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

UNIVERSITY OF NORTH GEORGIA

UNG CYBERHAWKS

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 86 SCORECARD

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

Score Category	Team Points	Percent of Points	Team Ranking
Anomalies	537	26.85%	71
Security Documentation	291	29.10%	84
C-Suite Panel	670	67.00%	77
Red Team	1956	78.24%	8
Blue Team	1980	99.00%	38
Green Team Surveys	487	32.47%	55
Deductions	0		
Overall	**5921**	**59.21%**	**55**

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	537

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

1	yes		27	Not Answered		53	no
2	yes		28	yes		54	yes
3	yes		29	Not Answered		55	yes
4	yes		30	Not Answered		56	yes
5	yes		31	Not Answered		57	yes
6	no		32	Not Answered		58	yes
7	yes		33	yes		59	yes
8	yes		34	Not Answered		60	no
9	yes		35	Not Answered		61	yes
10	yes		36	Not Answered		62	yes
11	no		37	yes		63	no
12	Not Answered		38	yes		64	yes
13	yes		39	Not Answered		65	Not Answered
14	no		40	yes		66	no
15	no		41	Not Answered		67	Not Answered
16	Not Answered		42	Not Answered		68	Not Answered
17	Not Answered		43	Not Answered		69	Not Answered
18	Not Answered		44	Not Answered		70	Not Answered
19	Not Answered		45	Not Answered		71	Not Answered
20	Not Answered		46	yes		72	Not Answered
21	yes		47	no		73	Not Answered
22	Not Answered		48	yes		74	Not Answered
23	Not Answered		49	yes		75	Not Answered
24	Not Answered		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	291

Strong Points	*Areas of Improvement*
• Great job providing something to get scored. • Thank you for competing in Cyberforce. • Your system overview provided good descriptions of what was going on in each machine. • A good system overview was provided.	• There is a template that is provided that gives a great base start and just need information filled in. • did not use template • you list a lot of ports per host but only provide 1 service • missing known vulnerabilities and system hardening • Your map diagram should have been created off of your Asset Inventory, you had the IP addresses of all of the machines and their OS, not sure why you didn't add it to the map. Even though you were missing parts of your report, what you did have should have been presented in the most professional format possible. (some points are better than none points) • A device was missing from the asset list and network diagram. • Vulnerabilities and hardening steps were not mentioned or listed at all. It appears as though the documentation was unfinished when submitted.

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	670

Strong Points	*Areas of Improvement*
• I think the strongest point of this presentation was the high priority recommendations - creating a BCP, changing access information, and updating all systems are quick and efficient ways to safeguard the network for relatively low cost. • The wrap up at the end was nicely done and helped convey the points better.	• I think a little more rehearsing would have helped the flow of the presentation - no one introduced the team and it was a little hard to hear and absorb the information. Maybe utilizing visuals would have helped to drive home some of the points. • Relationship for why you have the strategies to reduce risks. • Creating a visual aids, slides or other screen materials during presentation is

• The team did not create any visual aids, slides or other screen materials that can connect the audience to the presentation that can help them retain what was been presented or even help them to know the areas to ask questions or seek more clarification. • All members participated in the presentation	highly recommendable and important in presentations. Because it does not help only you the presenter, but also helps your audience to connect to the topic of discussion, helping them to stay focus, retain what was been presented as well as to know the areas to ask questions or seek more clarification. • There was no slide deck that i was able to see.

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
75	75	75	100	100	75	100	100	50	100

Whack a Mole	
WAM1	WAM2
281	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	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	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
487