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

DEFENDING U.S. ENERGY INFRASTRUCTURE

COLLEGE OF COASTAL GEORGIA

HAIL THE SAIL!

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 45 SCORECARD

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

Score Category	Team Points	Percent of Points	Team Ranking
Anomalies	633	31.65%	52
Security Documentation	926	92.60%	17
C-Suite Panel	921	92.10%	14
Red Team	1675	67.00%	22
Blue Team	1970	98.50%	45
Green Team Surveys	1180	78.67%	23
Deductions	0		
Overall	**7305**	**73.05%**	**23**

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	633

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

1	yes
2	yes
3	yes
4	yes
5	yes
6	yes
7	yes
8	yes
9	yes
10	no
11	no
12	no
13	yes
14	no
15	no
16	yes
17	no
18	yes
19	yes
20	yes
21	yes
22	Not Answered
23	no
24	no
25	Not Answered
26	Not Answered
27	Not Answered
28	yes
29	no
30	Not Answered
31	no
32	Not Answered
33	Not Answered
34	Not Answered
35	Not Answered
36	Not Answered
37	no
38	yes
39	Not Answered
40	yes
41	Not Answered
42	Not Answered
43	Not Answered
44	yes
45	yes
46	yes
47	no
48	yes
49	no
50	yes
51	yes
52	yes
53	Not Answered
54	Not Answered
55	yes
56	yes
57	no
58	yes
59	yes
60	no
61	yes
62	yes
63	yes
64	no
65	Not Answered
66	Not Answered
67	Not Answered
68	Not Answered
69	Not Answered
70	no
71	Not Answered
72	Not Answered
73	Not Answered
74	Not Answered
75	Not Answered
76	yes
77	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	926

Strong Points	*Areas of Improvement*
• Well designed network diagram. Thorough asset inventory. • The document was very professional and thorough. • Hardening steps easily understood and at good level for c-suite. Nice network map, separate symbols for servers and desktops, showed firewall. • The system hardening section is very well written and is easily understandable for the intended audience. • The system overview was well written and clear • Easy to interpret, well developed network diagram • Good description of vulnerabilities - use of CVE's, remediation's are clear and plan is presented in the event the vulnerability can't be right away describe • The system hardening steps were clear and made sense and used • Appropriate and well developed tools used for system hardening, which are used in most best security practices	• Did not identify all vulnerabilities. • A system overview meant for senior leadership should thoroughly explain the system, not generally mention functionality. Consider audience when writing an overview for a briefing. • Your documentation was good, but lacked some details such as mitigations were high level, some vulnerabilities only listed CVE instead of description, that would have taken it to the next level. Even though you are presenting to C-suite, it is good to provide thorough explanations. • It is recommended to provide leadership with more information on the found vulnerabilities than just the CVE IDs. • The system overview was well written and clear, however for future you may want to consider adding users (or groups of users) that use the system. • For future presentations you may want to add a blurb identifying that tools used are compatible with the operational environment (ie slow ping & use a passive scan) in the system hardening description

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	921

Strong Points	*Areas of Improvement*
• There were several strong points for this entry. Among them are that the presenters were informed, well-paced, and succinct in making their points. The recommended actions were relevant to real-world scenarios that, if implemented, would effectively mitigate the impacts of cyber breaches. The content was also structured	• To improve this presentation, the team could have compressed the entry relative to time. While not a critical flaw, taking more time (as opposed to 5 minutes) needs to be carefully considered as it is a most critical resource for senior level managers. Finding ways to communicate more efficiently with only the allotted time

in a logical way that would resonate well with senior level management. • The content was thorough and professional • Good use of embedded speaker video. • Presentation was very informative and slides were professional.	is a challenge that benefit the peers you work with, the managers you work for, and the staff that support you. • The video was just a little too long • There is mention that the cost of security training would cost money. More specifics are needed. Discussion of related staffing requirements is missing. • Your presentation exceeded the allotted time by 40 min.

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	100	50	50	100	100	100	100	50	100

Whack a Mole	
WAM1	WAM2
0	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
1570	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
1180