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

UNIVERSITY OF HOUSTON

CRYPTIC CRUSADERS

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 17 SCORECARD

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

Score Category	Team Points	Percent of Points	Team Ranking
Anomalies	763	38.15%	33
Security Documentation	858	85.80%	42
C-Suite Panel	857	85.70%	39
Red Team	1338	53.52%	41
Blue Team	1935	96.75%	50
Green Team Surveys	990	66.00%	37
Deductions	0		
Overall	**6741**	**67.41%**	**37**

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	763

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

1	yes	27	no	53	no
2	yes	28	no	54	no
3	yes	29	no	55	yes
4	yes	30	Not Answered	56	no
5	yes	31	yes	57	yes
6	yes	32	yes	58	yes
7	yes	33	yes	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	yes	63	yes
12	yes	38	no	64	no
13	yes	39	no	65	Not Answered
14	no	40	no	66	no
15	no	41	Not Answered	67	Not Answered
16	yes	42	Not Answered	68	no
17	yes	43	no	69	no
18	yes	44	Not Answered	70	yes
19	no	45	no	71	yes
20	yes	46	yes	72	yes
21	yes	47	no	73	yes
22	yes	48	yes	74	yes
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	858

Strong Points	*Areas of Improvement*
• Very good identification of all assets; also very good identification of vulnerabilities and mitigations. Overall, very good submission. • Your hardening advice is fundamental and easily understandable for your audience. • Windows hardening details were solid, loved seeing all the CVE numbers in the known vulns too. • Network diagram was well done and reminiscent of engineering documentation. Vulnerability descriptions and mitigations were presented without jargon.	• Hardening needed justifications for why this and not another action. • When reporting ports from an nmap scan, don't include the filtered ones, typically. • Linux hardening details were lacking, including the ephemeral ports in asset inventory doesn't add value • Inclusion of the Operating System version would have been nice to see. The system description could have been enhanced by focusing on overall purpose and impact rather than individual asset definitions

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	857

Strong Points	*Areas of Improvement*
• Overall this was a very strong submission, the 4 high-priority recommendations are solid, and you call out the need for more talent to implement properly • The technical recommendations, along with the detailed outline of open-source tools and expertise, are outstanding! • Great overview of the risks • The risks were explained very well, and the entire presentation maintained a professional atmosphere.	• Make sure everyone's audio is as good as you can get it remotely; if someone sounds like they're on an old telephone, some managers think you're "phoning it in" • The recommendations around business risks are well-considered; adding more business-specific controls alongside the technical ones could further strengthen this section • No mention of system hardening • The strategy could have more clearly stated which concerns it was addressing. For the priorities, the C-Suite may not know what Zeek, Suricata, and Wazuh are, so a brief explanation/description would be helpful. Also, a better explanation of why the priorities should be implemented should be presented to the C-Suite.

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
100	25	50	25	25	0	0	25	25	50

Whack a Mole	
WAM1	WAM2
281	281

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
1535	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
990