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

VIRGINIA TECH

PWN@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 70 SCORECARD

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

Score Category	Team Points	Percent of Points	Team Ranking
Anomalies	949	47.45%	15
Security Documentation	800	80.00%	59
C-Suite Panel	837	83.70%	47
Red Team	1225	49.00%	49
Blue Team	1975	98.75%	42
Green Team Surveys	624	41.60%	48
Deductions	0		
Overall	**6410**	**64.10%**	**48**

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	949

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

1	yes	27	no	53	yes
2	yes	28	no	54	yes
3	yes	29	no	55	yes
4	yes	30	Not Answered	56	no
5	yes	31	yes	57	yes
6	yes	32	yes	58	yes
7	yes	33	yes	59	yes
8	yes	34	yes	60	yes
9	yes	35	Not Answered	61	yes
10	yes	36	yes	62	no
11	no	37	no	63	yes
12	yes	38	no	64	yes
13	yes	39	no	65	Not Answered
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	no	69	Not Answered
18	yes	44	Not Answered	70	yes
19	yes	45	no	71	yes
20	Not Answered	46	yes	72	yes
21	yes	47	no	73	Not Answered
22	Not Answered	48	yes	74	yes
23	yes	49	yes	75	Not Answered
24	yes	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	800

Strong Points	*Areas of Improvement*
• Strong network diagram and Vulnerability section. • Good detail on your assets and network diagram. • Network diagram was well done. • Many vulnerabilities idenitfied with justified mitigations and hardening steps; clear diagram and legend.	• A bit more time on System Hardening and Asset Inventory would have been helpful. Still, fantastic job! • The vulnerability and system hardening needed more detail. • The sections on system hardening and known vulnerabilities need improvement. For system hardening, provide detailed steps with justifications for implementing or skipping measures. The known vulnerabilities section should identify most vulnerabilities with appropriate mitigation strategies. Present this information clearly for senior leadership, emphasizing the importance and implications for organizational security. • Missing a VM in assets; unclear if last two hardening steps were implemented; diagram should be landscape to avoid head tilting.

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	837

Strong Points	*Areas of Improvement*
• Thorough explanation of risks and asks from management • The team slides were clear and straightforward. The presenters effectively engaged the audience by not reading directly from the slides. Additionally, the presentation adhered to an acceptable time frame. • I've been assigned 9 videos to review, this was my 6th and it was easily the best so far. Excellent discussion of risks and possible mitigations. Full notes in next answer.	• What is the reference for the costs of fines and lost contracts? • I recommend refining the slides and incorporating the company logo to enhance their professional appearance. Additionally, I suggest utilizing a virtual background to minimize distractions. It would be beneficial to outline each team member's specific contributions. I also advise including detailed information on specific products and their associated costs. Currently, only one tool has been identified.

• Professional presentation with meaningful contribution from all presenters.	• REQUIRED ELEMENTS - 4/4 • RISKS TO CORE BUSINESS - 4/4 • "reduced energy delivery capacity" are you trying to say that losing contracts will hurt revenue? if so i would phrase this as "reduced demand for power". "energy delivery capacity" makes me think of the maximum energy that can be transmitted over a given set of transmission or distribution lines, which is a real concern that is distinct from what i think you're trying to say here. no point reduction just fyi. • would have liked to see specific numbers given in this section, but really really like how you broke down each risk into subrisks to effectively give me 12 risks, all well considered and presented • discussion of risk of cancelled gov contracts, but no other discussion of risk of degraded energy output (examples: 120V 60Hz signal is literally degraded, causing critical stability risk to entire bulk electric sytem; many industrial processes would have to be restarted from scratch if there is disruption of more than 15 minutes to electric power, extremely expensive in time and resources; injury/loss of life due to lack of power) • minimal jargon • STRATEGY TO REDUCE RISKS - 3/4 • strategy is excellent, but no direct connection back to risks just presented • HIGH PRIORITY RECOMMENDATIONS - 3/4 • +1 for RBAC, gonna be an ongoing effort but one month is reasonable for first pass. not requiring a tool for this one because "make sure AD is well configured" is enough of a hurdle on its own, but consider tools like bloodhound to aid this analysis • enhance threat detection and monitoring is good, no tools given • security awareness training is good, but where is that $2K estimate coming from? that's two weeks of a $50K worker's time, which makes sense, but if that's where the number comes from give that at the bottom of the slide, or cite your source. also, no security awareness tool was given,

	which seems to imply this will all be done in house. this can be done, but there are enough resources available nowadays that I think it's cost-effective for most companies to pay a 3rd party. • regular ongoing vulnerability assessments - again, good idea, but just because a vuln assessment tool is free doesn't mean the assessment is free. at minimum, you're going to have to pay an employee to run nmap/Metasploit scans and interpret the results; realistically, you're gonna hire a 3rd party. free tools like openVAS given • NEXT SLIDE: okay i'm giving you a point for identifying the need for additional workers, which addresses my main complaint with the prior item. you also call out security onion, openVAS, and wazuh here. all are good tools but i would have liked to see you discuss SO and Wazuh more, probably in the High Priority Recommendations section. • QUALITY - 4/4 • audio quality for christopher is spotty but workable • OVERALL - excellent, excellent presentation with minimal concerns, which are highlighted above • More clearly provide long-term strategy/policy recommendations that directly relate to the identified business risks.

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	25	100	100	25	0	50	0	50	50

Whack a Mole	
WAM1	WAM2
375	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
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
624