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

DAKOTA STATE UNIVERSITY

DSU TROJANHORSES

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 42 SCORECARD

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

Score Category	Team Points	Percent of Points	Team Ranking
Anomalies	652	32.60%	45
Security Documentation	876	87.60%	36
C-Suite Panel	925	92.50%	11
Red Team	1544	61.76%	32
Blue Team	2000	100.00%	1
Green Team Surveys	1403	93.53%	20
Deductions	0		
Overall	**7400**	**74.00%**	**20**

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	652

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

1	yes	27	no	53	Not Answered
2	yes	28	yes	54	Not Answered
3	yes	29	no	55	yes
4	yes	30	Not Answered	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	no	60	yes
9	yes	35	Not Answered	61	no
10	yes	36	Not Answered	62	yes
11	no	37	yes	63	yes
12	no	38	yes	64	no
13	yes	39	Not Answered	65	Not Answered
14	yes	40	no	66	yes
15	yes	41	Not Answered	67	Not Answered
16	yes	42	Not Answered	68	Not Answered
17	yes	43	Not Answered	69	Not Answered
18	yes	44	yes	70	yes
19	yes	45	yes	71	yes
20	Not Answered	46	yes	72	yes
21	no	47	no	73	Not Answered
22	Not Answered	48	no	74	Not Answered
23	no	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	876

Strong Points	*Areas of Improvement*
• I found the report to be clear and concise and targeted towards senior leadership. • Nicely done on identifying and documenting the vulnerabilities. • Excellent work on the diagram; it's well-labeled, easy to read, and includes the appropriate ports and IP addresses. The system hardening steps are also thoroughly detailed, providing clear and concise guidance.	• The asset inventory and the network diagram are a little off. MapBox was captured on the diagram but missing from the inventory. • Applying more attention to detail for e.g. the asset section of the report. • The system overview is well-constructed but would benefit from using less technical language and focusing on a higher-level explanation of the project and its objectives. Additionally, some hosts were missing from the asset inventory.

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	925

Strong Points	*Areas of Improvement*
• The presentation seems professionally done throughout • The presentation was very clean, straightforward, and concise with important key messages. • Very professional slides, background, and speakers. • Presentation included clear and concise information targeted to the C-Suite. • Financial risks were clearly stated. The presentation overall was also very professional.	• Nothing found • Numbers for time estimations and cost would be helpful to support prioritization and acceptance of recommendations. • Tool/Application recommendations should have been elaborated on more to discuss cost and functionality, rather than just the name and general purpose. • The slides showed three strategies but only one was addressed in the presentation. The strategies also did not direction address mentioned risks. • No reasoning on why priorities should be implemented. What is the ROI? What happens if I don't implement recommended priorities?

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	75	50	50	25	25	75	75	100

Whack a Mole	
WAM1	WAM2
281	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
1403