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

HIGHLINE COLLEGE

THUNDERBIRDS

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 84 SCORECARD

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

Score Category	Team Points	Percent of Points	Team Ranking
Anomalies	371	18.55%	85
Security Documentation	859	85.90%	41
C-Suite Panel	898	89.80%	22
Red Team	1013	40.52%	64
Blue Team	1508	75.40%	78
Green Team Surveys	197	13.13%	76
Deductions	0		
Overall	**4846**	**48.46%**	**76**

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	371

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

1	yes	27	Not Answered	53	Not Answered
2	yes	28	Not Answered	54	Not Answered
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	no
9	yes	35	Not Answered	61	yes
10	yes	36	Not Answered	62	yes
11	no	37	no	63	yes
12	Not Answered	38	Not Answered	64	no
13	Not Answered	39	Not Answered	65	Not Answered
14	yes	40	Not Answered	66	Not Answered
15	Not Answered	41	Not Answered	67	Not Answered
16	yes	42	Not Answered	68	Not Answered
17	no	43	no	69	Not Answered
18	yes	44	yes	70	Not Answered
19	no	45	no	71	Not Answered
20	Not Answered	46	yes	72	Not Answered
21	yes	47	no	73	Not Answered
22	yes	48	yes	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	859

Strong Points	*Areas of Improvement*
• The team listed vulnerabilities for all the hosts with appropriate mitigation. Also, this team listed the tools utilized within the System Hardening. Great Job! • Great job on ensuring the correct audience for discussing the overall summary of the network. • Identified vulnerabilities. Only needed one more to get the max score for that category. • A strong point in this entry is the comprehensive and structured approach to asset inventory, vulnerability assessment, and system hardening. The detailed list of hosts, operating systems, and associated services, along with corresponding vulnerabilities and mitigation strategies, provides a clear, organized view of the network's security posture. Additionally, the use of tools like NMAP, Nessus, and OpenVAS for vulnerability scanning and the implementation of strong password policies based on NIST recommendations demonstrate a proactive and thorough strategy for securing the environment.	• Formatting and system hardening could have been better. • Ensure that everything is listed correctly in your network diagram and you understand every machine there. • For system hardening, provide more detail on steps taken and the justification. • This entry could be improved by providing more context on the impact or risk level of the identified vulnerabilities. For example, prioritizing the mitigations based on the criticality of the vulnerabilities (such as considering the potential for remote code execution, data breaches, or service disruptions) would help in guiding resource allocation for remediation. Additionally, while the technical details are strong, a clearer explanation of how these efforts tie back to business continuity, client trust, and operational efficiency would strengthen the overall narrative, helping non-technical stakeholders understand the value of these measures.

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	898

Strong Points	*Areas of Improvement*
• Well spoken and appropriate vocabulary used for audience. • Your slides were really good. Nice graphics and well laid out. There was good presentation flow and you ended on a positive note.	• Ensure that there is proper and direct reasoning behind risks. • The slide on strategies to reduce risk had a little more jargon than C-Suite would want to know, and a separate slide to introduce your team would have been good.

• This team did excellently well, the only reason I gave them proficient under strategy to reduce risks(User Access Controls) is simply due to choice of technical words that was not explained. Example zero trust, from business standpoint, not everyone knows the meaning. I do because I have cybersecurity background. Others include Principle of least privilege, multifactor authentication etc. I expected a little explanation for multifactor authentication like using more than one method to authenticate an acct, like email , cell phone, and token. Others include Principle of least privilege explaining that users are only authorized to have access to specific minimum resources as needed or required to do their job. • The presentation was spot on.	• This team did excellently well. My only recommendation would be, in a business presentation, when you include technical terms, assume your audience are not highly technically inclined and explain the meaning. Example zero trust, from business standpoint, not everyone knows the meaning. I do because I have cybersecurity background. Others include Principle of least privilege, multifactor authentication etc. A little explanation for multifactor authentication like using more than one method to authenticate an acct, such as email , cell phone, and token. Others include Principle of least privilege explaining that users are only authorized to have access to specific minimum resources as needed or required to do their job. Overall Excellent Job! • Adding more than 2 presenters would have really helped.

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 point*s. 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 point*s. 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
50	50	50	75	0	25	0	100	25	0

Whack a Mole	
WAM1	WAM2
93	93

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
1400	108

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
197