5/13/2023

SoCal Cyber Cup Final Round

Post-Incident Review

(compiled/documented by Iirai Costner)

Slacker Hackers

SDCCE CYBER CLUB:

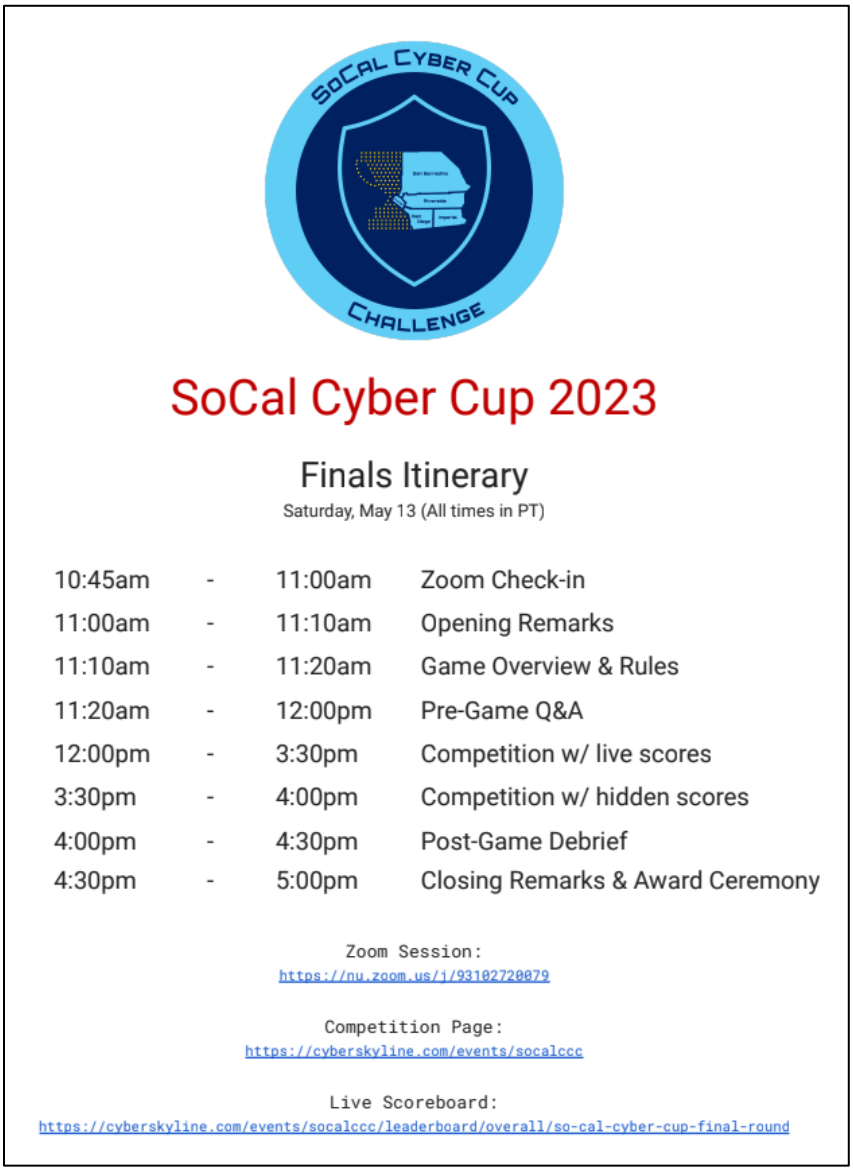
IIRAI COSTNER
JACK COSTNER
ANNA LIZA SMITH
BRANDON SMITH
RUSLAN ZHUMADILOV
ANATOLII KLESHNEV
ANDREW BURKE

Post-Incident Review

SoCal Cyber Cup – Final Round

1. **Incident Overview**:

- Date and time of the incident: The incident occurred on Saturday, May 13, 2023. It is highly likely the incident occurred between 12pm-4pm. Our team was first alerted of the incident at around 12:14pm.



SoCal Cyber Cup 2023

Finals Itinerary

Saturday, May 13 (All times in PT)

10:45am	-	11:00am	Zoom Check-in
11:00am	-	11:10am	Opening Remarks
11:10am	-	11:20am	Game Overview & Rules
11:20am	-	12:00pm	Pre-Game Q&A
12:00pm	-	3:30pm	Competition w/ live scores
3:30pm	-	4:00pm	Competition w/ hidden scores
4:00pm	-	4:30pm	Post-Game Debrief
4:30pm	-	5:00pm	Closing Remarks & Award Ceremony

Zoom Session:
https://nu.zoom.us/j/93102720079

Competition Page:
https://cyberskyline.com/events/socalccc

Live Scoreboard:
https://cyberskyline.com/events/socalccc/leaderboard/overall/so-cal-cyber-cup-final-round

- Description of the incident:

The incident involved multiple IOCs and already-retrieved CTF flags were discovered across 4 different servers: Database (Redis), Web Server (Node), File Server (FTP), File Server (SMB), and we received several alerts through the system indicating various parts of our server went down/offline. Our only "warning" of this attack was through an email sent to one of our Cyber Club team leads.

On Wednesday, May 10, 2023 @ 10:57am, Alphonso Brown received an email with pertinent information regarding the upcoming incident. Email included 2 attachments – The "SoCal Cyber Cup Finals Itinerary" (displayed above), and the "SoCal Cyber Cup 2023 Diagram" (found below). Email states:

Hello Alphonso Brown,

Congratulations on your school qualifying for the SoCal Cyber Cup Finals, which will be held this Saturday, May 13, from 11am - 5pm PT. The SoCal Cyber Cup Finals will be held entirely online and will only require a browser to access the competition, just like the Qualifier.

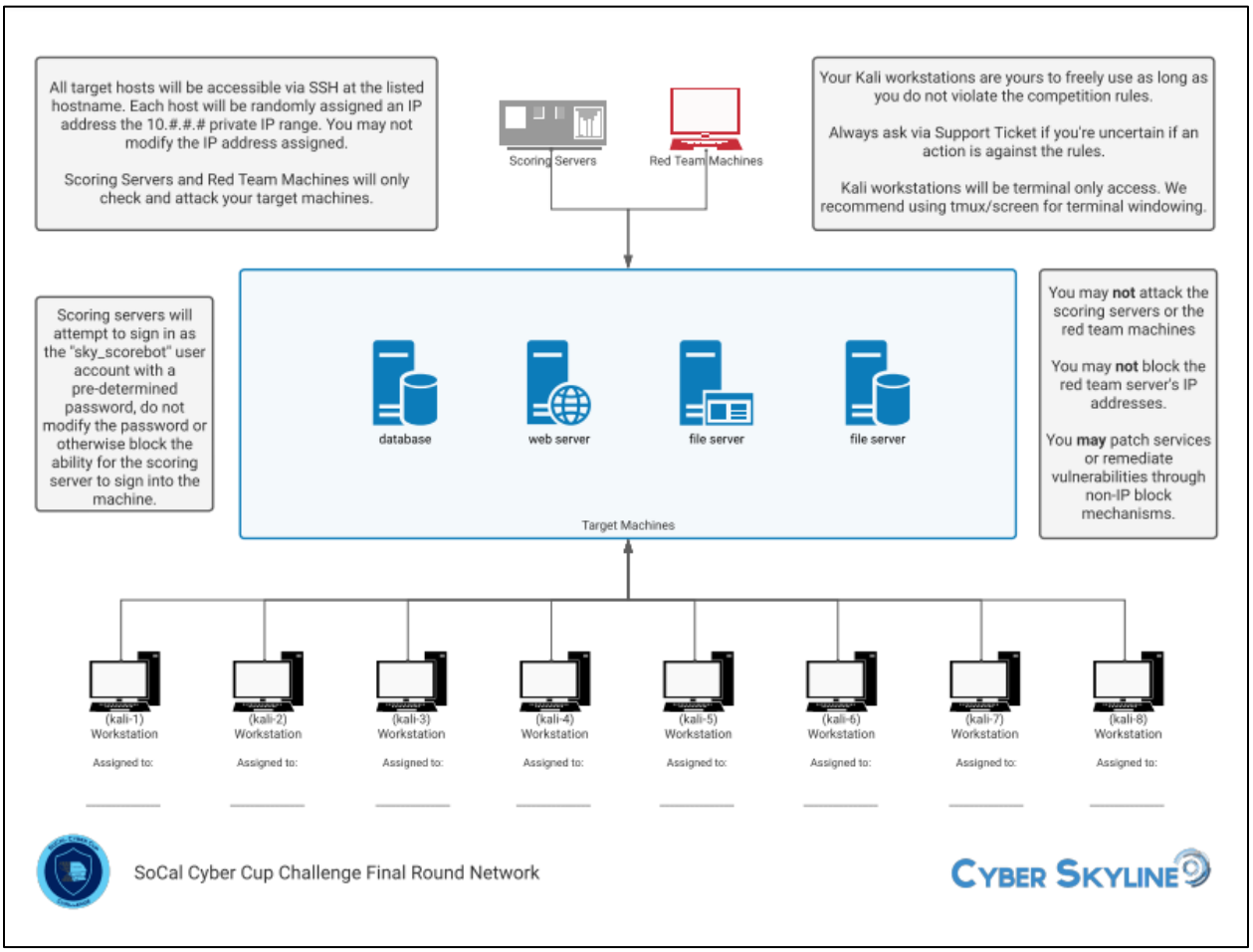
The competition will run from 12pm - 4pm PT. There will be a kickoff that starts at 11am and winners will be announced during the closing remarks that start at 4pm. During the kickoff, we will have a Q&A session for participants to ask their outstanding questions before the competition starts. There will also be a post-game debrief during the closing remarks to walk through the attacks run by the red team. The full itinerary is attached to this email. You can join the Zoom session here: https://nu.zoom.us/XXXXXXXX

During the Finals, teams will be responsible for defending their virtual computer network from live red team attacks. Teams will be provided with 8 Kali machines, which can be used to connect to the computers they will need to defend. Participants will only be responsible for defending their network; they are NOT allowed to attack other targets outside of their network, including other teams. Attacks against the teams will be conducted by a scripted red team, which will ensure a consistent experience for all the teams.

Teams will be competing to obtain the most points. Points will be awarded for 1) completing system administration tasks and 2) passing system checks. There are multiple types of system checks which will check to see if a service is accessible & usable, if a red team exploit was successful, or if a system has the red team's indicator of compromise. Scoring is entirely additive - if a team fails a system check they won't receive the points for that check, but they will not lose points. A live service scoreboard will be made available so teams can see which checks they are passing/failing; however, the scoring for those checks will be delayed.

To maintain a contained environment for the competition, none of the devices will have an external Internet connection, but teams will have the ability to transfer data to/from their network via the clipboard. Teams are also restricted to only using external tools that have been made publicly available prior to the competition and do not require payment to use.

The rules of the competition are available here:
https://docs.google.com/document/d/1JB5xSCt7Zu7Q-xKVZ8UYPntFgJCB2IDGR3FY1AI-lnQ



Another email was sent to Kirsten Lachenmayr on Friday, May 12, 2023 @ 11:36am:

Kirsten Lachenmayr May 13, 2023, 8:54 AM (6 days ago)
to me

From: Nancy Jones <njones2@nu.edu>
Sent: Friday, May 12, 2023 11:36 AM
To: Nancy Jones <njones2@nu.edu>
Subject: SoCal Cyber Cup-Answers to Questions

[EXTERNAL Email: Do not click any links or open attachments if you do not trust the sender and know the content is safe.]

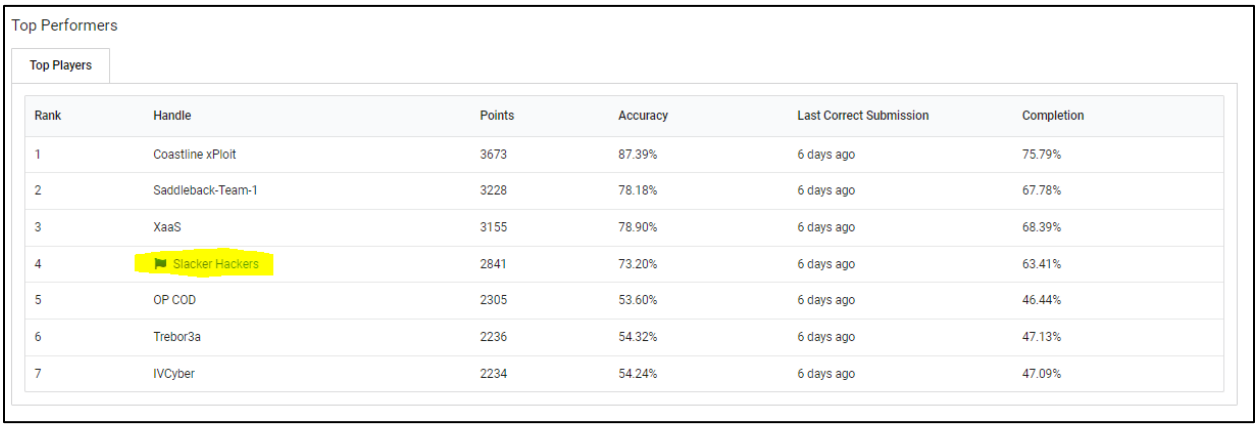
There were two questions that were submitted with the rosters and the following are the responses to the questions. Tomorrow during the Instruction/Discussion time Cyber Skyline will also take additional questions if you have any.

Here are the responses for the two questions for you to send to the coaches:

Q - Just wanted to check in and see if there were any specific requirements to allow any unique traffic or URL's for the competition?
A - The requirements for the finals are the same as the qualifier. You just need to be able to access *.cyberskyline.com and *.cityinthe.cloud from a web browser. A system test is available here: https://cyberskyline.com/support/system/test

Q - What operating systems will be on the 4 boxes? (not the 8 Kali workstations)
A - This will be information the players will need to discover when the game starts.

- Impact on the organization: Losing our ability to rank 1st in the "College" category:



Top Performers

Top Players

Rank	Handle	Points	Accuracy	Last Correct Submission	Completion
1	Coastline xPloit	3673	87.39%	6 days ago	75.79%
2	Saddleback-Team-1	3228	78.18%	6 days ago	67.78%
3	XaaS	3155	78.90%	6 days ago	68.39%
4	Slacker Hackers	2841	73.20%	6 days ago	63.41%
5	OP COD	2305	53.60%	6 days ago	46.44%
6	Trebor3a	2236	54.32%	6 days ago	47.13%
7	IVCyber	2234	54.24%	6 days ago	47.09%

2. **Root Causes**:

- Detailed analysis of the root causes of the incident: Several vulnerabilities were discovered and exploited by the "red team". Through our analysis, our team has concluded that we lacked defense-in-depth, security awareness, threat intelligence, monitoring and incident response, coordination, and leadership to remediate the incident effectively. Lack of preparation in establishing our security posture pre-incident is most likely the cause of our team's downfall.

- Identification of vulnerabilities or weaknesses that were exploited:
  - Initial unfamiliarity with interface: For the first 15 minutes, our team scrambled to figure out the work interface. The "red team" clearly took advantage of this by implanting various IOCs into our servers, and even took our CTF flags.
  - SMB server: /etc/sudoers.d was not hardened, and so a new sudoer was added to the server allowing unauthorized access. Server was misconfigured in a way that files can be written by any user.
  - Redis server: Directory traversal issues and has an ACL config file that was ignored (which could have been used as a fix).
  - Node server: Had a config file that pointed to REDIS, so attacker can get into Redis through Node.
  - FTP server: Either the vsftpd or ProFTPD config file were set with default permissions, so no anonymous users were disabled, allowing the red team to create multiple logins into the server.
  - One of our team members emailed the Co-Founder and CTO of Cyber Skyline, Toby Lin, on May 20th, (1 week after the incident occurred), inquiring of a complete list of vulnerabilities done to the servers, and below is Toby's official response:

For the Node.js server there was a command injection backdoor and a directory traversal vulnerability through the server's connection to the Redis database. The Redis database had no authentication whatsoever, so that's the biggest problem there... The FTP server allowed anonymous read/write which is a poor security configuration. The Samba server, similarly, allowed full file system read write by anyone so the red team can just arbitrarily inject files onto those systems.

3. **Incident Response and Mitigation**:

- Description of the actions taken to respond to the incident:
  - A collaborative Google sheets document was created, shared, and used during the competition by all team members. This online spreadsheet had several tabs that had columns to fill out about each server, Miscellaneous/team notes, Linux commands, LinPeas info dump per server, Floater to-do list.
  - Routine assessment actions:
    - Took note of several things for spreadsheet:
      - Server IP address
      - List of User accounts
      - Source Ips/Destination ports connected to servers
      - CRONTAB
  - System hardening actions:
    - Changed SSH to only allow certain users
    - Whitelisting with IPTables to allow certain ports
    - Changed all username/passwords
    - Changed root password
    - Created new account for just our team use
    - Added to sudoers list and remove unauthorized sudoers
    - Performed LinPeas extract and review for each server
    - Searched for flags.txt
    - Restarted servers
  - SMB server /etc/sudoers.d config file included a sudoer that allowed unauthorized access into the server. File permissions were not changed but user was deleted from the login list. LinPeas ran multiple times throughout the rest of the competition to ensure no new users were added to the list. SMB stayed in the green the rest of the time.
  - Redis server issues were never resolved. A team member used available resources to research how to navigate through the vulnerabilities of Redis, but server was not remediated in the end.
  - Attempted to update/patch a server

- Timeline of the incident response process: The timeline of the incident response process wasn't formally recorded or streamlined/organized as well as it could've been. Our team spent the first

15 minutes getting acquainted with the interface, while some team members went ahead and changed passwords before all of us realized CTF flags from the "System Administration" module were prompting for passwords we had already modified or deleted.

Lunch came, and in the middle of eating and answering questions, everyone was in hectic/panic mode as we scrambled to figure out what needed to be done.

Other questions from the "System Administration" module asked for CTF flags (format: SKY-XXXX-XXXX). By the time our team settled in with the online working environment, all our flag.txt files text content was changed to "red team wuz here". And then once we realized we couldn't grab the flags and switched to the "Network" module, most of our servers' services were down/red X'd. We spent the rest of our time either in research mode or in system assessment and system hardening until the incident/event ended at 4pm.

- Effectiveness of the response and mitigation measures:
  - The collaborative Google sheet worked well within our team but got messy/disorganized after a while as some copy-paste created unnecessarily resized/huge cells, making reading some parts of a column challenging.
  - Routine assessment checks/hardening actions (as listed above): worked well. It helped remediate various server issues.
  - SMB server system assessment/hardening worked well when someone was completely dedicated to it and watching it ("king of the hill" style).
  - Redis was never remediated after research, which kept the server at the "red"/X'd
  - Attempt to patch a server failed. Couldn't load it since it was compiled and because system was air-gapped, we had no means of loading into the server.

4. **Impact Assessment**:

- Assessment of the impact on the organization, including financial, reputational, and operational consequences:
  - The only known consequence is losing our chance at the 1st place spot in the competition. We ranked 4th in the College category and 9th in Overall (against 22 other organizations):

Top Performers

Top Players

Rank	Handle	Points	Accuracy	Last Correct Submission	Completion
1	Coastline xPloit	3673	87.39%	6 days ago	75.79%
2	Saddleback-Team-1	3228	78.18%	6 days ago	67.78%
3	XaaS	3155	78.90%	6 days ago	68.39%
4	Slacker Hackers	2841	73.20%	6 days ago	63.41%
5	OP COD	2305	53.60%	6 days ago	46.44%
6	Trebor3a	2236	54.32%	6 days ago	47.13%
7	IVCyber	2234	54.24%	6 days ago	47.09%

Top Performers

Top Players

Rank	Handle	Points	Accuracy	Last Correct Submission From Start	Completion
1	Coastline xPloit	3673	87.39%	2 hours	75.79%
2	CyberAegis Tempest	3449	84.01%		72.90%
3	walmart les amateurs	3383	81.94%	2 hours	71.37%
4	Saddleback-Team-1	3228	78.18%	3 hours	67.78%
5	Rice Warriors	3216	75.28%	3 hours	65.22%
6	XaaS	3155	78.90%	2 hours	68.39%
7	Cyber Dogs	3148	75.97%	3 hours	65.93%
8	Westview HS	2982	68.89%	1 hour	59.81%
9	Slacker Hackers	2841	73.20%		63.41%

- Identification of any regulatory or legal implications: The Rules of Conduct for the competition:

SoCal Cyber Cup Rules of Conduct (Simplified)

1. You may collaborate with anyone on your team (per the Team Roster on cyberskyline.com) without restriction. This does NOT apply to anyone outside of your team, including others from your school who are on different teams and your coaches
2. Coaches may NOT assist students during the Qualifier or Final Round, but they may assist students in the Practice Round (Gymnasium).
3. You may discuss all challenges from each game after they have ended with coaches & fellow players; however, you may NOT post questions or answers online at any point (even after the games have ended).
4. Behave in a professional manner, including on SoCal Cyber Cup social media channels, communication channels, and when interacting with SoCal Cyber Cup representatives.
5. You must follow all rules of engagement specified in the challenge instructions. This may include limitations on your interactions with domain names, IP addresses, ports, devices, services, accounts, etc.
6. Do not attack the competition platform (cyberskyline.com).
7. Do not sabotage any game elements, including online resources (e.g. modifying another player's competition environment or editing a Wikipedia page to provide false information).
8. Do not modify any unique IDs assigned to you by the competition platform and do not access competition resources using another competitor's unique ID.
9. Do not violate any local, state, federal, or international laws.

Can I…	During the Games	Before/After the Games
discuss challenges with others?	Only within your team	Yes
give or receive tips/techniques/tools/hints or other assistance with others?	Only within your team	Yes
post challenges or answers online?	No	No
sabotage online resources (e.g. Wikipedia) to confuse others?	No	No
run attacks against other teams?	No	No
run automated tools against challenges on cityinthe.cloud?	Only on specified targets	No

5. **Lessons Learned**:

A debrief tab was created on the Google collaboration sheet after the event and was open to all team members to reflect on their experience, any lessons learned, and recommendations of how to improve or prepare for next year. I've copy-pasted and organized our notes based on similar entries, and added some additional commentary for further clarification:

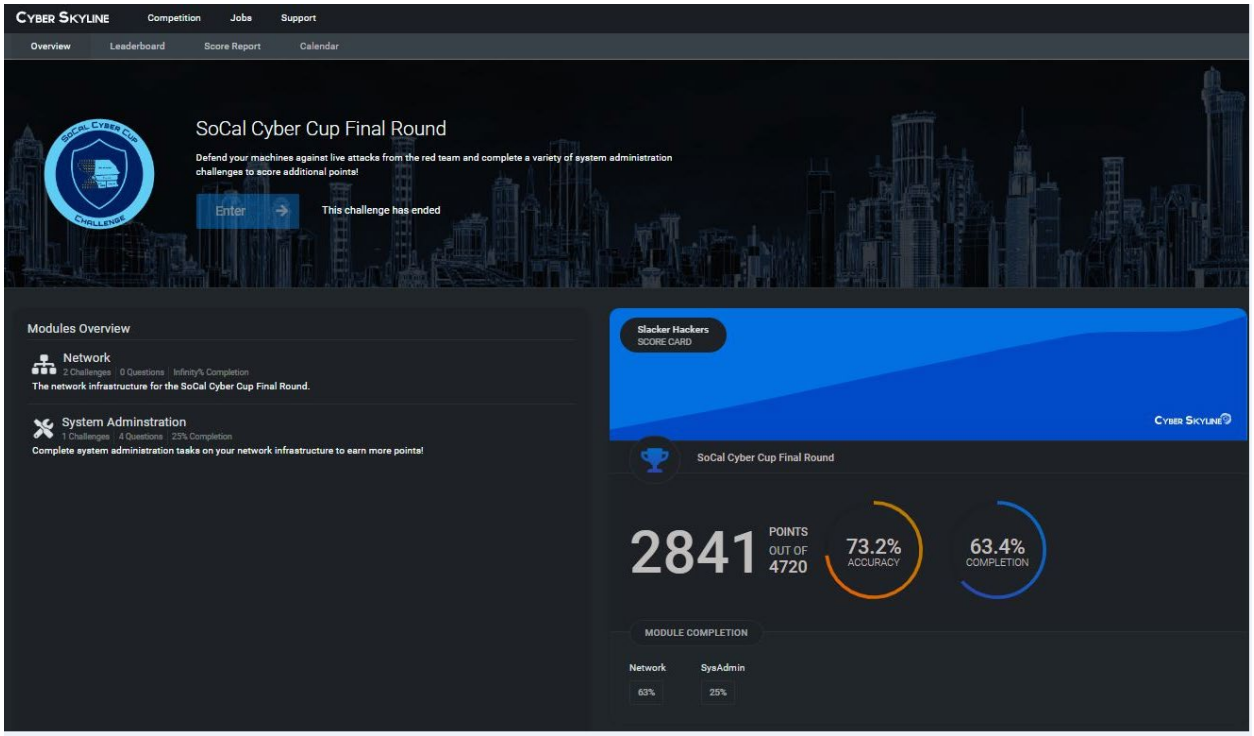
- Key lessons learned from the incident:

    - **A leader or coordinator should take up a large portion of the cyber club meeting time each week and should take the helm for the start of the competition:**
        - *Coordinator is needed at the start of round to make sure the flags are being retrieved first, and that no one is doubling efforts.* (Iirai)
        - *Leadership required. Lack of Management and coordination* (Ruslan)
        - *Coordinator/lead should take charge of some time in weekly meetings to go over Practice Round modules, open up conversation to some possible strategies to be done or progress on current strategies being set in place, etc.* (Iirai)
        - *Create an outline of "mini-deadlines" for what to discuss/prepare for each week during club meetings -- deadlines for scripts, deadlines for etc...* (Iirai)

    - **Preparation on days/weeks/months leading to the Final Round:**
        - *For the team members who aren't as experienced but planning to compete in any round, either find out what they want to do during the competition, or if they don't know, just find "easy things" for them to do so they can help and have them trained on that thing at least a month before competition. Coordinator should find time to accommodate them, so they know their place while competing and not need to bother their fellow teammates during the actual competition with any technical know-how. The actual competition day should*

NOT be spent learning simple key concepts like how to enter a Linux command. (Iirai)

- *Training for the Qualifying Round during club meetings - go over each module during meetings.* (Iirai)
- *When you have questions, go straight to CyberSkyline's support team for confirmation* (Iirai)
- *Do not assume it'll be air-gapped like it was for this time -- just don't assume anything. All scripts, all preparation done, come up with plan B's just in case! Don't even assume that we'll have the ability to copy-paste next year. No assumptions until you can clear it with CyberSkyline's support team.* (Iirai)
- *Familiarize yourself with the different servers and its corresponding config files.* (Iirai)
- *Familiarize yourself with the interface. Everything went through their online web interface, hence... we didn't use our own Kali workstations to ssh into their workstations into the servers.* (Iirai)
- *Become familiar with the "Practice Round" interface. It's very similar to what Final round interface will look like. System Administration was the CTF questions that should be completed first! Network was the area to defend the network for the rest of the time.*



- **Our pre-incident timing and setup:**
  - *We **<u>need extra time</u>** to get inside the room and set up well BEFORE the Zoom check-in call. **EXTRA TIME!** Because the doors to the room weren't opened in time for the Zoom call's Opening Remarks, I know we missed a LOT of key things*

from that discussion that would've helped during the competition, because we were busy trying to get inside, get our equipment set up, and settle in. (Iirai)
    - *We need to receive ALL email communication from CyberSkyline -- esp any regarding Zoom links and other important set up data and diagrams. If you don't have this by the Thursday before the competition, email Alphonso!* (Iirai)
    - *Note to self: Be sure to order a sandwich before I get into my "cyber defending zone".* (Jack)
    - *If we can get into the room and get settled in during the Zoom call, we can also spend THAT time eating our brunch/lunch meal (before competition starts at 12pm) instead of having to stuff our faces trying to eat and type at the same time.* (Iirai)

- **Right when the competition begins (12pm):**
    - *Coordinator should coordinate group for the first 15 minutes until all flags from System Administration are captured.* (Iirai)
    - *No rush. Take time to build strategy* (Ruslan)
    - *Read questions and tasks before changing passwords or doing something* (Anatolii)
    - *Make a backup of files changed such as the password file- also to add another admin but change the name of the admin so we aren't locked out- disable main admin* (Anna)
    - *The flags that were changed were IOCs. You're supposed to delete them.* (Jack)
    - *Read questions and tasks first* (Ruslan)

➢ <u>Recommendations for improvements and preventive measures</u>:

Some of the recommendations listed below will have to be confirmed if it's even possible… send a support desk ticket to make sure it's allowed.

- **Preparation/pre-competition:**
    - *go through this worksheeet: https://www.sans.org/blog/blue-team-defender-guide-capture-the-flag-cheat-sheet/* (Anna)
    - *Go through LinPeas line by line to see what info is available* (Iirai)
    - *Come up with different "gameplays"* (Iirai)
    - *Can we have the desks not facing the window? -- (causes a glare)* (Iirai)
    - *Projector screen should show pertinent information - come up with a web page/screen layout that includes the cyber skyline rank, who's currently working on what, etc* (Iirai)
    - *Know how to copy files and programs via text files. How to re-compile them again* (Ruslan)

- **Automation:**
    - *write script to set up ssh keys and deploy to servers* (Anna)
    - *Do an automated flag search* (Brandon)

        - *Check to see if rsync is installed* (Anna)
        - *auto set firewall rules depending on services on server* (Brandon)
        - *write script to search for flags or do a recursive grep that will search multiple files for phrases like the red team was here.* (Anna)

    - **Servers/Workstations:**
        - *need to locate source files on Node server (or any other type of web server)* (Brandon)
        - *reorganize spreadsheet so that each server has its own tab to dump info about that server.* (Anna)
        - *LinPeas worked really well! This should be the first thing to manually install into each server so anyone can run it at any time.* (Iirai)
        - *maybe leverage the tools included in the kali workstation more such as port scanning etc.* (Anna)

    - **System Hardening**:
        - *getent group sudo and sudo iptables -L are 2 good commands to check on current server hardening status - I did this and LinPeas with SMB and it helped! :) My win was getting and keeping SMB all in the green.* (Iirai)
        - *What if we disable accounts instead of changing their passwords, that way the hashes will remain; this will give us time to copy hashes if we do have to reset the passwords* (Jack)
        - *Use LinPeas to help with system hardening* (Iirai)

6. **Best Practices**:

- Identification of cybersecurity best practices that can be implemented to prevent similar incidents in the future:
    - **Ensuring we have backup files of our config and other files was brought up several times on the debrief collaboration sheet**:
        - *backup all default config files to the workstations* (Brandon)
        - *Check config files* (Ruslan)

- Recommendations for strengthening the overall cybersecurity posture:
        - *We should have copies of every config files; ahead of time we can have copies of files, and compare them with the config files online so we have a default "baseline" config file and it's easy to copy-paste* (Jack)
        - *See if there's a way to lock down config files like the ssh, iptables, crontab-- limit users to write to these files. (change permissions)* (Jack)
        - *Auto-backup the shadow files and server configs, also diff the starting configs with any edits* (Brandon)

7. **Follow-Up Actions**:

- Action items identified based on the lessons learned:

- There is talk on our Slack group chat of some team members attempting to re-create the lab into their own home lab… probably by using docker on an orange pi. Also talk about creating custom automated scripts to run during competition (still needs to be confirmed by support team if we're able to use) to assist with system hardening.
- More discussion on even having text copies of default config files for each server, and coming up with scripts to compare this baseline version against the version on the servers.
- Proper coordination and leadership was clearly lacking during the competition and in the months leading up to it. This has to change, especially leading the people who are not as experienced as other team members, and find actual tasks for them to do on the day-of.
- Preparation/setup time is crucial to our success, especially trying to get settled into the room and eating light foods DURING the Zoom check-in call time.

- Assigning responsibilities and timelines for implementing the recommended actions:
  - Responsibilities and timelines will be determined in 2024 when our team receives the next official SoCal Cyber Cup schedule and timeline.
  - Highly recommend dividing the number of total modules in the Practice Round by total number of cyber club meeting days leading up to the Qualifying Round. Then going over each module in detail during the meetings so everyone is on the same page and has homework to do for the week to complete the module on their own. This will ensure everyone going in to the Qualifying Round knows what their best strengths are, and this can help divvy us up into teams.

8. **Documentation and Communication**:

- Record of all relevant documents, reports, and evidence related to the incident:
  Our only document is our Google collaboration document. Most of what was relevant in the Google sheets document has been written up here.

- Communication plan for sharing the lessons learned within the organization:
  I will be uploading this Lessons Learned document on our Slack group chat, accessible to all of our current team members. In 2024, we will also be releasing this document to new team members who qualify for the Finals Round.

9. **Review and Revision**:

- Schedule for periodic reviews and updates to the Lessons Learned document:
  From now until the Qualifying Round for 2024 is over, we will continue to update this document as well as our Google collaboration sheet.

- Process for incorporating new insights and experiences from future incidents:
  After our 2024 SoCal Cyber Cup competition, it is highly recommended the team members stay after the Zoom debrief call to discuss key items (success and ways to improve for 2025) for the next Lessons Learned document.