Paul Badu Yakubu
badupaul10@gmail.com

NCL Spring 2024 Individual Game Scouting Report

Dear Paul Badu Yakubu,

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/3FP4KGQBY7VX

Congratulations for your participation in the NCL Spring 2024 Individual 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

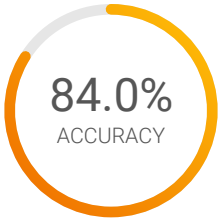
NCL SPRING 2024 INDIVIDUAL GAME

EXPERIENCED STUDENTS RANK
278TH PLACE OUT OF 526

PERCENTILE
48TH

YOUR TOP CATEGORIES

OPEN SOURCE INTELLIGENCE	CRYPTOGRAPHY
63RD PERCENTILE	53RD PERCENTILE



Average: 75.7%

cyberskyline.com/report
ID: 3FP4KGQBY7VX

Paul Badu Yakubu
badupaul10@gmail.com

NCL Spring 2024 Individual Game

The NCL Individual Game is designed for student players nationwide to compete in realtime in the categories listed below. The Individual Game evaluates the technical cybersecurity skills of the individual, without the assistance of others.

278 TH PLACE OUT OF 526
EXPERIENCED STUDENTS RANK

360 POINTS OUT OF 3000
PERFORMANCE SCORE

84.0% ACCURACY

16.0% COMPLETION

48th Experienced Students Percentile

Average: 1487.0 Points

Average: 75.7%

Average: 55.7%

Cryptography

110 POINTS OUT OF 370

100.0% ACCURACY

COMPLETION: 42.9%

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 300

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

250 POINTS OUT OF 430

78.9% ACCURACY

COMPLETION: 60.0%

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

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 300

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

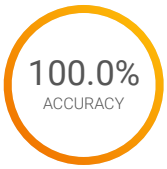
Identify techniques used to encrypt or obfuscate messages and leverage tools to extract the plaintext.

251 ST PLACE OUT OF 526
EXPERIENCED STUDENTS RANK

110 POINTS OUT OF 370
PERFORMANCE SCORE

53rd Experienced Students Percentile

Average: 235.3 Points



Average: 86.9%

Average: 72.1%

Bases (Easy)

40 POINTS OUT OF 40

100.0% ACCURACY

COMPLETION: 100.0%

Analyze and obtain the plaintext from messages encoded with common number bases

Ancient Cipher (Easy)

70 POINTS OUT OF 70

100.0% ACCURACY

COMPLETION: 100.0%

Analyze and obtain the plaintext for a message encrypted with the Atbash substitution cipher

Boxed In (Medium)

0 POINTS OUT OF 80

0.0% ACCURACY

COMPLETION: 0.0%

Analyze and obtain the plaintext for a message encrypted with a Box Cipher, a type of Transposition Cipher

Validation (Medium)

0 POINTS OUT OF 80

0.0% ACCURACY

COMPLETION: 0.0%

Analyze and decode a x509 certificate used for public key cryptography

Love's the AES (Hard)

0 POINTS OUT OF 100

0.0% ACCURACY

COMPLETION: 0.0%

Decrypt an AES-encrypted message by exploiting an insecure key generation method

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: 133.6 Points	Average: 82.6%	Average: 58.0%

Key Check (Easy)

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

Analyze Python source code to exploit an insecurely-stored secret that uses a rotating XOR cipher

Cross Lock (Medium)

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

Analyze a DotNET executable written in C# using decompilation tools to find a hardcoded secret

High Alert (Hard)

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

Analyze and exploit a buffer overflow vulnerability in a binary application

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: 161.9 Points	Average: 65.5%	Average: 59.6%

Lost (Easy)

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

Utilize open-source forensics tools to extract a deleted JPEG image from an ext4 image

Backdoor (Medium)

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

Perform a forensics analysis on a router's firmware image to investigate a backdoor

Shuffled (Hard)

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

Analyze a PNG file and recalculate a CRC checksum to restore the file and retrieve lost information

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.

N/A	0 POINTS OUT OF 300	0.0%	0.0%
EXPERIENCED STUDENTS RANK	PERFORMANCE SCORE	ACCURACY	COMPLETION
	Average: 176.0 Points	Average: 78.0%	Average: 68.7%

Entry (Easy)

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

Analyze a web access log to identify trends in traffic patterns

Places (Medium)

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

Analyze a SQLite database containing Internet browsing history to create a timeline of user actions

Buffed (Hard)

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

Parse a log of protobuf messages to extract key information

Network Traffic Analysis Module

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

N/A	0 POINTS OUT OF 300	0.0%	0.0%
EXPERIENCED STUDENTS RANK	PERFORMANCE SCORE	ACCURACY	COMPLETION
	Average: 198.5 Points	Average: 65.5%	Average: 72.4%

Shell (Easy)

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

Analyze network traffic on a compromised Telnet server to create an investigative report

Missing (Medium)

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

Identify and extract sensitive information that was exfiltrated from a computer network using UDP

Route (Hard)

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

Analyze a packet capture of routers exchanging OSPF information to create a report on the configuration of the network

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.

197 TH PLACE OUT OF 526
EXPERIENCED STUDENTS RANK

250 POINTS OUT OF 430
PERFORMANCE SCORE

78.9% ACCURACY

60.0% COMPLETION

63rd Experienced Students Percentile

Average: 301.5 Points

Average: 74.3%

Average: 72.3%

Rules of Conduct (Easy)

30 POINTS OUT OF 30

100.0% ACCURACY

COMPLETION: 100.0%

Introductory challenge on acceptable conduct during NCL

Guess Who (Easy)

100 POINTS OUT OF 100

71.4% ACCURACY

COMPLETION: 100.0%

Identify and use basic OSINT tools to find public information of a given IP

Exit Node (Easy)

100 POINTS OUT OF 100

85.7% ACCURACY

COMPLETION: 100.0%

Search online databases to gather information on a Tor Exit Node

Stuck on The Net (Medium)

20 POINTS OUT OF 100

50.0% ACCURACY

COMPLETION: 20.0%

Utilize the Wayback Internet Archive Machine to view old data that is no longer available on the Internet

Plane (Hard)

0 POINTS OUT OF 100

0.0% ACCURACY

COMPLETION: 0.0%

Use publicly available open source tools to analyze the flight patterns of planes

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: 150.3 Points

0.0%
ACCURACY

Average: 92.4%

0.0%
COMPLETION

Average: 54.6%

Hashing (Easy)

0 POINTS OUT OF 15

0.0% ACCURACY

COMPLETION: 0.0%

Generate password hashes for MD5, SHA1, and SHA256

Rockyou (Easy)

0 POINTS OUT OF 15

0.0% ACCURACY

COMPLETION: 0.0%

Crack MD5 password hashes for password found in the rockyou breach

Windows (Easy)

0 POINTS OUT OF 30

0.0% ACCURACY

COMPLETION: 0.0%

Crack Windows NTLM password hashes using rainbow tables

Pattern (Medium)

0 POINTS OUT OF 45

0.0% ACCURACY

COMPLETION: 0.0%

Build a wordlist or pattern rule to crack password hashes of a known pattern

PDF (Medium)

0 POINTS OUT OF 50

0.0% ACCURACY

COMPLETION: 0.0%

Crack the insecure password for a protected PDF file

Wordlist (Hard)

0 POINTS OUT OF 75

0.0% ACCURACY

COMPLETION: 0.0%

Build a wordlist to crack passwords not found in common wordlists

Complexity (Hard)

0 POINTS OUT OF 70

0.0% ACCURACY

COMPLETION: 0.0%

Build a custom wordlist to crack passwords by augmenting permutation rules using known password complexity requirements

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: 190.3 Points	Average: 81.6%	Average: 67.5%

Port Scan (Easy)

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

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

Foreign (Medium)

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

Conduct reconnaissance on a server to identify details regarding its timezone and locale

Snail Mail (Hard)

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

Scan an email server to enumerate user accounts

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 300	0.0%	0.0%
EXPERIENCED STUDENTS RANK	PERFORMANCE SCORE	ACCURACY	COMPLETION
	Average: 182.1 Points	Average: 71.4%	Average: 68.0%

PiratePals (Easy)

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

Analyze the source code of a web application and craft an HTTP request to conduct a malicious payload attack on the web server

Pierre's Store (Medium)

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

Perform a replay attack on a web application by using a HAR file to craft a web request

Valley Directory (Hard)

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

Analyze a web application and exploit a session puzzling vulnerability in a web application to gain unauthorized access