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

GOVERNORS STATE UNIVERSITY

GOVSTATE1

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 43 SCORECARD

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

Score Category	Team Points	Percent of Points	Team Ranking
Anomalies	195	9.75%	91
Security Documentation	420	42.00%	83
C-Suite Panel	878	87.80%	33
Red Team	450	18.00%	87
Blue Team	410	20.50%	94
Green Team Surveys	74	4.93%	93
Deductions	0		
Overall	**2427**	**24.27%**	**93**

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	195

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

1	yes	27	Not Answered	53	no
2	no	28	no	54	no
3	yes	29	no	55	yes
4	yes	30	Not Answered	56	yes
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	yes
9	yes	35	Not Answered	61	yes
10	yes	36	no	62	yes
11	no	37	no	63	yes
12	no	38	no	64	no
13	no	39	Not Answered	65	Not Answered
14	no	40	no	66	no
15	no	41	Not Answered	67	Not Answered
16	no	42	Not Answered	68	Not Answered
17	no	43	Not Answered	69	Not Answered
18	yes	44	Not Answered	70	Not Answered
19	no	45	no	71	Not Answered
20	no	46	Not Answered	72	Not Answered
21	yes	47	Not Answered	73	Not Answered
22	no	48	Not Answered	74	Not Answered
23	Not Answered	49	Not Answered	75	Not Answered
24	no	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	420

Strong Points	*Areas of Improvement*
• Attempted to answer each section. • Well designed network diagram. • Thank you for participating in this years competition! • overall, you're your write up was well done • did well on hitting many different aspects of harding	• The report seemed very rushed overall - spending more time would result in a much better report/score. • Missing assets. Did not identify all vulnerabilities. System overview, and system hardening not specific to this system. Did not include software used in system hardening. • 192.168.x.x is not a space available for this competition. The space is 10.0.x.x. • missing many ports and missed mapbox. Did not find many known vulnerabilities • missing many ports missed mapbox on asset inventory, some portions needed stronger justification in Harding section needed to find more vulnerabilities

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	878

Strong Points	*Areas of Improvement*
• A strong point for this entry were the recommendations identified for consideration. They were technically appropriate and promote defense in depth within the site's network. Also, recommendations spanned technical, administrative, and physical enhancements further enhancing the layered security posture. • The content is technically sound • Presentation fit to specified time frame. All members presented. • Great teamwork separating and presenting the key points of the presentation.	• To improve this entry, the team could have established a consistent message across the presentation. At times, there was duplicity in the speaking roles, as well as a lack of visual materials to substantiate or detail your messaging to senior management. • The presentation could have been much more professional. • Recommend blurring background to reduce visible clutter from background. It is recommended to create an associated PowerPoint or Canva presentation so that executives can refer to this during and after the presentation. Are new hires required to implement these strategies? Speakers repeat topics discussions. It is

	recommended to have a cohesive draft so that all members address different points. • Having a presentation with slides can be very helpful for the audience to understand and recall key points.

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	0	0	0	0	0	0	0	0	0

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
410	0

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
74