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

UNIVERSITY OF NEVADA-RENO

UNR WOLF HACK

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 90 SCORECARD

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

Score Category	Team Points	Percent of Points	Team Ranking
Anomalies	935	46.75%	16
Security Documentation	880	88.00%	33
C-Suite Panel	858	85.80%	38
Red Team	1750	70.00%	18
Blue Team	2000	100.00%	1
Green Team Surveys	1445	96.33%	10
Deductions	0		
Overall	**7868**	**78.68%**	**10**

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	935

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

1	yes	27	Not Answered	53	Not Answered
2	yes	28	Not Answered	54	yes
3	yes	29	Not Answered	55	yes
4	yes	30	Not Answered	56	no
5	yes	31	no	57	no
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	no	37	yes	63	yes
12	yes	38	Not Answered	64	no
13	yes	39	yes	65	no
14	yes	40	yes	66	Not Answered
15	yes	41	yes	67	Not Answered
16	yes	42	Not Answered	68	Not Answered
17	yes	43	yes	69	Not Answered
18	yes	44	Not Answered	70	yes
19	yes	45	yes	71	yes
20	yes	46	yes	72	yes
21	yes	47	no	73	Not Answered
22	yes	48	no	74	no
23	yes	49	Not Answered	75	yes
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	880

Strong Points	*Areas of Improvement*
• A strength for this entry was the compilation of vulnerabilities with an added pseudo color scheme. This added attribute, which was not prescribed, enables more efficient decision making by senior leaders. Additionally, a strong compilation of vulnerabilities will enables more effective system hardening to be completed. Well done in these attributes. • Great details added, it really shows knowledge of the material. • nice executive summary (system overview), nice vulnerability table categorized with color coding, >50 vulnerabilities identified, 20 resolved, additional 20+ mitigations identified. • over all you're your write up was well done and it was impressed that you gathered many known vulnerabilities well done • Overall, your write up was well done. Did well on hitting all aspects of Harding and finding many know vulnerabilities	• This entry could have been approved by pulling in a standardized structure to the system hardening efforts. This might include a structure such as the categories prescribed in NIST CSF 2.0 - e.g., govern, detect, protect, identify, response, recover. Doing so adds professionalism, but also better enables senior management to apply the mitigations to specific cybersecurity elements of the organization. • Ensure that there is consistency throughout the entire document. • would have been nice to see the team remove the template prompts and make the document their own. • assets inventory missing map box VM; showed mapbox in diagram when not on asset inventory; small grammar errors and not keeping same format for some words ie. Sn1per and sn1per also left an unfinished sentence or paragraph • assets inventory missing mapbox VM; showed mapbox in diagram when not on asset inventory; small grammar errors and not keeping same format for some words ie. Sn1per and sn1per also left an unfinished sentence or paragraph in section •

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	858

Strong Points	*Areas of Improvement*
• I really liked that all members of the team got a chance to present on their topics. I think the high-priority recommendations	• I think the 2 things that could be improved are 1) rehearsing the material a little more - some presenters sounded like they were

were top notch and cost effective (adjusting policies, training, and backing up systems). There was also mention of changing the security culture of the company which could help provide long-term cyber security. • Really appreciated the briefing slides. • Professional slides and good team collaboration presenting. • Great presentation and good points that you addressed	speed reading thru a script while others spoke more freely and confidently about their topic, and 2) really developing the risks related to business concerns - two of the three listed were very similar and I didn't hear much/anything about the energy availability or the AOR. • Ensure that the quality of sound and that all presenters perform at similar speeds. • Some presenters spoke pretty fast; a consistent pace sounds better • The pace between the different presenters felt weird some were going to fast and some were going to slow

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
100	50	75	50	75	0	50	50	0	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
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
1445