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

DEFENDING U.S. ENERGY INFRASTRUCTURE

# UNIVERSITY OF ILLINOIS URBANA-CHAMPAIGN

## SIGPWNY

### 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 79 SCORECARD

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

| Score Category | Team Points | Percent of Points | Team Ranking |
|---|---|---|---|
| Anomalies | 844 | 42.20% | 23 |
| Security Documentation | 927 | 92.70% | 16 |
| C-Suite Panel | 765 | 76.50% | 69 |
| Red Team | 775 | 31.00% | 75 |
| Blue Team | 1800 | 90.00% | 59 |
| Green Team Surveys | 1019 | 67.93% | 52 |
| *Deductions* | 0 | | |
| Overall | **6130** | **61.30%** | **52** |

## 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** | 844 |

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

| | |
|---|---|
| 1 | yes |
| 2 | yes |
| 3 | yes |
| 4 | yes |
| 5 | yes |
| 6 | yes |
| 7 | yes |
| 8 | yes |
| 9 | yes |
| 10 | yes |
| 11 | no |
| 12 | Not Answered |
| 13 | yes |
| 14 | yes |
| 15 | yes |
| 16 | yes |
| 17 | yes |
| 18 | yes |
| 19 | yes |
| 20 | Not Answered |
| 21 | no |
| 22 | yes |
| 23 | Not Answered |
| 24 | no |
| 25 | Not Answered |
| 26 | Not Answered |
| 27 | Not Answered |
| 28 | no |
| 29 | no |
| 30 | Not Answered |
| 31 | Not Answered |
| 32 | Not Answered |
| 33 | Not Answered |
| 34 | yes |
| 35 | Not Answered |
| 36 | Not Answered |
| 37 | yes |
| 38 | yes |
| 39 | yes |
| 40 | yes |
| 41 | Not Answered |
| 42 | Not Answered |
| 43 | no |
| 44 | yes |
| 45 | yes |
| 46 | yes |
| 47 | no |
| 48 | yes |
| 49 | yes |
| 50 | yes |
| 51 | yes |
| 52 | yes |
| 53 | Not Answered |
| 54 | Not Answered |
| 55 | yes |
| 56 | no |
| 57 | yes |
| 58 | yes |
| 59 | yes |
| 60 | yes |
| 61 | yes |
| 62 | yes |
| 63 | yes |
| 64 | yes |
| 65 | Not Answered |
| 66 | yes |
| 67 | Not Answered |
| 68 | Not Answered |
| 69 | Not Answered |
| 70 | Not Answered |
| 71 | Not Answered |
| 72 | Not Answered |
| 73 | Not Answered |
| 74 | Not Answered |
| 75 | yes |
| 76 | yes |
| 77 | 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** | 927 |

| *Strong Points* | *Areas of Improvement* |
|---|---|
| • This was a very strong and comprehensive document.<br>• Great hardening steps to make the system overall secure.<br>• I like how you had a separate table for critical ports and services<br>• Logical and well formatted network diagram.<br>• Your System Hardening summary is excellent. It is very well organized per area, easy to read, and detailed. It shows both a technical expertise in vulnerability and configuration management area, and in your ability to present technical information in clear and organized manner. | • More professional language (e.g. "we will" instead of "we'll").<br>• There should be justification for why each hardening step was taken, not just listing out what happened but why it happened.<br>• More detail and understanding of the overall system was needed. when you list the ports and services in separate columns they should be on separate lines. Assume I don't know what port matches what service. That is confusing to senior leadership.<br>• Address senior leadership (non-technical, business people) more directly - avoid jargon, and shorten long sentences. Include all devices in the asset inventory<br>• Your Known Vulnerabilities table contains a good amount of identified vulnerabilities. However, when compared to your System Hardening summary, it looks like you did not listed all Known Vulnerabilities that you found. |

### 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** | 765 |

| *Strong Points* | *Areas of Improvement* |
|---|---|
| • A strong element of this entry was the talking points emphasizing considerations surrounding business risks and consequences. These are topics that directly impact companies before, during, and after real-world events. Also, the recommendations identified by the team remain equally impactful to the stakeholders<br>• Slides are clear. | • One element of this entry that could have been improved were the visual aspects of the submission. Consider that the slide content is already presented across the video, doing so again behind the presenter at the cost of actually seeing the team members offers low returns. Also, the video was clipped together as opposed to recorded in a single take, as would be reflective of a realistic meeting with senior management. |

| | |
|---|---|
| • Risks were clearly outlined, and financial risks were mentioned.<br>• The presentation overall was very professional.<br>• Clear strategy and recommendations to carry out.<br>• Good understanding and presentation on the "Understanding the Risks..." slide | • Video addresses recommendations and reasoning, but unclear what the strategy is.<br>• The strategy did not directly address the risks mentioned. They were related, but it was not stated how the strategy addressed those risks.<br>• Provide reasoning on why recommended priorities should be implemented. What is the ROI? What happens if I don't implement each priority? A general risk of failing to improve security was discussed, but nothing directly related to each priority.<br>• There has to be continuity between the risks and long-term strategy.<br>• You may want to consider another word besides "Failure" on the Improve Security posture. slide.<br>• You may want to think about if the High Priority Recommendations are appropriate for the C-Suite.<br>• |

## 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 | 100 | 75 | 0 | 0 | 0 | 0 | 0 | 100 |

| Whack a Mole | |
|---|---|
| WAM1 | WAM2 |
| 0 | 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 |
|---|---|
| 1400 | 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 |
|---|
| 1019 |