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

UNIVERSITY OF NORTH CAROLINA AT CHARLOTTE

49TH SECURITY DIVISION

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 3 SCORECARD

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

Score Category	Team Points	Percent of Points	Team Ranking
Anomalies	738	36.90%	35
Security Documentation	761	76.10%	64
C-Suite Panel	625	62.50%	83
Red Team	1175	47.00%	53
Blue Team	2000	100.00%	1
Green Team Surveys	1269	84.60%	45
Deductions	0		
Overall	**6568**	**65.68%**	**45**

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	738

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

1	yes		27	Not Answered		53	no
2	yes		28	no		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	no		63	yes
12	yes		38	Not Answered		64	no
13	yes		39	no		65	Not Answered
14	yes		40	no		66	yes
15	yes		41	Not Answered		67	Not Answered
16	yes		42	Not Answered		68	Not Answered
17	yes		43	yes		69	Not Answered
18	yes		44	yes		70	Not Answered
19	yes		45	yes		71	Not Answered
20	no		46	yes		72	Not Answered
21	yes		47	yes		73	Not Answered
22	Not Answered		48	no		74	Not Answered
23	yes		49	no		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	761

Strong Points	*Areas of Improvement*
• Well designed network diagram. • Good list of hardening approaches and overview of enterprise • The system overview and hardening tactics are very well explained for senior leadership • System hardening was quite in depth and detailed.	• Did not detect all vulnerabilities. System hardening could be formatted in a more readable format, perhaps using bullets to identify steps. Or creating new paragraphs for steps. • Found only some of the vulnerabilities on some of the systems • The document is poorly formatted, with entire blank pages between document sections. Please revise before submission! • Known vulnerabilities should have included all servers.

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	625

Strong Points	*Areas of Improvement*
• Good job of estimating costs for actions • The visual material was helpful in keeping the audience engaged. • The presentation was well-paced, clear, and concise. • The short-term actions were clearly presented.	• Don't use phrases such as "strong" policies. What kind of policies? What will the impact be? • Further coverage of the government as a client and the financial risks associated with this cyber attack. Overall, very good job by both presenters and the team who helped create this material. • The video could have concluded perfectly at the 5 minute mark by simply opening the floor for questions after Diego finished explaining the future dangers. Additionally, Matt's comment in the end was a bit distracting. Lastly, the second slide was not needed since team members were already introduced or mentioned on the first slide. Aside from all those few points you both did very well with not including 'umms' and 'ahhs' during your presentation.

	• By focusing primarily on business issues that the C-suite is interested in.

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 point*s. 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
100	100	75	100	75	100	75	100	0	0

Whack a Mole	
WAM1	WAM2
0	0

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
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

1269