Works closely with Black Team
- Attack systems during the competition
- Making exploits before the competition
- Logging attacks
- How to secure those attacks
- Strategy building
- breaking just enough
- Tools
- Kali Linux
- Team server

White

The “managers” of the Blue Team. White Team's main responsibility is to make sure that Blue Team participants are having a decent time (within reason), and learning. Indicators used during the past:

Education: The competition will be an educational tool to teach students about building systems and services, hardening, using tools, team dynamics, etc by the end of the competition.

Leading Indicators: Setting up a proper system for educational; Red Team’s attack plan; technical difficulties

Lagging indicators: Feedback given shows that one person did not learn anything

Competitive: No team or competitor has given up due to the lack of ability to continue caused by technical problems, Red Team, and/or lack of valiance for the duration of the competition.

Leading Indicators: Technical difficulties; Red Team’s attack plan; why winning is important

Lagging indicator: One competitor gave up

Fun: The majority of competitors are enjoying the competition even when things are getting stressful for the duration of the competition.

Leading indicators: Technical difficulties, red team’s attack plan, interesting injections, and solutions.

Lagging indicator: Feedback, Bored/angry competitor

Roles and Responsibilities (Not every single one of these tasks will *always* be applicable. But it is important to have a definition of all possible tasks to make sure you are oriented for success.)

- White Team Leader
    - Handling logistics of white team responsibilities for design, development and competition
    - Assigning tasks and responsibilities to white team members
    - Reports to Gold Team Leader

- Management students are recommended here
- Score Engine
    - Redesign, resetup, etc
    - Web form for passwords, users, IP addresses
    - Scoreboard
    - Services
    - Customer numbers
    - Graphical Interface Webpage
    - Scoring
    - How is scoring determined
    - Different with business elements added
- Injections
    - Idea of orders from higher up that need to be fulfilled
    - Triage of what needs to get done
    - Use of help teams towards the right direction
    - Use of office politics (retracting injects, arguments from CISO office)
    - How will these be sent to blue team?
    - Email (double edge sword)
    - Through web interface of the scoreboard
    - needs be pre built in
    - the ability to make changes
    - Passouts
- Business Elements
- Design, Development, Implementation, execution, reporting
- Competition help
- Competition Management
- Competition Survey
- Design, development, implementation, execution, reports

Blue

The Blue Team are the competitors. They are responsible for having fun and following the rules.

Tasks

Who owe's who what? Most of these tasks are within the relevant teams sections. However there is a concise running list below.

Red Team

- Schedule of Attacks
- Iterate to everyone that Red Team will NOT touch competitor accounts, change their password or names
- Red Team will NOT break DNS, will not stop access from competitors, they should always be able to SSH and RDP into machines
- Make sure implants will NOT break machines
- Setup Site 2 Site

The goal here is to decide all of this in a meeting with the leaders of Lockdown.

- Manage the VPN through Gretzky

Due Dates
Gold Team

Design

- Google Calendar schedule
  - This will contain tasks and due dates, no need to manage the little stuff, but rather the bigger deadlines

Resource Allocation (Human and Technical)

- Make master list of competitors
  - Who signed the CoC? Who signed the photo release?
  - Reach out to sponsors
  - Setup meeting time

Team Designations
Leader Designations
Participants to be Invited
White Team
Goals

- Stuff

Competition Agenda
Black Team
Theme

- Stuff

Injects

Planning

Infrastructure of Teams

Infrastructure of Competition
“Success doesn't just happen. It's planned for.”

Development

“Proper planning and preparation prevents poor performance.”

“A goal without a plan is just a wish.”

Who owe's who what?

Competition

Setup

- Site 2 Site VPN
  - Top port on the machine (i.e. the on-board NIC)
  - Left port on the wall
- The competitor rooms, make sure the laptops are tidy and connected and the room is generally clean
- Prizes

Registration

- Make sure to send registration form to competitors ahead of time, Gold Team to track this
- Make sure to put a nice and friendly person to greet competitors as they show up, (:

Closing

Clean Up

- UBNetDef is responsible for making sure the rooms and space we were allocated goes back to the state it came in.
- CLEAN YOU FOOLS

Debrief

- Gold Team to take notes
- What went well?
- What went poorly?
- How can we improve?