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

BINGHAMTON UNIVERSITY

BINGHAMTON BEARCATS

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 73 SCORECARD

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

Score Category	Team Points	Percent of Points	Team Ranking
Anomalies	390	19.50%	81
Security Documentation	638	63.80%	74
C-Suite Panel	812	81.20%	56
Red Team	863	34.52%	72
Blue Team	1748	87.40%	66
Green Team Surveys	770	51.33%	71
Deductions	0		
Overall	**5221**	**52.21%**	**71**

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	390

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	Not Answered
12	Not Answered
13	yes
14	yes
15	yes
16	yes
17	no
18	Not Answered
19	Not Answered
20	Not Answered
21	yes
22	Not Answered
23	Not Answered
24	no
25	Not Answered
26	Not Answered
27	Not Answered
28	Not Answered
29	Not Answered
30	Not Answered
31	no
32	Not Answered
33	Not Answered
34	Not Answered
35	Not Answered
36	Not Answered
37	no
38	Not Answered
39	Not Answered
40	yes
41	Not Answered
42	Not Answered
43	Not Answered
44	Not Answered
45	Not Answered
46	yes
47	no
48	yes
49	Not Answered
50	yes
51	yes
52	yes
53	Not Answered
54	Not Answered
55	yes
56	yes
57	yes
58	no
59	yes
60	yes
61	yes
62	yes
63	yes
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	Not Answered
77	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	638

Strong Points	*Areas of Improvement*
• Great job on identifying services and ports with multiple open-source tools, and your focus on system hardening tools adds an extra layer of security! • Your team has a good understanding of the network, • Asset inventory was well documented. • Well defined and asset list and network diagram • Asset detail identification & network mapping	• double-checking the port-to-service mapping could enhance accuracy, as one of the ports was matched to an incorrect service. This added verification will make your results even more reliable. • The vulnerabilities and system hardening where lacking. • The system overview would benefit from further elaboration to clarify the architecture and purpose. Additionally, the network diagram is missing some identified components. The section on known vulnerabilities requires considerable improvement, as it currently lists minimal vulnerabilities with even fewer mitigations suggested. • Describe how the system and its asset relates to the business. Be mindful of professional formatting. Provide greater vulnerability and mitigation detail • Be mindful of professional formatting (blank table rows). More fully relate system & assets to the business

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	812

Strong Points	*Areas of Improvement*
• Recommended actions were limited to 3 highest priority items and discussion seemed to convey an understanding that went farther than the words spoken. • Good selection of open source tools • This entry appropriately characterized the business risks, consequences, and high priority actions. These elements are important because they align to what real-	• Additional risk analysis or linking of risk likelihood or impact being reduced by the recommended actions. • Don't include your school and mascot. Strategy is only short-term incident response, but should include longer-term business continuity strategies • This entry could have been by the speakers by increasing the professionalism - e.g., wearing business

world senior management would seek to understand. • All presenters were appropriately attired and refrained from reading directly from the slides. • The introduction was really clear -it summarized the scenario in a way that contributed to continuity throughout the presentation. • Good high priority action items. • Good spelling out of acronyms on the slide. Spelling out acronyms on a slide, instead of writing them on the slide keeps the presentation moving, which is appreciated by any audience. •	attire, finding environments to record in that better reflect a corporate environment, and working on their transitions between speakers. These elements don't change the technical content of the information, but they do enable it to be better received. • I recommend utilizing slide layouts, shapes, and colors to effectively highlight key points. It would be beneficial to avoid using single bullet points to emphasize multiple items. Additionally, the presentation exceeded the allotted time, which can disrupt the agenda and hinder other groups from sharing important information. Please strive to adhere more closely to the designated time limits. It may also be prudent to minimize technical jargon when discussing the costs of recommendations, as C-suite executives may not be familiar with the concept that open-source software is often available at no cost. • After watching your presentation, I picked up on a couple of things you may want to consider in future presentations. • You may want to consider including information loss in the "Risk of not Following Recommendations". If PII or other sensitive information is released, there is the potential for legal consequences. • May consider pausing for a minute at the end for the c-suite to ask questions. •

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	0	0	25	50	50	0	0	0	100

Whack a Mole	
WAM1	WAM2
93	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
1580	168

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
770