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

# OAKLAND UNIVERSITY

## CYBEROU

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 30 SCORECARD

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

| Score Category | Team Points | Percent of Points | Team Ranking |
|---|---|---|---|
| Anomalies | 295 | 14.75% | 87 |
| Security Documentation | 755 | 75.50% | 65 |
| C-Suite Panel | 808 | 80.80% | 58 |
| Red Team | 1231 | 49.24% | 48 |
| Blue Team | 1818 | 90.90% | 57 |
| Green Team Surveys | 102 | 6.80% | 74 |
| *Deductions* | 0 | | |
| Overall | **5009** | **50.09%** | **74** |

## 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 | 295 |
|---|---|

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

| | | | | | |
|---|---|---|---|---|---|
| 1 | yes | 27 | no | 53 | Not Answered |
| 2 | yes | 28 | Not Answered | 54 | Not Answered |
| 3 | yes | 29 | Not Answered | 55 | yes |
| 4 | yes | 30 | Not Answered | 56 | yes |
| 5 | yes | 31 | Not Answered | 57 | yes |
| 6 | yes | 32 | Not Answered | 58 | yes |
| 7 | yes | 33 | Not Answered | 59 | yes |
| 8 | yes | 34 | Not Answered | 60 | no |
| 9 | no | 35 | Not Answered | 61 | yes |
| 10 | yes | 36 | no | 62 | yes |
| 11 | no | 37 | no | 63 | yes |
| 12 | no | 38 | Not Answered | 64 | yes |
| 13 | yes | 39 | no | 65 | Not Answered |
| 14 | yes | 40 | no | 66 | no |
| 15 | yes | 41 | Not Answered | 67 | Not Answered |
| 16 | no | 42 | Not Answered | 68 | Not Answered |
| 17 | no | 43 | Not Answered | 69 | Not Answered |
| 18 | yes | 44 | Not Answered | 70 | no |
| 19 | Not Answered | 45 | Not Answered | 71 | Not Answered |
| 20 | Not Answered | 46 | Not Answered | 72 | Not Answered |
| 21 | yes | 47 | Not Answered | 73 | Not Answered |
| 22 | Not Answered | 48 | Not Answered | 74 | Not Answered |
| 23 | yes | 49 | Not Answered | 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 | 755 |
|---|---|

| *Strong Points* | *Areas of Improvement* |
|---|---|
| • Asset inventory is thorough, with accurate identification of ports and services, and the network diagram is clear and well-organized.<br>• Your system overview was at the appropriate technical level and well written.<br>• Great job with identifying vulnerabilities and providing a solid asset inventory!<br>• A strong point of this entry is the detailed description of security hardening practices, including the use of specific tools like nmap for port scanning and various malware detection tools (e.g., ClamAV, Lynis, Linux Malware Detect) for different Linux distributions. This demonstrates an in-depth understanding of both general and targeted security measures for system protection and network hardening. | • System hardening could be further enhanced to strengthen security and reduce potential vulnerabilities.<br>• When listing assets, there are many more services that should be noted.<br>• Refine your network diagram with clearer logical connections, add detail to the system overview for executive clarity, expand on vulnerabilities identified, and enhance document professionalism and formatting.<br>• The entry could be improved by providing more context about the AWS network configuration and how it optimally supports the windmill system, particularly what specific AWS services or features are leveraged and why they are well-suited for the operational needs. Additionally, it would be beneficial to detail any monitoring practices or alert systems in place, as well as any routine maintenance checks beyond initial hardening, to provide a fuller picture of the ongoing security strategy. |

### 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 | 808 |
|---|---|

| *Strong Points* | *Areas of Improvement* |
|---|---|
| • Presentation of data was exceptional. Each slide was clear, concise, and contained relevant and impactful information. The cybersecurity roadmap was a great way to present a timeline, and the timeline was very realistic. The costs of taking no action were clear and impactful.<br>• Nice job elaborating the business risks. | • I would recommend an agenda or overview before getting into the content.<br>• The strategy and high priority recommendations needed more work and tie-in with the business risks.<br>• The discussion of risks was technical and needed to be re-worked for a broader, less technically advanced audience. |

| | |
|---|---|
| • Highlighting the cost of inaction was a good thing.<br>• The table and the roadmap was a really great addition to the presentation and it represented the content well. | • The only minor distraction was the notification sound, but you did an excellent job staying focused and continuing the presentation without letting it affect you. |

## 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 | 50 | 0 | 25 | 0 | 0 | 0 | 50 | 0 | 0 |

| Whack a Mole | |
|---|---|
| WAM1 | WAM2 |
| 281 | 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 |
|---|---|
| 1450 | 368 |

## 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 |
| --- |
| 102 |