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

TRITON COLLEGE

THE SOCIETY @ TCC

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 82 SCORECARD

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

Score Category	Team Points	Percent of Points	Team Ranking
Anomalies	291	14.55%	88
Security Documentation	750	75.00%	66
C-Suite Panel	851	85.10%	42
Red Team	1056	42.24%	59
Blue Team	1509	75.45%	76
Green Team Surveys	1057	70.47%	62
Deductions	0		
Overall	**5514**	**55.14%**	**62**

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	291

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

1	yes	27	Not Answered	53	Not Answered
2	no	28	yes	54	Not Answered
3	yes	29	Not Answered	55	yes
4	yes	30	Not Answered	56	no
5	yes	31	Not Answered	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	Not Answered	37	no	63	yes
12	no	38	Not Answered	64	no
13	yes	39	Not Answered	65	Not Answered
14	yes	40	Not Answered	66	Not Answered
15	no	41	Not Answered	67	Not Answered
16	Not Answered	42	Not Answered	68	Not Answered
17	no	43	Not Answered	69	Not Answered
18	yes	44	Not Answered	70	Not Answered
19	no	45	Not Answered	71	Not Answered
20	yes	46	Not Answered	72	Not Answered
21	no	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	yes
25	Not Answered	51	Not Answered	77	yes
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	750

Strong Points	*Areas of Improvement*
• Your asset inventory appears accurate and complete. • Excellent network diagram • Asset inventory and network diagram were easy to read and understand. • A strong point of this entry is the comprehensive approach to system hardening and vulnerability mitigation. The inclusion of specific actions such as auditing system accounts, ensuring updates and patches are applied, and using tools like NMAP and Malwarebytes for vulnerability scanning demonstrates a methodical and proactive effort to secure the system environment. Additionally, the focus on increasing system stability and security by configuring firewalls, securing ports, and using real-time monitoring tools like TacticalRMM to detect and resolve issues quickly is highly commendable.	• There are many more vulnerabilities and corrective actions to be discovered and discussed in your vulnerability table. • Known vulns section was a bit lacking, including ephemeral ports in asset inventory does not add value • Make sure to organize your known vulnerabilities better and cover more than two machines. • This entry could be improved by providing more clarity and organization in the way it presents the vulnerabilities and mitigation actions. The list of vulnerabilities and actions appears to be somewhat disorganized, with many issues scattered throughout, which could make it difficult for readers to follow. It would help to group related issues together, perhaps with a more structured format (e.g., categorized by system component or severity). Additionally, the use of more specific metrics or evidence of the effectiveness of the mitigations (such as how much system downtime was reduced or the improvement in system performance) would strengthen the argument for the success of these actions. More detailed explanations of each tool or process mentioned (e.g., why "John the Ripper" was chosen) could also provide greater context.

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	851

Strong Points	*Areas of Improvement*
• Historical Consequences slide is wonderful, excellent research and	• Use caution when going over the 5 minute allocation with management, turning

compelling argument on improving cybersecurity program • Well done providing sources and having real life examples of the repercussions. • Presenting on the potential consequences and historical consequences are powerful motivators for decision making. • Cites strong sources and examples throughout presentation (historical examples of risks and strong sources behind any stats mentioned). • Mentioned governmental support available from other agencies.	camera on during presentation helps sell the cybersecurity program too • The risks mentioned did not have any direct mitigations discussed. • Potential estimated timelines and costs would support recommendation decision making for C-suite executives. • Misspelled company name on the first slide is quite a negative look for your C-Suite audience.

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
75	0	100	0	25	25	25	50	25	0

Whack a Mole	
WAM1	WAM2
187	93

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

1325	184

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
1057