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

UNIVERSITY OF NEVADA-LAS VEGAS

LAYERZERO

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 53 SCORECARD

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

Score Category	Team Points	Percent of Points	Team Ranking
Anomalies	556	27.80%	66
Security Documentation	826	82.60%	51
C-Suite Panel	943	94.30%	6
Red Team	775	31.00%	75
Blue Team	1700	85.00%	69
Green Team Surveys	435	29.00%	69
Deductions	0		
Overall	**5235**	**52.35%**	**69**

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	556

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	yes
13	yes
14	no
15	no
16	Not Answered
17	Not Answered
18	Not Answered
19	Not Answered
20	yes
21	yes
22	yes
23	yes
24	no
25	Not Answered
26	Not Answered
27	Not Answered
28	yes
29	Not Answered
30	Not Answered
31	Not Answered
32	Not Answered
33	Not Answered
34	Not Answered
35	Not Answered
36	yes
37	yes
38	no
39	Not Answered
40	yes
41	Not Answered
42	Not Answered
43	no
44	no
45	no
46	yes
47	no
48	no
49	yes
50	yes
51	yes
52	yes
53	no
54	Not Answered
55	yes
56	no
57	yes
58	yes
59	yes
60	no
61	yes
62	yes
63	yes
64	yes
65	no
66	Not Answered
67	Not Answered
68	Not Answered
69	Not Answered
70	yes
71	yes
72	yes
73	Not Answered
74	no
75	no
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	826

Strong Points	*Areas of Improvement*
• Nicely done on the identified and documented vulnerabilities. • I like that you aligned your hardening strategy with an incident response lifecycle. • Strong overall. • Overall, this presentation was clear and easy to read. I have comments that may help with future security documents to be submitted to upper level management. • The Network Diagram had excellent information; however, the black background made it difficult to read. It’s also important to think of how a person with color blindness may not be able to read the diagram at all. •	• The overview focused on the individual components of the system as opposed to what the system provides as a whole. • Your vulnerabilities table didn't list anything for the web server. • Network diagram with the black background was hard to read. I recommend changing the colors to make it easier to read. • In the System overview, it may be helpful to the audience to give a “big picture” of the System being reported on. Some of the information , while technically correct, may not have an accurate picture of the system. • The Mitigations column in the Vulnerability Table doesn’t mention of the mitigation (stop-gap temporary actions had been done, or were waiting to be done or if the vulnerabilities have been remediated (Permanent actions) •

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	943

Strong Points	*Areas of Improvement*
• All aspects of the presentation were strong. Good job. • Very easy to follow, great summary of risks and mitigation strategies • Great addition adding the case study to further prove your teams' points of recommendations. • Thorough explanations, professional, and well structured.	• The solution to your problem 3 of "insufficient incident response capabilities" misses the mark in my opinion. Other actions such as training cybersecurity staff in incident response and or emergency management, or keeping a cybersecurity firm on retainer for 3rd party incident response team is closer to solving the problem. • Describe potential cost of breach up front; identify high priority actions clearer

	- Estimated costs to go along with estimated times would be helpful for decision making of accepting and prioritizing recommendations. - Properly address immediate strategy as high-priority recommendations. Make sure they are unique solutions which address the business risks.

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	50	25	25	25	75	0	75	0	50

Whack a Mole	
WAM1	WAM2
0	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
1300	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
435