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

EMBRY-RIDDLE AERONAUTICAL UNIVERSITY-PRESCOTT

BYTEWING

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 12 SCORECARD

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

Score Category	Team Points	Percent of Points	Team Ranking
Anomalies	572	28.60%	62
Security Documentation	893	89.30%	28
C-Suite Panel	828	82.80%	52
Red Team	1300	52.00%	43
Blue Team	2000	100.00%	1
Green Team Surveys	1461	97.40%	30
Deductions	0		
Overall	**7054**	**70.54%**	**30**

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	572

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	no
12	no
13	yes
14	no
15	no
16	yes
17	Not Answered
18	yes
19	no
20	Not Answered
21	no
22	Not Answered
23	Not Answered
24	no
25	Not Answered
26	Not Answered
27	Not Answered
28	yes
29	no
30	yes
31	no
32	Not Answered
33	Not Answered
34	yes
35	no
36	Not Answered
37	yes
38	no
39	no
40	yes
41	Not Answered
42	Not Answered
43	Not Answered
44	yes
45	no
46	yes
47	no
48	no
49	Not Answered
50	yes
51	yes
52	yes
53	no
54	Not Answered
55	yes
56	no
57	yes
58	yes
59	yes
60	yes
61	no
62	yes
63	yes
64	yes
65	no
66	yes
67	no
68	Not Answered
69	Not Answered
70	yes
71	no
72	yes
73	Not Answered
74	yes
75	Not Answered
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	893

Strong Points	*Areas of Improvement*
• Nicely done on the asset identification section. • I loved the network diagram. It was detailed and easy to read. List vulnerabilities for the given hosts. The system hardening procedures are comprehensive, technically sound, and well-justified. • Good list of vulnerabilities and mitigations • The network diagram and legend were excellent. Outstanding job on identifying the vulnerabilities.	• Some of the text was not readable on the pdf (seemed to go off the page) - a little more attention to detail would help. • The Asset Inventory could have been organized better for easier reading, and the system overview could have discussed the project in more depth. • First page is cut off, always open a PDF to preview it after converting. Looks like the system overview was rushed. Misspelled tool names. • Expand on the justification for the steps taken during hardening. The text was cutoff for the system overview, and the full page was unable to be seen.

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	828

Strong Points	*Areas of Improvement*
• Overall this was a rock-solid video. The "you can't defend what you don't know you have" comment on inventory management is one of my favorite phrases too. • Great job on compiling the potential impacts! and having all the team present. • Good that everyone dressed professionally and spoke clearly. • Team members professionally dressed and introduced. • Clear focus on free recommendations clearly designed to improve security posture.	• Use caution when recommending using the word "free" regarding costs. Sure, open source software and training material might not cost a dime to acquire, but actually implementing will take a large amount of technical resources. • Your risk management strategy is great, and with a few adjustments, it could more effectively address the potential impacts you've identified. Building on those insights will help strengthen the approach even further. Great start! • Other than being dressed professionally, it was not a very professional video. Sometimes simpler is better. • Felt like more of a YouTube video rather than professional C-Suite presentation (Less music).

	•

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
50	50	50	50	50	25	50	50	50	50

Whack a Mole	
WAM1	WAM2
375	0

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
1461