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

VIRGINIA TECH

ROOT@VT

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 74 SCORECARD

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

Score Category	Team Points	Percent of Points	Team Ranking
Anomalies	556	27.80%	66
Security Documentation	780	78.00%	62
C-Suite Panel	761	76.10%	71
Red Team	1013	40.52%	64
Blue Team	1474	73.70%	81
Green Team Surveys	192	12.80%	77
Deductions	0		
Overall	**4776**	**47.76%**	**77**

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	556

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

1	yes	27	no	53	no
2	yes	28	no	54	Not Answered
3	yes	29	Not Answered	55	yes
4	yes	30	no	56	no
5	yes	31	no	57	yes
6	yes	32	no	58	yes
7	yes	33	no	59	yes
8	yes	34	Not Answered	60	yes
9	yes	35	Not Answered	61	yes
10	yes	36	Not Answered	62	yes
11	no	37	yes	63	yes
12	no	38	Not Answered	64	no
13	yes	39	Not Answered	65	Not Answered
14	yes	40	Not Answered	66	Not Answered
15	yes	41	Not Answered	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	Not Answered	71	yes
20	Not Answered	46	no	72	yes
21	no	47	no	73	no
22	yes	48	no	74	yes
23	no	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	780

Strong Points	*Areas of Improvement*
• Nicely done system hardening. Good approach on addressing various vulnerabilities! • Good network diagram, list of vulnerabilities, and system hardening plan. • The asset inventory section is well executed. Great job! • Well justified hardening methodology	• Please review the service-to-port mapping to ensure each service is correctly aligned with its designated port for reliable connectivity. • Missing cover page. I did not know the team number if it wasn't for the file name. • The overview of the system would benefit from a more detailed explanation to enhance clarity regarding its purpose. Furthermore, the network diagram is lacking detail that should be included. • Relate the system and assets to the business. Ensure consistent and professional formatting.

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	761

Strong Points	*Areas of Improvement*
• The discussion about what risks would be realized from inaction was good. • Well designed slides. Clear delivery from speakers. Well researched presentation. • Great job with showing some long term recovery strategies. The way you presented them I think will go a long way with the C-Suite. • The presentation had a strong introduction that contributed to the continuity of the presentation. • The presenters all spoke clearly and there was no fumbling in either speech or with slides in the presentation. • It was great to include network segregation as a solution. It's a vital architecture in today's cybersecurity landscape.	• Additional analysis or rationale why the selected items for high priority implementation are the best choices or are best for reducing risks. • Tools mentioned verbally. Recommendation is to list tools on the slides for easier reference. States increase staff in IT Department. It may be recommended to create a separate information security department separate form IT to deal with the associated cybersecurity issues. Is there an associated estimated budget for this hiring? Social engineering not defined. May be best to frame for C-Suite as Security Awareness and/or Phishing training. Breaches listed on the last slide were not discussed. Also, recommend listing sources for these to allow viewers to

• It was great to cite other exploits in the industry- really draws the audience in.	read original sources for further details. Automated back up and recovery systems are discussed on the last slide, but no discussion of this topic is on the other slides. • When presenting to a C-Suite or board, they'll be on video and expect the same. • As I watched your presentation, I picked up a few things you may want to consider for future presentations. • Consider making more eye contact, it appeared the presenters were reading which doesn't provide a good connection to the audience. • The pictures and graphics on the slide were cool, however distracted from the information being presented. • On the "Financial Risk of this Incident" slide - client was misspelled as "cliental". A final preview of the presenting before giving it to your audience will help catch small things like like that. • Highest Priority Recommendations slide - maybe explain how the breach could be stopped by introducing network segmentation with the first bullet point, for a clearer message. IDS/IPS could had it's own bullet point so you could explain a little more about using the IPS/IDS to identify suspicious network traffic, which is critical in today's cybersecurity landscape. • May want to mention Information loss - there are laws around reporting the types of information that is compromised. In addition, if there loss of PII and/or sensitive information there could also be legal consequences. • The last bullet point on that slide is a little confusing - Update could mean many things - did you mean to say update software? It could also imply an update to factory controls systems, which is quite costly. •

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 point*s. 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	75	0	50	0	0	0	0

Whack a Mole	
WAM1	WAM2
187	0

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
1450	24

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
192