2026 Southeast Collegiate Cyber Defense Competition

Qualifiers Team Packet

Contents

1 Competition Schedule

We are excited to host the Southeast Collegiate Cyber Defense Competition. Please view the important events below.

Date	Event	Time
Feb 02, 2026	Test Environment Released	18:00 EST
Feb 03, 2026	Test Environment Closed	18:00 EST
Feb 07, 2026	Pre-Brief	08:40 EST
Feb 07, 2026	Virtual Qualifiers Begin	09:00 EST
Feb 07, 2026	Virtual Qualifiers End	17:00 EST
Feb 07, 2026	Debrief	17:15 EST

Table 1: High-Level Schedule, Qualifier Round

- **Discord (AMA)**: https://discord.gg/4Hvcyh5q9j
- **Mattermost Server**: https://10.250.250.5/

2 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.

2.1 Rules Introduction

The following are the approved national rules for the 2025 Collegiate Cyber Defense Competition (CCDC) season. Throughout these rules, the following terms are used:

- **Gold Team/Operations 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 competition teams' systems.
- **Black Team**: Competition support members that provide technical support, handle communications, and offer overall administrative assistance.
- **Blue Team/Competition Team**: The institution competitive teams consisting of students competing in a CCDC event.
- **Team Captain**: A student member of the Blue Team identified as the primary liaison between the Blue Team and the White 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**: 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.

2.2 Competitor Eligibility

1.1. Competitors in CCDC events must be full-time students of the institution they are representing.

1.1.1. Team members must qualify as full-time students as defined by the institution they are attending.

1.1.2. Individual competitors may participate in CCDC events for a maximum of five seasons. A competitor has a maximum of six years to complete their five seasons of eligibility. A CCDC season is defined as the period between the start of the first state event and the completion of the National CCDC event. Participation on a team in any CCDC event during a given season counts as participation for that entire season.

1.1.3. A competitor in their final semester prior to graduation is exempt from the full-time student requirement and may compete in CCDC events as a part-time student, provided the competitor has a demonstrated record of full-time attendance for the previous semester or quarter.

1.1.4. If a team member competes in a qualifying, state, or regional CCDC event and graduates before the next CCDC event in the same season, that team member will be allowed to continue to compete at CCDC events during the same season should their team win and advance to the next round of competition.

1.2. Competitors may only be a member of one team per CCDC season.

1.3. A team member may not participate in any role at CCDC events held outside the region in which their team competes during the same CCDC season.

1.4. Individuals who have participated in previous CCDC events in any role other than as a competitor must obtain eligibility approval from the director of the region in which their team competes prior to being added to the team roster. Once a candidate's eligibility has been approved, they will remain eligible for all CCDC events during the same season.

2.3 Team Composition

2.1. Each team must submit a roster of up to 12 competitors to the designated registration system. Rosters must be submitted by published deadlines and include a coach who is a staff or faculty member of the institution the team is representing. All competitors on the roster must meet all stated eligibility requirements. No changes to the team roster will be permitted after the team competes in their first CCDC event. The competition team must be chosen from the submitted roster. A competition team is defined as the group of individuals competing in a CCDC event.

2.2. Each competition team may consist of up to eight (8) members chosen from the submitted roster.

2.3. Each competition team may have no more than two (2) graduate students as team members.

2.4. If a member of a competition team advancing to a qualifying, state, regional, or national competition is unable to attend that competition, that team may substitute another student from the roster in their place prior to the start of that competition.

2.5. Once a CCDC event has begun, a team must complete the competition with the team that started the competition. Substitutions, additions, or removals of team members are prohibited except for extreme circumstances. Team Representatives must petition the Competition Director in writing for the right to perform a change to the competition team. The Competition Director must approve any substitutions or additions prior to those actions occurring. Teams or team members arriving after an event's official start time, for reasons beyond their control, may be allowed to join the competition provided a substitution has not already been made. Event coordinators will review the reason for tardiness and make the final determination.

2.6. Each team will designate a Team Captain for the duration of the competition to act as the team liaison between the competition staff and the teams before and during the competition. In the event of the Team Captain's absence, teams must have an identified team liaison serving as the captain in the competition space at all times during competition hours.

2.7. An institution is only allowed to compete with one team in any CCDC event or season. A CCDC team may only compete in one region during any given CCDC season. Exhibition teams are not eligible to win any CCDC event and will not be considered for placement rankings in any CCDC event.

2.4 Team Representatives

3.1. Each team must have at least one representative present at every CCDC event. The representative must be a faculty or staff member of the institution the team is representing.

3.2. Once a CCDC event has started, representatives may not coach, assist, or advise their team until the completion of that event (including overnight hours for multi-day competitions). Representatives may not enter their team's competition space during any CCDC event. Representatives

must not interfere with any other competing team.

3.3. The representative, or any non-team member, must not discuss any aspect of the competition event, specifically event injections, configurations, operations, team performance, or Red Team functions, with their team during CCDC competition hours and must not attempt to influence their team's performance in any way.

3.4. Team representatives/coaches may not participate on the Red Team, Gold Team, Operations Team, Black Team, White Team, or Orange Team at any CCDC event in the same season in which their team competes.

3.5. Team Captains are required to respond to organizers in a timely fashion.

2.5 Competition Rules

4.1. Teams are expected to follow all competition rules, regulations, and guidelines as outlined by competition officials.

4.2. Teams are required to maintain professional conduct throughout the competition. This includes respectful behavior towards other teams, competition staff, and Red/White Team members.

4.3. Use of prohibited tools or actions, such as intentionally disrupting other teams' environments or violating network policies, may result in disqualification.

4.4. Each competition team must operate only within the environment and resources assigned to them. Any unauthorized access or tampering with another team's environment is strictly prohibited.

4.5. Teams are strictly prohibited from removing information such as malware artifacts, indicators of compromise, or other technical information from the competition environment. This includes not only saving it to a student's computer but also uploading it to sites such as Virus Total or using automated tooling that would upload it to antivirus companies.

4.6. Teams for this round are going to be leveraging personal devices to access the competition infrastructure, during the time that they are engaged with the competition students may not access personal email accounts, social media, or other external communication platforms. Students may not leverage any keystroke recording, screen recording or video recording software. Students may not log into personal accounts while doing research related to the competition.

2.6 Professional Conduct

4.1. All participants, including competitors, coaches, White Team, Red Team, Ops Team, and Gold Team members, are expected to behave professionally at all times during all CCDC events including preparation meetings, receptions, mixers, banquets, competitions and so on.

4.2. In addition to published CCDC rules, Host Site policies and rules apply throughout the competition and must be respected by all CCDC participants.

4.3. All CCDC events are alcohol free events. No drinking is permitted at any time during competition hours.

4.4. Activities such as swearing, consumption of alcohol or illegal drugs, disrespectful or unruly behavior, sexual harassment, improper physical contact, becoming argumentative, willful violence, or willful physical damage have no place at the competition and will not be tolerated.

4.5. Violations of the rules can be deemed unprofessional conduct if determined to be intentional or malicious by competition officials.

4.6. Competitors behaving in an unprofessional manner may receive a warning from the White Team, Gold Team, or Operations Team for their first offense. For egregious actions or for subsequent violations following a warning, competitors may have a penalty assessed against their team, be disqualified, and/or expelled from the competition site. Competitors expelled for unprofessional conduct will be banned from future CCDC competitions for a period of no less than 12 months

from the date of their expulsion.

4.7. Individual(s), other than competitors, behaving in an unprofessional manner may be warned against such behavior by the White Team or asked to leave the competition entirely by the Competition Director, the Operations Team, or Gold Team.

2.7 Judging and Scoring

5.1. Scoring is based on a combination of service uptime, red team penalties, injection task performance, and incident reports as evaluated by the White Team.

5.2. Service uptime will be monitored and scored based on the availability and usability of critical services.

5.3. Injection tasks, provided throughout the competition, must be completed and submitted according to the guidelines and deadlines.

5.4. Incident response reports must be clear, detailed, and submitted on time to receive full credit.

5.5. Teams are required to keep user accounts that are delineated with the prefix 'seccdc' active and unchanged. This includes avoiding rotating credentials or removing admin privileges. These accounts are only to be used by Black Team for monitoring the health of the environment or changing the scenario and will not be used to attack teams.

5.6. Teams may be given a list of processes and IP addresses during competition day to whitelist. Teams are required to ensure that they do not remove those whitelisted binaries or block those whitelisted IP addresses.

Appeals and Disputes

6.1. Any appeals or disputes regarding competition results must be submitted in writing to the Competition Director within one hour of the event conclusion.

6.2. The Competition Director's decision regarding appeals or disputes is final.

2.8 Contact Information

For any questions or clarifications about the rules or the competition, please contact the SECCDC Operations Team via the question-and-answer section on discord.

3 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 service score based on the level and length of access obtained. Red Team periodically proves they access to various student machines. In the time-frame that Red Team has proven system-level access to a machine, a point penalty equal to half of the awarded service points (for that machine) is assessed.

Incident Response Red Team actions result in point deductions from a team's service score. Teams will have the opportunity to do incident response reporting. These reports will be assessed and on a per-host, time period, completeness, and quality basis to calculate how many points will be awarded back. Incident response can account for the return of up to 50% of the red team reductions. Incident Response Reports are only valid for the day they are submitted (example: a compromise found on day two that spanned both the first and second day will only result in points being returned from Day 2) and must be submitted during competition hours.

The following information is required for each report:

- **Affected Hosts**. The report must state the relevant hosts, by host-name. "All of them", "All Linux Machines", the "Mac OS-X machine", or other short-hand can not suffice. The report must include evidence for each listed host.

- **Time Frame**. The report must clearly delineate when the access started and stopped. If the evidence indicates that the access started before the beginning of "hands on keyboard" time (ex: the malware beacon was planted 24 hours before competition go-time) - simply indicate so in the report with evidence. The listed time frame must be explicit and will be the only time frame for which points can be awarded back by the graders.

- **Observed Activity**. The report must state what activity was observed from the malicious actor.

- **Persistence or Access Method**. The report must state what method of persistence/access was the malicious actor using with an explainer of how does it work. For instance, if the Red Team deployed a malware beacon, please denote the type (if known) and the location it was placed. **Please do not upload any malware samples outside of the competition network using tools such as Virus Total.**

- **Technical Analysis**. Include any technical analysis. If, for example, the method was utilizing a stolen credential via SSH - include analysis showing the logins from the malicious IP address(es). Alternatively, if the intrusion leveraged malware, include information about the domain or IP addresses it called back to.

- **Remediation Steps**. Include information about what steps were taken to restore the network to a secure state. If there is any impact to business operations, include that information as well.

- **Evidence Appendix.** Include screenshots substantiating the report.

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. Services which are non-functional (not able to be meaningfully interacted with) will also be scored with no points.

Service Types The following contains a list of service types, example checking criteria, and relevant information. Note the list for checking criteria is non-exhaustive and our checks may test for additional functionality not listed.

- **Domain Name System** DNS lookups will be performed against the DNS server. Each request will require a correct response in order to be scored points.
- **File Transfer Protocol** A user will login to the FTP server (anonymous access or credentialed access being scenario dependent) and attempt to upload a file. The file will then be downloaded and compared via hash. The service is required to allow login, upload, and download of the exact information in order to be scored.
- **Hypertext Transfer Protocol Suite / Secure** A request for a specific web page will be made. Depending on the web page, additional requests may be made submitting additional content such as search queries, comments, or logging in. The results will be stored in a file and compared to the expected result. The returned page must match the expected content and not return any error codes for points to be awarded.
- **Lightweight Directory Access Protocol** An authenticated query to the Active Directory LDAP service will be performed. The query must be successful and will require a response containing the correct information about an object in order to be scored points.
- **Kerberos** A user will need to connect and successfully authenticate using Kerberos authentication without error in order to be scored points.
- **Remote Desktop Protocol** A specified user will attempt to log in via RDP to the service. This will simulate an employee working from home. The login will have to be successful and a desktop fully appear in order to be scored points.
- **Server Message Block** A user will login to the SMB server (anonymous access or credentialed access being scenario dependent). The user may attempt to upload a file or access a file given at the start of the scenario. The file will then be downloaded and compared via hash. The service is required to allow login, upload, and download/retrieval of the exact information in order to be scored.
- **Secure Shell** A connection to the server will be made with a specified user, and commands will be executed as that user. The user may perform tasks such as downloading a file, editing a text document, checking permissions levels, or similar power-user tasks. The output of the commands is then checked against expected results. The login must be successful and the output correct in order to be scored.
- **WinRM** An authenticated WinRM session is connected and a PowerShell command is run. The outcome of this command is recorded and checked against expected values. The login must be successful and the output correct in order to be scored.
- **POP3** The Post Office Protocol is an application-layer Internet standard protocol used by e-mail clients to retrieve e-mail from a mail server. The scoring engine connects to the POP3 server, validates the connection, checks for mail, validates the existence of a specific piece of mail, and reads it. The login must be successful and the output match the expected content in order to be scored.

Authentication Some services require valid credentials for users to interact with them. Blueteamers

are expected to keep username and password information updated in the scoring engine (in the page for the check is an option to rotate credential information). Note that blueteamers may not be allowed to change IP Address information or usernames for some checks. **Please note the passwords are permitted to be Alpha Numeric and only the following special characters: `)('.,@|=:;/-!` All other special characters are forbidden.**

Black Team Agent (BTA) Machines will have a black team information agent to capture telemetry about competitor actions. The black team agent is not malicious. You are not allowed to modify, block, or obstruct the agent in any way.

File Requirements

- On Linux-based machines, the bta binary will be located at **/usr/sbin/bta** and utilizes an encrypted configuration file located at **/etc/bta.enc**. It will periodically update a status file you can view to see if BTA checkins located at **/usr/sbin/bta.status**
- On BSD-based machines, the bta binary will be located at **/usr/sbin/bta** and utilizes an encrypted configuration file located at **/etc/bta.enc**. It will periodically update a status file you can view to see if BTA checkins located at **/usr/sbin/bta.status**
- On Windows-based machines, the bta binary will be located at `C:\Program Files\BTA\bta.exe` and has an encrypted configuration file located in the same directory called **bta.enc**. It will periodically update a status file in that directory as well that you can view to see if BTA checkins called **bta.status**

Service Requirements

- On Linux-based machines, bta will run as a **systemd** service called "bta". It will run and must run with full root privileges.
- On BSD-based machines, bta will and run as a **rc.d** service called "bta". It will run and must run with full root privileges.
- On Windows-based machines, bta will run as a **Windows Service** called "BTA". It will run and must run with full SYSTEM privileges.

Network Requirements

- On all operating systems, BTA will require **outbound** network access so that it can reach **10.250.250.11 on port 443** and **169.254.169.254 on port 80**. BTA will periodically reach out to communicate with these locations. It must be able to reach out to these locations **without** going through a proxy.

Students are required to allowlist the process and IP Addresses listed in the network requirements in all countermeasures they deploy. **Blocking the black team agent will incur a substantial points penalty up to half the possible score allotted during the time period blocked. Again, do not block the black team agent.** Red team will not be using the Black Team agent or the server associated with it to compromise your network.

Reboots and Reversions During the course of the competition, due to competitor or red team action, machines may be unresponsive or completely broken. During the competition, team captains may request a "reboot" of the machine (which entails a hard power off/power on action by a black team member) or a "revert" action (which entails destroying all competitor-made actions to the machine and reverting it to the state it was initially given to them).

Note that both actions can be inherently destructive to competitor work and should only be a last resort. The requests, which shall be located in a "black-team-requests" channel on mattermost.

We may define a specific format at the top of the channel that you will be expected to follow. We may also announce during day 1 the existence of an alternative form or way of submitting this information. The White Team may assess point penalties for excessive reversions. An "excessive" reversion counts as:

- 2 or more reversions of the same machine during the competition, or
- 6 or more reversions across the entirety of all machines by one team during the competition, or
- Any point which the total number of requested reversions accounts for more than 15% of the total number of machines. (Example: Requesting two reversions when you have only eight machines).

Point penalties assessed for reversions vary based on the competition environment. Reversions authorized by White Team in the case of organizer or scoreboard error will not incur any point deductions. Please note that these requests are serviced on a best-effort basis and may be de-prioritized by Black Teams in the cases of major network outages, scenario requirements, or other issues. If you request a reboot or reversion, we will acknowledge and service it if the timing is appropriate. If we do not service a request on Day 1 (of a multi-day competition) that you would still like to be serviced on Day 2, please repeat the request in the channel.

4 Initial Connection Information

This year, blueteam members will be supplied credential information for an Apache Guacamole instance available over the internet without a VPN connection. During the infrastructure test period the organizers will send out an IP Address and Username/Password list to competitors and coaches. Competitors are expected to validate they can log in and interact with their instance. The instances will be shut off after 24 hours until competition day. Any installed software, created documents, or customization to the instances during the infrastructure test will be reset.

In the hours before the start of the competition (hands on keyboard), the organizers will again send IP Addresses and Username/Password information. Note that this instance may not be the same exact server as the one tested - it may have a new IP Address and be refreshed since the test period. Competitors are expected to log in and test functionality as soon as is feasible but may not have full access to the environment until hands on keyboard time.

In the Guacamole, the students will have root level access to 8 "Jump" machines that have access to the environment. These machines will be out of scope to the red team and will not be actively targeted. Students are capable and expected to create text documents, connect to their competition machines, access the scoreboard, and access the internal mattermost from their jump machine. It is expected that only one student accesses one jump machine and team captains coordinate ahead of time which team member will use which jump machine. Students are capable of installing packages on the machine, although, resources will be limited and all jump machines share resources.

5 Competition Network Information

Here are the scored machines on the network. The team is responsible for auditing all hosts on their assigned networks, except where otherwise mentioned. For the purposes of this section, **XX**/**X** is replaced by your team number. For instance, if you're team 7, your octet would be 57. If you're team 22, your octet would be 72. The scoreboard will contain specific information such as the services, service type, and credentials should any be necessary.

IP	Hostname
10.250.5X.10	frontier
10.250.5X.11	drifter
10.250.5X.12	mustang
10.250.5X.13	praire
10.250.5X.14	cactus
10.250.5X.15	governor
10.250.5X.250	sunset
10.250.5X.252	sunrise

Table 2: Scored Machines - Alpha Network

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 10.250.1XX.1
- AWS Artifacts 10.250.1XX.2-3

Supporting Infrastructure Supporting Infrastructure will occupy the 10.250.250.0/24 range. This infrastructure includes items such as scoring agents, internet access, competition DNS, red team jumphosts, traffic generators, and similar infrastructure required for the competition. Blocking this range may adversely impact your ability to connect to the environment, connect out of the environment, get services scored, or generally participate in the competition.

Examples of Specific Supporting Infrastructure

- Internal Mattermost Competition Chat Server: https://10.250.250.5/
- Internal Scoreboard, Service Status, and Inject Portal: https://10.250.250.10/

Scored Users The following user accounts must be maintained. Scored Administrative users are expected to have privileges over the domain and the local machine they log into. All users are expected to have privileges that allow them to remotely interact with and manage systems.

alexisj

Table 3: Scored Administrative Users

	yorktheodore	ashworthconstance
aubryimogene	beckerandrew	berrysophia
bookerrudolph	caldwelllaverne	douglasskaren
ellisonjessie	elmsworthcecil	estevesrudolph
fairchildestella	farnhamsam	foretcharley
guehomaurice	hesslerpat	jansenvirgil
laramiesylvester	nolanfrances	norrissamuel
northropbirdie	nugentnell	osterhausloretta
overtonbonnie	overtonmollie	patoutann
preussgwendolyn	quintalfelix	radcliffealice
reddinggail	reynoldslouise	schroederoliver
sutterglenn	vaughankarl	yardleyherman

Table 4: Scored Normal Users

Credential Information The following credential is used across the environment "Trying-Our-Best1". It should work by default as a login credential on all machines when paired with the username "alexisj". In web applications, databases, or other examples of decentralized authentication you may need to leverage the username "admin", or "root".

From: Rudolph "Rudy" Esteves
To: Wild West Parks Inc. Recruits
Subject: Welcome to the Edge of the Horizon!

Welcome to Wild West Parks Inc. (WWPI), where we don't just reach for the stars, we build entire frontiers among them. As part of our engineering security team, you are responsible for safeguarding the galaxy's most ambitious entertainment empire. Together, we will transform the final frontier into a destination, creating a universe where thrill, innovation, and imagination collide.

At WWPI, your mission is more than protecting data; it is safeguarding the very experiences that define the future of interstellar entertainment. From the neon-lit promenades of Frontier Station Alpha to the zero-gravity dueling arenas of Outlaw Orbit, our attractions are as daring as they are unforgettable. With millions of guests crossing our digital gates each day, the line between adventure and disaster is only as strong as our defenses.

Buckle up for a career at the edge of the frontier, where your expertise keeps the galaxy open for business. At Wild West Parks Inc., we do not just entertain the future; we defend it. Welcome to the adventure of a lifetime, ***where your job is not just to protect the park. . . it is to protect the horizon.***

On behalf of The Frontier,

Rudolph Esteves

Rudolph "Rudy" Esteves
Chairman & Chief Executive Officer
Wild West Parks Inc.