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

UNIVERSITY OF DENVER

DUCRYPTICS

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 37 SCORECARD

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

Score Category	Team Points	Percent of Points	Team Ranking
Anomalies	380	19.00%	82
Security Documentation	693	69.30%	72
C-Suite Panel	811	81.10%	57
Red Team	694	27.76%	83
Blue Team	1860	93.00%	53
Green Team Surveys	19	1.27%	82
Deductions	0		
Overall	**4457**	**44.57%**	**82**

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	380

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

1	yes	27	Not Answered	53	no
2	no	28	no	54	no
3	yes	29	no	55	yes
4	yes	30	Not Answered	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	yes
10	yes	36	Not Answered	62	yes
11	no	37	Not Answered	63	yes
12	no	38	Not Answered	64	yes
13	yes	39	Not Answered	65	no
14	yes	40	Not Answered	66	Not Answered
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	no
19	no	45	no	71	no
20	no	46	Not Answered	72	Not Answered
21	yes	47	Not Answered	73	Not Answered
22	Not Answered	48	Not Answered	74	Not Answered
23	Not Answered	49	Not Answered	75	Not Answered
24	no	50	Not Answered	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	693

Strong Points	*Areas of Improvement*
• Attention to portrait/landscape page formatting is appreciated. • Strong examples in system overview, always great to see disabling older TLS versions get mentioned • Vulnerability overview list was great, complete as well as well structured. • The formatting of the document is commendable. I would like to acknowledge the effective organization of the content and the clarity of the column headers in the tables. The structure of the vulnerability section stands out for its exceptional level of detail and organization compared to the other documents.	• Keep senior leadership (non-technical businesspeople) in mind when describing the system and making recommendations. Be sure to include all hosts in the asset inventory. Maintain consistent and concise formatting throughout the document. • System Hardening write-up was quite short, would have loved to see more detail • System overview was too technical, and missing the MapBox in your network diagram. • I recommend enhancing the network diagram by including additional content, as it currently lacks certain key elements, such as MapBox. Furthermore, please remove any instructions that were present in the original document.

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	811

Strong Points	*Areas of Improvement*
• The video appears professional and well made • Very well thought out list of strategies to reduce risks - both for short-term and long-term risks. I think a C-Suite would really appreciate your last slide that includes everyone's contact information. Also appreciated that throughout the presentation the other team members that weren't able to be there were given credit for the work they had done. • Presentation was great. It was easy for me to follow along and the slides had just the right amount of information. Clear and to the point.	• Immediate recommendations require additional funding • I think you can remove the slide about the company, you are presenting to the C-Suite so I would assume they know what the company does. I also noticed the presentation was pretty short (and it included a few second delay in starting and the slide about the company) - I think time could have been used more wisely to flesh out some of the risks and recommendations. • Need to sell those recommendations and why they are high priority. Bring up the future risks if they dont implement and how you can mitigate those risks for little

• The presentation and deck were great and prepared nicely.	to no cost. You had about 45 seconds to spare and would have been perfect to sell your recommendations. • I could not see any faces in the 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
50	50	25	75	25	0	0	25	0	50

Whack a Mole	
WAM1	WAM2
93	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	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
1500	360

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
19