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

UNIVERSITY OF ARKANSAS

NOTORIOUS P.I.G.

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 59 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	258	25.80%	85
C-Suite Panel	583	58.30%	88
Red Team	1188	47.52%	51
Blue Team	1795	89.75%	61
Green Team Surveys	60	4.00%	81
Deductions	0		
Overall	**4476**	**44.76%**	**81**

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
2	yes
3	yes
4	yes
5	yes
6	yes
7	yes
8	yes
9	yes
10	yes
11	no
12	Not Answered
13	yes
14	yes
15	yes
16	yes
17	yes
18	yes
19	yes
20	Not Answered
21	yes
22	yes
23	Not Answered
24	no
25	Not Answered
26	Not Answered

27	Not Answered
28	yes
29	Not Answered
30	Not Answered
31	Not Answered
32	Not Answered
33	Not Answered
34	yes
35	Not Answered
36	Not Answered
37	no
38	yes
39	yes
40	Not Answered
41	Not Answered
42	Not Answered
43	Not Answered
44	Not Answered
45	Not Answered
46	Not Answered
47	Not Answered
48	Not Answered
49	Not Answered
50	yes
51	yes
52	yes

53	Not Answered
54	no
55	yes
56	no
57	yes
58	no
59	yes
60	no
61	yes
62	yes
63	no
64	no
65	Not Answered
66	Not Answered
67	Not Answered
68	Not Answered
69	Not Answered
70	Not Answered
71	Not Answered
72	Not Answered
73	Not Answered
74	Not Answered
75	Not Answered
76	yes
77	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	258

Strong Points	*Areas of Improvement*
• Thank you for competing and this documentation is one of the hardest parts. • Great start to understanding the network. • Most of the assets were present • The network diagrams incorporate the majority of the key components.	• There were a significant amount of data missing from the documentation. • Review your documentation to make sure that everything is placed correctly. • I recommend organizing each service into its own row to clearly delineate which services correspond to which ports. Additionally, I suggest extending the network output from the router to minimize confusion, as it appears that these may represent different subnets. I recommend making sure all sections have been completed before submitting documents. • The team could significantly improve the quality of their presentation in the future by ensuring all required details are thoroughly addressed as per the questions outlined in the security document. A more comprehensive approach, including multiple relevant diagrams and detailed explanations, would enhance clarity and enable a proper evaluation.

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	583

Strong Points	*Areas of Improvement*
• A strength of this entry was the characterization of business impacts. 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. • The team effectively established a link between risk and probability with respect to business impacts, thereby illustrating	• This presentation could have been improved by using extra practice. Submitting the video with included cuts and resets served as a distraction from the intent of the simulated exercise. Retakes are certainly acceptable, however, this entry could have benefitted from additional refinement. • The contributions of all team members were not clearly identified. Additionally,

the importance of investing in the recommendations. I believe this approach will assist leadership in the decision-making process. • Good job providing cost estimates • Good explanation of major system vulnerabilities, importance of of measures, and cost associated to vulnerability mitigations	there were some audio issues, and certain editing elements were overlooked at the beginning, which affected the coherence of the initial scene. The overall length of the video exceeded the time limit. It is important to adhere to the strict time limits set during meetings with leadership, as exceeding the allocated time may result in agenda items being postponed to a later date, which may not be possible. • How do your strategies reduce your specific business risks? How do those tie to your immediate high priority actions? • Ensure ample time for video edit and or proper transition between presenters; presenters broke composure and distraction arose from confusion of who was briefing next

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	25	25	50	50	0	50

Whack a Mole	
WAM1	WAM2
187	375

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
1395	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
60