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

THE UNIVERSITY OF TEXAS AT SAN ANTONIO

ROWDYCHEESE

November 9, 2024

In-Person

Number of Teams	Max Team Points Received	Min Team Points Received	Mean Team Points Received	Total Points Possible
94	9153	1350	6115.31	10,000

TEAM 76 SCORECARD

This table highlights the *team's* efforts for the 2024 CyberForce Competition®.

Score Category	Team Points	Percent of Points	Team Ranking
Anomalies	646	32.30%	49
Security Documentation	976	97.60%	5
C-Suite Panel	882	88.20%	29
Red Team	2125	85.00%	2
Blue Team	1965	98.25%	47
Green Team Surveys	1481	98.73%	9
Deductions	0		
Overall	**8075**	**80.75%**	**9**

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. Most anomalies are mapped to the NIST NICE Framework and fall into one of seven work role categories: *Oversight & Governance, Design & Development, Implementation & Operation, Protection & Defense, Investigation, Cyberspace Intelligence, and Cyberspace Effects. Some anomalies may also be categorized as Energy or "Other".* For those mapped to the NIST NICE Framework, their will include the mapping to associated knowledge, skill, ability, and task roles within its respective category, offering students with a comprehensive idea of the wide range of responsibilities cybersecurity professionals face while in the field.

Anomaly Score	646

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

1	yes	27	Not Answered	53	Not Answered
2	no	28	yes	54	Not Answered
3	yes	29	no	55	yes
4	yes	30	no	56	no
5	yes	31	Not Answered	57	yes
6	yes	32	Not Answered	58	yes
7	yes	33	Not Answered	59	yes
8	yes	34	Not Answered	60	no
9	yes	35	Not Answered	61	yes
10	yes	36	Not Answered	62	yes
11	no	37	no	63	yes
12	Not Answered	38	Not Answered	64	no
13	yes	39	Not Answered	65	yes
14	yes	40	no	66	Not Answered
15	yes	41	Not Answered	67	Not Answered
16	yes	42	Not Answered	68	Not Answered
17	yes	43	Not Answered	69	Not Answered
18	yes	44	Not Answered	70	yes
19	yes	45	Not Answered	71	no
20	yes	46	yes	72	yes
21	yes	47	no	73	Not Answered
22	yes	48	yes	74	Not Answered
23	yes	49	yes	75	Not Answered
24	no	50	yes	76	yes
25	Not Answered	51	yes	77	yes
26	Not Answered	52	yes		

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	976

Strong Points	*Areas of Improvement*
• Content across the board was very high level, fantastic work. • Great job. Almost perfect score. • Overall, you did an excellent job! The vulnerability report section submitted was outstanding. • Technically sound and concise.	• The document format had a few inconsistencies. • Network diagram needed a little more detail as did the system hardening. • The System Overview section has room for improvement to clearly define its purpose and better engage senior leadership. • Nothing as such.

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	882

Strong Points	*Areas of Improvement*
• Amazing work! The presentation was clear, detailed, and effectively delivered within the allotted time. • Very professional and well designed presentation. Good use of head shots on the team slide. Good use of embedded videos of the speakers. • The business concerns/risks were directly tied to business finances. The recommended priorities were well explained, and the costs and return on investment were clearly stated. • This was a very strong presentation. The information was presented to the C-Suite in a way they would appreciate and be able to digest easily. • Using an information security label for the information that was presented relates your understand of who is allowed access to this information and communicates that understanding to the C-Suite. • Good understanding and communication of the scenario.	• Great work on the high-priority actions and long-term business strategy! These could be even more impactful by incorporating additional strategic approaches • Monthly full backups recommended. Is there a recommendation for differential or incremental back ups? Consider, can the company lose 1 month worth of data without repercussions? Items to consider: Are new hires conducting this work or the current IT staff? Will this pull them away from their current duties and lead to risks? Half the presentation time was regarding the risks. Recommendation is to provide more details on the strategy and recommendations by shortening the time spent on risks. • The timeline and costs of the strategy were mentioned, but the strategy was not directly tied to the business risks. • I have a few comments for things you may want to consider for future presentations. • Some of the the presenters sounded rushed. Consider practicing the presentation until the presentation can be

• The presentation had a strong introduction that contributed to the continuity of the presentation • Fantastic job of delivering the information to the C-Suite in an easily digestible way and communication on a level that allows them to immediately understand the issue and it's solutions •	made without needing to read it as it provides a good connection to the C-Suite. • For future, using the phrase "man-hours" isn't acceptable by most organizations. Another way to say that is just to say hours •

RED TEAM SCORING

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

This year we will be using ***Assume Breach*** for part of your Red team score. This will be worth *1000 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 point*s. 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	AB8	AB9	AB10
100	100	100	100	75	100	75	100	75	100

Whack a Mole	
WAM1	WAM2
375	375

AUTOMATED SCRIPT CHECK – VULNERABILITY

This portion of the Red team score will be worth *750 points*. This will be done via an automated scripted check.

Automated Script Score	450

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	AI Algorithm Score
1565	400

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
1481