UVI ThunderBird Cup v2.0 Workshop

Workshop Analysis 2016

Lee, Wellington | Morris, Tyler | Chu, Andrew | Joshua Russ
Sandia National Laboratories

Michelle Emerson-Lewis
Survey Evaluator

Abstract

The University of the Virgin Islands (UVI) workshop was used to implement and test the ThunderBird Cup v2.0 (TBC2) system. The TBC2 system integrated a client side scoring system and online scoreboard to keep students grades 6-12 engaged.

Table of Contents

ThunderBird Cup v2.0

The ThunderBird Cup v2.0 (TBC2) program falls under the Minority Serving Institution Pipeline Program (MSIPP) that aims to establish a world-class workforce development, education and research program that combines the strengths of Historically Black Colleges and Universities (HBCUs) and national laboratories to create a K-20 pipeline of students to participate in cybersecurity and related fields.

Purpose Statement

The ThunderBird Cup v2.0 system is designed to educate and engage students grades 6-12 in fields related to cybersecurity and provide an education model for mentors and teachers within the CECOR consortium.

Goals

- Provide cybersecurity focused exercises that engage students grades 6-12
- Provide the consortium with an education model for future TBC competitions
- Provide an integrated client/server scoring system to track students' progress

Program Explanation

The ThunderBird Cup v2.0 system is a cybersecurity awareness exercise created by Sandia National Laboratories. The program uses hands on training and competition to engage students in the exciting field of cybersecurity in the hope of leading them to further their education in STEM related fields.

History

The ThunderBird Cup program was first tested in 2014 at the University of the Virgin Islands (UVI). Students were given hands on experience in cybersecurity to help prepare them for the upcoming year of CyberPatriot. Since then, Sandia has implemented two more workshops at UVI that allow for testing of future ThunderBird cup systems and methods. Today, Sandia is beginning full development of the ThunderBird Cup v3.0 system.

Participant Breakdown

A total of 26 students ranging from grades 6-12 attended the week long workshop.
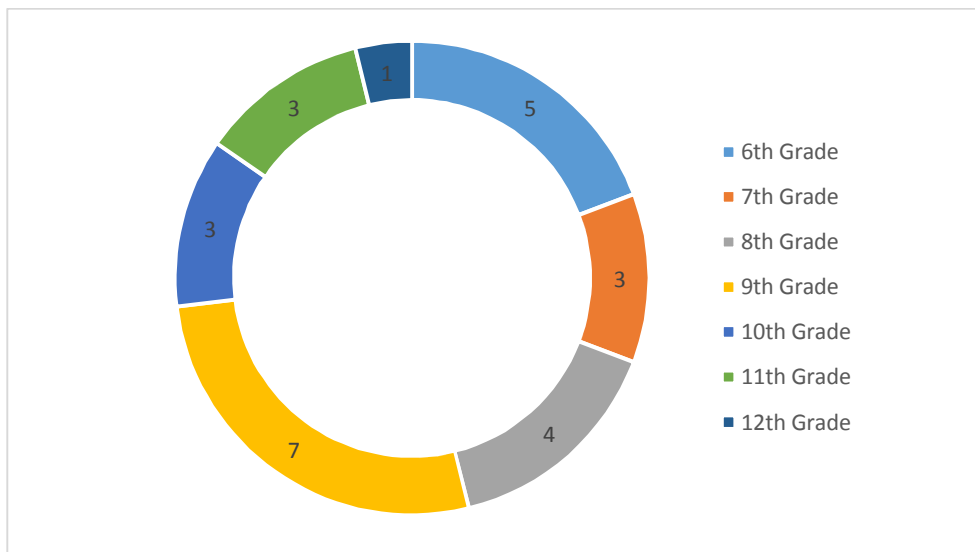
Training Breakdown

Lesson Breakdown

- Lesson 0 –Fundamentals
- Lesson 1 –Window Navigation
- Lesson 2 –Administrative Tools
- Lesson 3 –Malware Protection/Passwords
- Lesson 4 –Remote/File Sharing
- Lesson 5 –Programs/Task Scheduler

Each lesson included tutorial videos on the related subject along with "try it" exercise instructions to have students test their new skills on a training machine. Each student was placed in a predesigned team with a team mentor. Lessons one through five were self-guided and allowed teams to progress at a more comfortable pace. Team mentors provided explanations for exercises and answered questions during the training. At the end of each day teams competed against each other to test their new skills.

Storyline

The TBC2 storyline aims to provide the user with an engaging, interesting, and entertaining narrative, while simultaneously educating the participant on the importance of forensics and data collection as part of a cyber security scenario. In this iteration of TBC, the storyline is set in a "space" environment, with each team representing a certain "faction" within this environment. Throughout the duration of TBC2, the "factions" would find "artifacts" and the corresponding password to each one, allowing for the discovery and further understanding of how their challenge first began. At the end of TBC2, each team prepares a narrative of what they believe occurred before the incident, with the most accurate overview providing the corresponding team additional points.

The new TBC2 storyline has been a good improvement over that of the original. Through additional narrative, team, and challenge storyline material, the depth and ability to educate participants on the importance of forensics has significantly increased. However, it was observed that the storyline needs to be further integrated within the TBC system in order to inform the participants the importance of following and keeping track of the overall narrative. As participants often maintained focus only on the numeric score seen on the scoring module of TBC2, this often became the more prioritized object of the two, obstructing storyline and forensics progress.

Client/Server Scoring System

The TBC2 scoring system is a Sandia developed system that gathers preconfigured flags from connected clients and reports to the scoring server that allows for full analysis of team results. The client side system works in the background without the user's knowledge. The server side system allows teams to actively monitor what tasks they have completed and their overall score. Teams are also able to see other team's overall scores. Administrators are given special access to view what tasks each team has completed along with the power to reset point values and manage server data.

Client Scoring

The TBC2 scoring system worked very well at collecting and sending data to the server. Students were not able to get into the scoring client and don't have access to its source code or processes. However, team login prompts would sometimes not display or execute when the image started and teams would sometimes miss type a login resulting in a failed server connection. We are currently working on a solution for these problems and will have a full fix in ThunderBird Cup v3.0. Other than these issues, the scoring system worked as expected with no significant failures.

Server Scoring

The Thunderbird Cup Server worked well during the event. In terms of functionality, the server correctly reported completed tasks to each team and showed their points correctly on their user interface. Based on the information sent from the PowerShell scripts on the clients, the server correctly logged and kept track of each team's progress. However, we did encounter several issues with the scoring system in which incorrect scores would be reported at times on the scoreboard. It was determined that this issue was isolated from the task list and did not affect the teams in any way other than displaying incorrect scores on the graphical scoreboard. Another issue we encountered was with human error on entering in the pre-generated passwords. Some of the characters in the passwords were ambiguous (such as capital 'i' and lowercase 'L'). Due to this possibility, we are implementing a registration system so teams can create their own accounts with their own passwords. Despite these setbacks, the server ran well throughout the duration of the event.

Virtual Machines

A virtual machine is defined as one instance of an operating system along with one or more applications running in an isolated partition within the computer. It enables different operating system to run in the same computer at the same time. It is like running Windows 7 inside of Windows 7. We utilize virtual environments to allow for an easy roll out of our scoring system, have images that are preconfigured, and to have an environment that students can damage without impacting the actual computer.

Monday Evaluation Image Results

The data below was compiled by our ThunderBird Cup v2.0 scoring system at the end of Monday's evaluation image. Students are placed in teams of two or four and given the evaluation image before any educational material is presented. By providing an evaluation image, we are able to measure each teams educational level before the week starts. This Windows 7 image had a maximum of 106 points and teams actively competed for approximately one hour. All scores have been converted to percentages for readability.

MONDAY'S RESULTS

Team	Point Percentage
Team 8	54%
Team 7	23%
Team 6	18%
Team 5	33%
Team 4	54%
Team 3	34%
Team 2	56%
Team 1	35%
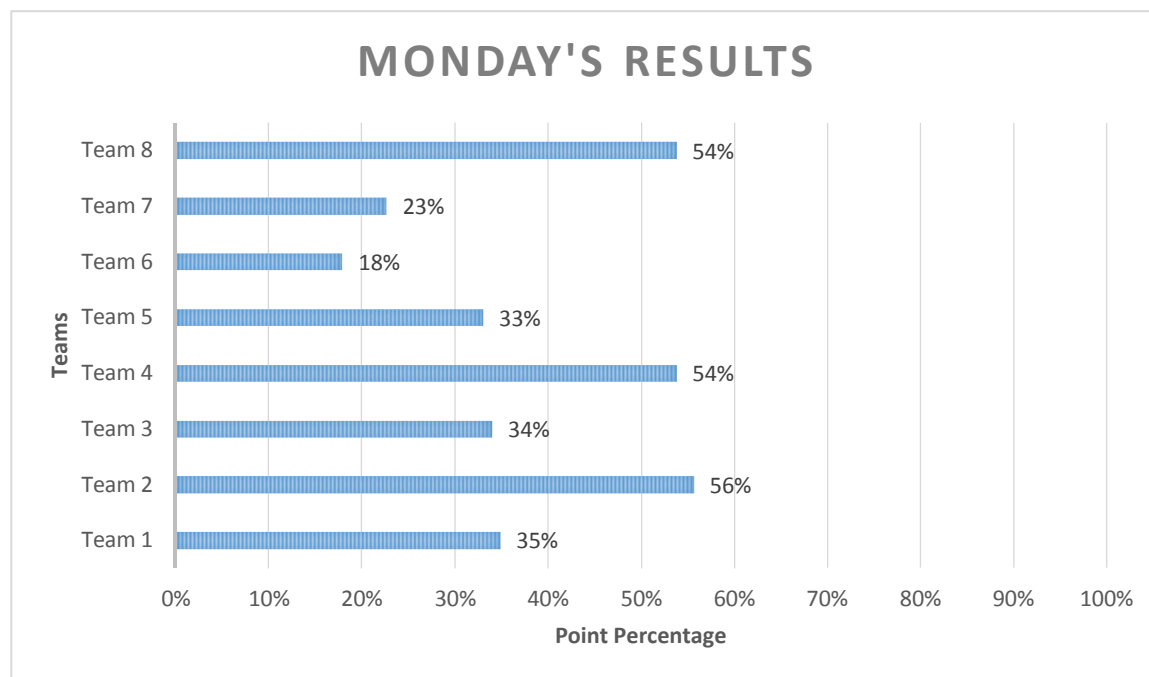
Tuesday Educational Image Results

The data below was compiled by our ThunderBird Cup v2.0 scoring system at the end of Tuesday's educational image. Teams are first presented to lessons zero through two and are given a training image throughout the lessons to test their new skills. Once the self-guided lessons are finished, teams start the educational image. This Windows 7 image had a maximum of 100 points and teams actively competed for approximately an hour and a half. All scores have been converted to percentages for readability.

TUESDAY'S RESULTS

Team	Point Percentage
Team 8	25%
Team 7	36%
Team 6	37%
Team 5	55%
Team 4	38%
Team 3	40%
Team 2	55%
Team 1	68%

Wednesday Educational Image Results

The data below was compiled by our ThunderBird Cup v2.0 scoring system at the end of Wednesday's educational image. Teams are presented to lessons three through four and are given a training image throughout the lessons to test their new skills. Once the self-guided lessons are finished, teams start the educational image. This Windows 2008 Server image had a maximum of 125 points and teams actively competed for approximately an hour and a half. All scores have been converted to percentages for readability.
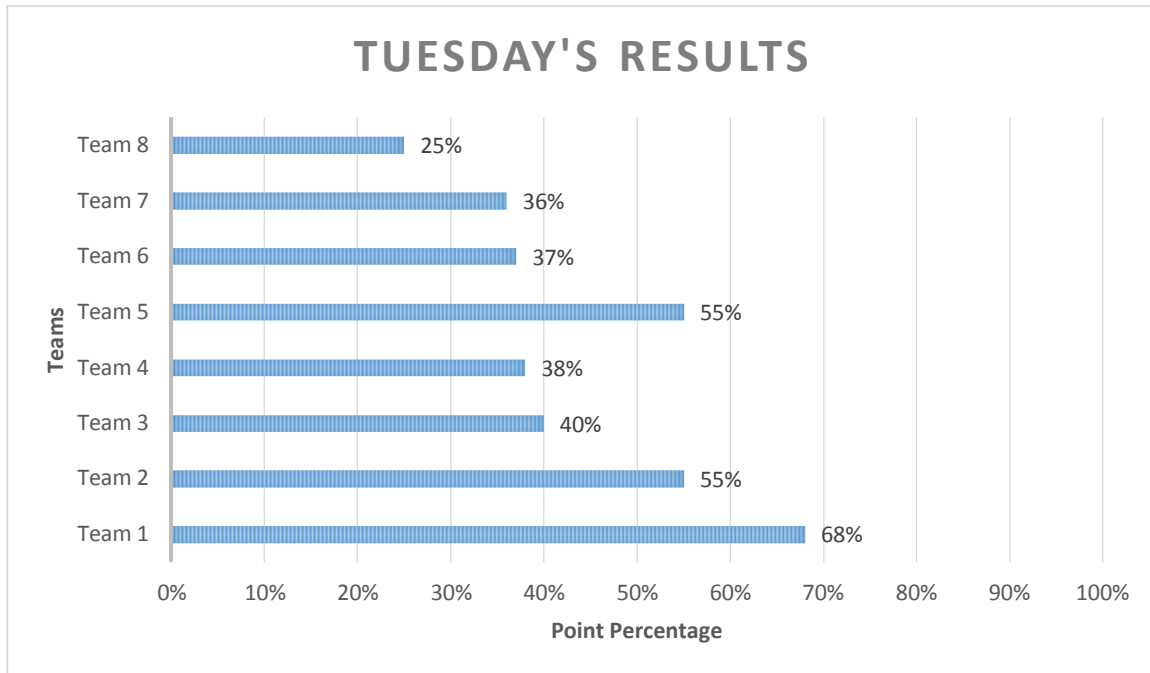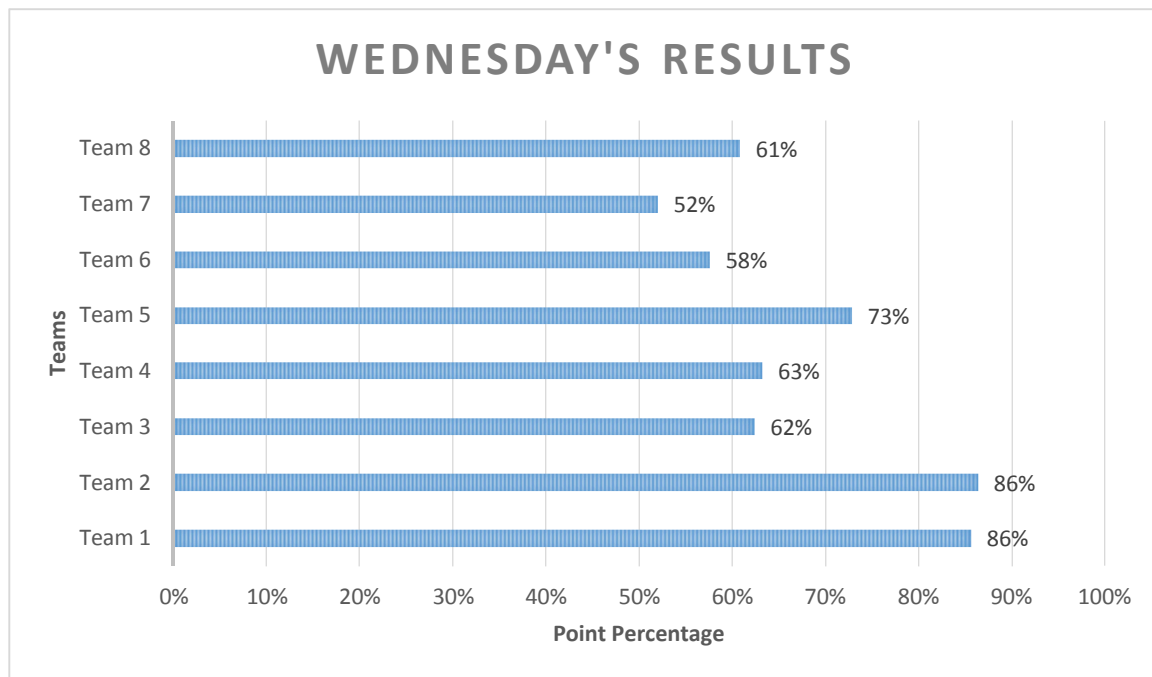
Thursday Educational Image Results

The data below was compiled by our ThunderBird Cup v2.0 scoring system at the end of Thursday's educational image. Teams are presented to lesson five and are given a training image throughout the lesson to test their new skills. Once the self-guided lessons are finished, teams start the educational image. This Windows 8.1 image had a maximum of 140 points and teams actively competed for approximately two hours. All scores have been converted to percentages for readability.

THURSDAY'S RESULTS

Team	Point Percentage
Team 8	82%
Team 7	56%
Team 6	71%
Team 5	86%
Team 4	88%
Team 3	60%
Team 2	95%
Team 1	94%

Friday Competition Image Results

The data below was compiled by our ThunderBird Cup v2.0 scoring system at the end of Friday's competition image. Teams are not given any educational lessons on this day and are presented with just the competition image. This image is the most difficult image out of all the days and is designed to truly test their educational retention. This Windows 7 image had a maximum of 130 points and teams actively competed for approximately two hours. All scores have been converted to percentages for readability.
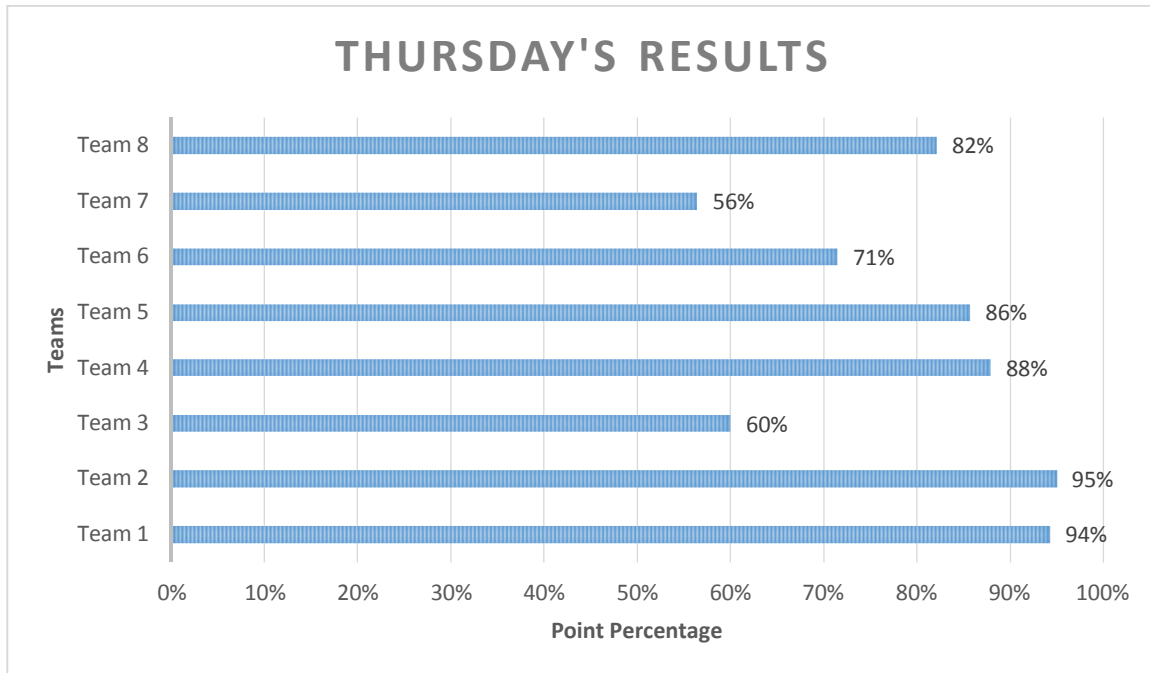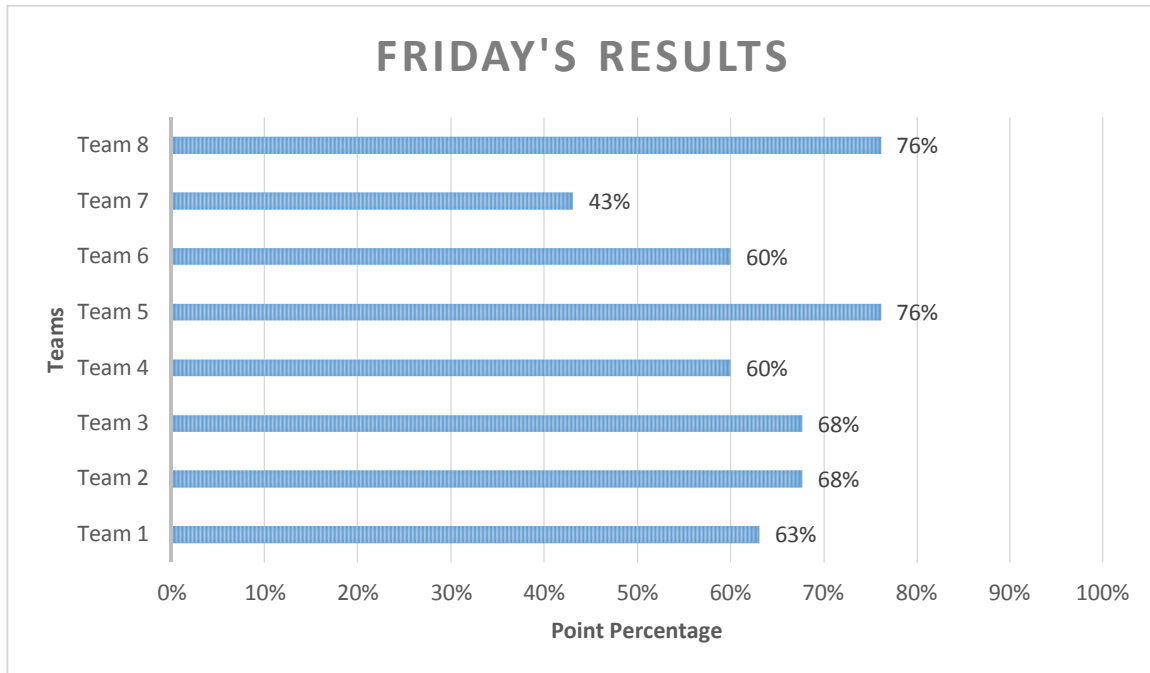
FRIDAY'S RESULTS

Team	Point Percentage
Team 8	76%
Team 7	43%
Team 6	60%
Team 5	76%
Team 4	60%
Team 3	68%
Team 2	68%
Team 1	63%

Multiday Results

The data below is a multiple day outlook for all eight teams. This data has an x-axis with the total number of 601 point from all five days. All scores have been converted to percentages for readability.

OVERALL RESULTS

■ Day 1   ■ Day 2   ■ Day 3   ■ Day 4   ■ Day 5

	Team 1	Team 2	Team 3	Team 4	Team 5	Team 6	Team 7	Team 8
■ Day 1	35%	56%	34%	54%	33%	18%	23%	54%
■ Day 2	68%	55%	40%	38%	55%	37%	36%	25%
■ Day 3	86%	86%	62%	63%	73%	58%	52%	61%
■ Day 4	94%	95%	60%	88%	86%	71%	56%	82%
■ Day 5	63%	68%	68%	60%	76%	60%	43%	76%

Total Percentage for Five Days
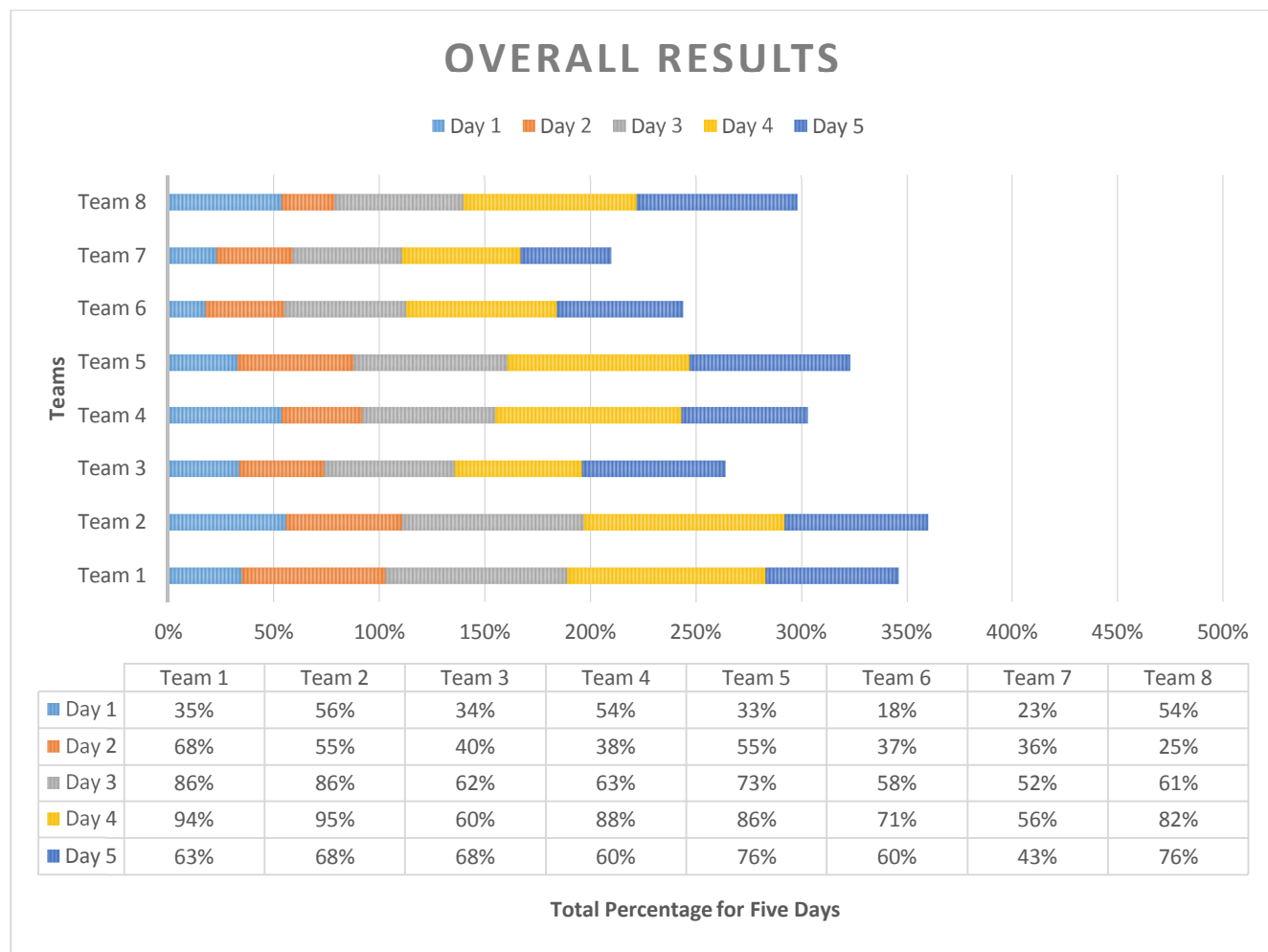
Virtual Machine Overview

Virtual environment testing allows us to gather quantitative data on how students are learning during the week session. The virtual environments used during the week long UVI workshop were designed to be very challenging for students. The day five image was especially difficult in order to gage the overall retention of the students. The data clearly indicates a major spike in scores as the week progressed and as the images became more challenging.

Team Mentor

Mentors were assigned to each of the eight teams participating. These mentors helped students with self-guided lessons, connecting images, and overall questions. Joshua Russ provides more insight into what occurred.

Joshua Russ | Sandia National Laboratories

The fast paced environment of the Thunderbird Cup pushes students to learn basic Cybersecurity tips competitively amongst their peers. I thought we created a great atmosphere for them to absorb as much knowledge as possible in a short week. Students were slow to socialize at first but once the competition started they did a lot more communicating amongst themselves. The student's ages were a bit scattered, making it seem unfair to some students. The teams were also somewhat unbalanced in terms of skill, however this can be hard to gage with the small amount of time we had with them. Overall the program was well executed and I feel we enticed most of the kids to stay pursuant of their Cybersecurity interests.

ThunderBird Cup Training Evaluation Results

Demographics and general participant information:

Participants were given both the pre- and the post-course evaluations surveys. A total of 28 participants completed the pre-course survey and 21 participants completed the post-course survey. Demographics for the pre- and post-course evaluation surveys are shown on Table 1. It appears that there was a decrease in participation by middle school students and black students.

Table 1

	Pre-Survey (n=29)	Post-Survey (n=21)
Male	54%	52%
% Middle School	61%	52%
% Black	39%	29%

In regards to goals, students indicated that they had plans to study in a number of different fields (Table 2, noted on the pre-test). Over 70% of students on the pre-course evaluation responded that their parents expected them to complete at least a 4-year degree or higher.

Table 2

Field of Study	
Cyber Security/Computer Science	29%
Engineering & Mathematics	25%
Biology/Medical	21%
Other	25%

In the pre-course evaluation, over 60% of students indicated that they were interested in interning at a national lab like Sandia National Laboratories. That percentage increased to 75% in the post-course evaluation. An overwhelming majority (75%) of students did not know of similar programs to the CyberPatriot Course.

Specific Outcome Results:

As shown in Figure 1, the mean on the post-course evaluations were higher than the pre-course evaluation for all 9 criteria. Pre and post-course evaluations showed a statistically significant improvement in students' understanding for most (7 out of 9) of the questions related to knowledge.

Figure 1: Knowledge Questions

Question	Pre-Course Survey Mean (n=28)	Post-Course Survey Mean (n=21)
I understand the similarity between infrastructure and cyber security (p < .001)	2.36	3.57
I understand what a Virtual Machine is and how it works (p = .011)	3.07	4.00
I understand what an Administrator is (p = .075)	3.54	4.19
I understand what are some of the most common Cyberattacks (p = .072)	3.25	3.81
I understand the connections between computers and security in real life (p = .012)	3.46	4.19
I understand how computer hardware works (p = .003)	2.61	3.48
I understand how security software works (p = .004)	2.57	3.48
I understand general Cybersecurity concepts (p = .02)	3.11	3.86
I understand computer systems and networks (p = .05)	2.82	3.43

In regards to the skills questions, the mean on the post-course evaluation was higher than the pre-course evaluation for all questions, except "I have experience in computer programming in Linux," which had no change from the pre- to post-course evaluation (shown on Figure 2). There were only two questions that showed statistically significant improvement for students: "I can do network monitoring," and "I can explain to others the main concepts of Cybersecurity."

Figure 2: Skills Questions

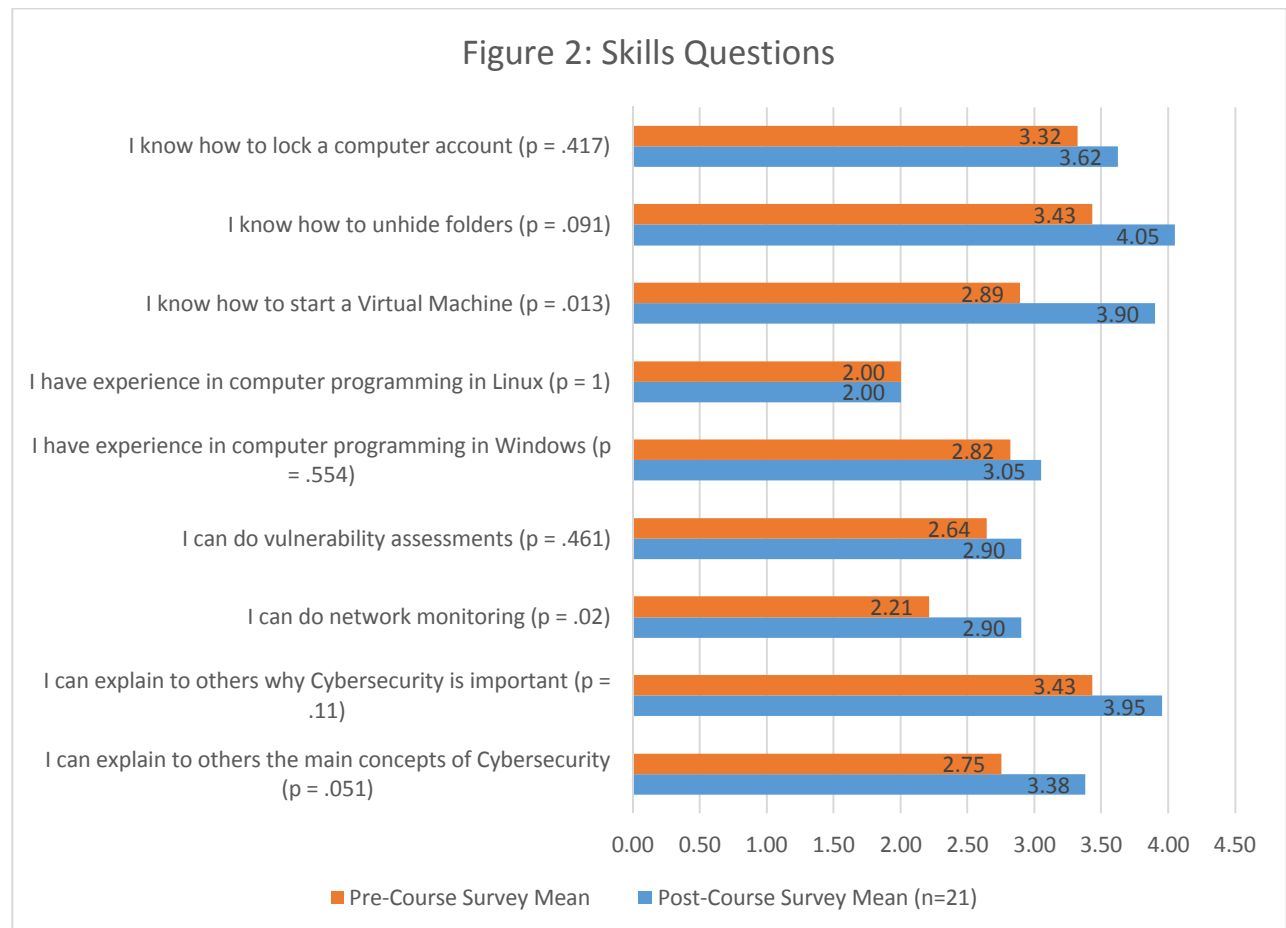| Question	Pre-Course Survey Mean	Post-Course Survey Mean (n=21)
I know how to lock a computer account (p = .417)	3.32	3.62
I know how to unhide folders (p = .091)	3.43	4.05
I know how to start a Virtual Machine (p = .013)	2.89	3.90
I have experience in computer programming in Linux (p = 1)	2.00	2.00
I have experience in computer programming in Windows (p = .554)	2.82	3.05
I can do vulnerability assessments (p = .461)	2.64	2.90
I can do network monitoring (p = .02)	2.21	2.90
I can explain to others why Cybersecurity is important (p = .11)	3.43	3.95
I can explain to others the main concepts of Cybersecurity (p = .051)	2.75	3.38

Figure 3 includes the pre- and post-course evaluation means for questions related to Motivations and Interests. Slight differences in means occurred between the pre- and post-course evaluation, some were higher and some were lower. None of the differences were statistically significant.

Figure 3: Motivations & Interests Questions

Question	Pre-Course Survey Mean	Post-Course Survey Mean (n=21)
I am interested in sharing with others my knowledge of Computer Science/Cybersecurity (p = .896)	3.71	3.67
I am interested in exploring career opportunities in Computer Science/Cybersecurity (p = .786)	3.61	3.71
I am interested in studying Computer Science/Cybersecurity (p = .899)	3.93	3.9
I am interested in doing CyberPatriot (p = .927)	3.54	3.57
I am comfortable asking for help from others (teachers, students, experts) when working on Computer Science/Cybersecurity problems (p = .462)	4.00	4.24