



POWERED BY
CYBER SKYLINE

The National Cyber League
A Community Where Cybersecurity Is a Passion

Cedar Longballa
longbacedar@gmail.com

NCL Fall 2024 Individual Game Scouting Report

Dear Cedar Longballa,

Thank you for participating in the National Cyber League (NCL) Fall 2024 Season! Our goal is to prepare the next generation of cybersecurity professionals, and your participation is helping achieve that goal.

The NCL was founded in May 2011 to provide an ongoing virtual training ground for collegiate students to develop, practice, and validate their cybersecurity skills in preparation for further learning, industry certifications, and career readiness. The NCL scenario-based challenges were designed around performance-based exam objectives of CompTIA certifications and are aligned to the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework published by the National Institute of Standards and Technology (NIST).

As you look to a future career in cybersecurity, we hope you find this report to be valuable in both validating skills and identifying areas for improvement across the nine NCL skills categories. You can use this NCL Scouting Report to:

- Validate your skills to employers in any job application or professional portfolio;
- Show case your achievements and strengths by including the Score Card view of your performance as part of your résumé or simply sharing the validation link so that others may view the detailed version of this report.

The NCL Fall 2024 Season had 9,260 students/players and 573 faculty/coaches from more than 540 two- and four-year schools & 230 high schools across all 50 U.S. states registered to play. The Individual Game Capture the Flag (CTF) event took place from October 25 through October 27. The Team Game CTF event took place from November 8 through November 10. The games were conducted in real-time for students across the country.

NCL is powered by Cyber Skyline's cloud-based skills evaluation platform. Cyber Skyline hosted the scenario-driven cybersecurity challenges for players to compete and track their progress in real-time.



To validate this report, please access: cyberskyline.com/report/GLLF4M98DHCX

Congratulations for your participation in the NCL Fall 2024 Individual Game! We hope you will continue to develop your knowledge and skills and make meaningful contributions as part of the Information Security workforce!

Dr. David Zeichick
NCL Commissioner



POWERED BY
CYBER SKYLINE

NATIONAL CYBER LEAGUE SCORE CARD

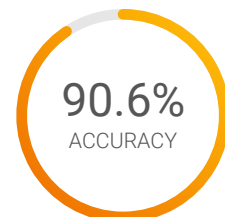
NCL FALL 2024 INDIVIDUAL GAME

YOUR TOP CATEGORIES

PASSWORD CRACKING
84TH PERCENTILE

OPEN SOURCE INTELLIGENCE
84TH PERCENTILE

NATIONAL RANK
3252ND PLACE
OUT OF 8483
PERCENTILE
62ND



Average: 67.8%

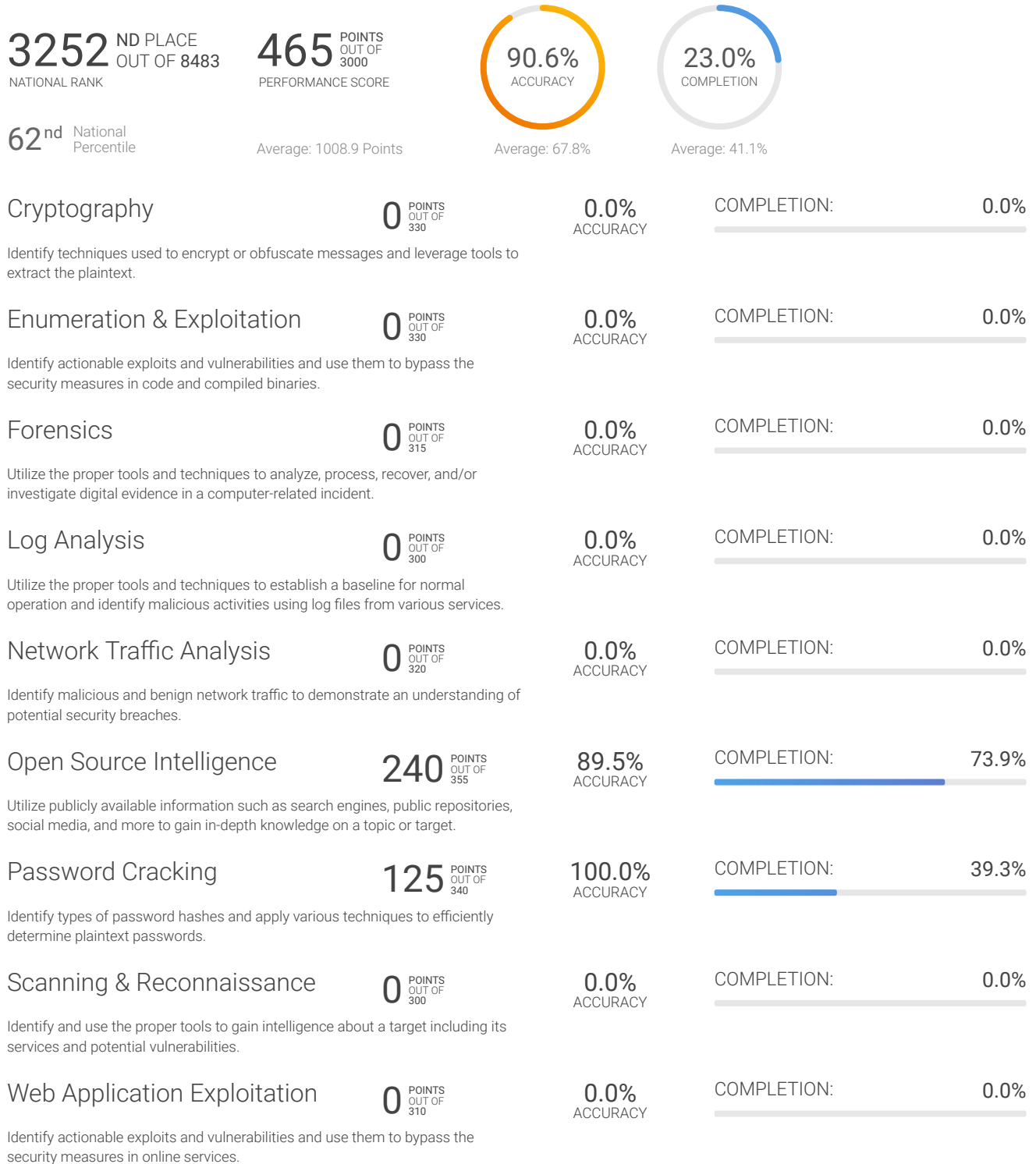
[cyberskyline.com/report](https://cyberskyline.com/report/GLLF4M98DHCX)
ID: GLLF4M98DHCX

Learn more at nationalcyberleague.org



NCL Fall 2024 Individual Game

The NCL Individual Game is designed for student players nationwide to compete in realtime in the categories listed below. The Individual Game evaluates the technical cybersecurity skills of the individual, without the assistance of others.



Note: Survey module (100 points) was excluded from this report.





Cryptography Module

Identify techniques used to encrypt or obfuscate messages and leverage tools to extract the plaintext.

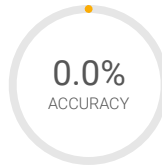
N/A

NATIONAL RANK

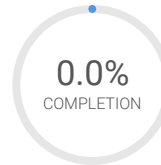
0 POINTS
OUT OF
330

PERFORMANCE SCORE

Average: 209.0 Points



Average: 72.6%



Average: 64.6%

Bases (Easy)

0 POINTS
OUT OF
30

0.0%
ACCURACY

COMPLETION: 0.0%

Analyze and obtain the plaintext from messages encoded with common number bases.

Shift (Easy)

0 POINTS
OUT OF
40

0.0%
ACCURACY

COMPLETION: 0.0%

Analyze and obtain the plaintext for a message encrypted with a shift cipher.

Number Codes (Easy)

0 POINTS
OUT OF
40

0.0%
ACCURACY

COMPLETION: 0.0%

Analyze and obtain the plaintext for a message encoded using ASCII codes.

NATO (Easy)

0 POINTS
OUT OF
40

0.0%
ACCURACY

COMPLETION: 0.0%

Analyze and obtain the plaintext for a message encoded using the NATO alphabet.

Message Signature (Medium)

0 POINTS
OUT OF
60

0.0%
ACCURACY

COMPLETION: 0.0%

Identify tampered emails by using PGP signatures.

Beep Beep (Medium)

0 POINTS
OUT OF
60

0.0%
ACCURACY

COMPLETION: 0.0%

Decoded a message that is spelled out using dial tone sounds.

Tampered (Hard)

0 POINTS
OUT OF
60

0.0%
ACCURACY

COMPLETION: 0.0%

Use CRC checksums to identify a tampered message.





Enumeration & Exploitation Module

Identify actionable exploits and vulnerabilities and use them to bypass the security measures in code and compiled binaries.

N/A

NATIONAL RANK

0 POINTS
OUT OF
330

PERFORMANCE SCORE

Average: 145.2 Points

0.0%

ACCURACY

Average: 72.5%

0.0%

COMPLETION

Average: 52.0%

Source (Easy)

0 POINTS
OUT OF
110

0.0%

ACCURACY

COMPLETION:

0.0%

Reverse engineer the source code of a Rust program to bypass a simple password authentication.

Speedy (Medium)

0 POINTS
OUT OF
110

0.0%

ACCURACY

COMPLETION:

0.0%

Reverse engineer the source code of a Golang program.

Passphrase (Hard)

0 POINTS
OUT OF
110

0.0%

ACCURACY

COMPLETION:

0.0%

Reverse engineer an ELF binary to break XOR encryption on a password.

Forensics Module

Utilize the proper tools and techniques to analyze, process, recover, and/or investigate digital evidence in a computer-related incident.

N/A

NATIONAL RANK

0 POINTS
OUT OF
315

PERFORMANCE SCORE

Average: 111.2 Points

0.0%

ACCURACY

Average: 50.5%

0.0%

COMPLETION

Average: 41.1%

Table (Easy)

0 POINTS
OUT OF
100

0.0%

ACCURACY

COMPLETION:

0.0%

Analyze an ARP table to investigate an ARP spoofing attack.

Plant (Medium)

0 POINTS
OUT OF
100

0.0%

ACCURACY

COMPLETION:

0.0%

Extract a Linux installer and cpio file to investigate a filesystem.

Incident Response (Hard)

0 POINTS
OUT OF
115

0.0%

ACCURACY

COMPLETION:

0.0%

Inspect and repair a live system that was tampered with to recover data.





Log Analysis Module

Utilize the proper tools and techniques to establish a baseline for normal operation and identify malicious activities using log files from various services.

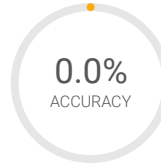
N/A

NATIONAL RANK

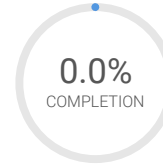
0 POINTS
OUT OF
300

PERFORMANCE SCORE

Average: 160.2 Points



Average: 53.9%



Average: 60.1%

Audit (Easy)

0 POINTS
OUT OF
100

0.0%
ACCURACY

COMPLETION: 0.0%

Analyze a system auth log file to investigate the behavior of users with elevated privileges.

Packet Log (Medium)

0 POINTS
OUT OF
100

0.0%
ACCURACY

COMPLETION: 0.0%

Identify traffic patterns from a log file of network traffic.

\$TICKER (Hard)

0 POINTS
OUT OF
100

0.0%
ACCURACY

COMPLETION: 0.0%

Parse a stock price log to identify a stock price that was manipulated.

Network Traffic Analysis Module

Identify malicious and benign network traffic to demonstrate an understanding of potential security breaches.

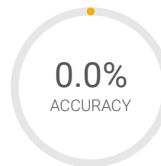
N/A

NATIONAL RANK

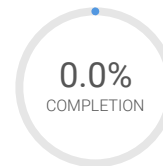
0 POINTS
OUT OF
320

PERFORMANCE SCORE

Average: 148.9 Points



Average: 63.2%



Average: 65.5%

Address (Easy)

0 POINTS
OUT OF
100

0.0%
ACCURACY

COMPLETION: 0.0%

Analyze the behavior of DHCP traffic from a client connecting to a network.

Home (Medium)

0 POINTS
OUT OF
110

0.0%
ACCURACY

COMPLETION: 0.0%

Analyze a packet capture and decode traffic from TP-Link smart switches.

Spec (Hard)

0 POINTS
OUT OF
110

0.0%
ACCURACY

COMPLETION: 0.0%

Implement a custom specification to decode raw packets.



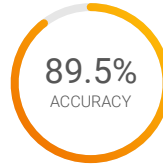


Open Source Intelligence Module

Utilize publicly available information such as search engines, public repositories, social media, and more to gain in-depth knowledge on a topic or target.

1439 TH PLACE
OUT OF 8483
NATIONAL RANK

240 POINTS
OUT OF 355
PERFORMANCE SCORE



Average: 73.0%



Average: 65.9%

84th National
Percentile

Average: 200.2 Points

Rules of Conduct (Easy)

25 POINTS
OUT OF 25

100.0%
ACCURACY

COMPLETION: **100.0%**

Introductory challenge on acceptable conduct during NCL.

Vinyl (Easy)

40 POINTS
OUT OF 40

100.0%
ACCURACY

COMPLETION: **100.0%**

Analyze an image using metadata and file properties.

Coordinates (Easy)

60 POINTS
OUT OF 60

75.0%
ACCURACY

COMPLETION: **100.0%**

Geolocate the physical location of a server using an IP address.

NFT (Medium)

60 POINTS
OUT OF 60

100.0%
ACCURACY

COMPLETION: **100.0%**

Conduct blockchain analysis to attribute the ownership of a NFT.

Git (Medium)

0 POINTS
OUT OF 75

0.0%
ACCURACY

COMPLETION: **0.0%**

Obtain private company information that was posted on social media.

Password (Hard)

55 POINTS
OUT OF 95

66.7%
ACCURACY

COMPLETION: **66.7%**

Use coordinates and a SSID to search for a location and find information from public images.



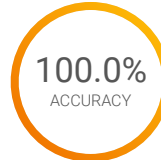


Password Cracking Module

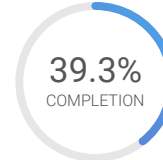
Identify types of password hashes and apply various techniques to efficiently determine plaintext passwords.

1366 TH PLACE
OUT OF 8483
NATIONAL RANK

125 POINTS
OUT OF 340
PERFORMANCE SCORE



Average: 87.6%



Average: 36.6%

84th National
Percentile

Average: 101.6 Points

Hashing (Easy)

15 POINTS
OUT OF 15

100.0%
ACCURACY

COMPLETION: **100.0%**

Generate password hashes for MD5, SHA1, and SHA256.

Rockyou (Easy)

30 POINTS
OUT OF 30

100.0%
ACCURACY

COMPLETION: **100.0%**

Crack MD5 password hashes for password found in the rockyou breach.

Windows (Easy)

30 POINTS
OUT OF 30

100.0%
ACCURACY

COMPLETION: **100.0%**

Crack Windows NTLM password hashes using rainbow tables.

Pattern (Medium)

0 POINTS
OUT OF 45

0.0%
ACCURACY

COMPLETION: **0.0%**

Build a wordlist or pattern rule to crack password hashes of a known pattern.

ZIP (Medium)

50 POINTS
OUT OF 50

100.0%
ACCURACY

COMPLETION: **100.0%**

Crack the insecure password for a protected zip file.

Wordlist (Hard)

0 POINTS
OUT OF 65

0.0%
ACCURACY

COMPLETION: **0.0%**

Build a wordlist to crack passwords not found in common wordlists.

Complexity (Hard)

0 POINTS
OUT OF 105

0.0%
ACCURACY

COMPLETION: **0.0%**

Build a custom wordlist to crack passwords by augmenting permutation rules using known password complexity requirements.





Scanning & Reconnaissance Module

Identify and use the proper tools to gain intelligence about a target including its services and potential vulnerabilities.

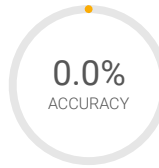
N/A

NATIONAL RANK

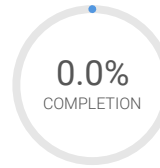
0 POINTS
OUT OF
300

PERFORMANCE SCORE

Average: 138.6 Points



Average: 56.8%



Average: 50.0%

Scan (Easy)

Use nmap to scan a machine and discover open ports.

0 POINTS
OUT OF
100

0.0%
ACCURACY

COMPLETION: 0.0%

Domains (Medium)

Perform reconnaissance on a domain's DNS records to gain information about its assets.

0 POINTS
OUT OF
100

0.0%
ACCURACY

COMPLETION: 0.0%

ICS (Hard)

Perform reconnaissance on an ICS system by using the Modbus protocol.

0 POINTS
OUT OF
100

0.0%
ACCURACY

COMPLETION: 0.0%

Web Application Exploitation Module

Identify actionable exploits and vulnerabilities and use them to bypass the security measures in online services.

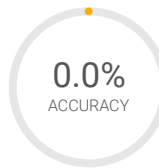
N/A

NATIONAL RANK

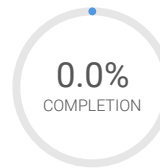
0 POINTS
OUT OF
310

PERFORMANCE SCORE

Average: 102.7 Points



Average: 56.0%



Average: 43.1%

Candy Store (Easy)

Find and exploit a client side authentication vulnerability in a web application.

0 POINTS
OUT OF
100

0.0%
ACCURACY

COMPLETION: 0.0%

Shopping v2 (Medium)

Exploit a type coercion bug in a Node.js application.

0 POINTS
OUT OF
100

0.0%
ACCURACY

COMPLETION: 0.0%

Indie Metro (Hard)

Perform a NoSQL injection attack on a website.

0 POINTS
OUT OF
110

0.0%
ACCURACY

COMPLETION: 0.0%

