# Final Project

## By Sebastian Medina

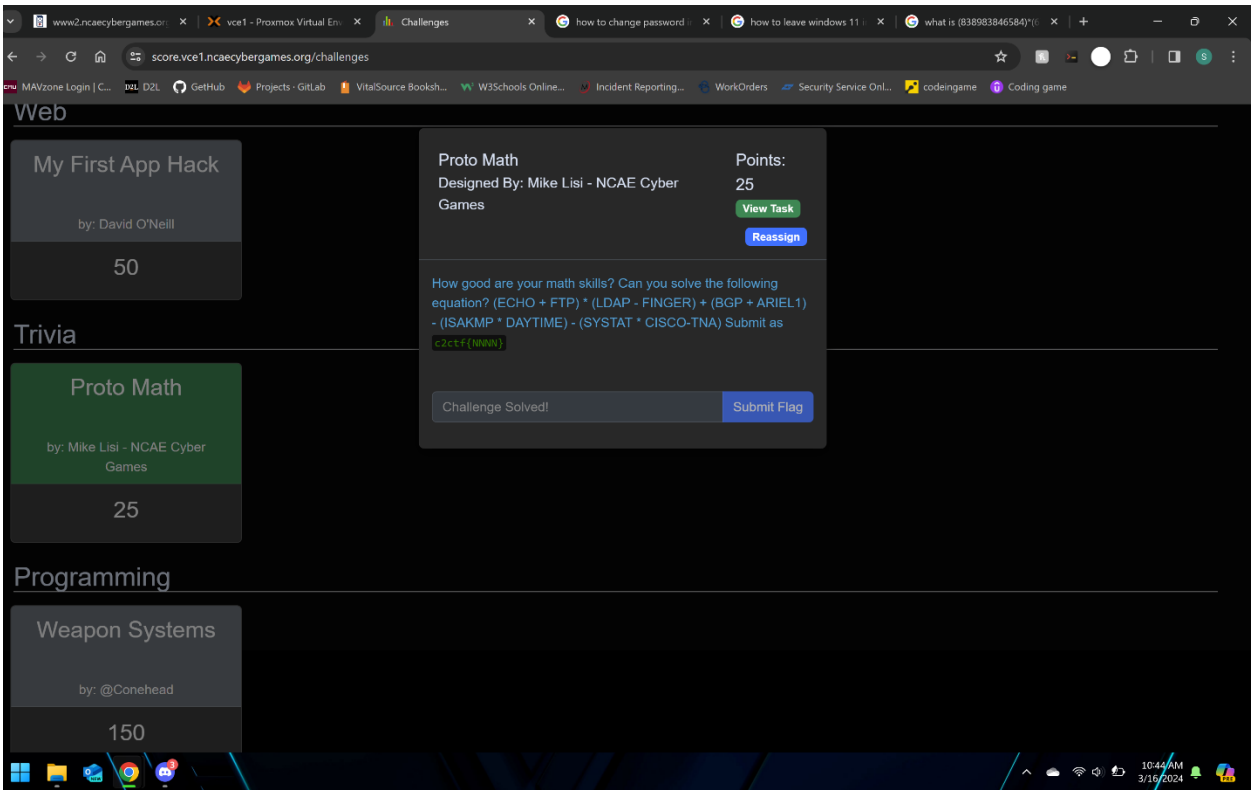
**Content:**

**Final Project Summary** **pg1**

## Summary from NCAE Cybergames:

I decided to do the NCAE Cybergames for my final project. I was in a group with 9 people and Abraham Avila was our team captain. This competition took place on March 16th from 9 AM till 4 PM. Before this day our group would meet every Friday at 3 PM to practice CTF if you were on the CTF part of the team, or Infrastructure if you were on the infrastructure part of the team. I was on the CTF team so I would practice CTF every Friday. Whenever I was practicing CTF I was mostly focusing on Cryptography and Reverse Engineering problems because those were the topics that my group assigned to me. While practicing I used try hack me to learn as much about the two topics I can learn, then I would go on the NCAE cybergames website and do their practice problems that best resembled my two topics that I was assigned. I think having this practice once a week was helpful and I was not caught off guard the day of the competition.

March 16th rolls around and our group shows up an hour early so we can get prepared and ready for the competition. When 9 came around the competition was off and the first few problems for CTF were launched. So right away our team found out that more and more CTF problems will be dropped as the competition continues. So, the first few CTF problems were simple, and we flew by them as a team. Below is one of the first problems I worked on.



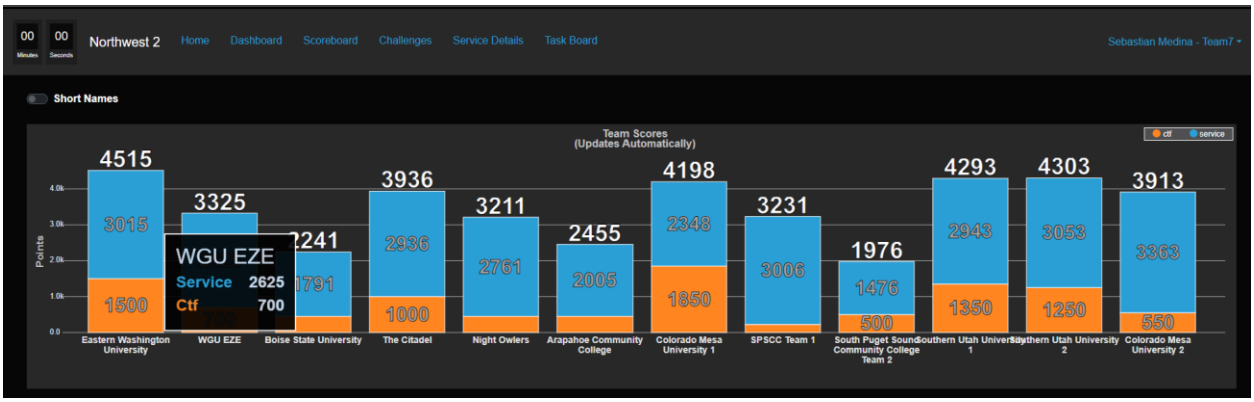

The team and I worked on CTF problems until around noon where we got a lunch break. Once we came back our team noticed that there were way more CTF problems to complete.

The problems that I worked on were the first three hunting problems where I used net witness tool to help me with the problem. While in net witness I did a sql query for the most recent content and I found “Content = ‘text/plain’ ”. I then clicked on this choice, and it took me to an email. Within this email at the bottom was the flag for the first problem. Also, within this email there was a photo attached to the email that hinted that the photo seems to hold more information. I

then used the tool “APERI’NSOLVE” on the image to get the 2nd flag for the hunter problems. For the third one I worked with Same Evans, and we did another query in net witness to look for all attachments what pop up was another letter that had a flag however it was encrypted with a Caesar cypher. Sam then ran this though a decryption for Caesar cypher to get the third flag. Also, another problem that I worked on was the Enclave oil spill. For this one we noticed three rooms that were different form the other five. One room is where you started, another room had a computer that was off and one room you could not get in, all the other rooms had a computer that was on. To solve this one, I just wandered around until the room that was always locked was unlocked, I then went to that room, and it then turned on the computer where the computer was always turned off. I then went into the room that had the computer that was always off but now was on and that computer had the flag.

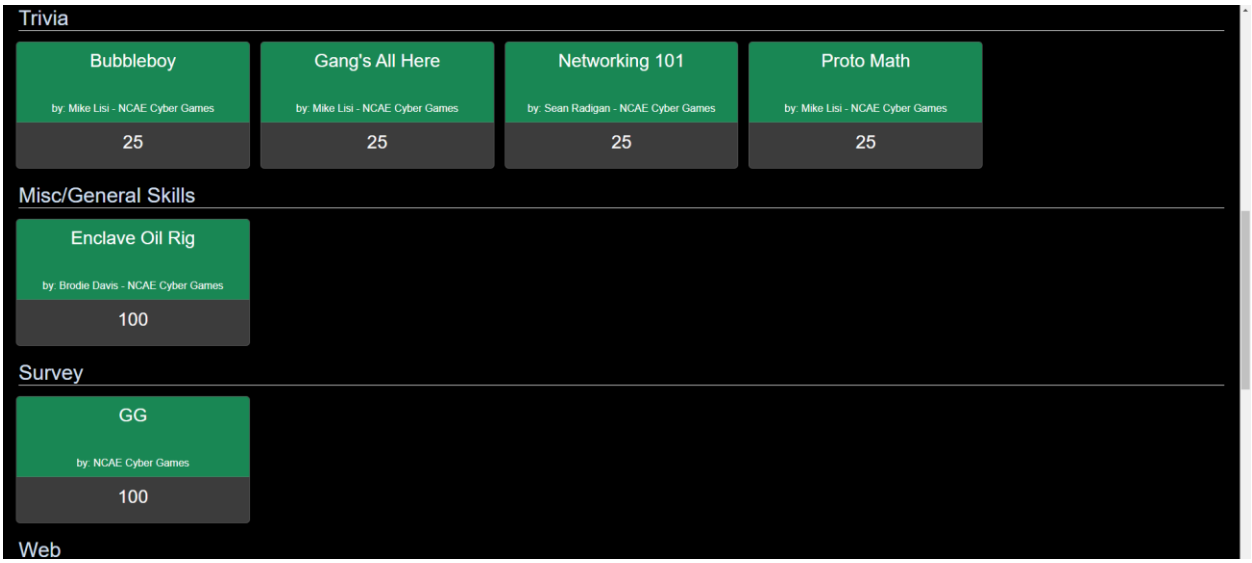
More and more problems started to appear at this point. What we noticed was that the problems started to have levels and problems you must solve first before you can move on to the next one. We kept working on the CTF problems and gained a good score just of CTF. I did not really work on infrastructure, but I do know that the people who did work on it struggled a little bit before we got some systems up and running. We noticed that the other CMU team started to beat us towards the end. So, our CTF team started working together on problems to get

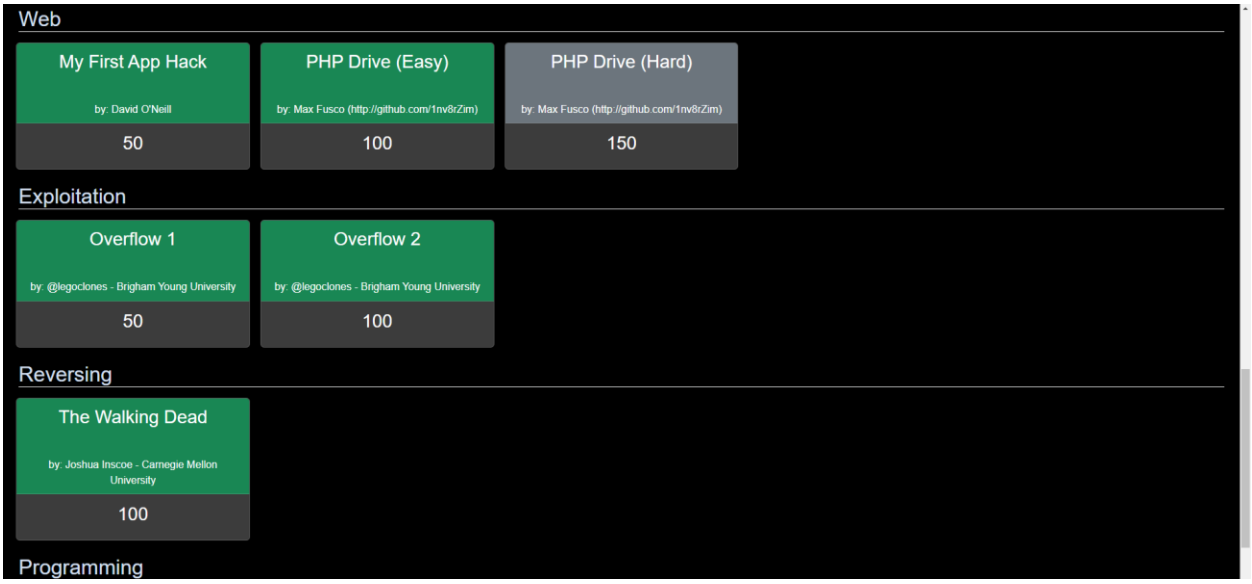
some of the CTF that are worth more points done. I found this helpful because more than one person working on a problem was a lot easier to figure out the issue. I was assigned to work with both Sam Evans and Kyle Verbrugge. We kept working until the competition stopped and we ended up getting fourth in the competition.

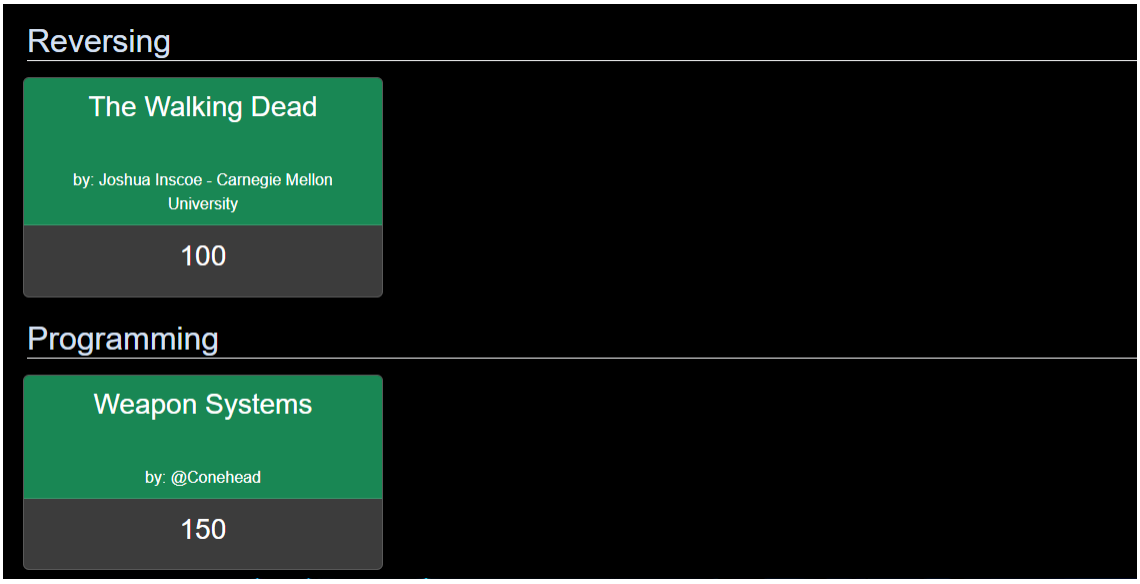



What I think carried us to this position was the CTF team. We worked on and almost completed all the CTF problems by the end. This competition was a lot of fun and I really enjoyed it. If I was still in school next year, I would compete in this competition again. Below are all the problems our CTF team completed for this competition.


Wyze Guys
1 - Monday Morning Mayhem
by: Jarrett Iannotti
50
2 - From the Source
by: Jarrett Iannotti
50
3 - Time to Dig In
by: Jarrett Iannotti
100
4 - Who Dere?
by: Jarrett Iannotti
150
Hunting
1 - Syndicate Threat
by: Cody Spooner - NCAE Cyber Games
50
2 - We are all Pals
by: Cody Spooner - NCAE Cyber Games
100
3 - Pal Manifesto
by: Cody Spooner - NCAE Cyber Games
100
4 - Syndicate Heist
by: Cody Spooner - NCAE Cyber Games
100
5 - Incident Report
by: Cody Spooner - NCAE Cyber Games
250
Misc
A Blank Slate
by: Joshua Inscoe - Carnegie Mellon University
50


Trivia
Bubbleboy
by: Mike Lisi - NCAE Cyber Games
25
Gang's All Here
by: Mike Lisi - NCAE Cyber Games
25
Networking 101
by: Sean Radigan - NCAE Cyber Games
25
Proto Math
by: Mike Lisi - NCAE Cyber Games
25
Misc/General Skills
Enclave Oil Rig
by: Brodie Davis - NCAE Cyber Games
100
Survey
GG
by: NCAE Cyber Games
100
Web


Web
My First App Hack
by: David O'Neill
50
PHP Drive (Easy)
by: Max Fusco (http://github.com/1nv8rZim)
100
PHP Drive (Hard)
by: Max Fusco (http://github.com/1nv8rZim)
150
Exploitation
Overflow 1
by: @legoclones - Brigham Young University
50
Overflow 2
by: @legoclones - Brigham Young University
100
Reversing
The Walking Dead
by: Joshua Inscoe - Carnegie Mellon University
100
Programming


Reversing
The Walking Dead
by: Joshua Inscoe - Carnegie Mellon University
100
Programming
Weapon Systems
by: @Conehead
150