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

TEXAS A&M UNIVERSITY

RET2REV

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 81 SCORECARD

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

Score Category	Team Points	Percent of Points	Team Ranking
Anomalies	800	40.00%	28
Security Documentation	931	93.10%	15
C-Suite Panel	932	93.20%	10
Red Team	1444	57.76%	38
Blue Team	1975	98.75%	42
Green Team Surveys	1186	79.07%	26
Deductions	0		
Overall	**7268**	**72.68%**	**26**

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	800

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

1	yes	27	Not Answered	53	yes
2	yes	28	no	54	yes
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	yes	60	no
9	yes	35	no	61	no
10	yes	36	Not Answered	62	yes
11	Not Answered	37	yes	63	yes
12	no	38	yes	64	no
13	yes	39	yes	65	Not Answered
14	yes	40	no	66	yes
15	no	41	Not Answered	67	Not Answered
16	yes	42	Not Answered	68	yes
17	yes	43	Not Answered	69	Not Answered
18	yes	44	Not Answered	70	yes
19	yes	45	yes	71	no
20	yes	46	Not Answered	72	yes
21	no	47	Not Answered	73	Not Answered
22	yes	48	Not Answered	74	yes
23	yes	49	yes	75	Not Answered
24	no	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	931

Strong Points	*Areas of Improvement*
• Your system hardening section is well written. • Overall strong entry, known vulns section details were fantastic • The network diagram was well done and looked pleasing. • The document is easy to read, comprehensive, and shows that you understand how to describe and document systems. I really appreciate your System Hardening section, because it describes what was done, how, and why certain steps were taken. Very well done.	• Your system inventory is missing the map box, while the network diagram has it. • System Overview had strong business support explanation, but I would have liked to see more explained about how each specific VMs supports specific business functions • Make sure that the asset inventory and network diagram match up. • The document contains comments from the template, and these comments should have been removed.

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	932

Strong Points	*Areas of Improvement*
• Overall solid submission, great to see the NIST OT guidelines being suggested • Clear language was used and professionally spoken. • The team made a very professional presentation that clearly outlined their speaking points. • Slides are company branded and professional. • Jargon is avoided, yet information being presented is in-depth while still being understandable. • Recommendations were spot on.	• While I fully agree with your recommendation to firewall safety-critical systems (this is more than half of my dayjob), I would have liked to see more about how you would implement high-priority recommendations without creating a work stoppage or firewall-induced network outage. • Lacked good reasoning behind the strategy to reduce risks. • The team provided timelines but potential cost estimations would support decision making for recommendations as well. • While rapid unscheduled disassembly can be humorous, certain C-Suite members may not appreciate it.

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	100	100	50	25	100	50	25	25	0

Whack a Mole	
WAM1	WAM2
375	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
1575	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
1186