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

SOUTHEASTERN LOUISIANA UNIVERSITY

BRUTE FORCE LIONS

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 8 SCORECARD

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

Score Category	Team Points	Percent of Points	Team Ranking
Anomalies	768	38.40%	30
Security Documentation	723	72.30%	69
C-Suite Panel	670	67.00%	77
Red Team	1638	65.52%	23
Blue Team	2000	100.00%	1
Green Team Surveys	913	60.87%	38
Deductions	0		
Overall	**6712**	**67.12%**	**38**

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	768

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

1	yes	27	Not Answered	53	Not Answered
2	yes	28	no	54	yes
3	yes	29	Not Answered	55	yes
4	yes	30	Not Answered	56	no
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	yes	62	yes
11	no	37	no	63	yes
12	yes	38	Not Answered	64	yes
13	yes	39	yes	65	no
14	yes	40	no	66	no
15	no	41	no	67	Not Answered
16	yes	42	Not Answered	68	Not Answered
17	yes	43	no	69	no
18	yes	44	Not Answered	70	yes
19	yes	45	yes	71	Not Answered
20	Not Answered	46	yes	72	yes
21	yes	47	no	73	Not Answered
22	yes	48	yes	74	Not Answered
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	723

Strong Points	*Areas of Improvement*
• Good list of vulnerabilities and mitigations • Your network diagram was well laid out, vulnerabilities and mitigations were easily understood and appropriate for C-suite • good job on findng so many vulnerabilietes • Known Vulnerabilities covered many simple security issues.	• System overview is too brief. Didn't list vulnerabilities in the 3 assumed breach systems • Both the system overview and system hardening were sparse, you could have been more thorough for both. The formatting of the overall report had several blank pages that should have been deleted. • System overview only defined hardware and did not go into detail no map box on asset inventory needed more justification on the Harding section • System overview lacking. • System hardening steps

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	670

Strong Points	*Areas of Improvement*
• I liked the way the slides were crafted. Careful attention to detail was put into them and it shows. I like how most points of technical recommendation were broken down and made easy to understand to people that may not be in the industry! • Clear identification of business risks. • The team met all rubric requirement except for the video length. Video length is a little less than 5 minutes, however very rich in content that I could care less of the little time missed. • The team had 2 active presenters and it was good to see the business value they provide.	• I would've liked to see more slides that would've given some additional opportunity to add detail and address each point individually. Another would be to recommend one logging solution to the C-Suite. • Provide reasoning for recommendations and connect strategy to risk reduction. • I love your presentation and how everything was explained in details. I also love the fact that you presented in such a way that anyone without a technical background could understand everything. The only thing you should work on is maximizing your time. Your video was a little less than 5 minutes but absolutely rich in content. Try to maintain the approximate time in the future. Good work!

	• This entry could have been improved by adding multiple members and presenting one slide each. Good to see the face of panel members.

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
75	50	100	75	0	50	75	100	50	50

Whack a Mole	
WAM1	WAM2
187	375

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
913