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

DRURY UNIVERSITY

PANTHERGUARD

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 66 SCORECARD

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

Score Category	Team Points	Percent of Points	Team Ranking
Anomalies	527	26.35%	73
Security Documentation	845	84.50%	46
C-Suite Panel	807	80.70%	59
Red Team	881	35.24%	71
Blue Team	1708	85.40%	66
Green Team Surveys	1472	98.13%	51
Deductions	0		
Overall	**6240**	**62.40%**	**51**

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	527

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

1	yes	27	Not Answered	53	yes
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	no
9	yes	35	Not Answered	61	yes
10	yes	36	yes	62	yes
11	Not Answered	37	yes	63	yes
12	yes	38	Not Answered	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	yes	42	no	68	Not Answered
17	yes	43	no	69	Not Answered
18	yes	44	Not Answered	70	no
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	Not Answered	49	Not Answered	75	Not Answered
24	Not Answered	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	845

Strong Points	*Areas of Improvement*
• The network diagram is technically sound, showcasing a clear and logical design. Furthermore, the asset inventory list is thorough. • The hardening strategy is detailed and layered • Excellent job identifying and listing vulnerabilities. Thorough and detailed steps and justification for hardening. • You did a really good job with the asset inventory.	• System hardening provides an opportunity for improvement, particularly in comprehensiveness and technical soundness. A more robust justification for the team's actions is essential to ensure a methodical approach aligned with best practices. • Your network diagram includes main servers but lacks detail in logical structure and connections • Be more specific during overview on what each system does. Fix formatting of asset list to be more concise and less lengthy. • The System Hardening section contains terms such as "should be", "can be". It is not clear what is theoretical, and what was actually done.

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	807

Strong Points	*Areas of Improvement*
• The presentation was professional and well put together making it easy to follow. The change in speakers helps keep the audience engaged. • I like how all presenters had a consistent background and not much jargon. • Good depth for a C-suite presentation • Clear and concise, great job getting right to the point and delivering the information. You also used good examples to explain your actions so the C-Suite can understand.	• Some speakers spoke quickly and seemed to be reading from a script. I recommend practicing with bullets to help keep you on track without reading what you want to say. Overall, well done! • Make the presentation more engaging. I can tell you all are just reading from a script. The overall message I got was the plan was to create a plan. Give me specifics for the compliance agencies that oversee the organization. Give me NIST guidelines and why. Also, do not put your LinkedIn in the video. We now know who your school is.

	• Focus seems to be on monitoring, not much on hardening or how to mitigate the existing breaches • Remember this is your C-Suite, go out of your way to make it easy for them to follow up. Telling your CEO or COO to contact you through linkedin is not the way.

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	50	25	0	0	0	50	0	25

Whack a Mole	
WAM1	WAM2
0	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	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	108

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
1472