U.S. DEPARTMENT OF ENERGY'S CYBERFORCE COMPETITION®
DEFENDING U.S. ENERGY INFRASTRUCTURE

NORTH CAROLINA A&T STATE UNIVERSITY

AGGIES

November 15, 2025

In-Person

Number of Teams	Max Team Points Received	Min Team Points Received	Mean Team Points Received	Total Points Possible
93	8,783	1,267	6,146.81	10,000

TEAM 5 SCORECARD

This table highlights the *team's* efforts for the 2025 CyberForce Competition®.

Score Category	Team Points	Percent of Points	Team Ranking
Anomalies	129	8.60%	91
Security Documentation	707	56.56%	89
C-Suite Panel	850	68.00%	86
Red Team	125	5.00%	87
Blue Team	1291	64.55%	87
Green Team Surveys	57	3.80%	90
Deductions	0		
Overall	**3159**	**31.59%**	**90**

ANOMALY SCORING

Anomalies simulate the real-world challenges that cybersecurity professionals face daily in the industry. These carefully crafted challenges not only test technical skills but also emphasize daily time management skills that professionals must demonstrate to effectively perform their roles. This year, challenges were longer, and some required more than one person to answer, effectively requiring teams to evaluate risk versus reward.

Anomaly Score	129

Below highlights whether the anomaly was correct or incorrect for your team.

1	No	10.7		17	Yes
2		10.8		18	Yes
3		10.9		19	Yes
4		11.1		20	No
5		11.2		21	
6		11.3		22	
7		11.4		23	
8		11.5		24	
9		11.6		25	
10.1		11.7		26	
10.2		12		27.1	
10.3		13		27.2	
10.4		14		28	No
10.5		15	Yes	29	
10.6		16		30	

ORANGE TEAM

SECURITY DOCUMENTATION

Blue team participants should use the Security Documentation section as an opportunity to highlight unique approaches to securing their infrastructure.

Security Documentation Score	707

Strong Points	*Areas of Improvement*
• Good document for senior leadership except for CVE numbers. Well thought out. • The network diagram and system hardening sections had good detail. Great work! • Very well written system hardening plan • The System Overview and the System Hardening narratives are well written and thorough.	• Router IP is outside of subnet. Use vulnerability names vice CVE numbers. • Areas for improvement include enhancing the detail in the system overview section by providing both definitions and the purpose of the systems. Additionally, the known vulnerabilities section is noticeably incomplete, with only 19 vulnerabilities provided and several CVEs listed without any descriptions. Furthermore, the aesthetic appeal and some formatting aspects need attention and could benefit from adjustments to achieve a more professional

Strong Points	Areas of Improvement
	look, ensuring that either italics are removed or maintained consistently throughout the report. • PLC and HMI are assumed breach VMs that are not supposed to be patched, please clarify which actions were taken vs. which actions were proposed in the Known Vulnerabilities and System Hardening sections • The network diagram contained all the components, logical connections and a legend, and there are no points deducted for it being represented by a whiteboard drawing, but the thing is, the readability. It's very difficult to read the writing with blue ink and the legend, maybe there's a glare on the whiteboard, but this could be improved for a senior leadership presentation. Additionally, while the System Hardening does describe all the mitigations applied, considering that this is a report to senior management, it could be improved by adding sub headers for areas you recommend changes. For example, segmentation was described. Have a header that says "Segmentation" and describe the actions taken, then "Least Privilege" and describe the actions taken, vulnerabilities addressed, etc., you can see the pattern here. By organizing and calling out recommendations with sub headers, you are displaying to senior management the policy changes along with the CVE's addressed or other mitigations taken. Finally, consider recommending a section regarding a plan on Verification, Updates/Patching, or System Auditing so senior management has an idea of the actions that need to be taken in the future to maintain the level of system hardening you have implemented.

C-SUITE PANEL

C-Suite Panel will be a pre-recorded video based on the task outlined in this document. This video should be recorded and placed somewhere accessible to judges.

C-Suite Panel Score	850

Strong Points	*Areas of Improvement*
• Timeline was a nice add and helped connect costs in a different way. • You've done a fantastic job outlining the business summary, with strong details on risks and effective strategies for mitigation. Great work! • The team did a good job identifying risks and directly tying proposed solutions back to these risks. • The presentation started with a good introduction, the Team ID# is listed in the title slide but isn't spoken to during the opening speech. There are two active presenters and the remaining team members are acknowledged. The quality of the visuals is good, they are clean, simple and easy to follow as the speaker presents. However, there is no recorded video of the speakers so judging dress code cannot be completed. • Enthusiastic delivery tone. • This was to the point and professional.	• Audio presentation could have been more professional - especially given the lack of a visual presenter. Strategy is not just a set of actions that will be taken to solve the risk. The actions also did not address the business risks directly or explain how they connected. • Areas for improvement include identifying how the risks have affected the company and suggesting actions to improve overall security, with complete and consistent reasoning. Incorporating the 'why' behind these actions will help demonstrate how they would effectively reduce risks. • The design of the slideshow did not necessarily feel geared towards a C-Suite audience. I'd also recommend having your team on camera. • The team summarized the business risks with minimal emphasis on specific financial impacts to the bottom line and are addressed in isolation. • There is one high priority recommendation (the fail-safe approach) that could be considered high-priority from a cybersecurity perspective. This was a difficult presentation to grade because while the risk reduction steps and the proposed actions are important, they aren't high-priority. There was no mention of air-gapping systems, intrusion detection systems, firewalls, network segmentation, cyber training, etc. In this instance, time stamping data to record incidents of compromise provides no proactive protections, simply a record of an attack after the fact. Encrypting data is very important, yes, but in the aftermath of a cyberattack is not as important. And building an in-house maintenance crew does not necessarily lend to increased cybersecurity awareness; organizational training would be a better recommendation if increased awareness is the goal. • When introducing team members that did not participate in the video presentation ensure to state their role in the project. • Speakers should identify themselves when they are speaking as they are not on camera.

Strong Points	*Areas of Improvement*
	• Risks discussion contains some jargon. Should be written so that non technical C-Suite members can comprehend. • Risk is not quantified. How much will the company potentially lose due to these risks? Loss of income, and reputation, fines? • Recommendations: Other high priority recommendations are missing such as: logging, least privilege, back ups, incident response plan, etc. • Timeline and costs should be explained with more details: are these costs for equipment, software, personnel? How were these estimates calculated? • Final reference slide with references and specific software/hardware recommendations would be beneficial for the c-suite as a list of take aways from the meeting. • Presentation went over the 5 minute time limit. Would recommend running through the presentation a couple of times to tighten the timing and phrasing. • There were also some times in the strategy seemed not the most concise. • The prices seemed to have no much of foundation and the slide was a bit off in values.

RED TEAM SCORING

RED TEAM FLAG INPUTS (ASSUME BREACH & WHACK A MOLE)

This year we will be using ***Assume Breach*** as part of your Red team score. This will be worth *1,750 points*. The purpose of the assume breach model is for your team to investigate and accurately report back incident details after experiencing a successful execution of an attack chain. The **Whack a Mole** portion of the Red team score will be worth *750 points*. This will be done in a traditional method of "hacking" through holes created through known vulnerabilities in the system.

Assume Breach						
AB1	AB2	AB3	AB4	AB5	AB6	AB7
0	0	0	0	0	0	0

Whack a Mole		
WAM1	WAM2	WAM3
0	0	125

BLUE TEAM SCORE

The Blue team scoring (service scans) is completely based on the Blue team's ability to keep services active. In an industry environment, every security professional's primary responsibility is to keep business operational and secure. Service uptime is based on the required services and their respective uptimes. Teams earn points for each availability scan that results in positive service uptime for a total of 2000 points. Throughout the day, services will be validated as operational by the scoreboard polling system. Each service is scored and weighted the same, which means availability is scored purely on the service being operational.

Service Scans	ICS Score
1075	216

Each team was scanned *27 times* throughout the competition. Below identifies your team's number of successful service scans per required service. Each successful scan was awarded 5 points.

SMTP	IMAP	SMB (task)	NFS	SSH	HTTP	WinRM	LDAP	MariaDB	phpmyadmin	SMB (db)
0	0	27	26	27	0	27	27	27	27	27

The ICS Score was determined by the number of barrels you were able to produce during the competition. The max number of barrels a team should be able to produce (+/- slight variance) was 45,000 barrels. There were two periods in which minimal barrels, if any, should have been produced due to significant weather. The total number of points awarded was 515.

No. of Barrels Produced	Percentage of Total Barrels
18926.63	42.06%

GREEN TEAM SCORE

The Green team will review and complete surveys to evaluate each Blue team system's usability and user experience. Points will be awarded based on the user's ability to complete the tasks outlined in the user acceptance testing guide at the end of this document. The Green team will assess their ability to validate these tasks. The guide that will be provided to Green team users is available in the Rubrics section. It is in your best interest to run through this user testing to ensure that you can complete all the steps they are.

Green Team Score
57

Green Team Survey Comments
• Database file at path [/var/www/html/database/database.sqlite] does not exist. Ensure this is an absolute path to the database. (Connection: sqlite, SQL: select * from 'sessions' where 'id' = 0VToUkwxnKkVvGrXAP0NpsnVfdWZWHnqrba9V0c7 limit 1)
• Internal Server Error
• Page not loading
• "Internal Server Error Database file at path [/var/www/html/database/database.sqlite] does not exist. Ensure this is an absolute path to the database. (Connection: sqlite, SQL: select * from 'sessions' where 'id' = 20FYUTdMPPJlPckAvgUFuRMSnwnhKl2scldT0fE8 limit 1)"

Green Team Survey Comments
• Database file at path [/var/www/html/database/database.sqlite] does not exist. Ensure this is an absolute path to the database. (Connection: sqlite, SQL: select * from 'sessions' where 'id' = rSXtMbkcgQyvhIfqzaecr4hCCILF9W9se6LCuXM0 limit 1) • Site completely broken, no access to anything. • no site loads • Site does not load • Site is down • Hello Team 5. I am unable to access your website. I am receiving an Internal Server Error. This is the error code I am getting: Database file at path [/var/www/html/database/database.sqlite] does not exist. Ensure this is an absolute path to the database. (Connection: sqlite, SQL: select * from 'sessions' where 'id' = yBrwUrbDblqmdP3pxYCCzcgrUhFuhiXLto145Ahn limit 1) • Your site is giving a database error! • Internal Server Error • Site is not accessible • Could not connect. • Footer doesn't stay at the bottom of home-screen • Sorry can't get to website. • the site is down • Site does not load • Webpage did not load. Error message: Internal Server Error • the site is down • Could not access website • 'Internal Server Error' • "Internal Server Error • Illuminate\Database\QueryException • Database file at path [/var/www/html/database/database.sqlite] does not exist. Ensure this is an absolute path to the database. (Connection: sqlite, SQL: select * from 'sessions' where 'id' = iuCLbpid2jxQUk6n2JFsBqhC3VfbKRg0qvZ14ZVK limit 1)" • server error • Site is down • web.blue0005.cfc.local refused to connect.