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

UNIVERSITY OF NORTHERN IOWA

UNISEC

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 87 SCORECARD

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

Score Category	Team Points	Percent of Points	Team Ranking
Anomalies	592	29.60%	57
Security Documentation	503	50.30%	82
C-Suite Panel	668	66.80%	79
Red Team	1256	50.24%	45
Blue Team	2000	100.00%	1
Green Team Surveys	1398	93.20%	47
Deductions	0		
Overall	**6417**	**64.17%**	**47**

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	592

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	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	yes
9	yes	35	Not Answered	61	yes
10	yes	36	Not Answered	62	yes
11	no	37	yes	63	no
12	yes	38	Not Answered	64	no
13	yes	39	Not Answered	65	yes
14	yes	40	yes	66	Not Answered
15	yes	41	Not Answered	67	Not Answered
16	yes	42	Not Answered	68	yes
17	yes	43	Not Answered	69	Not Answered
18	yes	44	Not Answered	70	Not Answered
19	yes	45	yes	71	Not Answered
20	yes	46	Not Answered	72	Not Answered
21	yes	47	Not Answered	73	Not Answered
22	yes	48	Not Answered	74	Not Answered
23	yes	49	Not Answered	75	Not Answered
24	no	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	503

Strong Points	*Areas of Improvement*
• Good list of the asset inventory. • Great start and good job not just using AI to generate a default list. • Great point in the system hardening guide about scanning for unknown machines using nmap • The tables were well-organized, easy to navigate, concise, and utilized appropriate terminology. • The entry provides a detailed description of the system's purpose, functionality, and interaction with hardware components, showcasing a clear understanding of the infrastructure.The exhaustive list of assets, operating systems, IP addresses, ports, and services indicates meticulous documentation and a strong grasp of the system's architecture. A wide range of vulnerabilities was identified and addressed with specific, actionable mitigations. The emphasis on adhering to best practices (e.g., the principle of least privilege) demonstrates a robust approach to security. Acknowledging the trade-off between usability and security needs shows a practical understanding of real-world system management challenges.	• You would not address senior leadership saying we did a simple google search to find a hardening checklist. Your are suppose to be Cyber experts. And don't say next time we will use AI to come up with a checklist. • Why did you list the active directory server as DNS server. It is much more. • Needed a legend and better detail on the network diagram • There were a lot more vulnerabilities • Know and explain why each step you took is important. • Would have been good to talk to the steps you used to harden the system that you found online. • I recommend explicitly referencing the specific steps taken to address identified issues, along with the tools utilized in the System Hardening section. It may be beneficial to mention the open-source tools employed and their contributions to enhancing system security. • Some vulnerability descriptions lack sufficient context or technical detail. For instance, the entry mentions "insecure password" without elaborating on how it was identified (e.g., was it weak, default, or reused?).While many mitigations are listed, the reasoning behind prioritizing certain vulnerabilities over others is not explicitly stated. Including this rationale would provide insight into the decision-making process.While the entry prudently avoids reliance on immature AI tools, a discussion of potential future AI-based hardening techniques (and safeguards against their misuse) could add depth and forward-thinking appeal.While usability trade-offs are mentioned, specific examples of how they were balanced with

	security measures would make this more compelling.

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	668

Strong Points	*Areas of Improvement*
• The team demonstrated commendable effectiveness in maintaining consistent terminology throughout the discussion of business concerns, risks, and recommendations, which enhanced the clarity of the presentation. • VERY good strategies. Including a recovery plan is important, considering what the C-suite is likely going through right now. They relate well to business risks. • Presentation was professional and topics were addressed as well as recommendations. • Well detailed risks, response strategies, and recommendations across the board. Strong bottom-line risks presented up front, as well as "cost of non-compliance" explanation	• I suggest that the presenters enable their video feeds to evaluate their professional attire during the presentation. Furthermore, I recommend minimizing the use of technical jargon in the business concerns section and placing greater emphasis on effectively addressing the impact on customers. Additionally, it would be beneficial to discuss the costs associated with each recommendation. • Provide cost estimates for your high priority actions • no comment • Overall, presentation could benefit from more energy at the beginning of presentation and fiscal cost associated to risk and 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
0	50	50	25	50	0	25	25	0	75

Whack a Mole	
WAM1	WAM2
375	281

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
1398