Mitchell Arndt
moarnd1@ilstu.edu

# NCL Spring 2024 Team Game Scouting Report

Dear Mitchell Arndt (Team "SnailMail bouta be EscargotMail @ Illinois State University"),

Thank you for participating in the National Cyber League (NCL) Spring 2024 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 2024 Season had 8,020 students/players and 584 faculty/coaches from more than 480 two- and four-year schools & 240 high schools across all 50 U.S. states registered to play. The Individual Game Capture the Flag (CTF) event took place from April 5 through April 7. The Team Game CTF event took place from April 19 through April 21. 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/0K415YYP72L5

Congratulations for your participation in the NCL Spring 2024 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

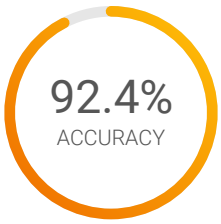
NCL SPRING 2024 TEAM GAME

**NATIONAL RANK**
**17TH PLACE OUT OF 4199**

**PERCENTILE**
**100TH**

**YOUR TOP CATEGORIES**

| LOG ANALYSIS | OPEN SOURCE INTELLIGENCE | WEB APPLICATION EXPLOITATION |
|---|---|---|
| 100TH PERCENTILE | 100TH PERCENTILE | 100TH PERCENTILE |




Average: 65.4%

cyberskyline.com/report
ID: 0K415YYP72L5

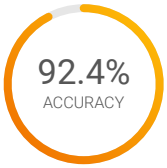
Mitchell Arndt
moarnd1@ilstu.edu

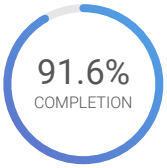
# NCL Spring 2024 Team Game

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.

**17** TH PLACE OUT OF 4199
NATIONAL RANK

**2715** POINTS OUT OF 3000
PERFORMANCE SCORE




**100**th National Percentile

Average: 1074.1 Points

Average: 65.4%

Average: 40.2%

## Cryptography

**245** POINTS OUT OF 345

90.9% ACCURACY

COMPLETION: 90.9%

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

## Enumeration & Exploitation

**210** POINTS OUT OF 300

100.0% ACCURACY

COMPLETION: 87.5%

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

## Forensics

**300** POINTS OUT OF 300

100.0% ACCURACY

COMPLETION: 100.0%

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

## Log Analysis

**415** POINTS OUT OF 415

100.0% 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

77.3% ACCURACY

COMPLETION: 100.0%

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

## Open Source Intelligence

**325** POINTS OUT OF 325

100.0% 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

**220** POINTS OUT OF 300

100.0% ACCURACY

COMPLETION: 69.2%

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

## Scanning & Reconnaissance

**300** POINTS OUT OF 300

87.5% 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 315

90.0% 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.

Mitchell Arndt
moarnd1@ilstu.edu

# Cryptography Module

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

**48** TH PLACE OUT OF 4199
NATIONAL RANK

**245** POINTS OUT OF 345
PERFORMANCE SCORE

90.9% ACCURACY

90.9% COMPLETION

99th National Percentile

Average: 132.3 Points

Average: 74.5%

Average: 64.7%

## Decoding 1 (Easy)

45 POINTS OUT OF 45

100.0% ACCURACY

COMPLETION: 100.0%

Analyze and obtain plaintext from messages encrypted with a shift cipher

## Decoding 2 (Easy)

50 POINTS OUT OF 50

100.0% ACCURACY

COMPLETION: 100.0%

Analyze and obtain plaintext from messages encoded with common number bases

## Decoding 3 (Medium)

50 POINTS OUT OF 50

100.0% ACCURACY

COMPLETION: 100.0%

Analyze and obtain plaintext from messages encrypted with the Rail Fence transposition cipher

## Secure Communication (Medium)

100 POINTS OUT OF 100

50.0% ACCURACY

COMPLETION: 100.0%

Decrypt and encrypt PGP messages using the provided public and private keys

## Message (Hard)

0 POINTS OUT OF 100

0.0% ACCURACY

COMPLETION: 0.0%

Analyze and decode a message by using frequency analysis

Mitchell Arndt
moarnd1@ilstu.edu

## Enumeration & Exploitation Module

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

52 ND PLACE OUT OF 4199
NATIONAL RANK

99th National Percentile

210 POINTS OUT OF 300
PERFORMANCE SCORE

Average: 122.3 Points

100.0% ACCURACY

Average: 61.4%

87.5% COMPLETION

Average: 56.6%

| | | | |
|---|---|---|---|
| Gopher (Easy) | 100 POINTS OUT OF 100 | 100.0% ACCURACY | COMPLETION: 100.0% |
| Analyze Go source code to exploit an insecurely-stored secret that uses an XOR cipher | | | |
| Drop (Medium) | 100 POINTS OUT OF 100 | 100.0% ACCURACY | COMPLETION: 100.0% |
| Analyze a sample of malware written in Powershell to identify its behavior | | | |
| Playground (Hard) | 10 POINTS OUT OF 100 | 100.0% ACCURACY | COMPLETION: 50.0% |
| Exploit a binary program by using ROP gadgets and stack pivoting to gain command execution | | | |

## Forensics Module

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

27 TH PLACE OUT OF 4199
NATIONAL RANK

100th National Percentile

300 POINTS OUT OF 300
PERFORMANCE SCORE

Average: 126.7 Points

100.0% ACCURACY

Average: 67.6%

100.0% COMPLETION

Average: 51.4%

| | | | |
|---|---|---|---|
| Filesystem (Easy) | 100 POINTS OUT OF 100 | 100.0% ACCURACY | COMPLETION: 100.0% |
| Analyze a filesystem image and utilize forensic tools to extract a sensitive file | | | |
| Word (Medium) | 100 POINTS OUT OF 100 | 100.0% ACCURACY | COMPLETION: 100.0% |
| Extract hidden data from Word documents and reassemble the data to form a viewable image | | | |
| Analog (Hard) | 100 POINTS OUT OF 100 | 100.0% ACCURACY | COMPLETION: 100.0% |
| Recover an image by programmatically converting raw VGA voltages to RGB pixel values | | | |

Mitchell Arndt
moarnd1@ilstu.edu

## 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.

6 TH PLACE OUT OF 4199
NATIONAL RANK

415 POINTS OUT OF 415
PERFORMANCE SCORE

100.0% ACCURACY

100.0% COMPLETION

100th National Percentile

Average: 205.9 Points

Average: 44.2%

Average: 52.8%

### Secure Shell (Easy)

100 POINTS OUT OF 100

100.0% ACCURACY

COMPLETION: 100.0%

Analyze a SSH server log to identify compromise attempts from threat actors

### NASA Servers (Medium)

145 POINTS OUT OF 145

100.0% ACCURACY

COMPLETION: 100.0%

Analyze a web server log and identify traffic patterns

### Employee Access (Hard)

170 POINTS OUT OF 170

100.0% ACCURACY

COMPLETION: 100.0%

Analyze data transfer logs to find anomalies and identify an insider threat

## Network Traffic Analysis Module

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

33 RD PLACE OUT OF 4199
NATIONAL RANK

300 POINTS OUT OF 300
PERFORMANCE SCORE

77.3% ACCURACY

100.0% COMPLETION

100th National Percentile

Average: 172.2 Points

Average: 65.6%

Average: 57.6%

### Announcement (Easy)

100 POINTS OUT OF 100

100.0% ACCURACY

COMPLETION: 100.0%

Analyze a network packet capture of SSDP traffic to identify devices on a network

### Wire (Medium)

100 POINTS OUT OF 100

100.0% ACCURACY

COMPLETION: 100.0%

Dissect the raw binary of an ARP packet

### Kickback (Hard)

100 POINTS OUT OF 100

54.5% ACCURACY

COMPLETION: 100.0%

Analyze the raw data from an IR remote capture to identify the behavior that occurred

Mitchell Arndt
moarnd1@ilstu.edu

# 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.

13 TH PLACE OUT OF 4199
NATIONAL RANK

325 POINTS OUT OF 325
PERFORMANCE SCORE

100.0% ACCURACY

100.0% COMPLETION

100th National Percentile

Average: 230.4 Points

Average: 77.0%

Average: 82.8%

## Rules of Conduct (Easy)

25 POINTS OUT OF 25

100.0% ACCURACY

COMPLETION: 100.0%

Introductory challenge on acceptable conduct during NCL

## Lucky Charms (Easy)

100 POINTS OUT OF 100

100.0% ACCURACY

COMPLETION: 100.0%

Locate a physical location by performing conversions between different coordinate systems

## Hidden in Plain Sight (Medium)

100 POINTS OUT OF 100

100.0% ACCURACY

COMPLETION: 100.0%

Utilize open source tools to identify and decode a message encoded using an esoteric language

## Lost (Hard)

100 POINTS OUT OF 100

100.0% ACCURACY

COMPLETION: 100.0%

Utilize open source tools to perform an analysis on a slightly redacted photo and geolocate the subject of the image

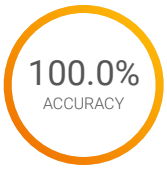
Mitchell Arndt
moarnd1@ilstu.edu

# Password Cracking Module

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

27 TH PLACE OUT OF 4199
NATIONAL RANK

220 POINTS OUT OF 300
PERFORMANCE SCORE





100th National Percentile

Average: 107.7 Points

Average: 86.4%

Average: 33.0%

## Hashing (Easy)

30 POINTS OUT OF 30

100.0% ACCURACY

COMPLETION: 100.0%

Generate password hashes for MD4, MD5, SHA512

## Rockyou (Easy)

45 POINTS OUT OF 45

100.0% ACCURACY

COMPLETION: 100.0%

Crack SHA1 password hashes for password found in the rockyou breach

## Defaults (Medium)

70 POINTS OUT OF 100

100.0% ACCURACY

COMPLETION: 70.0%

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

## DOCX (Medium)

45 POINTS OUT OF 45

100.0% ACCURACY

COMPLETION: 100.0%

Crack the password for a protected Microsoft Word file

## Fantasy (Hard)

30 POINTS OUT OF 80

100.0% ACCURACY

COMPLETION: 37.5%

Build a custom wordlist to crack passwords not found in common wordlists and augment with rules for special characters

Mitchell Arndt
moarnd1@ilstu.edu

## Scanning & Reconnaissance Module

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

29 TH PLACE OUT OF 4199
NATIONAL RANK

300 POINTS OUT OF 300
PERFORMANCE SCORE

87.5% ACCURACY
Average: 60.0%

100.0% COMPLETION
Average: 48.3%

100th National Percentile
Average: 140.5 Points

### Blocked (Easy)

100 POINTS OUT OF 100

100.0% ACCURACY

COMPLETION: 100.0%

Conduct reconnaissance on a server by identifying blocked IPs and ports

### Scan (Medium)

100 POINTS OUT OF 100

66.7% ACCURACY

COMPLETION: 100.0%

Perform a UDP port scan and identify services running on a remote host

### Paper (Hard)

100 POINTS OUT OF 100

100.0% ACCURACY

COMPLETION: 100.0%

Conduct reconnaissance on an LDAP server to identify the users within an organization

## Web Application Exploitation Module

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

13 TH PLACE OUT OF 4199
NATIONAL RANK

300 POINTS OUT OF 315
PERFORMANCE SCORE

90.0% ACCURACY
Average: 50.1%

100.0% COMPLETION
Average: 29.3%

100th National Percentile
Average: 75.7 Points

### Jojamart (Easy)

100 POINTS OUT OF 100

100.0% ACCURACY

COMPLETION: 100.0%

Identify and exploit a SQL injection vulnerability to gain unauthorized access to sensitive data

### Records (Medium)

100 POINTS OUT OF 100

100.0% ACCURACY

COMPLETION: 100.0%

Conduct an automated attack to crawl a web server and obtain sensitive information

### File Share (Hard)

100 POINTS OUT OF 115

75.0% ACCURACY

COMPLETION: 100.0%

Identify and exploit a NoSQL injection vulnerability to gain unauthorized access to a web server database