I2CCDC

Intro 2 Cyber Collegiate Defense Competition

Instructor's Guide

v0.12023

This Careers Preparation National Center product was funded by a National Centers of Academic Excellence in Cybersecurity grant (H98230-22-1-0329), which is part of the National Security Agency.

Contents

****Instructor's Guide really begins here**** 4
Teams are to be given 4
Timeframe 5
Objectives 5
Rules 5
How To Use (Based on Outline Above) 6
Scoring 7
Sample Scoring Rubric 8
Optional/Future Ideas 8
Conclusion 8

Hello and welcome to the I2CCDC! This is a fun, mini competition you can do with your class, club, team, etc. This is the instructor's guide. This will detail how the competition was built to run, how it was run previously, and provides some fun tips you may want to try.

Remember the purpose of this competition is to have fun and build skills.

The competition was built as a final exam for the first Intro to Cybersecurity course at Montreat College [If you wish to skip the origin of the competition then go to page 4 or click here]. With 34 students, the teams were divided into 4 groups. Over the course of 3 class periods, they took everything they had learned over the semester to harden their given device. They then chose a team leader who was responsible for all communication and holding on the team's progress which was stored in a USB device. They would also be performing business injects while working on hardening. At the conclusion of the competition, the instructor checks for inject completion by running a script, daily task completion as turned in on the USB, and how effectively hardened the machine was with a vulnerability scanner. Each of them was given a desktop computer with power cord, monitor with power cord, VGA cable, USB drive, mouse, keyboard, and surge strips if they needed it. They were not permitted to use AI for the competition, but they were allowed to use their personal laptop for the benefit of the team. Given the nature of the class, they met once all together & then separately (2 teams each) in a different location for their labs. This introduced an unexpected dynamic (which is why I mention it here). The competition was scheduled to take place over 3 days (during their class periods) which roughly equated to about a 4.5-5-hour work day. There are 15 injects created for the competition, which were randomly sent throughout the day. To ensure all 15 were sent, some injects were sent together. This was intentional to not only provide pressure, but to see if the teams would divide and conquer, given the size of the groups. There were also 2 sub-injects inserted randomly to add more challenges.

The teams had 2 forms: Daily Duties & Justification. The Daily Duties was the form where they documented steps, evidence of inject completion, and any additional system hardening done as they worked. The justification form is a fun component to the competition, as students have to be careful about the injects they work on throughout the competition as some injects are malicious. Should they come across a request that is either unethical, illegal, against company policy, or their own moral code, then they are to fill out a justification form which explains what it was, did the team decide on it unanimously and why they are refusing to do the work. It is up to the instructor to either permit or deny the justification. The challenge is that should a justification form be denied; the team may not complete the inject. This brings an ethical and professional challenge. Professional, because they may not necessarily disagree with the request, but they know it goes against company policy. They will also have to communicate with others why they don't believe an inject should be completed, which poses a time challenge as well as a completion challenge. As they worked, I wandered around "helping but not helping" at times and keeping tabs on how the team was working together, if at all. Unexpected challenges (like lack of

internet in the chapel where they met all together) was worked into the competition (The company cyber basement flooded so we had to relocate your work. Sorry the desktop does not have Wi-Fi, but you have a laptop and an Ethernet cable…I'm sure you can figure out something to get connected.) to encourage critical thinking, creativity and see whether or not they will rise to the challenge (start researching how to connect and bridge) or simply ask for the answer (and there were some!). An unexpected scoring moment came when a team left their USB behind after class. As a completely unbiased party, I could not return it to them, but another team's captain picked it up. They tried to return it to me, but I was not the manager of both companies, so I wasn't going to waste time going to a rival to help them out. Instead, the captain had a choice. Do the right thing and return the USB to the team that left it. Or keep it and keep an edge over one team out of four… the USB never saw that team again. I don't even think that USB was returned to me at the end, I'm almost certain it wasn't. Needless to say, that will be a fun section on their scoring report. On the last day of the competition, I pulled the team captains out of the classroom for about 20-25 minutes just to see if everything would stop (for some it did!) or if they would continue to research and try out new things. Some injects were scheduled to come in during that time, so for the ones who stopped, there was a penalty when the captains returned. This was also where I introduced another challenge. The students in Intro to Cyber got Raspberry Pis. But only the captains got to build it, which took time. After they built it, they had a choice to either let the team build theirs as well (which the captains would have to show them) or just let them have them or hold off on letting them have them. I had 2 teams choose to let them have them but not build them, and 2 teams decide to not let them have them at all. This was a test to see how, as leaders, they took in account the team's culture and morale. As everyone was aware that they could get a Raspberry Pi so managing attention became a challenge for the captains, as they were also banned from touching the keyboard and mouse. At the conclusion of the competition, they turn in their USB as well as any passwords for the auditor to do their job. Failure to do so will result in immediate loss in the competition. While the auditor is… well… auditing, the teams will have the opportunity to fill out a 360-feedback form about each other and how they felt the team as a whole operated. Within the questionnaire are some questions of self-reflection for them to fill out as well.

The only thing missing from this competition was the 525,600 minutes of attacks from the red team like in the actual CCDC, but this was fun and stressful enough for the freshmen. They really seemed to enjoy the competition, and I hope this sparks the drive in them to try every competition out there.

But of course, in the spirit of the SECCDC, in their final inject they are fired. 😊

****Instructor's Guide really begins here****

This competition was built to be scalable. It can be run with as few as 2 people on 2 different devices or VMs or with as many as feasibly workable. The operators of this competition are free to modify any of the game parts below as well as the rules of engagement. For step-by-step expectations, it is recommended that the instructor reads the Rules of Engagement Document. It includes a more in-depth look at the Daily Duties & Justification Forms from the team's perspective which the author decided was more beneficial than including it here. This is to serve as something that can be run as close to out of the box as possible but customizable for the needs of the teams, organization, college, university, class, etc.

Teams are to be given

- An image or device with a Windows 10 or 11 image – *However many are needed for the teams*
- Power cable for PC - *1*
- Power cable for Monitor - *1*
- Keyboard - *1*
- Mouse - *1*
- Ethernet cable [if needed] - *1*
- USB – *1*
- Surge Strip - *1*
- Access to the Daily Duties & Justification Forms, as well as a submission method/portal

Timeframe

- At minimum 1 – 5 hour session if using all 15 injects; if not, adjust time at instructor's discretion
- If using sub injects, consider the time given

Objectives

- Students are to work collaboratively in teams for a company to harden their given device using the knowledge acquired over the semester and through research throughout the competition.
- They will be scored on the following (based on sending 15+2, with the expectation that at least 2 will not be completed or justification failed):

    - Completion of injects – 750 Points Max
    - Quality of injects – 750 Points Max
    - Sub Injects – 300 Points Max (2 sub injects currently)
    - Teamwork – Instructor Observation – 200 Points Max
- Throughout the day, the team captain will receive injects of tasks to perform on the device for the company they work for.
- The goal is to have the highest score!

Rules

1. Teams may not use AI, but they are allowed to use the internet to research ways to harden the device or complete tasks.
2. Over the allotted time frame, students are allowed to work within the specified environment by the operator. The rules below are intended as a foundation, and modifications may be made to them. It is the operator's discretion on how rules are conveyed and distributed, it is the team's responsibility to read and understand the rules.
3. Operators reserve the right to tamper with hardware during non-competition hours.
4. Only the team captain communicates with the manager & boss. Unless the manager or boss specifically requests an employee.
5. Only team captains are to submit the daily duties & justification reports.
    a. Team captains have the ability to designate officers to perform part of their roles or duties, should a team captain decide to do so, they must notify management. Failure to do so will result in their work being discarded until submitted properly.
    b. Captains are also responsible for communicating what management sends to the team.
    c. Captains are responsible for the USB drive given to the team; it is not replaceable.
6. Teams may communicate with each other.
    a. Communication does not always have to be beneficial, but must be respectful.
7. Teams are not allowed to intentionally disrupt the work of others and/or damage the hardware of other teams; however, should a team leave things behind after the final call for the competition day, it is fair game.
    a. Bonus points may be awarded for doing the right thing and documenting it (for instructor awareness not bragging rights).
8. Teams are expected to document their work on the daily duties. They are expected to document their evidence (screenshots) on this form as well.
9. Teams may make ethical and professional calls on completing an inject or not. If a team decides not to complete an inject, they may fill out a justification form. They must fill it out completely, failure to do so will result in their attempt being discarded and no points awarded.

a. They are to include all the names of the team members.
b. State whether or not the team was in agreement on not fulfilling the task.
c. The Task or inject name.
d. Fill in the reason for not completing the task.
e. Operators reserve the right to further discussion or ask about a Team's stance or reasoning behind points on a justification form. They also reserve the right to pull any team member to ask them about the form as well.
f. Once an operator makes a call on a justification form, no one, not even the operator or game creator may change this decision. It stands until the end of the competition.

Once the form has been filled out, the team captain must turn it in. The operator will make the call on whether or not the justification is approved or denied and either award or deny points. The team cannot receive points for completing the task if they submit a justification form. Justification forms are geared towards ethical and professional challenges hidden within the injects. They can also be used to correct or suggest better alternatives than the inject at hand.

10. At the conclusion of the competition, they are to turn in everything given to them at the start, as well as everything needed to audit the device.
    a. Failure to do so will result in disqualification.
    b. Arguing about scoring or points can result in disqualification.
    c. Unprofessional or unbecoming behavior can result in disqualification.
    d. Violations to code of conducts (at respective location) and student agreements WILL result in disqualifications with no chance to appeal.
        i. This may also impact future competition participation.
11. All students are required to fill out a 360-feedback form at the conclusion of the competition.

How To Use (Based on Outline Above)

Have the teams gather their devices and components and allow them to begin by setting up their work area. Instruct them on a method of deciding a team captain. After each team has decided a team captain, meet with the captains and outline what their job role is, their duties, and the abilities and responsibilities they have. Return to the teams. Introduce the competition from a company perspective (this encourages creativity; the more you put in, the more your students will put in and get out).

Inform them of the rules and begin by sending the first inject. Use the schedule send feature to schedule other injects throughout the day.

RECOMMENDATION: Send a few injects together, add urgent messaging, and challenge students to prioritize and manage time. For 2 days, send injects close to the end of time to have them thinking about the next work day.

Walk around the classroom and monitor the teams, make note of positives and negatives. Answer questions within the realm of the competition (unless necessary to be serious), give positive creative answers to encourage students to continue to think critically and not rely (or try to get information) out of the proctor. Remember light-hearted and fun, but challenging. Allow teams to form their systems and provide suggestions when things seem to go awry. Once teams are comfortable and flowing, then things should run smoothly.

NOTE: Injects will cause some panic, remind students that that is okay and part of the game. It is not expected that students will complete all the injects. If they do, increase the strength of the injects.

At the conclusion of the competition, students are to submit whatever they have left and turn in their equipment.

Scoring

As this competition does not have an active red team, our method of scoring is more of an audit and vulnerabilities check.

See the included script for ***an example. If you use a script, it may differ from others****.*

Ideally, run a script that checks for the good injects and the bad injects (the injects that posed an ethical or professional challenge or was intentionally sent to decrease the security of the student's device).

Additionally, run a script to check for CVEs that could be reasonably expected to be closed from students' work. This is something that only instructors will know about their students, so can be excluded entirely from a check.

Give proper scoring for each image or device after running the script.

Compare what the script reported to what was submitted. Ensure it matches, the operator reserves the discretion to deduct points for insufficient documentation or lack of documentation.

Similarly, for sub injects, apply the same methods as described above.

Finally apply points for feedback based on instructor/operator observation, this may be substituted or omitted, and the 360-feedback form may replace it or influence it. The operator may make the decision on this matter.

Afterwards, apply any special points that can be justified and total them for a winner. Announce the winner however you see fit.

RECOMMENDATION: At the conclusion, ask for feedback to improve the competition next time.

Sample Scoring Rubric

Category	Description	Points Possible	Points Earned
Completion of Injects	*Was the task completed? If so, award full points. If justification was used to not complete the task, if sufficient and legitimate award full points. If not, award determined points.*	750	
Quality of Injects	*Was the task properly documented? Proper documentation is defined as, descriptive enough that a new hire (not intern) could follow the steps and achieve either the same results or replicate positive results for auditing. Was the justification form filled out properly? Award full points if yes.*	750	
Sub Injects	*Were the sub injects completed properly? Sub injects are at more of the discretion of the operator than regular injects, they serve to help break ties and challenge the team beyond the norm.*	300	
Teamwork	*Instructor Observation, entirely determined by the operator. Considering 360 feedback is entirely optional, and does not have to be stated prior.*	200	
Total Score		2000	
Notes			

Optional/Future Ideas

- If decided, students can be required to hook up their own device at the start of the competition or each competition day. It is suggested to encourage them to become more comfortable with the hardware, as well as check for disconnected wires.
- Improve ethical challenges by including mock policies, procedures, etc.
- If able, include a pen testing class or similar for added challenges.

- Pull the team captains or top worker from the teams from time to time.
- Add a debrief session at the conclusion of the competition.
- Add a presentation component.

Conclusion

This competition was built for 2 primary reasons. To give freshmen students exposure to a CCDC like competition and to serve as a foundation for others to either use, build off of, or use for ideas. We hope that this has been beneficial to you and that you have a great time with your students throughout this competition. Feel free to add to it to make it closer to the CCDC experience or reimagine it to help develop entirely new skills!