CYBERFORCE COMPETITION®

U.S. DEPARTMENT OF ENERGY'S

DEFENDING U.S. ENERGY INFRASTRUCTURE

OAKLAND COMMUNITY COLLEGE

[REDACTED]

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 1 SCORECARD

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

Score Category	Team Points	Percent of Points	Team Ranking
Anomalies	555	27.75%	69
Security Documentation	561	56.10%	78
C-Suite Panel	655	65.50%	82
Red Team	1200	48.00%	50
Blue Team	1084	54.20%	89
Green Team Surveys	221	14.73%	83
Deductions	150		
Overall	4126	41.26%	83

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	555

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

#		#		#	
1	yes	27	no	53	no
2	yes	28	yes	54	Not Answered
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	no	34	no	60	yes
9	yes	35	Not Answered	61	no
10	yes	36	yes	62	yes
11	no	37	no	63	yes
12	yes	38	no	64	no
13	yes	39	no	65	Not Answered
14	no	40	yes	66	no
15	yes	41	Not Answered	67	Not Answered
16	yes	42	Not Answered	68	Not Answered
17	yes	43	no	69	Not Answered
18	yes	44	Not Answered	70	yes
19	yes	45	no	71	yes
20	no	46	yes	72	Not Answered
21	yes	47	no	73	Not Answered
22	Not Answered	48	yes	74	Not Answered
23	yes	49	no	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	561

Strong Points	Areas of Improvement
• Well designed network diagram. • Some good concepts in system hardening • Strong system hardening tactics, especially the monitoring portion. • Asset Inventory listed most systems and ports, information presented in an organized and logical manner.	• More details needed in System Overview. Did not identify all assetts. Did not identify a majority of the vulnerabilities. Missing steps for system hardening. • Many sections were lacking detail and quantity • The system overview is extremely brief and generally summarizaes the system. The asset inventory and known vulnerability sections are also lacking. • System hardening steps were generalized and broad, could have elaborated with the allowed word count.

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	655

Strong Points	Areas of Improvement
• The ability to provide strategies to reduce risks to address the business concerns for its' success and the continuity of security recommendations for the future. • This student was very well-spoken and dressed professionally. Minimal jargon used and clear explanation of priorities is provided. • Overall business risks caused by degraded energy outputs and outages were addressed • The video is consise.	• Having more active members participate equally or acknowledged contributions for off-screen team members. • No visual aids were provided outside of title slide. There was only one apparent team member for this team. The speaker seemed to be reading from a script, some additional practice with extemporaneous speaking would help this student with future public speaking, especially when the audience may interrupt with questions. Overall, a good job! • Yes. Only one person presented and nobody else on the team was mentioned. • Follow the rubric! Provide justifications and reasoning for strategy and high priority actions

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
25	50	50	25	25	50	50	50	0	50

Whack a Mole	
WAM1	WAM2
187	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
1080	4

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
221