DRURY UNIVERSITY

PANTHERWATCH

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 29 SCORECARD

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

Score Category	Team Points	Percent of Points	Team Ranking
Anomalies	525	26.25%	74
Security Documentation	920	92.00%	21
C-Suite Panel	756	75.60%	72
Red Team	1850	74.00%	14
Blue Team	1970	98.50%	45
Green Team Surveys	1469	97.93%	19
Deductions	0		
Overall	7490	74.90%	19

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	525

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

1	yes	27	no	53	no
2	yes	28	Not Answered	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	no	60	no
9	yes	35	Not Answered	61	yes
10	yes	36	yes	62	yes
11	no	37	no	63	yes
12	Not Answered	38	Not Answered	64	yes
13	yes	39	no	65	Not Answered
14	yes	40	no	66	Not Answered
15	yes	41	yes	67	Not Answered
16	yes	42	Not Answered	68	Not Answered
17	yes	43	Not Answered	69	Not Answered
18	yes	44	Not Answered	70	yes
19	yes	45	no	71	no
20	Not Answered	46	no	72	no
21	no	47	yes	73	Not Answered
22	Not Answered	48	yes	74	Not Answered
23	no	49	yes	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	920

Strong Points	Areas of Improvement
• Great job on creating a clean and clear network diagram, along with nicely stated vulnerabilities. • Excellent identification of the vulnerabilities • Justified hardening steps for vulnerabilites; clear language throughout • 1. You provided a very detailed summary of Known Vulnerabilities. You took the time to prioritized remediation based on the risk level / criticality of each security weakness. • 2. Your System Hardening summary is excellent. It is very well organized per area, easy to read, and detailed. It shows both a technical expertise in vulnerability and configuration management area, and in your ability to present technical information in clear and organized manner.	• Refining the vulnerability details to align to senior leadership's perspective would enhance clarity, and a thorough check of port-to-service mapping would improve accuracy. • Missed the Map Box on the network diagram. • Can add arrows/color to diagram; small formatting issues (extra blank page at the end, document was landscape) • I did not find any areas that can be improved. It is a very well prepared document.

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	756

Strong Points	Areas of Improvement
•	•

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
50	50	50	75	50	25	75	75	100	100

Whack a Mole	
WAM1	WAM2
375	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
1570	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
1469