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

UNIVERSITY OF KANSAS

JAYHACKERS

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 51 SCORECARD

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

Score Category	Team Points	Percent of Points	Team Ranking
Anomalies	662	33.10%	43
Security Documentation	567	56.70%	77
C-Suite Panel	825	82.50%	53
Red Team	1088	43.52%	56
Blue Team	1990	99.50%	32
Green Team Surveys	1493	99.53%	41
Deductions	0		
Overall	**6625**	**66.25%**	**41**

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	662

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

1	yes	27	Not Answered	53	Not Answered
2	yes	28	no	54	Not Answered
3	yes	29	Not Answered	55	yes
4	yes	30	Not Answered	56	yes
5	yes	31	no	57	yes
6	yes	32	no	58	no
7	yes	33	Not Answered	59	yes
8	yes	34	yes	60	no
9	yes	35	no	61	yes
10	yes	36	Not Answered	62	yes
11	no	37	yes	63	yes
12	Not Answered	38	no	64	yes
13	yes	39	no	65	yes
14	yes	40	yes	66	yes
15	yes	41	Not Answered	67	yes
16	yes	42	Not Answered	68	Not Answered
17	yes	43	yes	69	Not Answered
18	yes	44	Not Answered	70	yes
19	yes	45	Not Answered	71	no
20	Not Answered	46	Not Answered	72	no
21	no	47	Not Answered	73	Not Answered
22	yes	48	Not Answered	74	Not Answered
23	Not Answered	49	yes	75	Not Answered
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	567

Strong Points	*Areas of Improvement*
• Good overview of the system and discovery of your assets. • Good use of the tools you have already installed. • This presentation provided a comprehensive overview of the system, utilizing terminology suitable for a leadership audience. It briefly addressed the functionality of each component and its application by operators and customers. • The entry provides a clear breakdown of the network infrastructure, detailing the components (e.g., PLC, CNC, MapBox) and the IT system. This level of detail helps establish a solid understanding of the system architecture, which is critical for vulnerability management and defense strategies.Each identified vulnerability is paired with a corresponding mitigation plan, which demonstrates a systematic approach to addressing security issues. The inclusion of specific CVEs and targeted mitigations reflects an understanding of industry-standard practices.The asset inventory is extensive and lists attributes such as IP addresses, ports, and services. This reflects good operational security practices and the importance of asset management in cybersecurity.The use of tools like Nessus, nmap, and HardeningKitty, combined with manual audits, shows a robust approach to vulnerability assessment and system defense.The emphasis on maintaining day-to-day security (e.g., re-enabling Windows Defender, performing malware scans) underlines a commitment to sustainable cybersecurity practices.	• if you list your ports on the network diagram, make sure you list them all. Your system hardening needs detailed action items and a stepped approach. • Expand more on the hardening steps and explain why each step is important to the overall security. • I recommend enhancing the System Hardening section with additional justification and details to provide clarity on the technical steps implemented and the tools utilized. • The asset table contains repetitive entries (e.g., PLC and CNC rows listed multiple times). Streamlining this section by consolidating duplicate entries would enhance readability and clarity.While the tools and processes used are listed, the justification for selecting these tools (e.g., why Nessus and HardeningKitty were chosen over alternatives) could be expanded to demonstrate strategic decision-making.The vulnerability mitigation section could be better tailored for a senior leadership audience by summarizing critical risks, impacts, and prioritized actions, rather than listing technical details comprehensively.Some mitigations, such as the decision to remove or update certain policies, could be further justified to explain how they address the associated vulnerabilities or prevent future exploitation.

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	825

Strong Points	*Areas of Improvement*
• The format or style of recording in person with slides displayed on a projector is strong, for me, as it seems a more likely way to present to the c-suite, rather than online-only. • Good work introducing the discussion of using a cybersecurity framework. • Clarity of strategies and high priority recommendations • Very professional environmental setting and clear presentation.	• Additional work linking recommended actions and immediate wins to identified risks is needed. • Associated software products, licenses, hardware and staffing cost specific recommendations not addressed. • Clear connection with financial risk • Cost and time estimations would be helpful for acceptance and prioritization of recommendations.

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
50	0	75	75	25	100	25	25	25	50

Whack a Mole	
WAM1	WAM2
0	187

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
1590	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
1493