NCL Spring 2026 Team Game Scouting Report

Dear Nicholas Massei (Team "NSU Cyberhawks"),

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.

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/3PGR56HXTTL4

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

POWERED BY CYBER SKYLINE

NATIONAL CYBER LEAGUE SCORE CARD

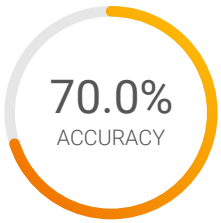
NCL SPRING 2026 TEAM GAME

NATIONAL RANK
301ST PLACE OUT OF 3634

PERCENTILE
92ND

YOUR TOP CATEGORIES

ENUMERATION & EXPLOITATION	CRYPTOGRAPHY	PASSWORD CRACKING
96TH PERCENTILE	95TH PERCENTILE	95TH PERCENTILE



Average: 61.4%

cyberskyline.com/report
ID: 3PGR56HXTTL4

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.

301 ST PLACE OUT OF 3634
NATIONAL RANK

2095 POINTS OUT OF 3000
PERFORMANCE SCORE

70.0% ACCURACY
Average: 61.4%

75.1% COMPLETION
Average: 46.1%

92nd National Percentile
Average: 1222.1 Points

Cryptography

300 POINTS OUT OF 360

50.0% ACCURACY

COMPLETION: **92.9%**

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

Enumeration & Exploitation

260 POINTS OUT OF 300

93.3% ACCURACY

COMPLETION: **93.3%**

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

Forensics

95 POINTS OUT OF 300

35.0% ACCURACY

COMPLETION: **41.2%**

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

Log Analysis

200 POINTS OUT OF 300

66.7% ACCURACY

COMPLETION: **70.0%**

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

150 POINTS OUT OF 300

60.0% ACCURACY

COMPLETION: **50.0%**

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

Open Source Intelligence

275 POINTS OUT OF 385

75.5% ACCURACY

COMPLETION: **82.2%**

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

305 POINTS OUT OF 355

85.7% ACCURACY

COMPLETION: **92.3%**

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

Scanning & Reconnaissance

200 POINTS OUT OF 300

100.0% ACCURACY

COMPLETION: **64.3%**

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

Web Application Exploitation

210 POINTS OUT OF 300

77.8% ACCURACY

COMPLETION: **82.4%**

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.

196 TH PLACE OUT OF 3634
NATIONAL RANK

300 POINTS OUT OF 360
PERFORMANCE SCORE

50.0% ACCURACY
Average: 57.2%

92.9% COMPLETION
Average: 56.1%

95th National Percentile
Average: 165.2 Points

Paper Chase (Easy)

30 POINTS OUT OF 30

20.0% ACCURACY

COMPLETION: 100.0%

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

Hex password (Easy)

60 POINTS OUT OF 60

80.0% ACCURACY

COMPLETION: 100.0%

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

Decoding (Easy)

60 POINTS OUT OF 60

50.0% ACCURACY

COMPLETION: 100.0%

Identify and decrypt different cipher schemes.

Unc's Encryption (Medium)

100 POINTS OUT OF 100

75.0% 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

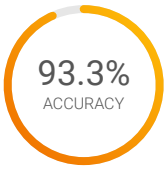
Identify actionable exploits and vulnerabilities and use them to bypass the security measures in code and compiled binaries.

165 TH PLACE OUT OF 3634
NATIONAL RANK

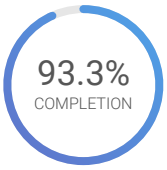
96th National Percentile

260 POINTS OUT OF 300
PERFORMANCE SCORE

Average: 166.3 Points



Average: 74.0%



Average: 60.6%

Getting into the Router (Easy)

100 POINTS OUT OF 100

83.3% 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

100.0% ACCURACY

COMPLETION: 100.0%

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

Malware Sample (Hard)

60 POINTS OUT OF 100

100.0% ACCURACY

COMPLETION: 80.0%

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

Forensics Module

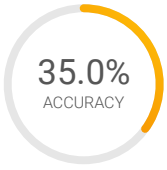
Utilize the proper tools and techniques to analyze, process, recover, and/or investigate digital evidence in a computer-related incident.

524 TH PLACE OUT OF 3634
NATIONAL RANK

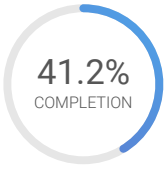
86th National Percentile

95 POINTS OUT OF 300
PERFORMANCE SCORE

Average: 155.4 Points



Average: 51.5%



Average: 52.0%

Parallel (Easy)

60 POINTS OUT OF 100

40.0% ACCURACY

COMPLETION: 80.0%

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

In Plain Sight (Medium)

35 POINTS OUT OF 100

30.0% ACCURACY

COMPLETION: 60.0%

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

Reg Recon (Hard)

0 POINTS OUT OF 100

0.0% ACCURACY

COMPLETION: 0.0%

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.

461 ST PLACE OUT OF 3634
NATIONAL RANK

200 POINTS OUT OF 300
PERFORMANCE SCORE

66.7% ACCURACY
Average: 59.5%

70.0% COMPLETION
Average: 63.7%

88th National Percentile
Average: 177.9 Points

Unwelcome Robots (Easy)	100 POINTS OUT OF 100	90.0% 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	45.5% ACCURACY	COMPLETION: 100.0%
Extract information from a common Linux log format.			
Survival Bias (Hard)	0 POINTS OUT OF 100	0.0% ACCURACY	COMPLETION: 0.0%
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.

434 TH PLACE OUT OF 3634
NATIONAL RANK

150 POINTS OUT OF 300
PERFORMANCE SCORE

60.0% ACCURACY
Average: 64.4%

50.0% COMPLETION
Average: 59.6%

89th National Percentile
Average: 181.7 Points

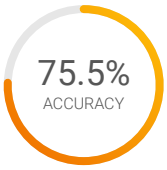
WitSec (Easy)	90 POINTS OUT OF 100	80.0% ACCURACY	COMPLETION: 80.0%
Extract an image from HTTP network traffic.			
Crafty Communique (Medium)	60 POINTS OUT OF 100	57.1% ACCURACY	COMPLETION: 72.7%
Extract information about players and chat messages from Minecraft server packets.			
What is on the LAN? (Hard)	0 POINTS OUT OF 100	0.0% ACCURACY	COMPLETION: 0.0%
Find specific devices and traffic types on a network from a packet capture.			

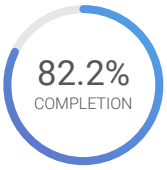
Open Source Intelligence Module

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

364 TH PLACE OUT OF 3634
NATIONAL RANK

275 POINTS OUT OF 385
PERFORMANCE SCORE





90th National Percentile

Average: 221.0 Points

Average: 62.3%

Average: 64.5%

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

83.3% ACCURACY

COMPLETION: 100.0%

Identify key search terms and execute search for information.

ATT&CKED (Easy)

75 POINTS OUT OF 75

64.3% 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

73.3% ACCURACY

COMPLETION: 100.0%

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

This Way Pleaae! (Medium)

15 POINTS OUT OF 50

60.0% ACCURACY

COMPLETION: 75.0%

Interpret coded messages to uncover a targeted operation.

Tracking the Tracker (Hard)

0 POINTS OUT OF 75

0.0% ACCURACY

COMPLETION: 0.0%

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.

211 TH PLACE OUT OF 3634
NATIONAL RANK

305 POINTS OUT OF 355
PERFORMANCE SCORE

85.7% ACCURACY

92.3% COMPLETION

95th National Percentile

Average: 178.2 Points

Average: 72.3%

Average: 59.5%

ID Me (Easy)

40 POINTS OUT OF 40

100.0% ACCURACY

COMPLETION: 100.0%

Identify MD5, SHA256, bcrypt, and JWT strings.

Bitcoin Hashes (Easy)

45 POINTS OUT OF 45

85.7% ACCURACY

COMPLETION: 100.0%

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

Lightly Seasoned (Easy)

40 POINTS OUT OF 40

75.0% ACCURACY

COMPLETION: 100.0%

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

2-Ways (Medium)

50 POINTS OUT OF 50

100.0% ACCURACY

COMPLETION: 100.0%

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

l33t p45$vv0rclz (Medium)

100 POINTS OUT OF 100

66.7% ACCURACY

COMPLETION: 100.0%

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

Unlocking 2 (Hard)

30 POINTS OUT OF 80

100.0% ACCURACY

COMPLETION: 50.0%

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

Scanning & Reconnaissance Module

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

328 TH PLACE OUT OF 3634
NATIONAL RANK

200 POINTS OUT OF 300
PERFORMANCE SCORE

100.0% ACCURACY

64.3% COMPLETION

91st National Percentile

Average: 183.5 Points

Average: 73.3%

Average: 62.4%

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 IoCs.

AppScan (Hard)

0 POINTS OUT OF 100

0.0% ACCURACY

COMPLETION: 0.0%

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.

215 TH PLACE OUT OF 3634
NATIONAL RANK

210 POINTS OUT OF 300
PERFORMANCE SCORE

77.8% ACCURACY

82.4% COMPLETION

95th National Percentile

Average: 138.6 Points

Average: 59.8%

Average: 49.7%

Pairs (Easy)

80 POINTS OUT OF 80

50.0% ACCURACY

COMPLETION: 100.0%

Identify sensitive data stored in HTML attributes.

Stylish (Medium)

100 POINTS OUT OF 100

100.0% ACCURACY

COMPLETION: 100.0%

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

Modern Tech Stack (Hard)

30 POINTS OUT OF 120

85.7% ACCURACY

COMPLETION: 66.7%

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