



# NCL Spring 2026 Team Game Scouting Report

Dear Dale Faubion (Team "while true; do figlet WIN | wall; done;"),

Thank you for participating in the National Cyber League (NCL) Spring 2026 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 2026 Season had 7,520 students/players and 583 faculty/coaches from more than 440 two- and four-year schools & 220 high schools across all 50 U.S. states registered to play. The Individual Game Capture the Flag (CTF) event took place from April 10 through April 12. The Team Game CTF event took place from April 24 through April 26. 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/32K13Q49EJC7](https://cyberskyline.com/report/32K13Q49EJC7)

Congratulations for your participation in the NCL Spring 2026 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

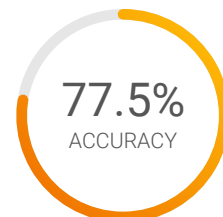


## NATIONAL CYBER LEAGUE SCORE CARD

NCL SPRING 2026 TEAM GAME

**EXPERIENCED STUDENTS RANK**  
**37<sup>TH</sup> PLACE**  
**OUT OF 341**  
**PERCENTILE**  
**90<sup>TH</sup>**

### YOUR TOP CATEGORIES



Average: 71.7%

[cyberskyline.com/report/32K13Q49EJC7](https://cyberskyline.com/report/32K13Q49EJC7)

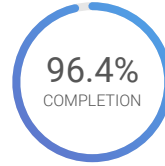
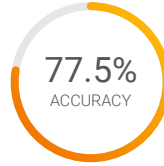


# NCL Spring 2026 Team Game

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.

**37<sup>TH</sup> PLACE**  
OUT OF 341  
EXPERIENCED STUDENTS RANK

**2845** POINTS  
OUT OF 3000  
PERFORMANCE SCORE



**90<sup>th</sup>** Experienced Students  
Percentile

Average: 1942.6 Points

Average: 71.7%

Average: 68.8%

## Cryptography

**300** POINTS  
OUT OF 360

**86.7%**  
ACCURACY

COMPLETION: **92.9%**

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

## Enumeration & Exploitation

**300** POINTS  
OUT OF 300

**93.8%**  
ACCURACY

COMPLETION: **100.0%**

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

## Forensics

**230** POINTS  
OUT OF 300

**52.0%**  
ACCURACY

COMPLETION: **76.5%**

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

**300** POINTS  
OUT OF 300

**80.0%**  
ACCURACY

COMPLETION: **100.0%**

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

## Open Source Intelligence

**360** POINTS  
OUT OF 385

**65.2%**  
ACCURACY

COMPLETION: **95.6%**

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

**355** POINTS  
OUT OF 355

**100.0%**  
ACCURACY

COMPLETION: **100.0%**

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

## Scanning & Reconnaissance

**300** POINTS  
OUT OF 300

**100.0%**  
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

**300** POINTS  
OUT OF 300

**77.3%**  
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.



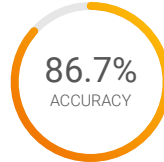


# Cryptography Module

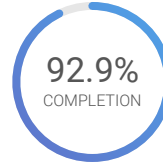
Identify techniques used to encrypt or obfuscate messages and leverage tools to extract the plaintext.

**54** TH PLACE  
OUT OF 341  
EXPERIENCED STUDENTS RANK

**300** POINTS  
OUT OF  
360  
PERFORMANCE SCORE



Average: 72.3%



Average: 72.6%

**85**th Experienced Students  
Percentile

Average: 230.1 Points

## Paper Chase (Easy)

**30** POINTS  
OUT OF  
30

**100.0%**  
ACCURACY

COMPLETION: **100.0%**

Manually extract a flag from an image of a punch card.

## Hex password (Easy)

**60** POINTS  
OUT OF  
60

**66.7%**  
ACCURACY

COMPLETION: **100.0%**

Recover a password that has been XOR-encrypted and encoded in UTF-16.

## Decoding (Easy)

**60** POINTS  
OUT OF  
60

**100.0%**  
ACCURACY

COMPLETION: **100.0%**

Identify and decrypt different cipher schemes.

## Unc's Encryption (Medium)

**100** POINTS  
OUT OF  
100

**100.0%**  
ACCURACY

COMPLETION: **100.0%**

Exploit poor implementation of ECDSA signatures through r value reuse.

## Collisions (Medium)

**50** POINTS  
OUT OF  
50

**100.0%**  
ACCURACY

COMPLETION: **100.0%**

Forge a message that produces a truncated SHA1 hash collision.

## Checkpoint (Hard)

**0** POINTS  
OUT OF  
60

**0.0%**  
ACCURACY

COMPLETION: **0.0%**

Flip bits in AES-CBC ciphertext to forge a trusted session token.



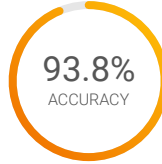


## Enumeration & Exploitation Module

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

**27<sup>TH</sup> PLACE**  
OUT OF 341  
EXPERIENCED STUDENTS RANK

**300** POINTS  
OUT OF 300  
PERFORMANCE SCORE



Average: 80.1%



Average: 76.2%

**93<sup>RD</sup>** Experienced Students  
Percentile

Average: 217.9 Points

### Getting into the Router (Easy)

**100** POINTS  
OUT OF 100

**100.0%**  
ACCURACY

COMPLETION: **100.0%**

Decompile a compiled python library and fix the bugs in it to retrieve the correct password.

### Casserole (Medium)

**100** POINTS  
OUT OF 100

**83.3%**  
ACCURACY

COMPLETION: **100.0%**

Craft and execute a shellcode with NOP sleds in order to exploit a binary.

### Malware Sample (Hard)

**100** POINTS  
OUT OF 100

**100.0%**  
ACCURACY

COMPLETION: **100.0%**

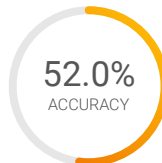
Chain a buffer overflow with a use-after-free vulnerability to bypass a software MTE simulator protecting a DGA botnet client.

## Forensics Module

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

**72<sup>ND</sup> PLACE**  
OUT OF 341  
EXPERIENCED STUDENTS RANK

**230** POINTS  
OUT OF 300  
PERFORMANCE SCORE



Average: 61.2%



Average: 70.5%

**79<sup>TH</sup>** Experienced Students  
Percentile

Average: 212.1 Points

### Parallel (Easy)

**100** POINTS  
OUT OF 100

**83.3%**  
ACCURACY

COMPLETION: **100.0%**

Carve out recursive file embedding in images and files using file signatures.

### In Plain Sight (Medium)

**100** POINTS  
OUT OF 100

**50.0%**  
ACCURACY

COMPLETION: **100.0%**

Identify IoCs and extract a zip file using hex carving from an RTF document.

### Reg Recon (Hard)

**30** POINTS  
OUT OF 100

**33.3%**  
ACCURACY

COMPLETION: **42.9%**

Identify Indicators of Compromise in Windows registry.



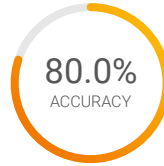


## Log Analysis Module

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

**27<sup>TH</sup> PLACE**  
OUT OF 341  
EXPERIENCED STUDENTS RANK

**300** POINTS  
OUT OF 300  
PERFORMANCE SCORE



Average: 67.6%



Average: 77.5%

**93<sup>RD</sup>** Experienced Students  
Percentile

Average: 220.1 Points

### Unwelcome Robots (Easy)

**100** POINTS  
OUT OF 100

**100.0%**  
ACCURACY

COMPLETION: **100.0%**

Parse Apache combined log format access logs to identify a threat actor.

### Falling Off a Log (Medium)

**100** POINTS  
OUT OF 100

**100.0%**  
ACCURACY

COMPLETION: **100.0%**

Extract information from a common Linux log format.

### Survival Bias (Hard)

**100** POINTS  
OUT OF 100

**54.5%**  
ACCURACY

COMPLETION: **100.0%**

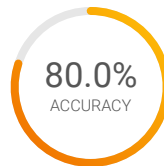
Process and cross reference json logs and provided intelligence to synthesize key information.

## Network Traffic Analysis Module

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

**66<sup>TH</sup> PLACE**  
OUT OF 341  
EXPERIENCED STUDENTS RANK

**300** POINTS  
OUT OF 300  
PERFORMANCE SCORE



Average: 74.8%



Average: 79.1%

**81<sup>ST</sup>** Experienced Students  
Percentile

Average: 238.8 Points

### WitSec (Easy)

**100** POINTS  
OUT OF 100

**83.3%**  
ACCURACY

COMPLETION: **100.0%**

Extract an image from HTTP network traffic.

### Crafty Communique (Medium)

**100** POINTS  
OUT OF 100

**78.6%**  
ACCURACY

COMPLETION: **100.0%**

Extract information about players and chat messages from Minecraft server packets.

### What is on the LAN? (Hard)

**100** POINTS  
OUT OF 100

**80.0%**  
ACCURACY

COMPLETION: **100.0%**

Find specific devices and traffic types on a network from a packet capture.



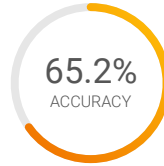


# Open Source Intelligence Module

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

**54** TH PLACE  
OUT OF 341  
EXPERIENCED STUDENTS RANK

**360** POINTS  
OUT OF 385  
PERFORMANCE SCORE



Average: 70.9%



Average: 76.7%

**85**th Experienced Students  
Percentile

Average: 274.3 Points

## Rules of Conduct (Easy)

**45** POINTS  
OUT OF 45

**100.0%**  
ACCURACY

COMPLETION: **100.0%**

Introductory challenge on acceptable conduct during NCL.

## MEROPS (Easy)

**50** POINTS  
OUT OF 50

**71.4%**  
ACCURACY

COMPLETION: **100.0%**

Identify key search terms and execute search for information.

## ATT&CKED (Easy)

**75** POINTS  
OUT OF 75

**81.8%**  
ACCURACY

COMPLETION: **100.0%**

Research and distill threat reporting to map adversary Tactics, Techniques, and Procedures (TTPs) to the MITRE ATT&CK framework.

## Boarding Pass (Medium)

**90** POINTS  
OUT OF 90

**68.8%**  
ACCURACY

COMPLETION: **100.0%**

Decode a boarding pass barcode and use historical ADS-B data to discover information about a flight.

## This Way Pleaaee! (Medium)

**35** POINTS  
OUT OF 50

**30.0%**  
ACCURACY

COMPLETION: **75.0%**

Interpret coded messages to uncover a targeted operation.

## Tracking the Tracker (Hard)

**65** POINTS  
OUT OF 75

**46.2%**  
ACCURACY

COMPLETION: **85.7%**

Cross reference Kismet GPS/WiFi/BLE logs with publicly available data.



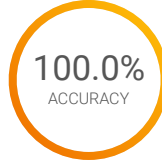


# Password Cracking Module

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

**1** ST PLACE  
OUT OF 341  
EXPERIENCED STUDENTS RANK

**355** POINTS  
OUT OF  
355  
PERFORMANCE SCORE



Average: 81.1%



Average: 77.7%

**100**<sup>th</sup> Experienced Students  
Percentile

Average: 252.7 Points

## ID Me (Easy)

Identify MD5, SHA256, bcrypt, and JWT strings.

**40** POINTS  
OUT OF  
40

**100.0%**  
ACCURACY

COMPLETION: **100.0%**

## Bitcoin Hashes (Easy)

Generate random strings and hash them until the output contains the requested characters.

**45** POINTS  
OUT OF  
45

**100.0%**  
ACCURACY

COMPLETION: **100.0%**

## Lightly Seasoned (Easy)

Use a known plaintext attack to extract a user's password from a database of hashed passwords.

**40** POINTS  
OUT OF  
40

**100.0%**  
ACCURACY

COMPLETION: **100.0%**

## 2-Ways (Medium)

Crack wireless passwords from packet captures using aircrack-ng and hashcat.

**50** POINTS  
OUT OF  
50

**100.0%**  
ACCURACY

COMPLETION: **100.0%**

## l33t p45\$vv0rc1z (Medium)

Perform a wordlist attack by generating possible candidates from known behaviors.

**100** POINTS  
OUT OF  
100

**100.0%**  
ACCURACY

COMPLETION: **100.0%**

## Unlocking 2 (Hard)

Generate BitLocker recovery key wordlists, crack the key, and decrypt the drive.

**80** POINTS  
OUT OF  
80

**100.0%**  
ACCURACY

COMPLETION: **100.0%**



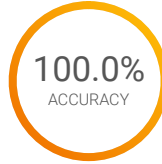


## Scanning & Reconnaissance Module

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

**17<sup>TH</sup> PLACE**  
OUT OF 341  
EXPERIENCED STUDENTS RANK

**300** POINTS  
OUT OF 300  
PERFORMANCE SCORE



**96<sup>th</sup>** Experienced Students  
Percentile

Average: 232.8 Points

Average: 83.9%

Average: 78.4%

### PrinT Farm (Easy)

**100** POINTS  
OUT OF 100

**100.0%**  
ACCURACY

COMPLETION: **100.0%**

Scan a target to identify vulnerable services and extract information.

### Off Topic (Medium)

**100** POINTS  
OUT OF 100

**100.0%**  
ACCURACY

COMPLETION: **100.0%**

Scan an IoT network and subscribe to MQTT topics to identify IoTs.

### AppScan (Hard)

**100** POINTS  
OUT OF 100

**100.0%**  
ACCURACY

COMPLETION: **100.0%**

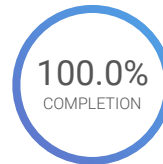
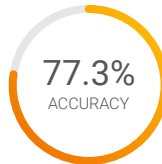
Analyze Static Application Security Testing tool outputs and develop a rule to improve vulnerability detection.

## Web Application Exploitation Module

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

**27<sup>TH</sup> PLACE**  
OUT OF 341  
EXPERIENCED STUDENTS RANK

**300** POINTS  
OUT OF 300  
PERFORMANCE SCORE



**93<sup>rd</sup>** Experienced Students  
Percentile

Average: 187.5 Points

Average: 67.9%

Average: 67.1%

### Pairs (Easy)

**80** POINTS  
OUT OF 80

**100.0%**  
ACCURACY

COMPLETION: **100.0%**

Identify sensitive data stored in HTML attributes.

### Stylish (Medium)

**100** POINTS  
OUT OF 100

**55.6%**  
ACCURACY

COMPLETION: **100.0%**

Discover and validate a LESS.js Server Side Template Injection (SSTI) vulnerability.

### Modern Tech Stack (Hard)

**120** POINTS  
OUT OF 120

**90.0%**  
ACCURACY

COMPLETION: **100.0%**

Exfiltrate secrets using three advanced web vulnerability classes: type confusion, mutation XSS, and web cache deception.

