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

LEWIS UNIVERSITY

CYBER FLYERS

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 20 SCORECARD

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

Score Category	Team Points	Percent of Points	Team Ranking
Anomalies	376	18.80%	83
Security Documentation	967	96.70%	8
C-Suite Panel	877	87.70%	35
Red Team	931	37.24%	68
Blue Team	1790	89.50%	62
Green Team Surveys	38	2.53%	75
Deductions	0		
Overall	**4979**	**49.79%**	**75**

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	376

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

1	yes	27	Not Answered	53	Not Answered
2	yes	28	Not Answered	54	Not Answered
3	yes	29	Not Answered	55	yes
4	yes	30	Not Answered	56	no
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	no
9	yes	35	Not Answered	61	yes
10	yes	36	Not Answered	62	yes
11	no	37	yes	63	yes
12	yes	38	Not Answered	64	yes
13	yes	39	Not Answered	65	Not Answered
14	no	40	no	66	no
15	no	41	Not Answered	67	Not Answered
16	yes	42	Not Answered	68	Not Answered
17	no	43	Not Answered	69	Not Answered
18	yes	44	Not Answered	70	yes
19	Not Answered	45	Not Answered	71	Not Answered
20	yes	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	Not Answered	50	Not Answered	76	yes
25	Not Answered	51	Not Answered	77	yes
26	Not Answered	52	Not Answered		

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	967

Strong Points	*Areas of Improvement*
• Most complete vulnerability list I have seen! • Genuinely outstanding job, no obvious mistakes that I could find. The System Overview in particular was very well written. • Very comprehensive answers in each section. The system overview was also perfectly tailored to the audience. • You did a great job demonstrating a all-encompassing approach to identifying vulnerabilities and systems hardening! Great job giving a highly detailed and well-justified remediation suggestion.	• System overview needed more content giving the link between the system and its purpose. Is this IT? OT? a mix? • Nothing jumped out at me, great work! • Closer attention to detail in formatting. • The network diagram could be improved with clearer logical and technical connections, better labeling, and a legend for symbols to enhance readability and coherence.

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	877

Strong Points	*Areas of Improvement*
• Discussion of current risks and what they mean to the company. • Very good visuals • This team covered all areas; listed clear summary of business and financial risks, provided strategy to reduce risks, recommended up to 3-4 high priority actions to improve overall security, appropriately dressed and video length approximately 5 minutes. • I loved the usage of flow charts on your slides! It is a great way to easily communicate with executives.	• Tying either policy and programmatic actions and risk reduction technical actions to the identified risks. • No mention of system hardening • For the future, my recommendation would be to list the high priority tasks with that heading as you did with strategy to reduce risk. This way your audience are not confused as to what the high priority recommendations were. Overall, excellent work. Keep up the good work. • I would've liked to see more overall polish of the slide deck and the flow charts contained within.

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	50	0	25	25	0	0	25	0	0

Whack a Mole	
WAM1	WAM2
93	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	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
1390	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
38