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

DEFENDING U.S. ENERGY INFRASTRUCTURE

UNIVERSITY OF MARYLAND-BALTIMORE COUNTY

UMBC CYBERDAWGS

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 85 SCORECARD

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

Score Category	Team Points	Percent of Points	Team Ranking
Anomalies	894	44.70%	19
Security Documentation	884	88.40%	30
C-Suite Panel	892	89.20%	25
Red Team	1738	69.52%	20
Blue Team	1870	93.50%	52
Green Team Surveys	1483	98.87%	12
Deductions	0		
Overall	**7761**	**77.61%**	**12**

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	894

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

1	yes	27	Not Answered	53	yes
2	yes	28	no	54	yes
3	yes	29	Not Answered	55	yes
4	yes	30	Not Answered	56	no
5	yes	31	no	57	yes
6	yes	32	Not Answered	58	yes
7	yes	33	Not Answered	59	yes
8	yes	34	yes	60	yes
9	yes	35	Not Answered	61	yes
10	yes	36	Not Answered	62	yes
11	no	37	yes	63	yes
12	Not Answered	38	yes	64	yes
13	yes	39	yes	65	no
14	yes	40	yes	66	yes
15	no	41	Not Answered	67	Not Answered
16	yes	42	Not Answered	68	Not Answered
17	yes	43	Not Answered	69	Not Answered
18	yes	44	Not Answered	70	yes
19	no	45	yes	71	yes
20	Not Answered	46	yes	72	yes
21	yes	47	no	73	yes
22	yes	48	no	74	yes
23	yes	49	yes	75	yes
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	884

Strong Points	*Areas of Improvement*
• Great job on the formatting for system overview and system hardening. It was easy to follow. • Overall it was really well done and the attention to detail is appreciated. • Your Asset inventory and System Hardening were descriptive, clearly written and appropriate for C-Suite. Nice break out in Asset Inventory, easy to read and appreciate color coding. • Asset list was well formatted and easy to read. • The hardening steps were well documented and justified.	• For the known vulnerabilities, the team listed only two hosts. • Make sure that you understand why NIST CSF has those requirements. • For your network map, if key had been at bottom would have had more room for map, bigger map would have been easier to read. No OS or services listed on map, no interconnections. • Vulnerabilities were only listed for three of the systems. Identify vulnerabilities for all systems.

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	892

Strong Points	*Areas of Improvement*
• Appreciated seeing who wrote each slide and how much they contributed. • You did a good job hitting all of the elements required and keeping the information free of jargon. • The team checked all boxes. Video was approximately 5 mins, members participated equally and all members acknowledged. The team clearly summarized business and financial risks and provided a complete strategy, as well as recommended 3-4 high priority actions. Visual aids, slides and other materials were consistent with professional appearance. • Presentation was detailed and spot on.	• Went beyond the asked task a bit too much. Focus should be more on what was being asked for. • The order in which the points were covered felt out of sequence. The presentation should have ended with solutions instead of consequences. There needed to be some graphics to break up the bullet points. • Excellent job. The only recommendation I have for presentation is constant practice, so that you can own your script and not make it look like you are reading from somewhere. Besides that, your team nailed it. Keep up the good work. • This could have been better if atleast 1 more member had participated.

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	50	100	50	100	50	50	75	50	100

Whack a Mole	
WAM1	WAM2
375	187

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
1470	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
1483