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

BRIGHAM YOUNG UNIVERSITY

BYU

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 11 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	873	87.30%	37
C-Suite Panel	665	66.50%	80
Red Team	1475	59.00%	35
Blue Team	1995	99.75%	26
Green Team Surveys	180	12.00%	53
Deductions	0		
Overall	**5956**	**59.56%**	**53**

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	no
2	yes	28	no	54	Not Answered
3	yes	29	Not Answered	55	yes
4	yes	30	Not Answered	56	yes
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	yes	62	yes
11	no	37	yes	63	yes
12	no	38	yes	64	no
13	yes	39	no	65	Not Answered
14	yes	40	no	66	no
15	yes	41	Not Answered	67	Not Answered
16	yes	42	yes	68	Not Answered
17	yes	43	Not Answered	69	Not Answered
18	yes	44	yes	70	yes
19	yes	45	yes	71	Not Answered
20	Not Answered	46	yes	72	yes
21	no	47	yes	73	Not Answered
22	yes	48	yes	74	Not Answered
23	Not Answered	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	873

Strong Points	*Areas of Improvement*
• This entries characterization of vulnerabilities was very thorough. I appreciate the effort to use two similar, but different, tools to establish a more comprehensive analysis. This mirrors actions that are often taken in real life and return far more secure systems when used in this way. Well done. • Nice job on the overview - targeted nicely for senior management. • Great detail in the network diagram • The network diagram is visually clear, with organized sections and adequate spacing between components. Labels are readable, and icons/symbols are used consistently. The System Hardening is organized well and easy to read with minimal technical jargon.	• This entry could have been improved by identifying all seven target machines/VMs. In this case, a MapBox was missed, which constituted the seventh asset. This led to an incomplete network diagram and therefore undiscovered vulnerabilities remain. • Nice job overall, but needed a little more attention to detail (e.g. missing the Map Box from the asset inventory). • MapBox missing from Asset Inventory. System hardening explanations are overly informal • While the network diagram was visually clear, its complexity made it challenging to follow. Additionally, the team missed some 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	665

Strong Points	*Areas of Improvement*
• Recommendation of security awareness training and scheduled backups is spot on. All too often we overlook the basics such as backing up systems and training employees to be more vigilant • The breach investigation is thoroughly put together—excellent work! • The depth of information that goes into each slide was well done. • Importance of backups highlighted.	• While I greatly appreciate the recommendation to backup, that's only one part of a disaster recovery plan. It would have been great to see more about plans to validate backups are actually being performed in a way that can be restored too. Finding vulns with OpenVAS is great, but presentation did not mention any effort to patch or accept risk. • Great job overall. Differentiating between technical recommendations and business-related strategies could make the approach even more effective and aligned with specific goals

	• Practice a couple times before hand to make sure you are ready to present and minimize downtime. • Pace and smoothness of presentation needs improvement. Felt generally not rehearsed. • Strategy to reduce identified risks felt unclear at best.

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	100	75	50	50	100	50	50	75	100

Whack a Mole	
WAM1	WAM2
375	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
1595	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
180