Andre Castillo
andre1525@gmail.com

NCL Fall 2024 Individual Game Scouting Report

Dear Andre Castillo,

Thank you for participating in the National Cyber League (NCL) Fall 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 Fall 2024 Season had 9,260 students/players and 573 faculty/coaches from more than 540 two- and four-year schools & 230 high schools across all 50 U.S. states registered to play. The Individual Game Capture the Flag (CTF) event took place from October 25 through October 27. The Team Game CTF event took place from November 8 through November 10. 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/FV47XCJRR7DK

CompTIA

Based on the performance detailed in this NCL Scouting Report, you have earned **9 hours** of Continuing Education Units (CEUs) as approved by CompTIA. You can learn more about the NCL - CompTIA alignment via nationalcyberleague.org/partners.

Congratulations for your participation in the NCL Fall 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 FALL 2024 INDIVIDUAL GAME

EXPERIENCED STUDENTS RANK
212TH PLACE OUT OF 691

PERCENTILE
70TH

YOUR TOP CATEGORIES

OPEN SOURCE INTELLIGENCE	NETWORK TRAFFIC ANALYSIS	LOG ANALYSIS
78TH PERCENTILE	78TH PERCENTILE	74TH PERCENTILE

Average: 76.9%

cyberskyline.com/report
ID: FV47XCJRR7DK

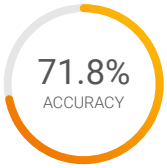
Andre Castillo
andre1525@gmail.com

NCL Fall 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.

212 TH PLACE OUT OF 691
EXPERIENCED STUDENTS RANK

1405 POINTS OUT OF 3000
PERFORMANCE SCORE



70th Experienced Students Percentile

Average: 1484.4 Points

Average: 76.9%

Average: 56.7%

Cryptography

260 POINTS OUT OF 330

65.0% ACCURACY

COMPLETION: **76.5%**

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

Enumeration & Exploitation

120 POINTS OUT OF 330

100.0% ACCURACY

COMPLETION: **50.0%**

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

Forensics

100 POINTS OUT OF 315

75.0% ACCURACY

COMPLETION: **37.5%**

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

60.0% ACCURACY

COMPLETION: **92.3%**

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

180 POINTS OUT OF 320

100.0% ACCURACY

COMPLETION: **85.7%**

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

Open Source Intelligence

280 POINTS OUT OF 355

72.0% ACCURACY

COMPLETION: **78.3%**

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

75 POINTS OUT OF 340

75.0% ACCURACY

COMPLETION: **32.1%**

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

Scanning & Reconnaissance

90 POINTS OUT OF 300

50.0% ACCURACY

COMPLETION: **30.0%**

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 310

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.

Andre Castillo
andre1525@gmail.com

Cryptography Module

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

207 TH PLACE OUT OF 691
EXPERIENCED STUDENTS RANK

260 POINTS OUT OF 330
PERFORMANCE SCORE

65.0% ACCURACY

76.5% COMPLETION

71 st Experienced Students Percentile

Average: 257.1 Points

Average: 79.5%

Average: 78.3%

Bases (Easy)

30 POINTS OUT OF 30

100.0% ACCURACY

COMPLETION: 100.0%

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

Shift (Easy)

40 POINTS OUT OF 40

40.0% ACCURACY

COMPLETION: 100.0%

Analyze and obtain the plaintext for a message encrypted with a shift cipher.

Number Codes (Easy)

40 POINTS OUT OF 40

100.0% ACCURACY

COMPLETION: 100.0%

Analyze and obtain the plaintext for a message encoded using ASCII codes.

NATO (Easy)

40 POINTS OUT OF 40

100.0% ACCURACY

COMPLETION: 100.0%

Analyze and obtain the plaintext for a message encoded using the NATO alphabet.

Message Signature (Medium)

0 POINTS OUT OF 60

0.0% ACCURACY

COMPLETION: 0.0%

Identify tampered emails by using PGP signatures.

Beep Beep (Medium)

50 POINTS OUT OF 60

50.0% ACCURACY

COMPLETION: 66.7%

Decoded a message that is spelled out using dial tone sounds.

Tampered (Hard)

60 POINTS OUT OF 60

75.0% ACCURACY

COMPLETION: 100.0%

Use CRC checksums to identify a tampered message.

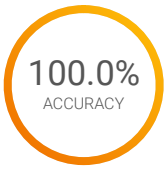
Andre Castillo
andre1525@gmail.com

Enumeration & Exploitation Module

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

214 TH PLACE OUT OF 691
EXPERIENCED STUDENTS RANK

120 POINTS OUT OF 330
PERFORMANCE SCORE



70th Experienced Students Percentile

Average: 189.9 Points

Average: 85.2%

Average: 62.9%

Source (Easy)

110 POINTS OUT OF 110

100.0% ACCURACY

COMPLETION: 100.0%

Reverse engineer the source code of a Rust program to bypass a simple password authentication.

Speedy (Medium)

10 POINTS OUT OF 110

100.0% ACCURACY

COMPLETION: 50.0%

Reverse engineer the source code of a Golang program.

Passphrase (Hard)

0 POINTS OUT OF 110

0.0% ACCURACY

COMPLETION: 0.0%

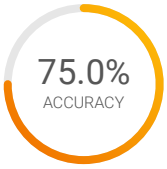
Reverse engineer an ELF binary to break XOR encryption on a password.

Forensics Module

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

198 TH PLACE OUT OF 691
EXPERIENCED STUDENTS RANK

100 POINTS OUT OF 315
PERFORMANCE SCORE



72nd Experienced Students Percentile

Average: 157.6 Points

Average: 61.5%

Average: 53.8%

Table (Easy)

100 POINTS OUT OF 100

75.0% ACCURACY

COMPLETION: 100.0%

Analyze an ARP table to investigate an ARP spoofing attack.

Plant (Medium)

0 POINTS OUT OF 100

0.0% ACCURACY

COMPLETION: 0.0%

Extract a Linux installer and cpio file to investigate a filesystem.

Incident Response (Hard)

0 POINTS OUT OF 115

0.0% ACCURACY

COMPLETION: 0.0%

Inspect and repair a live system that was tampered with to recover data.

Andre Castillo
andre1525@gmail.com

Log Analysis Module

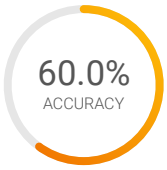
Utilize the proper tools and techniques to establish a baseline for normal operation and identify malicious activities using log files from various services.

181 ST PLACE OUT OF 691
EXPERIENCED STUDENTS RANK

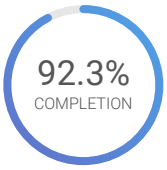
200 POINTS OUT OF 300
PERFORMANCE SCORE

74th Experienced Students Percentile

Average: 213.8 Points



Average: 69.8%



Average: 77.7%

Audit (Easy)

100 POINTS OUT OF 100

71.4% ACCURACY

COMPLETION: 100.0%

Analyze a system auth log file to investigate the behavior of users with elevated privileges.

Packet Log (Medium)

100 POINTS OUT OF 100

53.8% ACCURACY

COMPLETION: 100.0%

Identify traffic patterns from a log file of network traffic.

$TICKER (Hard)

0 POINTS OUT OF 100

0.0% ACCURACY

COMPLETION: 0.0%

Parse a stock price log to identify a stock price that was manipulated.

Network Traffic Analysis Module

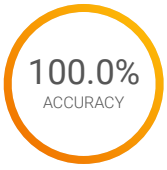
Identify malicious and benign network traffic to demonstrate an understanding of potential security breaches.

157 TH PLACE OUT OF 691
EXPERIENCED STUDENTS RANK

180 POINTS OUT OF 320
PERFORMANCE SCORE

78th Experienced Students Percentile

Average: 194.1 Points



Average: 74.7%

Average: 78.7%

Address (Easy)

100 POINTS OUT OF 100

100.0% ACCURACY

COMPLETION: 100.0%

Analyze the behavior of DHCP traffic from a client connecting to a network.

Home (Medium)

70 POINTS OUT OF 110

100.0% ACCURACY

COMPLETION: 80.0%

Analyze a packet capture and decode traffic from TP-Link smart switches.

Spec (Hard)

10 POINTS OUT OF 110

100.0% ACCURACY

COMPLETION: 50.0%

Implement a custom specification to decode raw packets.

Andre Castillo
andre1525@gmail.com

Open Source Intelligence Module

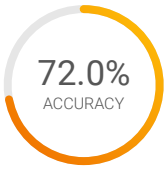
Utilize publicly available information such as search engines, public repositories, social media, and more to gain in-depth knowledge on a topic or target.

155 TH PLACE OUT OF 691
EXPERIENCED STUDENTS RANK

280 POINTS OUT OF 355
PERFORMANCE SCORE

78th Experienced Students Percentile

Average: 244.3 Points



Average: 79.9%

Average: 75.1%

Rules of Conduct (Easy)

25 POINTS OUT OF 25

100.0% ACCURACY

COMPLETION: 100.0%

Introductory challenge on acceptable conduct during NCL.

Vinyl (Easy)

40 POINTS OUT OF 40

100.0% ACCURACY

COMPLETION: 100.0%

Analyze an image using metadata and file properties.

Coordinates (Easy)

60 POINTS OUT OF 60

100.0% ACCURACY

COMPLETION: 100.0%

Geolocate the physical location of a server using an IP address.

NFT (Medium)

60 POINTS OUT OF 60

66.7% ACCURACY

COMPLETION: 100.0%

Conduct blockchain analysis to attribute the ownership of a NFT.

Git (Medium)

0 POINTS OUT OF 75

0.0% ACCURACY

COMPLETION: 0.0%

Obtain private company information that was posted on social media.

Password (Hard)

95 POINTS OUT OF 95

75.0% ACCURACY

COMPLETION: 100.0%

Use coordinates and a SSID to search for a location and find information from public images.

Andre Castillo
andre1525@gmail.com

Password Cracking Module

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

270 TH PLACE OUT OF 691
EXPERIENCED STUDENTS RANK

75 POINTS OUT OF 340
PERFORMANCE SCORE

75.0% ACCURACY

32.1% COMPLETION

61 st Experienced Students Percentile

Average: 148.6 Points

Average: 92.6%

Average: 50.4%

Hashing (Easy)

15 POINTS OUT OF 15

60.0% ACCURACY

COMPLETION: 100.0%

Generate password hashes for MD5, SHA1, and SHA256.

Rockyou (Easy)

30 POINTS OUT OF 30

100.0% ACCURACY

COMPLETION: 100.0%

Crack MD5 password hashes for password found in the rockyou breach.

Windows (Easy)

30 POINTS OUT OF 30

100.0% ACCURACY

COMPLETION: 100.0%

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.

ZIP (Medium)

0 POINTS OUT OF 50

0.0% ACCURACY

COMPLETION: 0.0%

Crack the insecure password for a protected zip file.

Wordlist (Hard)

0 POINTS OUT OF 65

0.0% ACCURACY

COMPLETION: 0.0%

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

Complexity (Hard)

0 POINTS OUT OF 105

0.0% ACCURACY

COMPLETION: 0.0%

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

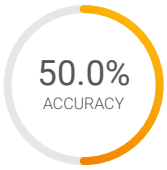
Andre Castillo
andre1525@gmail.com

Scanning & Reconnaissance Module

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

268 TH PLACE OUT OF 691
EXPERIENCED STUDENTS RANK

90 POINTS OUT OF 300
PERFORMANCE SCORE



62nd Experienced Students Percentile

Average: 172.1 Points

Average: 71.6%

Average: 61.6%

Scan (Easy)

90 POINTS OUT OF 100

60.0% ACCURACY

COMPLETION: 75.0%

Use nmap to scan a machine and discover open ports.

Domains (Medium)

0 POINTS OUT OF 100

0.0% ACCURACY

COMPLETION: 0.0%

Perform reconnaissance on a domain's DNS records to gain information about its assets.

ICS (Hard)

0 POINTS OUT OF 100

0.0% ACCURACY

COMPLETION: 0.0%

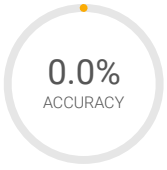
Perform reconnaissance on an ICS system by using the Modbus protocol.

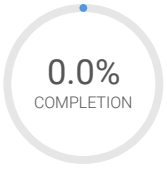
Web Application Exploitation Module

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

N/A
EXPERIENCED STUDENTS RANK

0 POINTS OUT OF 310
PERFORMANCE SCORE





Average: 138.7 Points

Average: 71.4%

Average: 55.6%

Candy Store (Easy)

0 POINTS OUT OF 100

0.0% ACCURACY

COMPLETION: 0.0%

Find and exploit a client side authentication vulnerability in a web application.

Shopping v2 (Medium)

0 POINTS OUT OF 100

0.0% ACCURACY

COMPLETION: 0.0%

Exploit a type coercion bug in a Node.Js application.

Indie Metro (Hard)

0 POINTS OUT OF 110

0.0% ACCURACY

COMPLETION: 0.0%

Perform a NoSQL injection attack on a website.