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

LEWIS UNIVERSITY

ORDER OF THE PURPLE FLAMINGO

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 62 SCORECARD

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

Score Category	Team Points	Percent of Points	Team Ranking
Anomalies	995	49.75%	14
Security Documentation	981	98.10%	2
C-Suite Panel	971	97.10%	2
Red Team	1313	52.52%	42
Blue Team	1980	99.00%	38
Green Team Surveys	1452	96.80%	13
Deductions	0		
Overall	**7692**	**76.92%**	**13**

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	995

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

1	yes	27	no	53	no
2	yes	28	no	54	Not Answered
3	yes	29	Not Answered	55	yes
4	yes	30	Not Answered	56	yes
5	yes	31	yes	57	yes
6	yes	32	yes	58	yes
7	yes	33	Not Answered	59	yes
8	yes	34	yes	60	no
9	yes	35	Not Answered	61	yes
10	yes	36	yes	62	yes
11	no	37	yes	63	yes
12	yes	38	Not Answered	64	no
13	yes	39	Not Answered	65	no
14	yes	40	yes	66	yes
15	yes	41	no	67	Not Answered
16	yes	42	yes	68	Not Answered
17	yes	43	no	69	Not Answered
18	yes	44	yes	70	yes
19	yes	45	no	71	Not Answered
20	yes	46	yes	72	yes
21	yes	47	yes	73	Not Answered
22	Not Answered	48	yes	74	yes
23	Not Answered	49	yes	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	981

Strong Points	*Areas of Improvement*
• Used concise and simplified language to address a non-technical senior leadership audience. • A strength of this entry was the thorough list of vulnerabilities discovered in the subject architecture. The team displayed their expertise by appropriately discovering and characterizing the associated risks, as well as identifying strategic mitigations. Well done. • A strong point of this entry is its thorough and well-organized approach to documenting vulnerabilities across multiple systems. The report clearly identifies specific vulnerabilities, provides explanations, and suggests targeted mitigations for each identified threat. This comprehensive and structured format allows readers to understand the security posture of each system, and the "Purpose" and "Scope" sections are effective in setting up the context and objectives of the investigation. • The information in each section was thorough and concepts well defined	• The system overview could have been tied more strongly to the business. The business and devices were described, but the two concepts were perhaps a little disjointed. • 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. • The entry could be improved by addressing clarity and readability. For instance, the document's structure could benefit from more consistent formatting, such as using bullet points or tables to break down information about each system's vulnerabilities and mitigations. Additionally, some explanations and mitigations are brief or vague, which could be enhanced by adding more detail. This could include specifying potential impacts of each vulnerability or mitigation and organizing the report with a summary of critical vulnerabilities to prioritize the most pressing issues. Also, refining some language and fixing typographical errors, like "oranage" for "orange" and "infrastructre" for "infrastructure," would improve professionalism. • Consider the audience that will read this report - it may be hard for a non-technical person to make it through this report easily

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	971

Strong Points	*Areas of Improvement*
• I like that you have a plan to maintain the supply in the event of an outage. In the industry we do the same thing. We lease power from other companies in our region and out of state for if we have a reduction for whatever reason. • Thorough overview of the current situation • Business risks, strategy and high priority recommendations were all tied together well. • The team demonstrated a comprehensive approach to risk assessment and provided a clear risk reduction strategy. They effectively identified immediate and potential long-term risks related to the cyber breach, including operational disruptions, government contract concerns, and financial repercussions. The step-by-step mitigation and contingency measures, including specific recommendations like regular audits, contingency planning, and cybersecurity training, show a structured approach to both immediate recovery and future prevention.	• The team went over time but was still missing details. • You need more reasoning for the high-priority actions. • Overall, I feel like you are still organizing a plan. You should go to the C-Suite with a well-thought-out plan and be able to move on that plan immediately. • Added a section on further risks was not needed, causing to go over on time • Contributions of some members were not explained/highlighted. • To strengthen the entry, the team could enhance clarity and focus by using more concise language and a streamlined presentation style. Some areas contained repetitive language, which made the overall flow less efficient. Additionally, more specific details on cost estimates or examples of the recommended tools for monitoring and penetration testing would give stakeholders clearer insights into feasibility and implementation.

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	50	50	75	50	75	25	100

Whack a Mole	
WAM1	WAM2
187	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
1580	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
1452