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

HAWKEYE COMMUNITY COLLEGE

HAWKEYES

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 46 SCORECARD

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

Score Category	Team Points	Percent of Points	Team Ranking
Anomalies	596	29.80%	56
Security Documentation	912	91.20%	25
C-Suite Panel	693	69.30%	75
Red Team	1550	62.00%	31
Blue Team	2000	100.00%	1
Green Team Surveys	936	62.40%	39
Deductions	0		
Overall	**6687**	**66.87%**	**39**

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	596

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

1	yes		27	Not Answered		53	yes
2	no		28	yes		54	Not Answered
3	yes		29	yes		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	no
9	yes		35	Not Answered		61	yes
10	yes		36	Not Answered		62	yes
11	yes		37	no		63	no
12	Not Answered		38	Not Answered		64	yes
13	yes		39	Not Answered		65	Not Answered
14	yes		40	yes		66	no
15	no		41	Not Answered		67	Not Answered
16	yes		42	Not Answered		68	no
17	yes		43	Not Answered		69	Not Answered
18	yes		44	Not Answered		70	Not Answered
19	yes		45	Not Answered		71	Not Answered
20	Not Answered		46	yes		72	Not Answered
21	yes		47	no		73	Not Answered
22	Not Answered		48	yes		74	Not Answered
23	Not Answered		49	yes		75	Not Answered
24	Not Answered		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	912

Strong Points	*Areas of Improvement*
• The network diagram was very creative and thorough. • Very nice network map, excellent legend with clearly defined symbols and meanings. Report was high level and appropriate for c-suite. • The system changes made are straightforward and great recommendations for the vulnerabilities found. • The system overview was well written and clear • Easy to interpret, well developed network diagram •	• The asset inventory was very thin. Also, it might be better to use individual records for each port within a service for the sake of clarity. • feel like there were some services and ports missed in the network and none of the vulnerabilities had CVEs so I feel that a little more thoroughness would have served you well • Paragraphs are recommended over lists for reports and documents for professional aesthetic and clear context. • System hardening – add tools that were used for each remediation

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	693

Strong Points	*Areas of Improvement*
• A strength of this entry was that they identified consequences of cyber breaches that directly parallel situations in real-world events. They also identified accurate, meaningful business concerns that senior management would very much want to know about. • The risk discussion was thorough • Good use of side by side video of speakers and slides. • Strong approach to impact assessment and identification of briefers' applicable role	• To improve this entry, the team should expand on the identified recommendations to include HOW they are to be achieved. The list items currently take the form of objectives and lack actionable steps to improve the security posture of the site. • There was very little in the way of immediate recommendations • More details needed on the recommendation of 'increase security'. Discussion of associated products, costs, and staffing is needed. • Presentation would benefit from more detailed/deeper dive in to high priority recommendations and stronger strategy to reduce business risks

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	75	75	25	0	0	0	0	50

Whack a Mole	
WAM1	WAM2
375	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
936