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

UNIVERSITY OF TOLEDO

UT CYBER TEAM

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 44 SCORECARD

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

Score Category	Team Points	Percent of Points	Team Ranking
Anomalies	480	24.00%	75
Security Documentation	936	93.60%	12
C-Suite Panel	608	60.80%	86
Red Team	300	12.00%	91
Blue Team	2000	100.00%	1
Green Team Surveys	984	65.60%	68
Deductions	0		
Overall	**5308**	**53.08%**	**68**

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	480

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

1	yes	27	no	53	no
2	yes	28	no	54	Not Answered
3	yes	29	Not Answered	55	yes
4	yes	30	Not Answered	56	no
5	yes	31	yes	57	yes
6	yes	32	Not Answered	58	yes
7	yes	33	Not Answered	59	yes
8	yes	34	Not Answered	60	no
9	yes	35	Not Answered	61	yes
10	yes	36	Not Answered	62	yes
11	no	37	no	63	yes
12	no	38	no	64	yes
13	yes	39	no	65	Not Answered
14	yes	40	Not Answered	66	no
15	yes	41	Not Answered	67	no
16	yes	42	Not Answered	68	Not Answered
17	yes	43	Not Answered	69	Not Answered
18	yes	44	Not Answered	70	yes
19	yes	45	no	71	yes
20	Not Answered	46	yes	72	yes
21	no	47	Not Answered	73	Not Answered
22	no	48	Not Answered	74	no
23	no	49	Not Answered	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	936

Strong Points	*Areas of Improvement*
• Good work on network diagram, and system hardening was well documented and easy to read. • Asset inventory and network map were both well documented and clearly laid out. Your list of vulnerabilities and mitigations was very thorough and your hardening techniques were well explained. • Excellent System Hardening description • Overall, your write up was well done. Did well on hitting all aspects of Harding. • did well overall	• System overview does not target senior leadership. • Your documentation was very professional, however you used a lot of jargon, and you listed tools instead of explaining what you were doing with the tools. • For the vulnerability list - "The audience for this section includes “senior leadership”. The descriptions of the vulnerabilities was well above the understanding of the c-suite. • Missing few ports have less then 90% of assets, some portions needed stronger justification in Harding section • missing few ports have less then 90% of assets, some portions needed stronger justification in Harding section

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	608

Strong Points	*Areas of Improvement*
• Good visual representations for a C-suite • A strength of this entry were the technical recommendations to recover from such an incident. The examples listed by the project team mirror those that a real-world management team would need to receive updates on to effectively lead a company back from the stated consequences. In this way, the mock update was effective, impactful, and great experience. • This presentation effectively addressed the interconnections between business concerns, potential risks, and security recommendations, providing clear explanations at a high level.	• No mention of government impacts and risks. No mention of the current breach • This entry could have been improved by involving additional members of the team to balance the presentation. Speaker 1 was articulate and informed, but only provided appx 25% of the material. Speaker 2 was effective as well, but carried appx 75% of the material. • I recommend including specific security tools relevant to the reference, along with their associated costs, to provide a clear justification for the expenses.

• Slides are visually appealing • Good presentation structure, with acknowledgements and detailed cost of strategy/recommendation break down	• Risk and Business Impact are not the same, Need to follow rubric more closely, speakers need to slow down at times • Slower and clearer presenter annunciation would help improve overall presentation of concepts

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
1600	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
984