Thomas Weis
thomasweis27@gmail.com

NCL Fall 2024 Individual Game Scouting Report

Dear Thomas Weis,

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/R07KBQ8JJ03F

CompTIA

Based on the performance detailed in this NCL Scouting Report, you have earned **9 hours** of Continuing Education Units (CEUs) as approved by CompTIA. You can learn more about the NCL - CompTIA alignment via nationalcyberleague.org/partners.

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

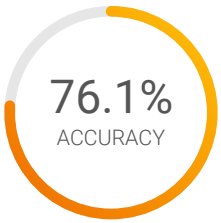
NCL FALL 2024 INDIVIDUAL GAME

NATIONAL RANK
734TH PLACE OUT OF 8484

PERCENTILE
92ND

YOUR TOP CATEGORIES

PASSWORD CRACKING	ENUMERATION & EXPLOITATION	OPEN SOURCE INTELLIGENCE
95TH PERCENTILE	91ST PERCENTILE	90TH PERCENTILE



Average: 67.8%

cyberskyline.com/report
ID: R07KBQ8JJ03F

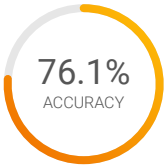
Thomas Weis
thomasweis27@gmail.com

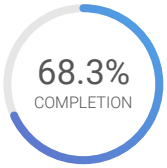
NCL Fall 2024 Individual Game

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.

734 TH PLACE OUT OF 8484
NATIONAL RANK

1830 POINTS OUT OF 3000
PERFORMANCE SCORE





92nd National Percentile

Average: 1008.9 Points

Average: 67.8%

Average: 41.1%

Cryptography

235 POINTS OUT OF 330

60.0% ACCURACY

COMPLETION: **70.6%**

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

Enumeration & Exploitation

220 POINTS OUT OF 330

100.0% ACCURACY

COMPLETION: **66.7%**

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

Forensics

100 POINTS OUT OF 315

42.9% ACCURACY

COMPLETION: **37.5%**

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

Log Analysis

260 POINTS OUT OF 300

91.7% ACCURACY

COMPLETION: **84.6%**

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

Network Traffic Analysis

190 POINTS OUT OF 320

68.8% ACCURACY

COMPLETION: **78.6%**

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

Open Source Intelligence

290 POINTS OUT OF 355

67.9% ACCURACY

COMPLETION: **82.6%**

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

Password Cracking

185 POINTS OUT OF 340

100.0% ACCURACY

COMPLETION: **60.7%**

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

Scanning & Reconnaissance

150 POINTS OUT OF 300

100.0% ACCURACY

COMPLETION: **50.0%**

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

Web Application Exploitation

100 POINTS OUT OF 310

100.0% ACCURACY

COMPLETION: **50.0%**

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

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

Thomas Weis
thomasweis27@gmail.com

Cryptography Module

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

1521 ST PLACE OUT OF 8484
NATIONAL RANK

235 POINTS OUT OF 330
PERFORMANCE SCORE

60.0% ACCURACY
Average: 72.6%

70.6% COMPLETION
Average: 64.6%

83rd National Percentile
Average: 209.0 Points

Bases (Easy)

30 POINTS OUT OF 30

100.0% ACCURACY

COMPLETION: 100.0%

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

Shift (Easy)

40 POINTS OUT OF 40

100.0% ACCURACY

COMPLETION: 100.0%

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

Number Codes (Easy)

40 POINTS OUT OF 40

100.0% ACCURACY

COMPLETION: 100.0%

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

NATO (Easy)

40 POINTS OUT OF 40

100.0% ACCURACY

COMPLETION: 100.0%

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

Message Signature (Medium)

35 POINTS OUT OF 60

28.6% ACCURACY

COMPLETION: 66.7%

Identify tampered emails by using PGP signatures.

Beep Beep (Medium)

50 POINTS OUT OF 60

40.0% ACCURACY

COMPLETION: 66.7%

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.

Thomas Weis
thomasweis27@gmail.com

Enumeration & Exploitation Module

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

793 RD PLACE OUT OF 8484
NATIONAL RANK

220 POINTS OUT OF 330
PERFORMANCE SCORE

100.0% ACCURACY

66.7% COMPLETION

91st National Percentile

Average: 145.2 Points

Average: 72.5%

Average: 52.0%

Source (Easy)

110 POINTS OUT OF 110

100.0% ACCURACY

COMPLETION: 100.0%

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

Speedy (Medium)

110 POINTS OUT OF 110

100.0% ACCURACY

COMPLETION: 100.0%

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.

1808 TH PLACE OUT OF 8484
NATIONAL RANK

100 POINTS OUT OF 315
PERFORMANCE SCORE

42.9% ACCURACY

37.5% COMPLETION

79th National Percentile

Average: 111.2 Points

Average: 50.5%

Average: 41.1%

Table (Easy)

100 POINTS OUT OF 100

42.9% ACCURACY

COMPLETION: 100.0%

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.

Thomas Weis
thomasweis27@gmail.com

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.

862 ND PLACE OUT OF 8484
NATIONAL RANK

260 POINTS OUT OF 300
PERFORMANCE SCORE

91.7% ACCURACY
Average: 53.9%

84.6% COMPLETION
Average: 60.1%

90th National Percentile
Average: 160.2 Points

Audit (Easy)

80 POINTS OUT OF 100

80.0% ACCURACY

COMPLETION: 80.0%

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

Packet Log (Medium)

80 POINTS OUT OF 100

100.0% ACCURACY

COMPLETION: 85.7%

Identify traffic patterns from a log file of network traffic.

$TICKER (Hard)

100 POINTS OUT OF 100

100.0% ACCURACY

COMPLETION: 100.0%

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.

937 TH PLACE OUT OF 8484
NATIONAL RANK

190 POINTS OUT OF 320
PERFORMANCE SCORE

68.8% ACCURACY
Average: 63.2%

78.6% COMPLETION
Average: 65.5%

89th National Percentile
Average: 148.9 Points

Address (Easy)

80 POINTS OUT OF 100

85.7% ACCURACY

COMPLETION: 85.7%

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

Home (Medium)

110 POINTS OUT OF 110

55.6% ACCURACY

COMPLETION: 100.0%

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.

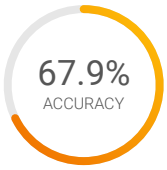
Thomas Weis
thomasweis27@gmail.com

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.

850 TH PLACE OUT OF 8484
NATIONAL RANK

290 POINTS OUT OF 355
PERFORMANCE SCORE



90th National Percentile

Average: 200.2 Points

Average: 73.0%

Average: 65.9%

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)

40 POINTS OUT OF 60

66.7% ACCURACY

COMPLETION: 66.7%

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

NFT (Medium)

30 POINTS OUT OF 60

50.0% ACCURACY

COMPLETION: 50.0%

Conduct blockchain analysis to attribute the ownership of a NFT.

Git (Medium)

60 POINTS OUT OF 75

80.0% ACCURACY

COMPLETION: 80.0%

Obtain private company information that was posted on social media.

Password (Hard)

95 POINTS OUT OF 95

37.5% ACCURACY

COMPLETION: 100.0%

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

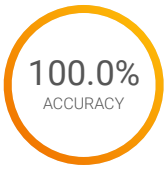
Thomas Weis
thomasweis27@gmail.com

Password Cracking Module

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

501 ST PLACE OUT OF 8484
NATIONAL RANK

185 POINTS OUT OF 340
PERFORMANCE SCORE



95th National Percentile

Average: 101.6 Points

Average: 87.6%

Average: 36.6%

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)

45 POINTS OUT OF 45

100.0% ACCURACY

COMPLETION: 100.0%

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)

15 POINTS OUT OF 65

100.0% ACCURACY

COMPLETION: 50.0%

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.

Thomas Weis
thomasweis27@gmail.com

Scanning & Reconnaissance Module

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

1178 TH PLACE OUT OF 8484
NATIONAL RANK

150 POINTS OUT OF 300
PERFORMANCE SCORE

100.0% ACCURACY

50.0% COMPLETION

87th National Percentile

Average: 138.6 Points

Average: 56.8%

Average: 50.0%

Scan (Easy)

90 POINTS OUT OF 100

100.0% ACCURACY

COMPLETION: 75.0%

Use nmap to scan a machine and discover open ports.

Domains (Medium)

60 POINTS OUT OF 100

100.0% ACCURACY

COMPLETION: 66.7%

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

ICS (Hard)

0 POINTS OUT OF 100

0.0% ACCURACY

COMPLETION: 0.0%

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

Web Application Exploitation Module

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

1292 ND PLACE OUT OF 8484
NATIONAL RANK

100 POINTS OUT OF 310
PERFORMANCE SCORE

100.0% ACCURACY

50.0% COMPLETION

85th National Percentile

Average: 102.7 Points

Average: 56.0%

Average: 43.1%

Candy Store (Easy)

90 POINTS OUT OF 100

100.0% ACCURACY

COMPLETION: 100.0%

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

Shopping v2 (Medium)

10 POINTS OUT OF 100

100.0% ACCURACY

COMPLETION: 50.0%

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

Indie Metro (Hard)

0 POINTS OUT OF 110

0.0% ACCURACY

COMPLETION: 0.0%

Perform a NoSQL injection attack on a website.