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

UNIVERSITY OF FLORIDA

THE_TECHNIQUE

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 83 SCORECARD

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

Score Category	Team Points	Percent of Points	Team Ranking
Anomalies	0	0.00%	92
Security Documentation	762	76.20%	63
C-Suite Panel	925	92.50%	11
Red Team	300	12.00%	91
Blue Team	1200	60.00%	85
Green Team Surveys	107	7.13%	89
Deductions	0		
Overall	**3294**	**32.94%**	**89**

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	0

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

1	Not Answered		27	Not Answered		53	Not Answered
2	Not Answered		28	Not Answered		54	Not Answered
3	Not Answered		29	Not Answered		55	Not Answered
4	Not Answered		30	Not Answered		56	Not Answered
5	Not Answered		31	Not Answered		57	Not Answered
6	Not Answered		32	Not Answered		58	Not Answered
7	Not Answered		33	Not Answered		59	Not Answered
8	Not Answered		34	Not Answered		60	Not Answered
9	Not Answered		35	Not Answered		61	Not Answered
10	Not Answered		36	Not Answered		62	Not Answered
11	Not Answered		37	Not Answered		63	Not Answered
12	Not Answered		38	Not Answered		64	Not Answered
13	Not Answered		39	Not Answered		65	Not Answered
14	Not Answered		40	Not Answered		66	Not Answered
15	Not Answered		41	Not Answered		67	Not Answered
16	Not Answered		42	Not Answered		68	Not Answered
17	Not Answered		43	Not Answered		69	Not Answered
18	Not Answered		44	Not Answered		70	Not Answered
19	Not Answered		45	Not Answered		71	Not Answered
20	Not Answered		46	Not Answered		72	Not Answered
21	Not Answered		47	Not Answered		73	Not Answered
22	Not Answered		48	Not Answered		74	Not Answered
23	Not Answered		49	Not Answered		75	Not Answered
24	Not Answered		50	Not Answered		76	Not Answered
25	Not Answered		51	Not Answered		77	Not Answered
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	762

Strong Points	*Areas of Improvement*
• Team 0083 hit all the core elements for the competition. Network Diagram to all the known vulnerabilities within various hosts. • I like that you added your future SIEM to the network diagram. • Everything was well organized and easy to read. • A strong point of this entry is the comprehensive identification of vulnerabilities across various systems, along with clear documentation of the mitigations taken for each vulnerability. The use of multiple trusted tools like WinPEAS, LinPEAS, Nessus, and Sysinternals, and the explanation of their roles in discovering escalation paths and vulnerabilities, shows a methodical and thorough approach to securing the system. Additionally, the system hardening steps, such as changing weak passwords and removing unnecessary services, demonstrate a proactive and disciplined approach to improving security.	• The System overview used vague language they could have been more specific • The system inventory and network diagram are missing the "map box." • Expand on why you took the hardening steps. Should be able to explain the purpose of each in depth. • The entry could have been improved by providing more detailed descriptions of the specific vulnerabilities found on each system, including the CVE identifiers and the exact patches or updates applied to mitigate them. While the entry lists tools and actions taken, it lacks specific examples of how these actions directly resolved vulnerabilities, which would provide a clearer understanding of the impact of the efforts. Additionally, providing more context on the next steps for unresolved vulnerabilities and offering specific recommendations for ongoing system monitoring or defense would enhance the completeness of the mitigation strategy.

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	925

Strong Points	*Areas of Improvement*
• Overall a very strong presentation, great to see the current events and NERC CIP cited • Went above and beyond with the amount of risks to the business and in general. • Your presentation had many outstanding elements. Your slides were very professional looking and you have numerous team members presenting.	• OpenVAS recommendation is great, but I'd also like to hear about how that would be implemented in a way that reduces risk of breaking OT environment during scans • Ensure that the reasoning behind ways to reduce risks directly relate back to the risks brought up.

• Mentioning cost and implementation time for each recommendation was very good.	• The only suggestion I have for you is to end your presentation on a solution instead of a problem. • Risks mentioned appeared vague and unclear.

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
0	0	0	0	0	0	0	0	0	0

Whack a Mole	
WAM1	WAM2
0	0

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	300

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
1200	0

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
107