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

DEFENDING U.S. ENERGY INFRASTRUCTURE

UNIVERSITY OF DENVER

DUEVENHACK?

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 91 SCORECARD

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

Score Category	Team Points	Percent of Points	Team Ranking
Anomalies	935	46.75%	16
Security Documentation	956	95.60%	10
C-Suite Panel	906	90.60%	17
Red Team	1469	58.76%	36
Blue Team	1575	78.75%	74
Green Team Surveys	744	49.60%	44
Deductions	0		
Overall	**6585**	**65.85%**	**44**

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	935

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	yes
4	yes	30	no	56	yes
5	yes	31	yes	57	yes
6	yes	32	yes	58	yes
7	yes	33	yes	59	yes
8	yes	34	yes	60	no
9	yes	35	no	61	yes
10	yes	36	no	62	yes
11	no	37	yes	63	yes
12	no	38	yes	64	no
13	yes	39	no	65	Not Answered
14	yes	40	no	66	no
15	yes	41	Not Answered	67	Not Answered
16	yes	42	Not Answered	68	Not Answered
17	yes	43	no	69	Not Answered
18	yes	44	Not Answered	70	yes
19	yes	45	yes	71	yes
20	Not Answered	46	yes	72	no
21	no	47	no	73	Not Answered
22	yes	48	yes	74	Not Answered
23	yes	49	Not Answered	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	956

Strong Points	*Areas of Improvement*
• A strength of this entry was the network diagram. It contained a strong foundation of knowledge and presented the architecture in a professional, descriptive manner. Well done. • Overall it was all really well put together and did a fantastic job. • Strong network diagram and legend, useful notations. vulnerabilities listing, ~50 identified and with mitigations noted. • overall you're your write up was well done • over all good job	• This entry could have been approved by pulling in a standardized structure to the system hardening efforts. This might include a structure such as the categories prescribed in NIST CSF 2.0 - e.g., govern, detect, protect, identify, response, recover. Doing so adds professionalism, but also better enables senior management to apply the mitigations to specific cybersecurity elements of the organization. • Instead of more hardening topics, it would have been nice to see more depth of the hardening steps discussed. • would have been nice to see template prompts removed. • missing few ports have less than 90%. Did well on system Harding just lacking comprehensive justification for many steps towards the end your formatting changed in the Harding section • Missing few ports have less then 90% of assets, some portions needed stronger justification in Harding section; towards the end your formatting changed in the Harding section

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*
• Going beyond just what the rubric is asking for to emphasize points. • Nice discussion of the business risks and connection with the high prio recommendations. • Professional slides and clear concise points that tied together well.	• Focus more on the cyber effect of the risks. • More clear focus on the strategy and its connection to the business risks. • N/A • Tie in your strategy to reduce business more closely to the risks

• Great presentation and good points that you addressed	

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
0	75	100	50	75	50	75	100	75	100

Whack a Mole	
WAM1	WAM2
281	187

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	300

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
1555	20

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

744