2024 Southeast Collegiate Cyber Defense Competition

Virtual Qualifier Team Packet

Contents

1 Competition Schedule

We are excited to host the Southeast Collegiate Cyber Defense Competition. Our first event begins on Jan 27, 2024 with a virtual ask-me-anything (AMA) and rules brief. The following weekend, we will provide tokens to register on Mattermost, and the credentials to login to the SECCDC scoring portal and test environment. The top 8 teams from qualifiers will be selected to attend the SECCDC Regional event at the Kennedy Space Center on March 23-24th.

Date	**Event**	**Time**	**Location**
Jan 27, 2024	Rules Briefing / AMS	10AM EST	Zoom
Feb 3, 2024	Test Environment Released	10AM EST	AWS / Portal / Mattermost
Feb 10, 2024	Virtual Qualifiers Begin	8 AM EST	AWS / Portal / Mattermost
Feb 12, 2024	Qualifing Teams Announced	12 PM EST	Zoom
Mar 23-24, 2024	SECCDC Regional Event	-	Kennedy Space Center

Table 1: High-Level Schedule

- **Zoom (AMA)**: https://fit.zoom.us/j/99708763031
- **Mattermost Server**: https://mattermost.seccdc.org/seccdc/messages/@enrollmentbot

The qualifiers will run from 8 AM EST to 4 PM on February 10th, 2024. Room judges (may be university faculty, staff, employee) must be logged into our competition communications platform (Mattermost) NLT 8:45. The competition will begin at 9 AM EST and run through 4:00 PM EST, with a slowdown for competitors to take lunch from 12:00-12:30.

Time	**Description**	**Location**
8:00 AM EST	Judge and Competitor Sign in	Mattermost (public facing)
8:30 AM EST	Infrastructure is Live	Competition VPN (internal)
8:45 AM EST	Judges Check In Complete	Mattermost (public facing)
9:00 AM EST	Competition Begin	Competition VPN (internal)
12:00 PM EST	Lunch Slowdown Start	-
12:30 PM EST	Lunch Slowdown End	-
4:00 PM EST	Competition End	-

Table 2: Virtual Qualifiers: February 10th, 2024

2 Sponsors

We are incredibly grateful for the support of our generous sponsors that make this competition available to competitors. Please note, this sponsorship reflects sponsor agreements finalized at the time of the Virtual Qualifiers. We anticipate additional sponsors for the in-person Regional event at the Kennedy Space Center. Please visit https://event.fit.edu/seccdc/sponsors/ for updated sponsorship information.

Titanium Sponsor

- RTX

Platinum Sponsors

- Amazon AWS
- Florida Institute of Technology
- L3 Harris Institute for Assured Information

Gold Sponsors

- Battelle
- National Security Agency
- Cisco

Silver Sponsors

- Palo Alto
- Fortra

3 Registered Teams

College or University	Coach's Name	Coach's Email Address
Alabama A&M University	Terry Miller	terry.miller@aamu.edu
Auburn University	Drew Springall	aaspring@auburn.edu
Augusta University	JoJon Cabrera	jocabrera@augusta.edu
Charleston Southern University	Julie Henderson	jhenderson@csuniv.edu
Clemson University	John Hoyt	hoytj@clemson.edu
College Of Charleston	Mohamad Baza	bazam@cofc.edu
College of Coastal Georgia	Dr. Nelbert St.Clair aka Doc	nstclair@ccga.edu
Columbus State University	Ehab Bedir	bedir_ehab@columbusstate.edu
East Tennessee State University	Biju Bajracharya	bajracharya@etsu.edu
ECPI University Columbia	Chris Flanery	cflanery@ecpi.edu
Florida Atlantic University	Dr. Hari Kalva	hkalva@fau.edu
Florida Polytechnic University	Ujan Mukhopadhyay	umukhopadhyay@floridapoly.edu
Florida State University	Shuyuan Metcalfe	smho@fsu.edu
Georgia Institute of Technology	Martin Kiriluk	martin.kiriluk@security.gatech.edu
Kennesaw State University	Humayun Zafar	hzafar@kennesaw.edu
Lipscomb University	Dr. Chris Simmons	chris.simmons@lipscomb.edu
Mississippi State University	Stephen Torri	storri@cse.msstate.edu
Montreat College	Greg Sayadian	greg.sayadian@montreat.edu
Polk State	John Stewart	jstewart@polk.edu
Shaw University	Nyteisha Bookert	Nyteisha.Bookert@shawu.edu
St. Petersburg College	Jeffrey Handy	Handy.Jeffrey@spcollege.edu
Tennessee Technological University	Travis Lee	tlee@tntech.edu
The Citadel	William Johnson	wjohns12@citadel.edu
The University of Alabama in Huntsville	Tathagata Mukherjee	tm0130@uah.edu
Trident Technical College	Frank Gibbes	frank.gibbes@tridenttech.edu
University of Central Florida	Tom Nedorost	thomas.nedorost@ucf.edu
University of Florida	Joseph Wilson	jnw@cise.ufl.edu
University of North Carolina at Charlotte	Dr. Bill Chu	billchu@charlotte.edu
University of North Carolina Wilmington	Geoffrey Stoker	stokerg@uncw.edu
University of North Florida	Larry Snedden	l.snedden@unf.edu
University of North Georgia	Daniel Baker	daniel.baker@ung.edu
University of South Alabama	Jeffrey McDonald	jtmcdonald@southalabama.edu
University of South Carolina	Tony Dillon	TLDILLON@cec.sc.edu
University of South Florida	Marbin Pazos Revilla	marbin@usf.edu
University of Tennessee at Chattanooga	Mengjun Xie	mengjun-xie@utc.edu
University of West Florida	Anthony Pinot	apinto@uwf.edu

4 Competition Rules

The competition is designed to test each team's ability to secure and administer networked computer systems while maintaining standard business functionality. The scenario involves team members simulating a group of new employees brought in to integrate, manage and protect a fictional small business. Teams are expected to manage the computer network, keep it operational, address vulnerabilities/misconfigurations, and control/prevent any unauthorized access. Each team will be expected to maintain and provide a set of public services such as: a website, an email server, a database server, an application server, and workstations used by simulated sales, marketing, and research staff. Each team will start the competition with a set of identically configured systems.

The objective of the competition is to measure each team's ability to maintain secure computer network operations in a simulated business environment. This is not just a technical competition, but also one built upon the foundation of business operations. A technical success that impacts the business operation will result in a lower score, as will a business success which results in security weaknesses. Throughout these rules, the following terms are used:

- **Black Team** - competition officials that organize, run, and manage the competition.
- **White Team** - competition officials that observe team performance in their competition area and evaluate team performance and rule compliance.
- **Red Team** - penetration testing professionals simulating external hackers attempting to gain unauthorized access to Blue Team systems.
- **Blue Team/Competition Team|** - the competitive teams consisting of students competing in the SECCDC.
- **Team Captain** - a student member of the Blue Team identified as the primary liaison between the Blue Team and the White Team or Black Team.
- **Team Co-Captain** - a student member of the Blue Team identified as the secondary or backup liaison between the Blue Team and the White Team, should the Team Captain be unavailable (i.e., not in the competition room).
- **Team representatives/Coach** - a faculty or staff representative of the Blue Team's host institution responsible for serving as a liaison between competition officials and the Blue Team's institution.

Unless otherwise stated, the SECCDC is governed by the National CCDC ruleset posted here: http://www.nccdc.org/index.php/competition/competitors/rules. These rules govern:

- Competitor Eligibility
- Team Composition
- Team Representatives
- Competition Conduct
- Internet Usage
- Permitted Materials
- Professional Conduct
- Questions, Disputes, and Disclosures
- Scoring
- Remote Site Judge[1]

[1]Remote judges for SECCDC may consist of a university faculty member, staff, or employee.

SECCDC Competition Specific Rules – in additional to the aforementioned National CCDC rules, the following rules will also be enforced during this event:

---

1. No unapproved operating system or application changes are permitted during the competition (servers or workstations) unless allowed via inject. You may patch, apply service packs, and update but you must defend what you are given for the first day. For example, you may upgrade from Debian 10.1 to 10.3, but not to Debian 11. You may upgrade from Apache 2.4.6 to Apache 2.4.9 but you may not migrate to Nginx.
2. You may not containerize any scored platform or service unless instructed to do so in an inject. You may use containers for non-scored systems and services your team creates for their own use such as an IPS, sniffer, or team file server.
3. You may not migrate or replicate any critical services to a different platform or system without authorization.
4. All inject responses and deliverables must be typed and delivered electronically in PDF format via the inject portal.
5. You must maintain both the functionality and content of all critical services. For example, a website that serves dynamic content must continue to serve up dynamic content. An FTP service that allows anonymous access must continue to allow anonymous access.
6. Password changes to user accounts for critical services must be provided to the Operations team in electronic format via the inject portal. For more details refer to Sectionsec:password in this team packet.
7. The **seccdc_black** user account is off-limits. You may not disable, modify credentials, or change the permissions of the account.
8. Injects will be delivered via the inject portal. Teams are responsible for monitoring the inject portal for injects and announcements. In the case of an issue with the inject portal, teams will utilize Mattermost as the alternative method for communication.
9. Team Captains may request reversions of machines to the original state, which are served on an as available basis. Each reversion will incur a 50 point deduction in score. There is no ability to snapshot or revert machines to anything other than the original state. The competition organizers may announce a "cut-off" for reversion requests during the competition, after which no more reversions may be granted.
10. As security professionals, teams must carefully balance the impact introducing security against the functionality of services. Teams are cautioned to gradually introduce security mechanisms while ensuring the functionality of services, realizing that scoring is delayed.

5 Scoring

The winner will be determined by the highest cumulative score at the end of the competition. Accumulated point values are broken down as follows:

- **Critical services** account for 50 percent of the possible points (based on a random polling interval of core services)
- **Successful completion of injects** accounts for 50 percent of the possible points (awarded points will vary by task, but will be part of a cumulative total)
- **Successful Red Team actions** will result in point deductions from a team's total score based on the level of access obtained, the sensitivity of information retrieved, critical services affected, and the persistence of the attack.

Functional Services Services are always expected to be operational or as specified throughout the competition. In addition to being up and accepting connections, the services must be functional and serve the intended business purpose. At semi-random intervals, services will be tested for functionality and content where appropriate. Each successfully served request will gain the team the specified number of points. Unresponsive services are always marked as failures.

6 Password Changes

If your team changes user level passwords for scored services that require a password (such as SSH) you must provide a comma separated value (csv) text file containing your password changes to the black team on the relevant inject and then notify the black team via Mattermost. The file should contain comma separated values with one user per line like this (no space after comma):

```
checkname,user,password
checkname,user2,password2
```

For example, if you change the service on the NebulaNet-http server for elvara.boss, you would submit

```
NebulaNet-http,elvara.boss,NewPasword123
```

The only information inside the file should be the check name, users, and passwords – do not include headers or any other additional information inside the file. You must provide one file for EACH service that requires password changes – do not include multiple services in the same file. Name the file "TeamXX_SERVICE_PWD" and replace XX with your team number and SERVICE with the critical service these password changes apply to. For example, a password file for the NebulaNet SSH service must be named "TeamXX_NebulaNet-SSH_PWD". An improperly named file will be rejected. Each file must have an unique name, so, if you must submit a password file for the same service twice you may append a number (ex: "TeamXX_NebulaNet-SSH_PWD2", "TeamXX_NebulaNet-SSH_PWD6").

Accepted files will be loaded into the scoring engine as is. You must allow 10 to 15 minutes for password changes to take effect. You DO NOT need to provide us with password changes to "root" or "administrator" accounts – only user accounts. Passwords can be up to 24 characters long and may consist of any combination of upper case letters, lower case letters, numbers, and the following special characters: . @ # $ % & ! ? : * _ - + =

Password change files must be uploaded to the Inject Portal under the "Password Changes" inject. You must message competitions officials in the appropriate channel on the Mattermost server each time you upload a password change file. Please remember you only need to submit password files for scored services that use passwords.

For the SECCDC 2024 round, the MySQL scoring check (fractalhash-custom) and the FTP scoring check _will not accept password changes.

7 Competition Network Information

Here are the scored services for the network. The team is responsible auditing all hosts for the on their assigned network (10.100.X.4-10.100.X.254), except where otherwise mentioned.

Service	IP	Hostname
SSH	10.100.X.4	QuasarQuiet
FTP	10.100.X.5	db01
SSH	10.100.X.5	db01
DNS	10.100.X.6	StarDNS
SSH	10.100.X.6	StarDNS
SSH	10.100.X.7	GlobalAD
SSH	10.100.X.8	FractalHash
MySQL	10.100.X.8	FractalHash
HTTP	10.100.X.9	web-webapp
HTTP	10.100.X.9	web-forum
SSH	10.100.X.10	NebulaNet
HTTP	10.100.X.10	NebulaNet

Table 3: Scored Services

The inject portal is a "trusted asset" – any materials you download can be considered trusted as the Red Team does not have access to post materials on the portal.

Off-Limits The following machines will not be managed by Blue Team and should not be interfered with or blocked:

- Default Gateway 10.100.X.1
- AWS Artifacts 10.100.X.2-3
- VPN Server 10.100.X.20
- Scoring_Test1 Provided to competitors at competition
- Scoring_Test2 Provided to competitors at competition
- Scoring_Test3 Provided to competitors at competition

Scored Users The following user accounts must be maintained. Administrative accounts are required to maintain their access for full points:

elara.boss	sarah.lee	lisa.brown
michael.davis	emily.chen	tom.harris
bob.johnson	david.kim	rachel.patel
dave.grohl	kate.skye	leo.zenith
jack.rover		

Table 4: Scored Administrative Users

lucy.nova	xavier.blackhole	ophelia.redding
marcus.atlas	yara.nebula	parker.posey
maya.star	zachary.comet	quinn.jovi
nina.eclipse	alice.bowie	ruby.rose
owen.mars	bob.dylan	samantha.stephens
parker.jupiter	carol.rivers	taurus.tucker
rachel.venus	emily.waters	una.veda
ruby.starlight	frank.zappa	ava.stardust
samantha.aurora	grace.slick	benny.spacey
sophia.constellation	harry.potter	celine.cosmos
tessa.nova	ivy.lee	dave.marsden
thomas.spacestation	kate.bush	emma.nova
una.moonbase	luna.lovegood	frank.astro
victor.meteor	mars.patel	grace.luna
wendy.starship	neptune.williams	henry.orbit
ivy.starling		

Table 5: Scored Normal Users

8 Required Software

For the virtual environment, you should have the following tools installed on your system.

- **MatterMost** - You must be able to access https://mattermost.com. You may use the stand-alone client or web-application. This will be used to manage all competition communication.
- **Wireguard** - The competition environment is hosted on a closed network. You must access the network through the wireguard VPN. You can download wireguard from https://www.wireguard.com.
- **SSH Client** In most cases, you must use a SSH client to interact with machines.
- **Docker** One inject will provide a container with source code for analysis. While running the container is not required to accomplish the outcomes, it may benefit competitors to run the container locally for testing.

9 Frequently Asked Questions

Q1 Will the environment have external connectivity to download tools, patches?

Yes. Although the entry to the network is controlled by a VPN, it is connected to the internet externally to allow downloading tools and patches. Please refer to the rules for what can be installed on the machines.

Q2 What should we do in the event of an epic fail that requires the attention of the competition director?

Contact the black team on Mattermost. Please understand we have 37 teams registered and it may take some time to address the issue. Please test the connectivity of your network well in advance of the competition.

Q3 How did you choose injects this year?

Injects were inspired by:

- speaking with real-life system administrations about the problems they face
- discussing with members of the NCCDC red team about successful strategies they have seen in the past
- past nationals injects

Q4 Will I have access to the Palo Alto firewall or AWS Control plane?
If you qualify for regionals at the Kennedy Space Center, but not during the virtual qualifer.

Q5 Any special skills I should ensure my team is prepared for?

Your team will be asked to identify the security implications of a program coded in Python. While no coding is required, you should have a team member that can trace the general flow of the program and identify security issues. Source code and a container are provided. You can (but are not required) to run the container locally for testing.

From: CEO Elara Vexx
To: Galatic Space Adventure New Hires
Subject: Welcome

Welcome aboard **Galactic Space Adventures**, where the sky isn't the limit—it's just the beginning! As the latest recruits in our interstellar journey, you are the guardians of our digital cosmos. Your mission, should you choose to accept it, is to safeguard the galaxy of data that powers our space-faring dreams. In the boundless expanse of cyberspace, our assets are more than just bytes and bits—they're the stars and planets in our corporate universe. Your expertise will shield our systems from the dark void of cyber threats and keep our digital worlds spinning safely.

As part of the international team, you'll be joining forces in the quest to propel humanity to new frontiers. We rely on the collective might of our team to ensure that our customer's dreams of zero-gravity entertainment and lunar escapades are not just safe but out of this world! Your journey with us will be one of exploration, innovation, and most importantly, security. Remember, in space, no one can hear you scream, but in cyberspace, even the silent whispers of vulnerability can be heard across galaxies. Be vigilant, be brave, and always be ready to tackle the unknown with a can-do attitude that says, "*Yes, I can secure this network, even in zero gravity!*"

Buckle up for an adventure where your skills will help navigate through nebulae of network challenges, asteroid fields of algorithms, and the vast voids of virtual security. Let's shoot for the stars and make every digital encounter a safe passage. Welcome to Galactic Space Adventures – where you don't just watch the stars, you protect them. Best cosmic wishes,

Elara Vexx

Elara Vexx

CEO
Galactic Space Adventures