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

DAKOTA STATE UNIVERSITY

DAKOTA STATE UNIVERSITY

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 31 SCORECARD

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

Score Category	Team Points	Percent of Points	Team Ranking
Anomalies	647	32.35%	48
Security Documentation	703	70.30%	70
C-Suite Panel	733	73.30%	73
Red Team	1488	59.52%	34
Blue Team	2000	100.00%	1
Green Team Surveys	1251	83.40%	35
Deductions	0		
Overall	**6822**	**68.22%**	**35**

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	647

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

1	yes	27	Not Answered	53	no
2	yes	28	yes	54	Not Answered
3	yes	29	no	55	yes
4	yes	30	no	56	no
5	yes	31	no	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	no	62	yes
11	no	37	no	63	no
12	no	38	no	64	no
13	yes	39	yes	65	no
14	yes	40	yes	66	Not Answered
15	yes	41	Not Answered	67	Not Answered
16	yes	42	no	68	Not Answered
17	yes	43	Not Answered	69	Not Answered
18	yes	44	yes	70	yes
19	yes	45	no	71	Not Answered
20	Not Answered	46	yes	72	no
21	yes	47	no	73	Not Answered
22	Not Answered	48	yes	74	no
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	703

Strong Points	*Areas of Improvement*
• Comprehensive system hardening section. • Good job on the system overview and network diagram. • The hardening procedures are thorough, with multiple tools and proactive configurations! • The entry's strong point lies in its comprehensive and structured approach to describing the network infrastructure and the detailed security measures implemented. The use of specific tools (e.g., Nessus, WinPEAS, Malwarebytes, LinPEAS) and practices (e.g., snapshots, attack surface reduction, user access control) demonstrates a thorough understanding of cybersecurity protocols. This adds credibility to the entry, as the reader can clearly see how various elements contribute to a robust security posture. Additionally, the mention of multiple CVEs adds relevance by addressing known security risks, which strengthens the entry's technical accuracy and attention to detail.	• Formatting-- the network diagram was very pixelated and lacked a symbol key. The colors in the asset inventory did not seem to serve a clear purpose. • There is room for improvement regarding the known vulnerabilities and system hardening sections. For known vulnerabilities section, additional vulnerabilities could potentially be identified, and it would be beneficial to include detail description and suggest mitigations. Regarding system hardening, providing a clear justification and outlining the specific septs taken would greatly strength this section. • The network diagram includes core elements but misses logical connections and minor components that would improve clarity. • The entry could be improved by enhancing readability and conciseness. The lengthy description could benefit from clearer organization with subheadings or bullet points to break down the content into more digestible sections, particularly under “System Hardening and Procedures Summary.” Additionally, some phrases are repeated or redundant (e.g., re-explaining the significance of snapshots), which could be streamlined. Finally, providing more context about the infrastructure’s specific security needs or challenges could make the entry even more compelling, helping the reader understand why certain measures were prioritized over others.

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	733

Strong Points	*Areas of Improvement*
• Problems were described succinctly without technical jargon. The risks and impacts of the vulnerabilities and of taking no action were very clear. • Nice job on the high priority recommendations. • The majority of the suggestions were focused on low to no cost actions. • All three points were communicated effectively and the quality of the presentation was excellent.	• The mapping from strategy/actions to the business risks was unclear, and I was also unclear as to which slide was presenting the business financial risks. There was a lot of explanation on impact, but not a lot of information as to how the proposed actions will affect the business's success or the government facilities' operations. Additionally, the recommendations amounted to ~$21k, which is not a low-cost effort for a minimal-to-no-funding scenario. • The sound and mouth movement were out of synch. - quality control. • Risks related to business concerns was unclear. • no comment

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	75	50	25	50	0	50	75	25	75

Whack a Mole	
WAM1	WAM2
375	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
1600	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
1251