NCL Spring 2025 Individual Game Scouting Report

Dear Eli Johnson,

Thank you for participating in the National Cyber League (NCL) Spring 2025 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 Spring 2025 Season had 9,216 students/players and 596 faculty/coaches from 510 two- and four-year schools & 288 high schools across all 50 U.S. states registered to play. The Individual Game Capture the Flag (CTF) event took place from April 11 through April 13. The Team Game CTF event took place from April 25 through April 27. 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/98430FH85T1X

Based on the performance detailed in this NCL Scouting Report, you have earned **11 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 Spring 2025 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

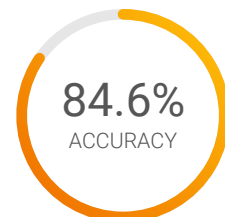## NATIONAL CYBER LEAGUE SCORE CARD
NCL SPRING 2025 INDIVIDUAL GAME

NATIONAL RANK
478TH PLACE
OUT OF 8573

PERCENTILE
95TH

YOUR TOP CATEGORIES

SCANNING & RECONNAISSANCE	PASSWORD CRACKING	LOG ANALYSIS
98TH PERCENTILE	96TH PERCENTILE	95TH PERCENTILE

84.6%
ACCURACY

Average: 66.8%

cyberskyline.com/report
ID: 98430FH85T1X

Learn more at nationalcyberleague.org

POWERED BY
CYBER SKYLINE

NCL Spring 2025 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.

478 TH PLACE OUT OF **8573**
NATIONAL RANK

95th National Percentile

2170 POINTS OUT OF 3000
PERFORMANCE SCORE

Average: 995.3 Points

84.6% ACCURACY

Average: 66.8%

79.7% COMPLETION

Average: 37.7%
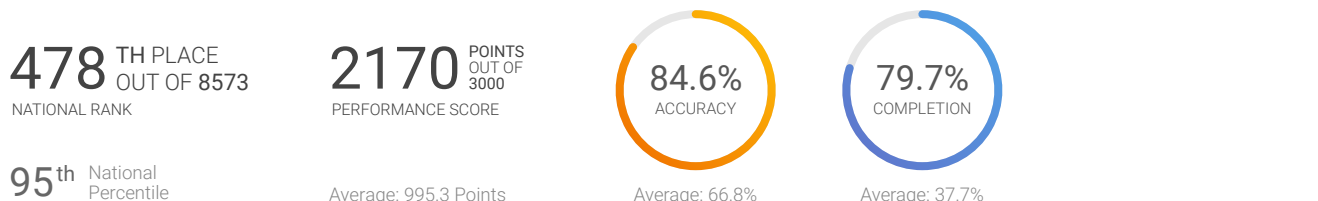
Cryptography
250 POINTS OUT OF 385 · 93.8% ACCURACY · COMPLETION: 78.9%

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

Enumeration & Exploitation
150 POINTS OUT OF 365 · 91.7% ACCURACY · COMPLETION: 57.9%

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

Forensics
230 POINTS OUT OF 305 · 62.5% ACCURACY · COMPLETION: 71.4%

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 · 80.0% ACCURACY · COMPLETION: 94.1%

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
200 POINTS OUT OF 300 · 73.3% ACCURACY · COMPLETION: 91.7%

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

Open Source Intelligence
250 POINTS OUT OF 310 · 93.8% ACCURACY · COMPLETION: 83.3%

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
250 POINTS OUT OF 335 · 100.0% ACCURACY · COMPLETION: 73.7%

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

Scanning & Reconnaissance
300 POINTS OUT OF 300 · 89.5% ACCURACY · COMPLETION: 100.0%

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

Web Application Exploitation
180 POINTS OUT OF 300 · 55.6% ACCURACY · COMPLETION: 55.6%

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

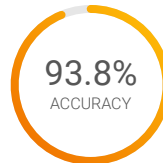Note: Survey module (100 points) was excluded from this report.

POWERED BY
CYBER SKYLINE
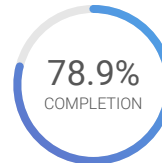
Cryptography Module

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

581 ST PLACE
OUT OF **8573**
NATIONAL RANK

94th National Percentile

250 POINTS
OUT OF
385
PERFORMANCE SCORE

Average: 143.1 Points

93.8%
ACCURACY

Average: 65.0%

78.9%
COMPLETION

Average: 44.2%

The Bases (Easy)

45 POINTS OUT OF 45   **100.0%** ACCURACY   COMPLETION: **100.0%**

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

Super Shifty (Easy)

55 POINTS OUT OF 55   **100.0%** ACCURACY   COMPLETION: **100.0%**

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

Pizza Time (Easy)

50 POINTS OUT OF 50   **100.0%** ACCURACY   COMPLETION: **100.0%**

Analyze and obtain the plaintext for a message encrypted with the rail fence cipher

Signed (Medium)

45 POINTS OUT OF 60   **75.0%** ACCURACY   COMPLETION: **75.0%**

Identify tampered files by verifying PGP signatures

Altered Clouds (Medium)

55 POINTS OUT OF 55   **100.0%** ACCURACY   COMPLETION: **100.0%**

Verify the integrity of files by computing HMAC values

Zugzwang (Medium)

0 POINTS OUT OF 60   **0.0%** ACCURACY   COMPLETION: **0.0%**

Decode a hidden file by implementing a decoder for a custom encoding scheme

Kracken (Hard)

0 POINTS OUT OF 60   **0.0%** ACCURACY   COMPLETION: **0.0%**

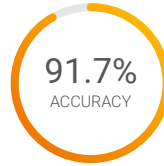Break XOR encryption using a bruteforce attack with a known crib

Enumeration & Exploitation Module

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

710 TH PLACE OUT OF **8573**
NATIONAL RANK

92 nd National Percentile

150 POINTS OUT OF 365
PERFORMANCE SCORE

Average: 111.7 Points

91.7% ACCURACY

Average: 67.9%

57.9% COMPLETION

Average: 41.6%

Not Affine (Easy)

75 POINTS OUT OF 75

100.0% ACCURACY

COMPLETION: 100.0%

Perform code analysis on C source code to reverse a series of bitwise operations

CrackMe (Medium)

25 POINTS OUT OF 90

100.0% ACCURACY

COMPLETION: 50.0%

Perform static analysis on a binary program and extract an image encoded within the binary

Hardware Discovery (Hard)

0 POINTS OUT OF 100

0.0% ACCURACY

COMPLETION: 0.0%

Follow a hardware schematic to interpret raw signal data that is encoded using pulse width modulation

Escalate (Hard)

50 POINTS OUT OF 100

100.0% ACCURACY

COMPLETION: 60.0%

Identify and exploit a vulnerability in a compiled C binary to read data from unclosed file descriptors
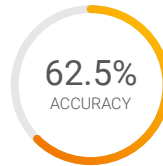
Forensics Module

Utilize the proper tools and techniques to analyze, process, recover, and/or investigate digital evidence in a computer-related incident.
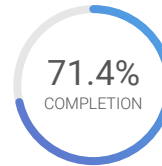
599 TH PLACE OUT OF **8573**
NATIONAL RANK

94th National Percentile

230 POINTS OUT OF 305
PERFORMANCE SCORE

Average: 144.7 Points

62.5% ACCURACY
Average: 58.4%

71.4% COMPLETION
Average: 48.4%

Overused (Easy)
105 POINTS OUT OF 105 — **100.0%** ACCURACY — COMPLETION: **100.0%**
Use Binwalk or other file carving tools to analyze and extract embedded files

Oops (Medium)
75 POINTS OUT OF 100 — **25.0%** ACCURACY — COMPLETION: **50.0%**
Utilize forensics tools to perform file recovery on a deleted image

Absence (Hard)
50 POINTS OUT OF 100 — **100.0%** ACCURACY — COMPLETION: **50.0%**
Recover a corrupted G-code file by correcting errors and fixing gaps within the file
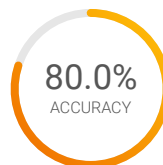
Log Analysis Module

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

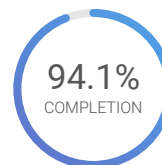**438** TH PLACE OUT OF **8573**
NATIONAL RANK

95th National Percentile

260 POINTS OUT OF 300
PERFORMANCE SCORE

Average: 164.5 Points

80.0% ACCURACY
Average: 56.8%

94.1% COMPLETION
Average: 59.9%

Ancient History (Easy)
100 POINTS OUT OF 100 — **63.6%** ACCURACY — COMPLETION: **100.0%**
Analyze HTTP access logs to calculate statistics and identify trends in web traffic

Leaked (Medium)
100 POINTS OUT OF 100 — **100.0%** ACCURACY — COMPLETION: **100.0%**
Analyze a SQL backup log file and calculate statistics on user data

Logins (Hard)
60 POINTS OUT OF 100 — **100.0%** ACCURACY — COMPLETION: **80.0%**
Parse a binary log and perform anomaly detection to identify a compromised user based on GeoIP data

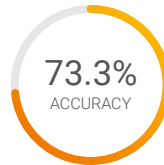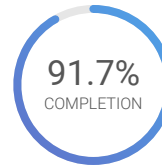# Network Traffic Analysis Module

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

627 TH PLACE OUT OF 8573
NATIONAL RANK

93 rd National Percentile

200 POINTS OUT OF 300
PERFORMANCE SCORE

Average: 124.6 Points

73.3% ACCURACY

Average: 66.3%

91.7% COMPLETION

Average: 56.9%

Lost in Resolution (Easy)

100 POINTS OUT OF 100

60.0% ACCURACY

COMPLETION: 100.0%

Analyze a packet capture with DNS traffic to identify DNS queries and responses

Wifi (Medium)

100 POINTS OUT OF 100

100.0% ACCURACY

COMPLETION: 100.0%

Analyze a packet capture of WiFi network traffic and crack the password to the WiFi network

Exfil (Hard)

0 POINTS OUT OF 100

0.0% ACCURACY

COMPLETION: 0.0%

Analyze a packet capture to identify and extract exfiltrated data that was encoded within x.509 certificate SAN fields
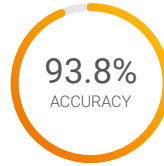
POWERED BY
CYBER SKYLINE

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.

716 TH PLACE OUT OF **8573**
NATIONAL RANK

92nd National Percentile

250 POINTS OUT OF 310
PERFORMANCE SCORE

Average: 196.4 Points

93.8% ACCURACY

Average: 70.9%

83.3% COMPLETION

Average: 66.8%

| Rules of Conduct (Easy) | 100 POINTS OUT OF 100 | 100.0% ACCURACY | COMPLETION: 100.0% |

Introductory challenge on acceptable conduct during NCL

| Honor (Easy) | 20 POINTS OUT OF 30 | 66.7% ACCURACY | COMPLETION: 66.7% |

Analyze an image to obtain data from metadata and file properties

| Controversial Challenge (Medium) | 30 POINTS OUT OF 30 | 100.0% ACCURACY | COMPLETION: 100.0% |

Perform a reverse image search to discover open-source information about a subject

| Nostalgia (Hard) | 50 POINTS OUT OF 50 | 100.0% ACCURACY | COMPLETION: 100.0% |

Utilize open source tools to analyze and geolocate a photo

| Meow Meow Meow (Hard) | 0 POINTS OUT OF 50 | 0.0% ACCURACY | COMPLETION: 0.0% |

Extract an image from an EML file and then perform a reverse image search to discover information about a target

| GitHub in Action (Hard) | 50 POINTS OUT OF 50 | 100.0% ACCURACY | COMPLETION: 100.0% |

Investigate public GitHub repositories to trace connections between user actions and their social media accounts
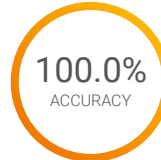
POWERED BY
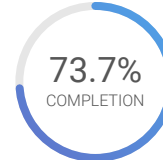CYBER SKYLINE

Password Cracking Module

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

359 TH PLACE OUT OF **8573**
NATIONAL RANK

96 th National Percentile

250 POINTS OUT OF **335**
PERFORMANCE SCORE

Average: 165.3 Points

100.0%
ACCURACY

Average: 86.9%

73.7%
COMPLETION

Average: 50.0%

Hash me outside! (Easy)
50 POINTS OUT OF **50**

100.0% ACCURACY

COMPLETION: 100.0%

Generate password hashes using MD5, SHA1, and SHA256

We Will Rockyou (Easy)
50 POINTS OUT OF **50**

100.0% ACCURACY

COMPLETION: 100.0%

Crack MD5 password hashes for password found in the RockYou breach

Oph the Grid (Medium)
50 POINTS OUT OF **50**

100.0% ACCURACY

COMPLETION: 100.0%

Crack Windows NTLM password hashes using rainbow tables

Totally Safe PDF (Medium)
50 POINTS OUT OF **50**

100.0% ACCURACY

COMPLETION: 100.0%

Crack the insecure password on a protected PDF file

put 0n th3 ma5k (Medium)
50 POINTS OUT OF **50**

100.0% ACCURACY

COMPLETION: 100.0%

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

Dice (Hard)
0 POINTS OUT OF **85**

0.0% ACCURACY

COMPLETION: 0.0%

Build a custom wordlist to crack passwords by augmenting permutation rules using known password complexity requirements
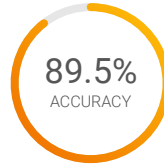
Scanning & Reconnaissance Module

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

195 TH PLACE OUT OF 8573
NATIONAL RANK

98th National Percentile

300 POINTS OUT OF 300
PERFORMANCE SCORE

Average: 171.8 Points

89.5% ACCURACY

Average: 72.8%

100.0% COMPLETION

Average: 54.2%

Portscan (Easy)
100 POINTS OUT OF 100 | **100.0%** ACCURACY | COMPLETION: 100.0%

Perform a port scan and identify services running on a remote host

Dig (Medium)
100 POINTS OUT OF 100 | **87.5%** ACCURACY | COMPLETION: 100.0%

Utilize DNS services to gain information about an organization's Intranet resources

School Directory (Hard)
100 POINTS OUT OF 100 | **85.7%** ACCURACY | COMPLETION: 100.0%
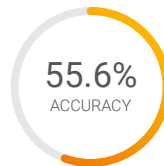
Conduct reconnaissance on an LDAP server

Web Application Exploitation Module

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

594 TH PLACE OUT OF 8573
NATIONAL RANK

94th National Percentile

180 POINTS OUT OF 300
PERFORMANCE SCORE

Average: 123.1 Points

55.6% ACCURACY

Average: 61.9%

55.6% COMPLETION

Average: 39.4%

Liber8Dogs (Easy)
100 POINTS OUT OF 100 | **66.7%** ACCURACY | COMPLETION: 100.0%

Find and exploit a path traversal vulnerability in a web application

Liber8tion_Login (Medium)
70 POINTS OUT OF 100 | **40.0%** ACCURACY | COMPLETION: 66.7%

Manipulate headers to exploit improper authorization checks in middleware found in CVE-2025-29927

dogstagram (Hard)
10 POINTS OUT OF 100 | **100.0%** ACCURACY | COMPLETION: 25.0%

Bypass data sanitization on a login form and exploit a server side request forgery vulnerability