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

UNIVERSITY OF TOLEDO

UT CYBER SECURITY CLUB

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 92 SCORECARD

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

Score Category	Team Points	Percent of Points	Team Ranking
Anomalies	566	28.30%	63
Security Documentation	865	86.50%	38
C-Suite Panel	843	84.30%	45
Red Team	625	25.00%	84
Blue Team	1612	80.60%	72
Green Team Surveys	230	15.33%	78
Deductions	0		
Overall	**4741**	**47.41%**	**78**

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	566

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

1	yes	27	Not Answered	53	no
2	yes	28	Not Answered	54	no
3	yes	29	Not Answered	55	yes
4	yes	30	no	56	yes
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	yes	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	yes	71	yes
20	Not Answered	46	yes	72	yes
21	no	47	no	73	Not Answered
22	Not Answered	48	no	74	Not Answered
23	no	49	no	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	865

Strong Points	*Areas of Improvement*
• System hardening was formatted in a way that was easy to follow. The inventory list was also formatted to minimize the number of rows which makes the list less overwhelming for senior leadership. • Well done on the known vulnerabilities and mitigation strategies section. • There was great consistency throughout the document. • Hardening steps defined very clear and effective methods of securing and hardening your systems.	• Formatting overall, report has some gaps throughout that could have been avoided by resizing content. • A bit more professionalism on the formatting is advisable. Plesae review deocuments for empty pages and excessive white space before submitting. Think about using separate rows for each port/service. Also, the system overview should not be completely italicized. Nobody in the professional world will accept writing like that. • Make sure to not just focus too heavily on CVEs and you look for other sources of security measures. • Known vulnerabilities should include findings from vulnerability scans as well as manual reconnaissance on the machines. Many vulnerabilities were missed since your results looked primarily from an automated scan.

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	843

Strong Points	*Areas of Improvement*
• Well done on the reasoning behind all the actions. • Nice combination of presenters and professional slides. • Well executed presentation addressing the power outages and how it can affect government facilities' and clients. • Very professionally presentation with well described actions.	• Not re-using the same strategies for strategy to reduce risk and the high priority risks. • There were minor sound issues that took away from the professionalism of the presentation. • For some parts of the video the audio could have been much more clear. • Don't tell your C-Suite you should find external experts when you're supposed to be the experts.

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	50	75	0	25	50	50	0	25	50

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	12

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
230