NCL Fall 2025 Team Game Scouting Report

Dear Mitchell Patton (Team "SANS 557"),

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/K32DDLQWB9M2

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

NATIONAL CYBER LEAGUE SCORE CARD
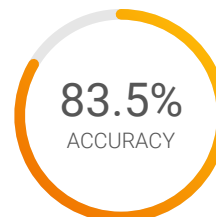
NCL FALL 2025 TEAM GAME

NATIONAL RANK

29TH PLACE OUT OF 4214

PERCENTILE

100TH

YOUR TOP CATEGORIES

OPEN SOURCE INTELLIGENCE	WEB APPLICATION EXPLOITATION	FORENSICS
100TH PERCENTILE	100TH PERCENTILE	100TH PERCENTILE

83.5% ACCURACY

Average: 56.1%

cyberskyline.com/report
ID: K32DDLQWB9M2

Learn more at nationalcyberleague.org

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.

29 TH PLACE OUT OF **4214**
NATIONAL RANK

100th National Percentile

2840 POINTS OUT OF 3000
PERFORMANCE SCORE

Average: 1098.3 Points

83.5% ACCURACY

Average: 56.1%

94.1% COMPLETION

Average: 37.8%

Cryptography

310 POINTS OUT OF 340   **94.4%** ACCURACY   COMPLETION: **94.4%**

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

Enumeration & Exploitation

350 POINTS OUT OF 390   **87.1%** ACCURACY   COMPLETION: **81.8%**

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

Forensics

275 POINTS OUT OF 300   **85.7%** ACCURACY   COMPLETION: **92.3%**

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   **80.0%** 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

285 POINTS OUT OF 300   **52.6%** ACCURACY   COMPLETION: **95.2%**

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

Open Source Intelligence

370 POINTS OUT OF 370   **93.1%** ACCURACY   COMPLETION: **100.0%**

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

275 POINTS OUT OF 325   **100.0%** ACCURACY   COMPLETION: **92.3%**

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

Scanning & Reconnaissance

300 POINTS OUT OF 300   **94.1%** 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

275 POINTS OUT OF 275   **86.7%** ACCURACY   COMPLETION: **100.0%**

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

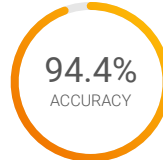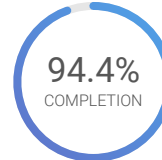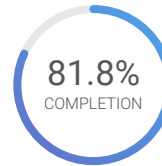Note: Survey module (100 points) was excluded from this report.

Cryptography Module

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

44 TH PLACE
OUT OF 4214
NATIONAL RANK

99th National Percentile

310 POINTS
OUT OF 340
PERFORMANCE SCORE

Average: 119.8 Points

94.4%
ACCURACY

Average: 40.9%

94.4%
COMPLETION

Average: 39.5%

Steganography (Easy)
Decode Whitespace, Trevanion, and Baconian Ciphers.

30 POINTS OUT OF 30 | **100.0%** ACCURACY | COMPLETION: 100.0%

Layer Cake (Easy)
Decode a plaintext string obfuscated by multiple layers of character encoding.

60 POINTS OUT OF 60 | **100.0%** ACCURACY | COMPLETION: 100.0%

Cryptic Cultures (Easy)
Decode ciphers from popular culture.

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

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

60 POINTS OUT OF 60 | **66.7%** ACCURACY | COMPLETION: 100.0%

Crypto Twister (Medium)
Exploit Mersenne Twister PRNG on a Rust TCP server.

75 POINTS OUT OF 75 | **100.0%** ACCURACY | COMPLETION: 100.0%

Chaos Theory (Hard)
Use entropy analysis and cryptographic fuzzing to decrypt a binary file.

40 POINTS OUT OF 70 | **100.0%** ACCURACY | COMPLETION: 75.0%

Enumeration & Exploitation Module

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

49 TH PLACE
OUT OF **4214**
NATIONAL RANK

99th National Percentile

350 POINTS OUT OF 390
PERFORMANCE SCORE
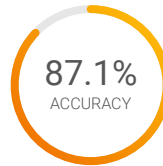
Average: 100.3 Points

87.1% ACCURACY

Average: 32.1%

81.8% COMPLETION

Average: 18.7%

Cooking Lunch (Easy)

Reverse engineer the required input of an obfuscated program.

100 POINTS OUT OF 100 — **100.0%** ACCURACY — COMPLETION: **100.0%**

Poliwhirl (Medium)

Reverse engineer an optimized RISC-V binary.

100 POINTS OUT OF 100 — **100.0%** ACCURACY — COMPLETION: **100.0%**

Cooking Dinner (Hard)

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

50 POINTS OUT OF 50 — **66.7%** ACCURACY — COMPLETION: **100.0%**

MAINFRAME - Access the Mainframe

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

100 POINTS OUT OF 140 — **85.7%** ACCURACY — COMPLETION: **75.0%**

Forensics Module

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

39 TH PLACE
OUT OF **4214**
NATIONAL RANK

100th National Percentile

275 POINTS
OUT OF 300
PERFORMANCE SCORE
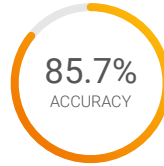
Average: 77.7 Points

85.7% ACCURACY

Average: 33.6%
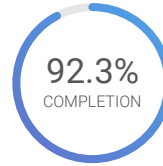
92.3% COMPLETION

Average: 24.8%

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)
50 POINTS OUT OF 75 — **66.7%** ACCURACY — COMPLETION: 80.0%

Recover artifacts from a process dump and decrypt the hidden message.

MAINFRAME - Hack the Gibson
25 POINTS OUT OF 25 — **100.0%** ACCURACY — COMPLETION: 100.0%

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.

52 ND PLACE
OUT OF **4214**
NATIONAL RANK

99th National Percentile

300 POINTS
OUT OF 300
PERFORMANCE SCORE
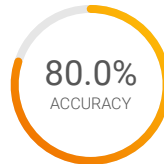
Average: 120.8 Points

80.0% ACCURACY

Average: 40.2%

100.0% COMPLETION

Average: 43.4%

LO(L)G (Easy)
100 POINTS OUT OF 100 — **100.0%** 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 — **100.0%** ACCURACY — COMPLETION: 100.0%

Parse and analyze Suricata eve.json logs to identify C2 activity.

Chronicles of XP (Hard)
100 POINTS OUT OF 100 — **58.3%** ACCURACY — COMPLETION: 100.0%

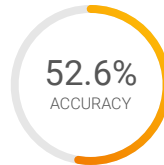Parse a custom binary file based on the provided specs to decode the data.
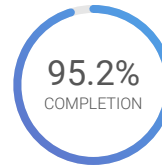
Network Traffic Analysis Module

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

41 ST PLACE
OUT OF **4214**
NATIONAL RANK

100th National
Percentile

285 POINTS
OUT OF
300
PERFORMANCE SCORE

Average: 105.8 Points

52.6%
ACCURACY

Average: 36.7%

95.2%
COMPLETION

Average: 36.1%

Snakes and Packets (Easy)

100 POINTS OUT OF 100

85.7% 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)

85 POINTS OUT OF 100

26.1% ACCURACY

COMPLETION: 85.7%

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.

29 TH PLACE
OUT OF **4214**
NATIONAL RANK

100th National Percentile

370 POINTS OUT OF 370
PERFORMANCE SCORE

Average: 197.1 Points

93.1%
ACCURACY
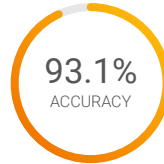
Average: 55.2%

100.0%
COMPLETION

Average: 64.9%

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 | **100.0%** 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 | **100.0%** ACCURACY | COMPLETION: 100.0%

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

Still Controversial? (Medium)

80 POINTS OUT OF 80 | **100.0%** ACCURACY | COMPLETION: 100.0%

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

Guiding Light (Hard)

100 POINTS OUT OF 100 | **50.0%** ACCURACY | COMPLETION: 100.0%

Triangulate a location using EXIF timestamp data and shadow lengths.
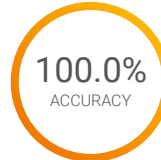
POWERED BY
CYBER SKYLINE

Password Cracking Module

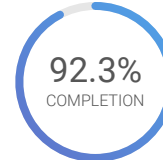Identify types of password hashes and apply various techniques to efficiently determine plaintext passwords.

66 TH PLACE
OUT OF **4214**
NATIONAL RANK

99th National
Percentile

275 POINTS
OUT OF
325
PERFORMANCE SCORE

Average: 101.8 Points

100.0%
ACCURACY

Average: 67.2%

92.3%
COMPLETION

Average: 36.9%

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

100.0% ACCURACY

COMPLETION: 100.0%

Crack NTLM Windows Passwords using the EFF's wordlists.

DBs (Medium)

70 POINTS OUT OF 70

100.0% ACCURACY

COMPLETION: 100.0%

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)

15 POINTS OUT OF 65

100.0% ACCURACY

COMPLETION: 60.0%

Crack passwords by creating a wordlist, augmenting permutation rules using known password complexity requirements.
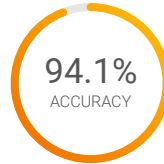
POWERED BY
CYBER SKYLINE

POWERED BY
CYBER SKYLINE

Scanning & Reconnaissance Module

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

51 ST PLACE
OUT OF **4214**
NATIONAL RANK

99th National Percentile

300 POINTS OUT OF 300
PERFORMANCE SCORE

Average: 105.6 Points

94.1% ACCURACY

Average: 41.8%

100.0% COMPLETION

Average: 37.2%

Open (Easy)
100 POINTS OUT OF 100   **83.3%** 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)
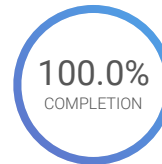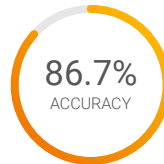**100** POINTS OUT OF 100   **100.0%** ACCURACY   COMPLETION: **100.0%**

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.

32 ND PLACE
OUT OF **4214**
NATIONAL RANK

100th National Percentile

275 POINTS OUT OF 275
PERFORMANCE SCORE

Average: 104.8 Points

86.7% ACCURACY

Average: 52.7%

100.0% COMPLETION

Average: 34.5%

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   **100.0%** ACCURACY   COMPLETION: **100.0%**

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

The Cucumber's Secret (Hard)
75 POINTS OUT OF 75   **75.0%** ACCURACY   COMPLETION: **100.0%**

Abuse unsafe Python pickle data streams in a web application.

POWERED BY
CYBER SKYLINE