Paul Badu Yakubu
badupaul10@gmail.com

# NCL Spring 2024 Team Game Scouting Report

Dear Paul Badu Yakubu (Team "Group 4"),

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. 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/3F0C8D0LV87X

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

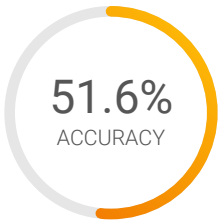
NCL SPRING 2024 TEAM GAME

EXPERIENCED STUDENTS RANK
185TH PLACE OUT OF 386

PERCENTILE
53RD

YOUR TOP CATEGORIES

| OPEN SOURCE INTELLIGENCE | CRYPTOGRAPHY |
|---|---|
| 61ST PERCENTILE | 53RD PERCENTILE |




Average: 74.5%

cyberskyline.com/report
ID: 3F0C8D0LV87X

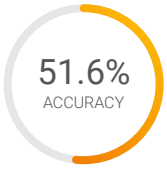
Paul Badu Yakubu
badupaul10@gmail.com

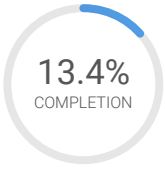
# NCL Spring 2024 Team Game

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.

**185** TH PLACE OUT OF 386
EXPERIENCED STUDENTS RANK

**370** POINTS OUT OF 3000
PERFORMANCE SCORE




**53rd** Experienced Students Percentile

Average: 1821.5 Points

Average: 74.5%

Average: 64.2%

## Cryptography

**65** POINTS OUT OF 345

62.5% ACCURACY

COMPLETION: 45.5%

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

## Enumeration & Exploitation

**0** POINTS OUT OF 300

0.0% ACCURACY

COMPLETION: 0.0%

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

## Forensics

**0** POINTS OUT OF 300

0.0% ACCURACY

COMPLETION: 0.0%

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

## Log Analysis

**0** POINTS OUT OF 415

0.0% ACCURACY

COMPLETION: 0.0%

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

**0** POINTS OUT OF 300

0.0% ACCURACY

COMPLETION: 0.0%

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

## Open Source Intelligence

**305** POINTS OUT OF 325

55.0% ACCURACY

COMPLETION: 91.7%

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

**0** POINTS OUT OF 300

0.0% ACCURACY

COMPLETION: 0.0%

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

## Scanning & Reconnaissance

**0** POINTS OUT OF 300

0.0% ACCURACY

COMPLETION: 0.0%

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

## Web Application Exploitation

**0** POINTS OUT OF 315

0.0% ACCURACY

COMPLETION: 0.0%

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.

Paul Badu Yakubu
badupaul10@gmail.com

# Cryptography Module

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

184 TH PLACE OUT OF 386
EXPERIENCED STUDENTS RANK

65 POINTS OUT OF 345
PERFORMANCE SCORE

62.5% ACCURACY
Average: 81.4%

45.5% COMPLETION
Average: 76.2%

53rd Experienced Students Percentile

Average: 179.9 Points

## 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)

20 POINTS OUT OF 50

40.0% ACCURACY

COMPLETION: 50.0%

Analyze and obtain plaintext from messages encoded with common number bases

## Decoding 3 (Medium)

0 POINTS OUT OF 50

0.0% ACCURACY

COMPLETION: 0.0%

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

## Secure Communication (Medium)

0 POINTS OUT OF 100

0.0% ACCURACY

COMPLETION: 0.0%

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

Paul Badu Yakubu
badupaul10@gmail.com

## Enumeration & Exploitation Module

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

| N/A | 0 POINTS OUT OF 300 | 0.0% | 0.0% |
|---|---|---|---|
| EXPERIENCED STUDENTS RANK | PERFORMANCE SCORE | ACCURACY | COMPLETION |
| | Average: 178.6 Points | Average: 81.2% | Average: 76.5% |

### Gopher (Easy)

0 POINTS OUT OF 100 | 0.0% ACCURACY | COMPLETION: 0.0%

Analyze Go source code to exploit an insecurely-stored secret that uses an XOR cipher

### Drop (Medium)

0 POINTS OUT OF 100 | 0.0% ACCURACY | COMPLETION: 0.0%

Analyze a sample of malware written in Powershell to identify its behavior

### Playground (Hard)

0 POINTS OUT OF 100 | 0.0% ACCURACY | COMPLETION: 0.0%

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.

| N/A | 0 POINTS OUT OF 300 | 0.0% | 0.0% |
|---|---|---|---|
| EXPERIENCED STUDENTS RANK | PERFORMANCE SCORE | ACCURACY | COMPLETION |
| | Average: 200.9 Points | Average: 82.7% | Average: 74.0% |

### Filesystem (Easy)

0 POINTS OUT OF 100 | 0.0% ACCURACY | COMPLETION: 0.0%

Analyze a filesystem image and utilize forensic tools to extract a sensitive file

### Word (Medium)

0 POINTS OUT OF 100 | 0.0% ACCURACY | COMPLETION: 0.0%

Extract hidden data from Word documents and reassemble the data to form a viewable image

### Analog (Hard)

0 POINTS OUT OF 100 | 0.0% ACCURACY | COMPLETION: 0.0%

Recover an image by programmatically converting raw VGA voltages to RGB pixel values

Paul Badu Yakubu
badupaul10@gmail.com

## 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.

**180** TH PLACE OUT OF 386
EXPERIENCED STUDENTS RANK

**0** POINTS OUT OF 415
PERFORMANCE SCORE

**0.0%** ACCURACY

**0.0%** COMPLETION

**54**th Experienced Students Percentile

Average: 318.5 Points

Average: 61.9%

Average: 79.7%

### Secure Shell (Easy)

**0** POINTS OUT OF 100

**0.0%** ACCURACY

COMPLETION: 0.0%

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

### NASA Servers (Medium)

**0** POINTS OUT OF 145

**0.0%** ACCURACY

COMPLETION: 0.0%

Analyze a web server log and identify traffic patterns

### Employee Access (Hard)

**0** POINTS OUT OF 170

**0.0%** ACCURACY

COMPLETION: 0.0%

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.

**N/A**
EXPERIENCED STUDENTS RANK

**0** POINTS OUT OF 300
PERFORMANCE SCORE

**0.0%** ACCURACY

**0.0%** COMPLETION

Average: 219.5 Points

Average: 73.8%

Average: 73.1%

### Announcement (Easy)

**0** POINTS OUT OF 100

**0.0%** ACCURACY

COMPLETION: 0.0%

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

### Wire (Medium)

**0** POINTS OUT OF 100

**0.0%** ACCURACY

COMPLETION: 0.0%

Dissect the raw binary of an ARP packet

### Kickback (Hard)

**0** POINTS OUT OF 100

**0.0%** ACCURACY

COMPLETION: 0.0%

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

Paul Badu Yakubu
badupaul10@gmail.com

# Open Source Intelligence Module

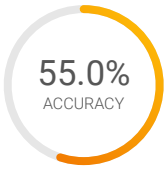
Utilize publicly available information such as search engines, public repositories, social media, and more to gain in-depth knowledge on a topic or target.

**152** ND PLACE OUT OF 386
EXPERIENCED STUDENTS RANK

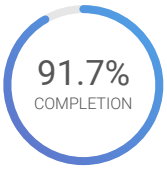
**305** POINTS OUT OF 325
PERFORMANCE SCORE

**61**st Experienced Students Percentile

Average: 288.8 Points




Average: 84.6%




Average: 93.5%

## Rules of Conduct (Easy)

25 POINTS OUT OF 25

83.3% ACCURACY

COMPLETION: 100.0%

Introductory challenge on acceptable conduct during NCL

## Lucky Charms (Easy)

80 POINTS OUT OF 100

25.0% ACCURACY

COMPLETION: 66.7%

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

50.0% ACCURACY

COMPLETION: 100.0%

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

Paul Badu Yakubu
badupaul10@gmail.com

# Password Cracking Module

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

N/A
EXPERIENCED STUDENTS RANK

0 POINTS OUT OF 300
PERFORMANCE SCORE

Average: 161.6 Points

0.0%
ACCURACY

Average: 91.3%

0.0%
COMPLETION

Average: 49.6%

## Hashing (Easy)

0 POINTS OUT OF 30

0.0% ACCURACY

COMPLETION: 0.0%

Generate password hashes for MD4, MD5, SHA512

## Rockyou (Easy)

0 POINTS OUT OF 45

0.0% ACCURACY

COMPLETION: 0.0%

Crack SHA1 password hashes for password found in the rockyou breach

## Defaults (Medium)

0 POINTS OUT OF 100

0.0% ACCURACY

COMPLETION: 0.0%

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

## DOCX (Medium)

0 POINTS OUT OF 45

0.0% ACCURACY

COMPLETION: 0.0%

Crack the password for a protected Microsoft Word file

## Fantasy (Hard)

0 POINTS OUT OF 80

0.0% ACCURACY

COMPLETION: 0.0%

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

Paul Badu Yakubu
badupaul10@gmail.com

## Scanning & Reconnaissance Module

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

| N/A | 0 POINTS OUT OF 300 | 0.0% | 0.0% |
|---|---|---|---|
| EXPERIENCED STUDENTS RANK | PERFORMANCE SCORE | ACCURACY | COMPLETION |
| | Average: 205.3 Points | Average: 76.4% | Average: 69.6% |

### Blocked (Easy)

0 POINTS OUT OF 100 | 0.0% ACCURACY | COMPLETION: 0.0%

Conduct reconnaissance on a server by identifying blocked IPs and ports

### Scan (Medium)

0 POINTS OUT OF 100 | 0.0% ACCURACY | COMPLETION: 0.0%

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

### Paper (Hard)

0 POINTS OUT OF 100 | 0.0% ACCURACY | COMPLETION: 0.0%

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.

| N/A | 0 POINTS OUT OF 315 | 0.0% | 0.0% |
|---|---|---|---|
| EXPERIENCED STUDENTS RANK | PERFORMANCE SCORE | ACCURACY | COMPLETION |
| | Average: 132.9 Points | Average: 65.1% | Average: 47.6% |

### Jojamart (Easy)

0 POINTS OUT OF 100 | 0.0% ACCURACY | COMPLETION: 0.0%

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

### Records (Medium)

0 POINTS OUT OF 100 | 0.0% ACCURACY | COMPLETION: 0.0%

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

### File Share (Hard)

0 POINTS OUT OF 115 | 0.0% ACCURACY | COMPLETION: 0.0%

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