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

THE UNIVERSITY OF TEXAS AT SAN ANTONIO

UNIVERSITY OF TEXAS SAN ANTONIO

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 88 SCORECARD

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

Score Category	Team Points	Percent of Points	Team Ranking
Anomalies	1349	67.45%	5
Security Documentation	997	99.70%	1
C-Suite Panel	937	93.70%	8
Red Team	1888	75.52%	13
Blue Team	2000	100.00%	1
Green Team Surveys	1477	98.47%	3
Deductions	0		
Overall	**8648**	**86.48%**	**3**

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	1349

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

1	yes	27	no	53	yes
2	yes	28	yes	54	yes
3	yes	29	no	55	no
4	yes	30	yes	56	yes
5	yes	31	no	57	yes
6	yes	32	Not Answered	58	yes
7	yes	33	Not Answered	59	yes
8	yes	34	yes	60	yes
9	yes	35	yes	61	yes
10	yes	36	Not Answered	62	yes
11	no	37	no	63	yes
12	yes	38	yes	64	yes
13	yes	39	yes	65	yes
14	yes	40	yes	66	yes
15	yes	41	Not Answered	67	yes
16	yes	42	yes	68	Not Answered
17	yes	43	yes	69	Not Answered
18	yes	44	yes	70	yes
19	yes	45	yes	71	yes
20	yes	46	yes	72	yes
21	no	47	yes	73	yes
22	yes	48	yes	74	yes
23	Not Answered	49	Not Answered	75	yes
24	no	50	yes	76	yes
25	Not Answered	51	yes	77	yes
26	no	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	997

Strong Points	*Areas of Improvement*
• Showed that you know the environment you are working in really well and could name everything happening. • good detail of the system and the parts they serve - CnC is Command and Control Computer Numerical Control is for milling • I like that you listed essential services and gave kernel level information • Everything thing about this report was very professional, well laid out, clear to read, and above and beyond. Excellent job. • Great overview, and well formatted asset list. • Outstanding job identifying vulnerabilities. The hardening steps were thoroughly explained and detailed, with solid justifications.	• Remember your target audience for each section. Sometimes simpler is better. • Throughout the documentation remember you are addressing senior leadership, and it is hard to not talk jargon. • There are two tiny things you could have added coding for compromised machines in your system map and you were over the word count for system hardening by 68 words. • Nothing of note.

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	937

Strong Points	*Areas of Improvement*
• Strongest point was your strategy to reduce risks - this was the first team I heard so far that mentioned conducting tabletop exercises, I think you fleshed out all the strategies really well. I also thought that your slide deck was well thought out and the speakers very prepared to talk about their sections. • Slides looked professional and thought that the resources at the end was a good touch. • Clear and concise points that were easy to follow, milestone roadmap was nice. • I love how the visuals were very engaging to follow along with your presentation	• I think the risks related to the business could have been expanded upon a little bit more. Also while I thought the slides for the high priority recommendations were beautiful I don't think a quick presentation to the C-Suite was an appropriate platform to show them - there was a ton of information that was simply impossible to take in or even read because this was just a quick brief, now if this was being presented to the employees of the company I think you would have had additional time to go thru those detailed slides and really talk about that information but the C-Suite just wants the quick and hard facts.

	• Expand better on the reasoning behind your strategies to reduce risk. • N/A • At some points it felt like you were too jargon heavy in you presentation

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 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	AB8	AB9	AB10
100	75	75	100	100	75	75	100	75	100

Whack a Mole	
WAM1	WAM2
187	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
1600	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
1477