NCL Fall 2025 Team Game Scouting Report

Dear Ryan Bronder (Team "SANS.edu 864"),

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. You were in the Experienced Students Bracket, consisting of students enrolled in advanced degrees or hold extensive industry working experience.

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/9XCTGHKUPEU2

Congratulations for your participation in the NCL Fall 2025 Team 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

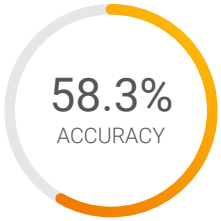
NCL FALL 2025 TEAM GAME

EXPERIENCED STUDENTS RANK
85TH PLACE OUT OF 454

PERCENTILE
82ND

YOUR TOP CATEGORIES

WEB APPLICATION EXPLOITATION	FORENSICS	PASSWORD CRACKING
92ND PERCENTILE	86TH PERCENTILE	86TH PERCENTILE



Average: 69.9%

cyberskyline.com/report
ID: 9XCTGHKUPEU2

NCL Fall 2025 Team Game

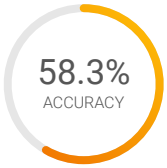
The NCL Team Game is designed for student players nationwide to compete in realtime in the categories listed below. The Team Game promotes camaraderie and evaluates the collective technical cybersecurity skills of the team members.

85 TH PLACE OUT OF 454
EXPERIENCED STUDENTS RANK

2280 POINTS OUT OF 3000
PERFORMANCE SCORE

82nd Experienced Students Percentile

Average: 1852.0 Points



Average: 69.9%

Average: 61.4%

Cryptography

250 POINTS OUT OF 340

65.2% ACCURACY

COMPLETION: 83.3%

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

Enumeration & Exploitation

200 POINTS OUT OF 390

88.2% ACCURACY

COMPLETION: 45.5%

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

Forensics

240 POINTS OUT OF 300

36.0% ACCURACY

COMPLETION: 69.2%

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

Log Analysis

205 POINTS OUT OF 300

34.9% ACCURACY

COMPLETION: 75.0%

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

220 POINTS OUT OF 300

88.9% ACCURACY

COMPLETION: 76.2%

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

Open Source Intelligence

270 POINTS OUT OF 370

37.9% ACCURACY

COMPLETION: 92.6%

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

235 POINTS OUT OF 325

95.2% ACCURACY

COMPLETION: 76.9%

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

Scanning & Reconnaissance

300 POINTS OUT OF 300

84.2% 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

260 POINTS OUT OF 275

85.7% ACCURACY

COMPLETION: 92.3%

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

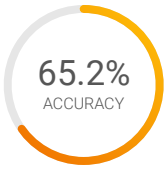
Identify techniques used to encrypt or obfuscate messages and leverage tools to extract the plaintext.

81 ST PLACE OUT OF 454
EXPERIENCED STUDENTS RANK

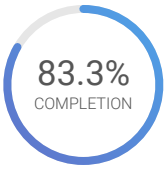
83rd Experienced Students Percentile

250 POINTS OUT OF 340
PERFORMANCE SCORE

Average: 201.0 Points



Average: 64.8%



Average: 64.5%

Steganography (Easy)

30 POINTS OUT OF 30

75.0% ACCURACY

COMPLETION: 100.0%

Decode Whitespace, Trevanion, and Baconian Ciphers.

Layer Cake (Easy)

60 POINTS OUT OF 60

100.0% ACCURACY

COMPLETION: 100.0%

Decode a plaintext string obfuscated by multiple layers of character encoding.

Cryptic Cultures (Easy)

45 POINTS OUT OF 45

42.9% ACCURACY

COMPLETION: 100.0%

Decode ciphers from popular culture.

Quagmire (Medium)

0 POINTS OUT OF 60

0.0% ACCURACY

COMPLETION: 0.0%

Reverse engineer the keys of a Quagmire II cipher through a known-plaintext attack.

Crypto Twister (Medium)

75 POINTS OUT OF 75

100.0% ACCURACY

COMPLETION: 100.0%

Exploit Mersenne Twister PRNG on a Rust TCP server.

Chaos Theory (Hard)

40 POINTS OUT OF 70

75.0% ACCURACY

COMPLETION: 75.0%

Use entropy analysis and cryptographic fuzzing to decrypt a binary file.

Enumeration & Exploitation Module

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

97 TH PLACE OUT OF **454**
EXPERIENCED STUDENTS RANK

200 POINTS OUT OF 390
PERFORMANCE SCORE

88.2% ACCURACY
Average: 55.5%

45.5% COMPLETION
Average: 39.3%

79th Experienced Students Percentile

Average: 193.7 Points

Cooking Lunch (Easy)

100 POINTS OUT OF 100

75.0% ACCURACY

COMPLETION: 100.0%

Reverse engineer the required input of an obfuscated program.

Poliwhirl (Medium)

50 POINTS OUT OF 100

100.0% ACCURACY

COMPLETION: 75.0%

Reverse engineer an optimized RISC-V binary.

Cooking Dinner (Hard)

0 POINTS OUT OF 50

0.0% ACCURACY

COMPLETION: 0.0%

Reverse engineer the functionality of an obfuscated program from the given output.

MAINFRAME - Access the Mainframe

50 POINTS OUT OF 140

90.0% ACCURACY

COMPLETION: 37.5%

Perform program execution, backdooring, and buffer overflow attacks on z/OS mainframes.

Forensics Module

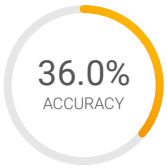
Utilize the proper tools and techniques to analyze, process, recover, and/or investigate digital evidence in a computer-related incident.

64 TH PLACE OUT OF **454**
EXPERIENCED STUDENTS RANK

240 POINTS OUT OF 300
PERFORMANCE SCORE

86th Experienced Students Percentile

Average: 159.2 Points



Average: 60.4%

Average: 51.0%

Colorwork (Easy)	100 POINTS OUT OF 100	100.0% ACCURACY	COMPLETION: 100.0%
Use manual and/or automated tools to find information hidden within an image.			
Technical Difficulties (Medium)	100 POINTS OUT OF 100	100.0% ACCURACY	COMPLETION: 100.0%
Manually apply an incremental patch to restore data from a corrupted backup archive.			
Split Keys (Hard)	20 POINTS OUT OF 75	15.4% ACCURACY	COMPLETION: 40.0%
Recover artifacts from a process dump and decrypt the hidden message.			
MAINFRAME - Hack the Gibson	20 POINTS OUT OF 25	37.5% ACCURACY	COMPLETION: 75.0%
Decode XMI files and crack RACF hashes to get mainframe logins.			

Log Analysis Module

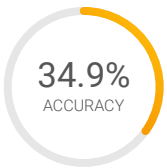
Utilize the proper tools and techniques to establish a baseline for normal operation and identify malicious activities using log files from various services.

113 TH PLACE OUT OF **454**
EXPERIENCED STUDENTS RANK

205 POINTS OUT OF 300
PERFORMANCE SCORE

76th Experienced Students Percentile

Average: 195.7 Points



Average: 60.0%

Average: 67.7%

LO(L)G (Easy)	90 POINTS OUT OF 100	25.0% ACCURACY	COMPLETION: 100.0%
Analyze the attack chain of ClickFix family malware in a Sysmon xml file.			
JSON Query (Medium)	100 POINTS OUT OF 100	62.5% ACCURACY	COMPLETION: 100.0%
Parse and analyze Suricata eve.json logs to identify C2 activity.			
Chronicles of XP (Hard)	15 POINTS OUT OF 100	66.7% ACCURACY	COMPLETION: 28.6%
Parse a custom binary file based on the provided specs to decode the data.			

Network Traffic Analysis Module

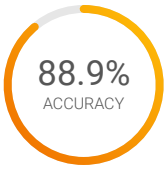
Identify malicious and benign network traffic to demonstrate an understanding of potential security breaches.

80 TH PLACE OUT OF 454
EXPERIENCED STUDENTS RANK

83rd Experienced Students Percentile

220 POINTS OUT OF 300
PERFORMANCE SCORE

Average: 188.2 Points



Average: 61.8%

Average: 64.0%

Snakes and Packets (Easy)

100 POINTS OUT OF 100

100.0% ACCURACY

COMPLETION: 100.0%

Analyze a packet capture to detect data exfiltration through SMTP.

An Offer You Can't Refuse (Medium)

100 POINTS OUT OF 100

100.0% ACCURACY

COMPLETION: 100.0%

Identify specific characteristics of a rogue DHCP server from a packet capture.

Patient Zero (Hard)

20 POINTS OUT OF 100

50.0% ACCURACY

COMPLETION: 28.6%

Examine and parse a custom protocol used to transmit patient information, similar to HL7.

Open Source Intelligence Module

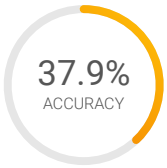
Utilize publicly available information such as search engines, public repositories, social media, and more to gain in-depth knowledge on a topic or target.

117 TH PLACE OUT OF 454
EXPERIENCED STUDENTS RANK

270 POINTS OUT OF 370
PERFORMANCE SCORE

75th Experienced Students Percentile

Average: 267.0 Points



Average: 69.3%

Average: 80.8%

Rules of Conduct (Easy)

30 POINTS OUT OF 30

100.0% ACCURACY

COMPLETION: 100.0%

Introductory challenge on acceptable conduct during NCL.

Cruise Ship (Easy)

50 POINTS OUT OF 50

50.0% ACCURACY

COMPLETION: 100.0%

Identify and locate a cruise ship by cross-referencing its itinerary with an EXIF timestamp.

Finding Room 47 (Easy)

50 POINTS OUT OF 50

100.0% ACCURACY

COMPLETION: 100.0%

Use OSINT to research clues from an old puzzle book.

Tooling (Medium)

60 POINTS OUT OF 60

33.3% ACCURACY

COMPLETION: 100.0%

Perform OSINT on an image using EXIF data and online research to find key information.

Still Controversial? (Medium)

60 POINTS OUT OF 80

17.9% ACCURACY

COMPLETION: 83.3%

Investigate publicly available information on a company's data breach.

Guiding Light (Hard)

20 POINTS OUT OF 100

25.0% ACCURACY

COMPLETION: 50.0%

Triangulate a location using EXIF timestamp data and shadow lengths.

Password Cracking Module

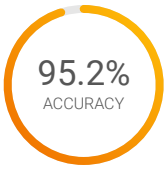
Identify types of password hashes and apply various techniques to efficiently determine plaintext passwords.

66 TH PLACE OUT OF 454
EXPERIENCED STUDENTS RANK

86th Experienced Students Percentile

235 POINTS OUT OF 325
PERFORMANCE SCORE

Average: 173.9 Points



Average: 85.2%

Average: 58.7%

Hash it Out (Easy)

40 POINTS OUT OF 40

100.0% ACCURACY

COMPLETION: 100.0%

Generate hashes for passwords with the MD5, NTLM, SHA1 and SHA256 hashing algorithms.

Zeitgeist (Easy)

50 POINTS OUT OF 50

100.0% ACCURACY

COMPLETION: 100.0%

Crack MD5 hashed passwords with a wordlist.

Peninsula-Password (Medium)

50 POINTS OUT OF 50

75.0% ACCURACY

COMPLETION: 100.0%

Crack NTLM Windows Passwords using the EFF's wordlists.

DBs (Medium)

45 POINTS OUT OF 70

100.0% ACCURACY

COMPLETION: 80.0%

Crack an NTLMv2 hash and Blake2b password to decrypt an MSSQL database.

Règles (Medium)

50 POINTS OUT OF 50

100.0% ACCURACY

COMPLETION: 100.0%

Crack modified passwords from a leaked database using Hashcat's rule attack mode.

Magic (Hard)

0 POINTS OUT OF 65

0.0% ACCURACY

COMPLETION: 0.0%

Crack passwords by creating a wordlist, 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.

67 TH PLACE OUT OF 454
EXPERIENCED STUDENTS RANK

300 POINTS OUT OF 300
PERFORMANCE SCORE

84.2% ACCURACY

100.0% COMPLETION

86th Experienced Students Percentile

Average: 204.7 Points

Average: 69.3%

Average: 69.8%

Open (Easy)

100 POINTS OUT OF 100

71.4% ACCURACY

COMPLETION: 100.0%

Scan a server to determine information about running services.

Git A Gander (Medium)

100 POINTS OUT OF 100

100.0% ACCURACY

COMPLETION: 100.0%

Manually scan a code repository for secrets in its commit history.

Walk (Hard)

100 POINTS OUT OF 100

85.7% ACCURACY

COMPLETION: 100.0%

Scan a server to discover an SNMP service and use nmap scripts and default credentials to reveal sensitive information.

Web Application Exploitation Module

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

40 TH PLACE OUT OF 454
EXPERIENCED STUDENTS RANK

260 POINTS OUT OF 275
PERFORMANCE SCORE

85.7% ACCURACY

92.3% COMPLETION

92nd Experienced Students Percentile

Average: 185.4 Points

Average: 75.4%

Average: 62.5%

Something's Fishy (Easy)

100 POINTS OUT OF 100

100.0% ACCURACY

COMPLETION: 100.0%

Find and exploit a client-side validated function to bypass checks and set an arbitrary score.

Picto (Medium)

100 POINTS OUT OF 100

66.7% ACCURACY

COMPLETION: 100.0%

Exploit open-box XSS on unsanitized rendered output in a browser.

The Cucumber's Secret (Hard)

60 POINTS OUT OF 75

100.0% ACCURACY

COMPLETION: 83.3%

Abuse unsafe Python pickle data streams in a web application.