In the UCF Horse Plinko Cyber Challenge I participated on Saturday October 5th, 2024, on a 3-man team as one of our team members did not show up. Despite being a man down my team managed to get 13th place out of 22 teams in the event with 1816.40 points, because of our considerable teamwork and effort. This challenge put my team and I in a fast-paced environment where we had to simultaneously protect and repair multiple boxes given to us while also doing various time limited challenges known as injections given to us during the event. I learned more about how to use Remote Desktop Connection, Server Manager, Windows Security, Computer Management, Linux, various protocols like ftp as a prominent example, general safe security practices, firewall configurations and how to proactively use and change them during an attack, VNC's, C2 servers, MySQL databases, and how to quickly and effectively research and find solutions, how red team use these and more to attack systems, how blue team can use their resources to effectively block them out, and finally how to use these skills in a real life, time-based, team environment. This not only helped me grow my hard technical skills but also my soft team skills and how to effectively communicate with teammates, create plans, and divide work to progress as fast as possible. I was not able to save anything from what I did in the event as I did not want to risk getting disqualified as it was mentioned in the rules to not copy data, and I did not want to mistakenly save something not allowed so instead I will just explain the processes and strategies we went through.

The strategies my team used were to change default passwords at the very start and make the password for each box different and storing them in our private discord chat that the event set up for us. reactive firewall configurations to block outbound connections whenever we find a malicious IP in our logs, monitoring our apps in case anything malicious was installed without our knowledge so we could stop it and remove it. When we found a problem that we couldn't stop we would go to the processes to see if there was anything odd running so we could disable it. Continuously monitoring our users to see if any new users were created, or if any previously disabled users had been activated and given elevated roles like the admin role that way, we could remove users, their user files, and remove roles and disable accounts after changing their passwords so the attackers couldn't simply log back in. And if none of this worked, we would look up the error codes to see if there were any fixes we could find online.

There were a few problems with this plan that I will now go into. This was my teammates and I's first cyber challenge and were unaware that we were allowed to install any programs or update preinstalled ones as we thought that it would be against the rules and did not want to risk being disqualified so we did not install any antivirus, we later found out after the event was over that we could have. The antivirus we would have installed if we had known would have been Malwarebytes. Another issue was that we had no knowledge of VNC's so when the red team installed that onto our systems and started remotely viewing our actions, we were unaware and therefore unable to stop them, this led to them finding all of our passwords when we went to change them as they could see us type them out and let them see how we set up countermeasures so they were able to find ways around them or even remotely control our systems to undo what we had just done to stop them. This gap was our biggest problem throughout the event as since we had no knowledge of VNC's we were stumped on how they were getting our passwords so fast and how they knew what we were planning to do. Now although this was our biggest problem, after the event this also became our greatest learning experience as when they revealed that they had used VNC's we were able to ask

them multiple questions and to have them show us how the program worked in detail and how we could have countered them which was stopping and removing the program.

For our communication and teamwork my team at first decided to have 2 people working on inject challenges at the same time while the final member hardened our systems and stopped the attackers. At first the attackers were slow to work and take down our systems which led this plan to succeed early on but as the event went on the red team started attacking faster and faster with more complex attacks, to respond to this I swapped myself from doing injects to helping with system hardening, stopping attacks, and repairing systems. This made us swap to having 1 person work on injects and having the remaining 2 work on countering the attackers. This was a fluid solution as if the attackers slowed down or encountered roadblocks with how we set up our defenses or the 1 person working on injects was having a problem they couldn't fix, we were able to move another person back to working on injects so we could claim more points which happened multiple times during the event. If we had our fourth and last team member present, the event would have gone more smoothly as we would have been able to continuously have 2 people working on both problems at the same time for the whole event but with our determination and persistence we managed to work through this disadvantage and succeed.