NCL Fall 2025 Individual Game Scouting Report

Dear Trevor Ritchie,

Thank you for participating in the National Cyber League (NCL) Fall 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 Fall 2025 Season had 8,520 students/players and 538 faculty/coaches from more than 490 two- and four-year schools & 200 high schools across all 50 U.S. states registered to play. The Individual Game Capture the Flag (CTF) event took place from October 24 through October 26. The Team Game CTF event took place from November 7 through November 9. 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/KTBRGJNJMUJE

CompTIA

Based on the performance detailed in this NCL Scouting Report, you have earned 21 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 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

POWERED BY CYBER SKYLINE

NATIONAL CYBER LEAGUE SCORE CARD

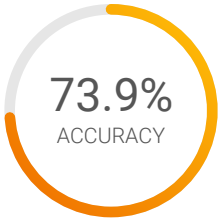
NCL FALL 2025 INDIVIDUAL GAME

NATIONAL RANK
168TH PLACE OUT OF 7873

PERCENTILE
98TH

YOUR TOP CATEGORIES

CRYPTOGRAPHY	SCANNING & RECONNAISSANCE	PASSWORD CRACKING
100TH PERCENTILE	100TH PERCENTILE	99TH PERCENTILE



Average: 61.0%

cyberskyline.com/report
ID: KTBRGJNJMUJE

NCL Fall 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.

168 TH PLACE OUT OF 7873
NATIONAL RANK

2565 POINTS OUT OF 3000
PERFORMANCE SCORE

73.9% ACCURACY
Average: 61.0%

93.3% COMPLETION
Average: 40.1%

98th National Percentile
Average: 974.0 Points

Cryptography

355 POINTS OUT OF 355

100.0% ACCURACY

COMPLETION: 100.0%

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

Enumeration & Exploitation

200 POINTS OUT OF 300

100.0% ACCURACY

COMPLETION: 87.5%

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

Forensics

230 POINTS OUT OF 300

50.0% ACCURACY

COMPLETION: 93.3%

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

Log Analysis

300 POINTS OUT OF 300

66.7% ACCURACY

COMPLETION: 100.0%

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

210 POINTS OUT OF 300

52.2% ACCURACY

COMPLETION: 85.7%

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

Open Source Intelligence

350 POINTS OUT OF 385

68.4% ACCURACY

COMPLETION: 92.9%

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

320 POINTS OUT OF 360

91.3% ACCURACY

COMPLETION: 91.3%

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

Scanning & Reconnaissance

300 POINTS OUT OF 300

93.8% 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

200 POINTS OUT OF 300

81.8% ACCURACY

COMPLETION: 75.0%

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.

Cryptography Module

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

44 TH PLACE OUT OF 7873
NATIONAL RANK

355 POINTS OUT OF 355
PERFORMANCE SCORE

100.0% ACCURACY

100.0% COMPLETION

100th National Percentile

Average: 157.0 Points

Average: 69.5%

Average: 58.2%

Baking Soda (Easy)

50 POINTS OUT OF 50

100.0% ACCURACY

COMPLETION: 100.0%

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

ROTten domains (Easy)

45 POINTS OUT OF 45

100.0% ACCURACY

COMPLETION: 100.0%

Analyze and obtain plaintext for messages encrypted with a shift cipher.

Convenience (Easy)

60 POINTS OUT OF 60

100.0% ACCURACY

COMPLETION: 100.0%

Analyze and obtain the plaintext from text encrypted with Vigenère cipher.

01101011 01100101 01111001 (Medium)

40 POINTS OUT OF 40

100.0% ACCURACY

COMPLETION: 100.0%

Decrypt a message using an XOR key.

Squirtle (Medium)

60 POINTS OUT OF 60

100.0% ACCURACY

COMPLETION: 100.0%

Analyze and exploit a DES encryption implementation using known weak keys.

Temet Nosce (Hard)

100 POINTS OUT OF 100

100.0% ACCURACY

COMPLETION: 100.0%

Exploit a flaw in AES encryption to decrypt text with an unknown secret key.

Enumeration & Exploitation Module

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

236 TH PLACE OUT OF 7873
NATIONAL RANK

200 POINTS OUT OF 300
PERFORMANCE SCORE

100.0% ACCURACY

87.5% COMPLETION

98th National Percentile

Average: 98.2 Points

Average: 60.4%

Average: 49.4%

Deno Finds a Way (Easy)	100 POINTS OUT OF 100	100.0% ACCURACY	COMPLETION: 100.0%
Review source code and exploit a command injection vulnerability to escalate privileges.			
Stacked (Medium)	100 POINTS OUT OF 100	100.0% ACCURACY	COMPLETION: 100.0%
Perform an HTTP-triggered stack overflow to retrieve critical information from the server.			
Sewer System (Hard)	0 POINTS OUT OF 100	0.0% ACCURACY	COMPLETION: 0.0%
Exploit a race condition in software to return protected data.			

Forensics Module

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

304 TH PLACE OUT OF 7873
NATIONAL RANK

230 POINTS OUT OF 300
PERFORMANCE SCORE

50.0% ACCURACY

100.0% COMPLETION

97th National Percentile

Average: 115.2 Points

Average: 45.9%

Average: 48.4%

Four & Six (Easy)	100 POINTS OUT OF 100	50.0% ACCURACY	COMPLETION: 100.0%
Use a forensics tool to examine unallocated space for files.			
This Bytes (Medium)	100 POINTS OUT OF 100	57.1% ACCURACY	COMPLETION: 100.0%
Research JPEG specifications to repair an image.			
Stage Left (Hard)	30 POINTS OUT OF 100	40.0% ACCURACY	COMPLETION: 66.7%
Fix a corrupted SQLite database file and analyze the tables.			

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.

191 ST PLACE OUT OF 7873
NATIONAL RANK

300 POINTS OUT OF 300
PERFORMANCE SCORE

66.7% ACCURACY

100.0% COMPLETION

98th National Percentile

Average: 160.8 Points

Average: 55.3%

Average: 61.1%

Process This (Easy)

100 POINTS OUT OF 100

85.7% ACCURACY

COMPLETION: 100.0%

Examine parsed Sysmon JSON process tree logs to determine a chain of events.

Brute Force (Medium)

100 POINTS OUT OF 100

100.0% ACCURACY

COMPLETION: 100.0%

Identify a brute force attack by analyzing patterns of malicious actor behavior in web server logs.

Stolen Swipe (Hard)

100 POINTS OUT OF 100

33.3% ACCURACY

COMPLETION: 100.0%

Parse and correlate ATM and EMV Field 55 logs (ISO 8583 standard) to identify a fraudulent transaction.

Network Traffic Analysis Module

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

397 TH PLACE OUT OF 7873
NATIONAL RANK

210 POINTS OUT OF 300
PERFORMANCE SCORE

52.2% ACCURACY

85.7% COMPLETION

95th National Percentile

Average: 112.2 Points

Average: 51.6%

Average: 45.0%

RMM Tool (Easy)

100 POINTS OUT OF 100

71.4% ACCURACY

COMPLETION: 100.0%

Analyze DNS packet requests and responses to identify a suspicious download.

Drive-by Download (Medium)

100 POINTS OUT OF 100

66.7% ACCURACY

COMPLETION: 100.0%

Identify details of a drive-by-download attack and de-obfuscate JavaScript.

The Insider (Hard)

10 POINTS OUT OF 100

14.3% ACCURACY

COMPLETION: 33.3%

Reconstruct a file from UDP packets and decode VBA script.

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.

328 TH PLACE OUT OF 7873
NATIONAL RANK

350 POINTS OUT OF 385
PERFORMANCE SCORE

68.4% ACCURACY
Average: 58.5%

92.9% COMPLETION
Average: 65.3%

96th National Percentile
Average: 213.9 Points

Rules of Conduct (Easy)

30 POINTS OUT OF 30

100.0% ACCURACY

COMPLETION: 100.0%

Introductory challenge on acceptable conduct during NCL.

Cooking Breakfast (Easy)

45 POINTS OUT OF 45

100.0% ACCURACY

COMPLETION: 100.0%

Parse Chef (esolang) code to determine what input it requires.

NotPetya (Easy)

100 POINTS OUT OF 100

88.9% ACCURACY

COMPLETION: 100.0%

Gather key information on NotPetya malware.

Flamed (Medium)

55 POINTS OUT OF 55

66.7% ACCURACY

COMPLETION: 100.0%

Use open source tools to find patterns between GPS locations.

Material (Medium)

80 POINTS OUT OF 80

83.3% ACCURACY

COMPLETION: 100.0%

Use the EDGAR database to filter 8-K filings.

I Cee Stuff (Hard)

40 POINTS OUT OF 75

25.0% ACCURACY

COMPLETION: 60.0%

Use ICS/OT OSINT tools do passive recon on infrastructure.

Password Cracking Module

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

113 TH PLACE OUT OF 7873
NATIONAL RANK

320 POINTS OUT OF 360
PERFORMANCE SCORE

91.3% ACCURACY

91.3% COMPLETION

99th National Percentile

Average: 163.6 Points

Average: 86.3%

Average: 50.2%

Hashing (Easy)

40 POINTS OUT OF 40

80.0% ACCURACY

COMPLETION: 100.0%

Generate hashes for passwords with the MD5, NTLM, and SHA256 hashing algorithms.

Crack You One More Time (Easy)

50 POINTS OUT OF 50

100.0% ACCURACY

COMPLETION: 100.0%

Crack MD5 and SHA1 password hashes using password cracking tools.

Oph the Dome (Easy)

60 POINTS OUT OF 60

100.0% ACCURACY

COMPLETION: 100.0%

Crack Windows NTLM password hashes using rainbow tables.

Redacted (Medium)

50 POINTS OUT OF 50

100.0% ACCURACY

COMPLETION: 100.0%

Crack an insecure password for a protected PDF file and recover redacted information.

MasKquerade (Medium)

60 POINTS OUT OF 60

100.0% ACCURACY

COMPLETION: 100.0%

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

Enterprise (Hard)

60 POINTS OUT OF 100

80.0% ACCURACY

COMPLETION: 66.7%

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

Scanning & Reconnaissance Module

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

71 ST PLACE OUT OF 7873
NATIONAL RANK

300 POINTS OUT OF 300
PERFORMANCE SCORE

93.8% ACCURACY

100.0% COMPLETION

100th National Percentile

Average: 152.1 Points

Average: 72.9%

Average: 58.2%

Portscan (Easy)

100 POINTS OUT OF 100

100.0% ACCURACY

COMPLETION: 100.0%

Use nmap to scan a machine and discover open ports.

Chain (Medium)

100 POINTS OUT OF 100

83.3% ACCURACY

COMPLETION: 100.0%

Enumerate SMB to locate and retrieve a private SSH key.

I'm TXT (Hard)

100 POINTS OUT OF 100

100.0% ACCURACY

COMPLETION: 100.0%

Enumerate a DNS service to discover hidden files in DNS TXT records.

Web Application Exploitation Module

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

402 ND PLACE OUT OF 7873
NATIONAL RANK

200 POINTS OUT OF 300
PERFORMANCE SCORE

81.8% ACCURACY

75.0% COMPLETION

95th National Percentile

Average: 120.0 Points

Average: 73.0%

Average: 31.8%

Browser (Easy)

100 POINTS OUT OF 100

100.0% ACCURACY

COMPLETION: 100.0%

Exploit a client-side validation weakness in a web application.

Ersatz Motel (Medium)

70 POINTS OUT OF 100

66.7% ACCURACY

COMPLETION: 80.0%

Perform a SQL Injection Union attack to retrieve information.

Micro Fail (Hard)

30 POINTS OUT OF 100

100.0% ACCURACY

COMPLETION: 60.0%

Access sensitive files on a webserver by chaining together a prototype pollution attack with an XML external entity injection attack.