



POWERED BY  
**CYBER SKYLINE**

The National Cyber League  
A Community Where Cybersecurity Is a Passion

Mitchell Patton

# NCL Fall 2025 Individual Game Scouting Report

Dear Mitchell Patton,

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/1QVGK0D635LD](https://cyberskyline.com/report/1QVGK0D635LD)

**CompTIA** Based on the performance detailed in this NCL Scouting Report, you have earned **12 hours** of Continuing Education Units (CEUs) as approved by CompTIA. You can learn more about the NCL - CompTIA alignment via [nationalcyberleague.org/partners](https://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

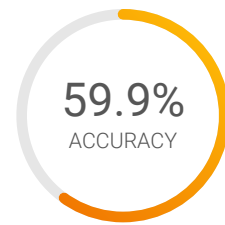
### YOUR TOP CATEGORIES

**NETWORK TRAFFIC  
ANALYSIS**  
97TH PERCENTILE

**WEB APPLICATION  
EXPLOITATION**  
96TH PERCENTILE

**OPEN SOURCE  
INTELLIGENCE**  
96TH PERCENTILE

**NATIONAL RANK**  
**443<sup>RD</sup> PLACE**  
**OUT OF 7873**  
**PERCENTILE**  
**95<sup>TH</sup>**



Average: 61.0%

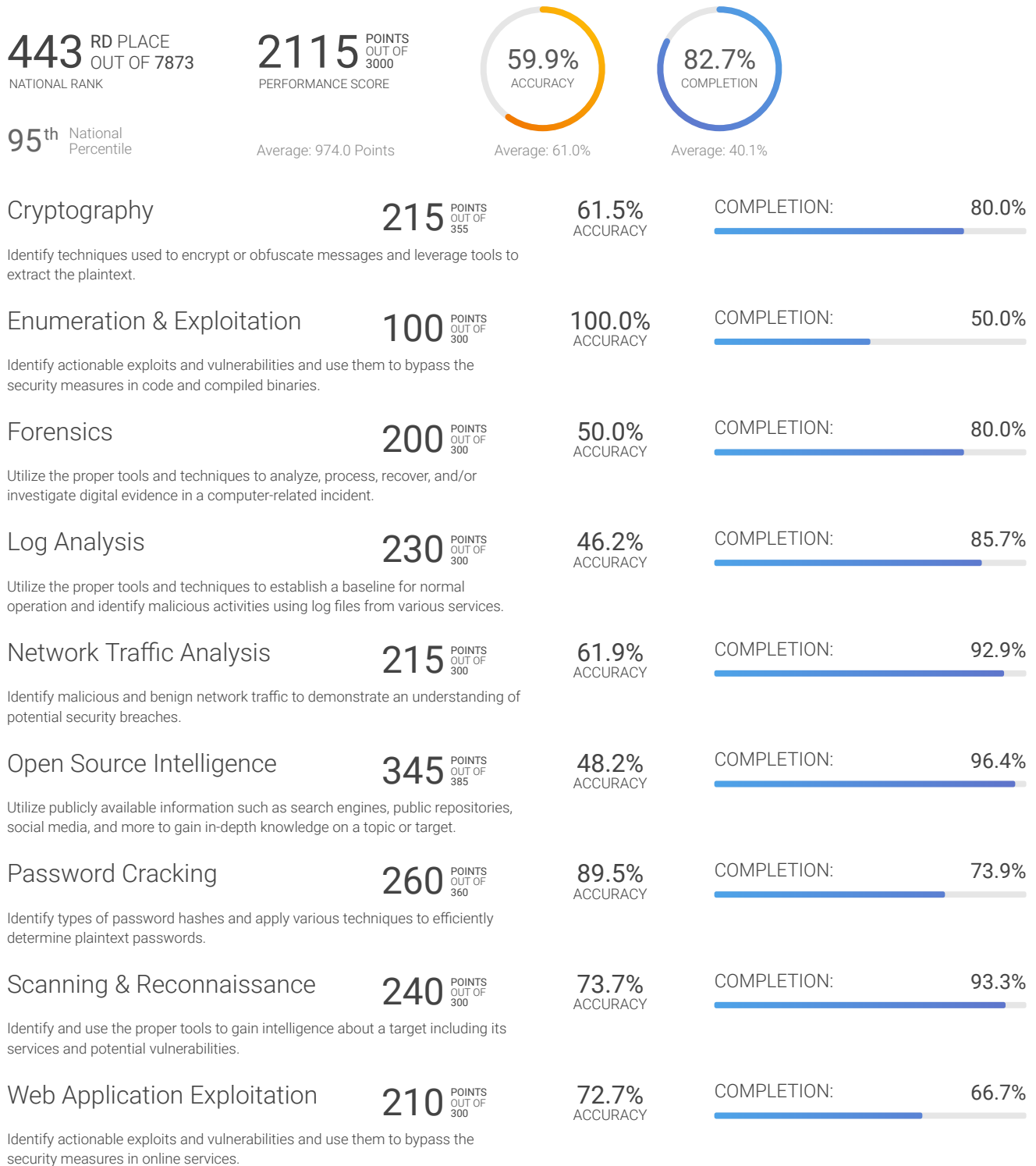
[cyberskyline.com/report/1QVGK0D635LD](https://cyberskyline.com/report/1QVGK0D635LD)

Learn more at [nationalcyberleague.org](https://nationalcyberleague.org)



## 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.



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



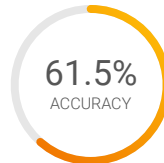


## Cryptography Module

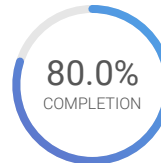
Identify techniques used to encrypt or obfuscate messages and leverage tools to extract the plaintext.

**948** TH PLACE  
OUT OF 7873  
NATIONAL RANK

**215** POINTS  
OUT OF 355  
PERFORMANCE SCORE



Average: 69.5%



Average: 58.2%

**88<sup>th</sup>** National  
Percentile

Average: 157.0 Points

### 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

**75.0%**  
ACCURACY

COMPLETION: **100.0%**

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

### Convenience (Easy)

**60** POINTS  
OUT OF 60

**66.7%**  
ACCURACY

COMPLETION: **100.0%**

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

### 01101011 01100101 01111001 (Medium)

**0** POINTS  
OUT OF 40

**0.0%**  
ACCURACY

COMPLETION: **0.0%**

Decrypt a message using an XOR key.

### Squirtle (Medium)

**30** POINTS  
OUT OF 60

**75.0%**  
ACCURACY

COMPLETION: **60.0%**

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

### Temet Nosce (Hard)

**30** POINTS  
OUT OF 100

**42.9%**  
ACCURACY

COMPLETION: **75.0%**

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



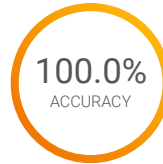


## Enumeration & Exploitation Module

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

**882** ND PLACE  
OUT OF 7873  
NATIONAL RANK

**100** POINTS  
OUT OF 300  
PERFORMANCE SCORE



Average: 60.4%



Average: 49.4%

**89<sup>th</sup>** National  
Percentile

Average: 98.2 Points

### 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)

**0** POINTS  
OUT OF 100

**0.0%**  
ACCURACY

COMPLETION: **0.0%**

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%**

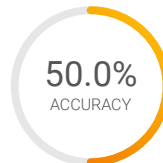
Exploit a race condition in software to return protected data.

## Forensics Module

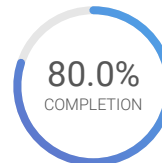
Utilize the proper tools and techniques to analyze, process, recover, and/or investigate digital evidence in a computer-related incident.

**481** ST PLACE  
OUT OF 7873  
NATIONAL RANK

**200** POINTS  
OUT OF 300  
PERFORMANCE SCORE



Average: 45.9%



Average: 48.4%

**94<sup>th</sup>** National  
Percentile

Average: 115.2 Points

### Four & Six (Easy)

**100** POINTS  
OUT OF 100

**53.3%**  
ACCURACY

COMPLETION: **100.0%**

Use a forensics tool to examine unallocated space for files.

### This Bytes (Medium)

**100** POINTS  
OUT OF 100

**44.4%**  
ACCURACY

COMPLETION: **100.0%**

Research JPEG specifications to repair an image.

### Stage Left (Hard)

**0** POINTS  
OUT OF 100

**0.0%**  
ACCURACY

COMPLETION: **0.0%**

Fix a corrupted SQLite database file and analyze the tables.



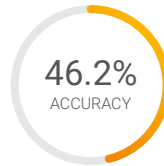


## Log Analysis Module

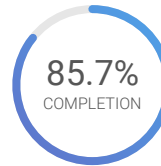
Utilize the proper tools and techniques to establish a baseline for normal operation and identify malicious activities using log files from various services.

**814** TH PLACE  
OUT OF 7873  
NATIONAL RANK

**230** POINTS  
OUT OF 300  
PERFORMANCE SCORE



Average: 55.3%



Average: 61.1%

**90<sup>th</sup>** National  
Percentile

Average: 160.8 Points

### Process This (Easy)

**100** POINTS  
OUT OF 100

**60.0%**  
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

**62.5%**  
ACCURACY

COMPLETION: **100.0%**

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

### Stolen Swipe (Hard)

**30** POINTS  
OUT OF 100

**12.5%**  
ACCURACY

COMPLETION: **33.3%**

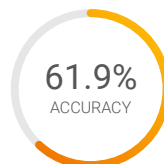
Parse and correlate ATM and EMV Field 55 logs (ISO 8583 standard) to identify a fraudulent transaction.

## Network Traffic Analysis Module

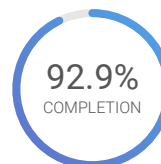
Identify malicious and benign network traffic to demonstrate an understanding of potential security breaches.

**285** TH PLACE  
OUT OF 7873  
NATIONAL RANK

**215** POINTS  
OUT OF 300  
PERFORMANCE SCORE



Average: 51.6%



Average: 45.0%

**97<sup>th</sup>** National  
Percentile

Average: 112.2 Points

### RMM Tool (Easy)

**100** POINTS  
OUT OF 100

**41.7%**  
ACCURACY

COMPLETION: **100.0%**

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

### Drive-by Download (Medium)

**100** POINTS  
OUT OF 100

**85.7%**  
ACCURACY

COMPLETION: **100.0%**

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

### The Insider (Hard)

**15** POINTS  
OUT OF 100

**100.0%**  
ACCURACY

COMPLETION: **66.7%**

Reconstruct a file from UDP packets and decode VBA script.



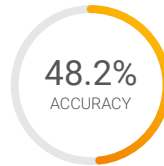


## Open Source Intelligence Module

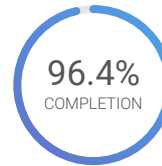
Utilize publicly available information such as search engines, public repositories, social media, and more to gain in-depth knowledge on a topic or target.

**387<sup>TH</sup> PLACE**  
OUT OF 7873  
NATIONAL RANK

**345** POINTS  
OUT OF 385  
PERFORMANCE SCORE



Average: 58.5%



Average: 65.3%

**96<sup>th</sup>** 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

**53.3%**  
ACCURACY

COMPLETION: **100.0%**

Gather key information on NotPetya malware.

### Flamed (Medium)

**15** POINTS  
OUT OF 55

**11.1%**  
ACCURACY

COMPLETION: **50.0%**

Use open source tools to find patterns between GPS locations.

### Material (Medium)

**80** POINTS  
OUT OF 80

**71.4%**  
ACCURACY

COMPLETION: **100.0%**

Use the EDGAR database to filter 8-K filings.

### I Cee Stuff (Hard)

**75** POINTS  
OUT OF 75

**29.4%**  
ACCURACY

COMPLETION: **100.0%**

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



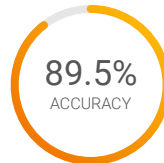


## Password Cracking Module

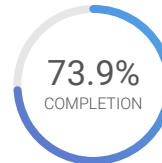
Identify types of password hashes and apply various techniques to efficiently determine plaintext passwords.

**1016** <sup>TH PLACE</sup>  
OUT OF 7873  
NATIONAL RANK

**260** <sup>POINTS</sup>  
OUT OF 360  
PERFORMANCE SCORE



Average: 86.3%



Average: 50.2%

**88<sup>th</sup>** National  
Percentile

Average: 163.6 Points

### Hashing (Easy)

**40** <sup>POINTS</sup>  
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** <sup>POINTS</sup>  
OUT OF 50

**100.0%**  
ACCURACY

COMPLETION: **100.0%**

Crack MD5 and SHA1 password hashes using password cracking tools.

### Oph the Dome (Easy)

**60** <sup>POINTS</sup>  
OUT OF 60

**100.0%**  
ACCURACY

COMPLETION: **100.0%**

Crack Windows NTLM password hashes using rainbow tables.

### Redacted (Medium)

**50** <sup>POINTS</sup>  
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** <sup>POINTS</sup>  
OUT OF 60

**80.0%**  
ACCURACY

COMPLETION: **100.0%**

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

### Enterprise (Hard)

**0** <sup>POINTS</sup>  
OUT OF 100

**0.0%**  
ACCURACY

COMPLETION: **0.0%**

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



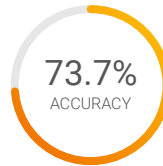


## Scanning & Reconnaissance Module

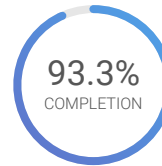
Identify and use the proper tools to gain intelligence about a target including its services and potential vulnerabilities.

**617<sup>TH</sup>** PLACE  
OUT OF 7873  
NATIONAL RANK

**240** POINTS  
OUT OF 300  
PERFORMANCE SCORE



Average: 72.9%



Average: 58.2%

**93<sup>rd</sup>** National  
Percentile

Average: 152.1 Points

### Portscan (Easy)

Use nmap to scan a machine and discover open ports.

**100** POINTS  
OUT OF 100

**100.0%**  
ACCURACY

COMPLETION: **100.0%**

### Chain (Medium)

Enumerate SMB to locate and retrieve a private SSH key.

**100** POINTS  
OUT OF 100

**83.3%**  
ACCURACY

COMPLETION: **100.0%**

### I'm TXT (Hard)

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

**40** POINTS  
OUT OF 100

**50.0%**  
ACCURACY

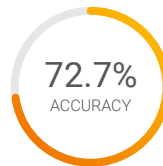
COMPLETION: **80.0%**

## Web Application Exploitation Module

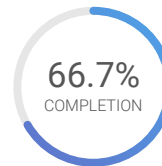
Identify actionable exploits and vulnerabilities and use them to bypass the security measures in online services.

**346<sup>TH</sup>** PLACE  
OUT OF 7873  
NATIONAL RANK

**210** POINTS  
OUT OF 300  
PERFORMANCE SCORE



Average: 73.0%



Average: 31.8%

**96<sup>th</sup>** National  
Percentile

Average: 120.0 Points

### Browser (Easy)

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

**100** POINTS  
OUT OF 100

**100.0%**  
ACCURACY

COMPLETION: **100.0%**

### Ersatz Motel (Medium)

Perform a SQL Injection Union attack to retrieve information.

**100** POINTS  
OUT OF 100

**71.4%**  
ACCURACY

COMPLETION: **100.0%**

### Micro Fail (Hard)

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

**10** POINTS  
OUT OF 100

**50.0%**  
ACCURACY

COMPLETION: **20.0%**

