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

# WESTERN WASHINGTON UNIVERSITY

## CASCADIA CYBER SENTINELS

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 14 SCORECARD

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

| Score Category | Team Points | Percent of Points | Team Ranking |
|---|---|---|---|
| Anomalies | 841 | 42.05% | 25 |
| Security Documentation | 740 | 74.00% | 67 |
| C-Suite Panel | 887 | 88.70% | 26 |
| Red Team | 2000 | 80.00% | 6 |
| Blue Team | 1995 | 99.75% | 26 |
| Green Team Surveys | 843 | 56.20% | 22 |
| *Deductions* | 0 | | |
| Overall | **7306** | **73.06%** | **22** |

## 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 | 841 |
|---|---|

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

| | | | | | |
|---|---|---|---|---|---|
| 1 | yes | 27 | no | 53 | yes |
| 2 | yes | 28 | Not Answered | 54 | Not Answered |
| 3 | yes | 29 | Not Answered | 55 | no |
| 4 | yes | 30 | Not Answered | 56 | yes |
| 5 | yes | 31 | yes | 57 | yes |
| 6 | yes | 32 | yes | 58 | yes |
| 7 | yes | 33 | yes | 59 | yes |
| 8 | yes | 34 | yes | 60 | no |
| 9 | yes | 35 | yes | 61 | yes |
| 10 | yes | 36 | yes | 62 | yes |
| 11 | no | 37 | yes | 63 | yes |
| 12 | yes | 38 | Not Answered | 64 | yes |
| 13 | yes | 39 | yes | 65 | no |
| 14 | no | 40 | yes | 66 | yes |
| 15 | no | 41 | no | 67 | Not Answered |
| 16 | no | 42 | Not Answered | 68 | Not Answered |
| 17 | no | 43 | no | 69 | Not Answered |
| 18 | yes | 44 | Not Answered | 70 | no |
| 19 | no | 45 | yes | 71 | Not Answered |
| 20 | no | 46 | yes | 72 | Not Answered |
| 21 | yes | 47 | no | 73 | Not Answered |
| 22 | yes | 48 | yes | 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 | 740 |
|---|---|

| *Strong Points* | *Areas of Improvement* |
|---|---|
| • The network diagram was done professionally.<br>• The team provided a detailed asset inventory with all relevant information, including hostnames, IP addresses, ports, and services. Their network diagram was well-structured, visually clear, and included a legend, making it easy for anyone, including senior leadership, to understand the layout and connections within the network. The team excelled in identifying vulnerabilities, providing a comprehensive list that covered a range of issues from software misconfigurations to weak security settings.<br>• Well done diagram and asset inventory<br>• Well done on the asset list, identifying the port number and protocol. | • Inclusion of OS (e.g., instead of "Windows" do "Windows Server 2016", "Windows Server 2019", etc.) Remove instructions from template for more professional appearance.<br>• The system overview could have benefited from more transparent, straightforward language catering to a non-technical senior leadership audience. Simplifying technical jargon and focusing on high-level goals, risks, and benefits would have helped. The tables could've been organized to be more readable.<br>• System overview needs a little more detail, think of it like an executive summary. Limited response on vulnerabilities and system hardening<br>• Be more specific in system overview.<br>• Only 14 vulnerabilities were identified. There was only one hardening step mentioned, with little justification. |

### 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 | 887 |
|---|---|

| *Strong Points* | *Areas of Improvement* |
|---|---|
| • The information presented at the appropriate level for the intended audience. The content was actionable, succinct, and accurate.<br>• Loved the uniqueness of the video while keeping it professional.<br>• Initially, I was concerned that the slides would be difficult to see due to the distance. However, i appreciated how you zoomed in on each slide before bringing on the next topic. | • This presentation could have been improved by speaking versus reading the identified content. At times, this did come across scripted. As you complete these tasks in industry, the "scripted feel" will evolve into more of an informed conversation.<br>• In the reasoning, make sure to emphasize the business impact of performing different cyber techniques.<br>• no comment |

| | |
|---|---|
| • The risks caused by degraded output and outages were clearly described. | • The recommendations could have required less significant funding. |

## 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 point*s. 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 | 100 | 100 | 75 | 100 | 75 | 75 | 100 | 25 | 50 |

| 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 |
|---|---|
| 1595 | 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 |
|---|

843