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

UNIVERSITY OF FLORIDA

DARTH GATOR

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 32 SCORECARD

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

Score Category	Team Points	Percent of Points	Team Ranking
Anomalies	1166	58.30%	9
Security Documentation	916	91.60%	22
C-Suite Panel	923	92.30%	13
Red Team	1981	79.24%	7
Blue Team	2000	100.00%	1
Green Team Surveys	1459	97.27%	7
Deductions	0		
Overall	**8445**	**84.45%**	**7**

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	1166

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

1	yes	27	yes	53	yes
2	yes	28	yes	54	yes
3	yes	29	no	55	yes
4	yes	30	yes	56	yes
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	yes
9	yes	35	Not Answered	61	no
10	yes	36	Not Answered	62	yes
11	yes	37	yes	63	no
12	no	38	yes	64	no
13	yes	39	yes	65	yes
14	yes	40	yes	66	yes
15	yes	41	Not Answered	67	Not Answered
16	yes	42	Not Answered	68	yes
17	yes	43	Not Answered	69	Not Answered
18	yes	44	yes	70	yes
19	yes	45	yes	71	yes
20	Not Answered	46	yes	72	yes
21	yes	47	no	73	yes
22	yes	48	yes	74	yes
23	yes	49	yes	75	yes
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	916

Strong Points	*Areas of Improvement*
• Extremely comprehensive known vulnerabilities section and clear explanations in system hardening section. • Overall great job! Asset inventory and known vulnerabilities sections were well done. • You identified a large set of vulnerabilities with appropriate mitigation, meeting the requirements for a detailed and comprehensive listing. Your hardening strategy is well-thought-out and layered, addressing system and network hardening effectively. • A strong point for this entry is its comprehensive approach to network security, covering multiple layers of defense-in-depth strategies. It details the use of a variety of tools for monitoring, auditing, and hardening each system component, demonstrating a well-thought-out, multifaceted approach to cybersecurity. Additionally, it highlights specific techniques such as least privilege enforcement, port auditing, and endpoint logging, which effectively minimize the network's attack surface and enhance its overall security posture.	• More comprehensive network diagram. • There is room for improvement regarding the system overview purpose and justifications for the system hardening section. • The network diagram lacks clarity in logical interconnections and flow • The entry could be improved by providing a more organized and concise structure, potentially breaking down the explanation into clearer sections with headings for each security measure, such as "Account Security," "Host-Based Hardening," "Network Monitoring," and "Centralized Logging."

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	923

Strong Points	*Areas of Improvement*
• I appreciate the agenda at the beginning. This presentation had an extremely clear flow with very strong, specific examples. Presenters got to the point about the risks, and emphasized the importance of protecting their infrastructure, especially	• Mapping of risk reduction strategies back to the specific business risks (i.e. operational, legal/regulatory, etc.) will make your argument more clear. Additionally, the slide on risks of not implementing recommendations needed

with the stats at the end. Quote was a good and unique touch. • Nice usage of additional statistics on e.g. the increase of attacks to help bolster the importance of the high priority recommendations. • Excellent overview of the risks to the system. In general, excellent presentation. • The financial risks were very detailed and informative, as were the risk reduction strategies and the potential consequences of not implementing them.	additional clarification of each category; presenter simply read each one off the slide. • The strategy needed more discussion/connection with the business risks. • Your recommendations are mostly short-term - should have also included some longer-term plans. • The video did exceed the 5 minute mark but overall the content was solid and the quality of the presentation was great.

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
75	100	100	100	100	100	75	75	75	75

Whack a Mole	
WAM1	WAM2
375	281

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
1459