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

UNIVERSITY OF CENTRAL FLORIDA

A TEAM WITH A DREAM

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 4 SCORECARD

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

Score Category	Team Points	Percent of Points	Team Ranking
Anomalies	1722	86.10%	1
Security Documentation	973	97.30%	7
C-Suite Panel	906	90.60%	17
Red Team	2075	83.00%	3
Blue Team	2000	100.00%	1
Green Team Surveys	1477	98.47%	1
Deductions	0		
Overall	**9153**	**91.53%**	**1**

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	1722

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

1	yes
2	yes
3	yes
4	yes
5	yes
6	yes
7	yes
8	yes
9	yes
10	yes
11	yes
12	Not Answered
13	yes
14	yes
15	yes
16	yes
17	yes
18	yes
19	yes
20	Not Answered
21	yes
22	yes
23	yes
24	no
25	yes
26	Not Answered
27	no
28	yes
29	yes
30	yes
31	yes
32	yes
33	yes
34	yes
35	yes
36	yes
37	yes
38	Not Answered
39	yes
40	yes
41	yes
42	yes
43	yes
44	yes
45	yes
46	yes
47	yes
48	yes
49	yes
50	yes
51	yes
52	yes
53	yes
54	yes
55	yes
56	yes
57	yes
58	yes
59	yes
60	no
61	yes
62	yes
63	yes
64	yes
65	yes
66	yes
67	yes
68	yes
69	yes
70	yes
71	no
72	yes
73	yes
74	yes
75	yes
76	yes
77	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	973

Strong Points	*Areas of Improvement*
- Very detailed in every section, great job - The documentation was very thorough and well written for the intended audience. - did well on finding so many vulnerabilites - Known vulnerabilities and hardening steps were extremely thorough and detailed. It was apparent that you spent a good amount of time securing systems.	- Overall hard to find anything to criticize - Nothing, this is an exemplary example of a security report. - missing few ports have less then 90% of assets, some portions needed stronger justification in Harding section - System overview went a bit too technical for your average C-Suite audience.

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	906

Strong Points	*Areas of Improvement*
- There were nice visuals throughout the presentation, and it looked very professional - You went beyond "reputation" and actually spelled out how and why reputation will be hurt. Very impressive. - Professional presentation with appropriate pacing and natural transition - Great presentation and good points that you addressed	- N/A - C-suite does not differentiate between external and internal costs. Training is expensive. How many hours per person per year of training? That is something they can quantify. - Some audio was a little low, some sections felt a bit scripted, some recommended strategies (high-level, long-term) felt more tactical (specific, short-term) - Connect your Strategy to Reduce Business Risks to your Risks Related to Business

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	50	100	100	50	75	100	100	100	100

Whack a Mole	
WAM1	WAM2
375	375

Automated Script Check – Vulnerability

This portion of the Red team score will be worth *750 point*s. 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