



POWERED BY
CYBER SKYLINE

The National Cyber League
A Community Where Cybersecurity Is a Passion

Maxine Jones
mjones89@csu.edu

NCL Spring 2024 Individual Game Scouting Report

Dear Maxine Jones,

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/8QFKYUGJAGNP



Based on the performance detailed in this NCL Scouting Report, you have earned **14 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 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

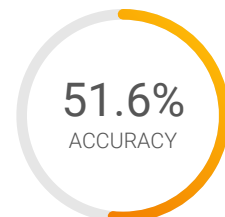
YOUR TOP CATEGORIES

FORENSICS
93RD PERCENTILE

**NETWORK TRAFFIC
ANALYSIS**
93RD PERCENTILE

**WEB APPLICATION
EXPLOITATION**
92ND PERCENTILE

NATIONAL RANK
547TH PLACE
OUT OF 7406
PERCENTILE
93RD



Average: 67.4%

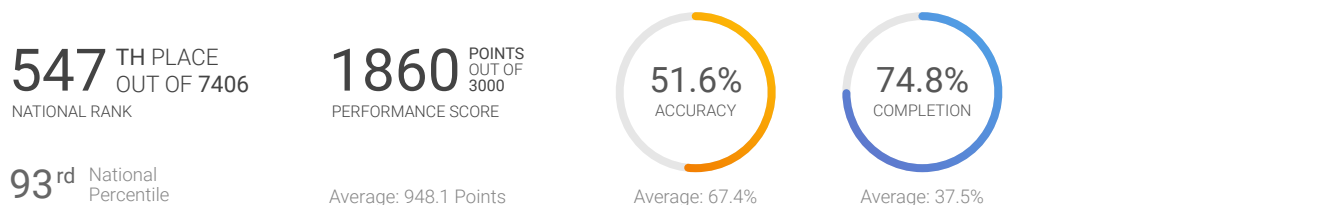
cyberskyline.com/report/8QFKYUGJAGNP

Learn more at nationalcyberleague.org



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.



Cryptography

250 POINTS
OUT OF 370

50.0%
ACCURACY

COMPLETION: **78.6%**

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

Enumeration & Exploitation

90 POINTS
OUT OF 300

75.0%
ACCURACY

COMPLETION: **60.0%**

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

Forensics

185 POINTS
OUT OF 300

38.5%
ACCURACY

COMPLETION: **62.5%**

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

Log Analysis

195 POINTS
OUT OF 300

70.0%
ACCURACY

COMPLETION: **82.4%**

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

220 POINTS
OUT OF 300

38.2%
ACCURACY

COMPLETION: **81.3%**

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

Open Source Intelligence

335 POINTS
OUT OF 430

43.1%
ACCURACY

COMPLETION: **88.0%**

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

155 POINTS
OUT OF 300

69.6%
ACCURACY

COMPLETION: **61.5%**

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

Scanning & Reconnaissance

155 POINTS
OUT OF 300

52.9%
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

175 POINTS
OUT OF 300

80.0%
ACCURACY

COMPLETION: **80.0%**

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.



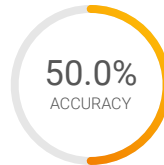


Cryptography Module

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

1261 ST PLACE
OUT OF 7406
NATIONAL RANK

250 POINTS
OUT OF 370
PERFORMANCE SCORE



Average: 78.8%



Average: 57.6%

83rd National
Percentile

Average: 184.5 Points

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)

65 POINTS
OUT OF 70

50.0%
ACCURACY

COMPLETION: **100.0%**

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

Boxed In (Medium)

80 POINTS
OUT OF 80

33.3%
ACCURACY

COMPLETION: **100.0%**

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

Validation (Medium)

80 POINTS
OUT OF 80

66.7%
ACCURACY

COMPLETION: **100.0%**

Analyze and decode a x509 certificate used for public key cryptography

Love's the AES (Hard)

-15 POINTS
OUT OF 100

0.0%
ACCURACY

COMPLETION: **0.0%**

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



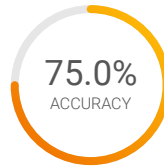


Enumeration & Exploitation Module

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

2106 TH PLACE
OUT OF 7406
NATIONAL RANK

90 POINTS
OUT OF 300
PERFORMANCE SCORE



Average: 74.6%



Average: 44.9%

72nd National
Percentile

Average: 96.8 Points

Key Check (Easy)

100 POINTS
OUT OF 100

100.0%
ACCURACY

COMPLETION: **100.0%**

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

Cross Lock (Medium)

-10 POINTS
OUT OF 100

50.0%
ACCURACY

COMPLETION: **50.0%**

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%**

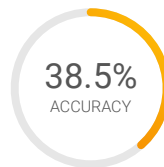
Analyze and exploit a buffer overflow vulnerability in a binary application

Forensics Module

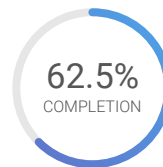
Utilize the proper tools and techniques to analyze, process, recover, and/or investigate digital evidence in a computer-related incident.

531 ST PLACE
OUT OF 7406
NATIONAL RANK

185 POINTS
OUT OF 300
PERFORMANCE SCORE



Average: 49.6%



Average: 39.8%

93rd National
Percentile

Average: 102.5 Points

Lost (Easy)

90 POINTS
OUT OF 100

60.0%
ACCURACY

COMPLETION: **100.0%**

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

Backdoor (Medium)

-5 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)

100 POINTS
OUT OF 100

100.0%
ACCURACY

COMPLETION: **100.0%**

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



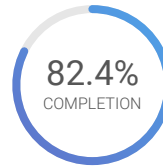
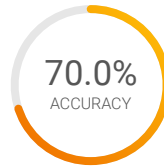


Log Analysis Module

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

777 TH PLACE
OUT OF 7406
NATIONAL RANK

195 POINTS
OUT OF 300
PERFORMANCE SCORE



90th National
Percentile

Average: 123.4 Points

Average: 68.3%

Average: 48.4%

Entry (Easy)

100 POINTS
OUT OF 100

100.0%
ACCURACY

COMPLETION: **100.0%**

Analyze a web access log to identify trends in traffic patterns

Places (Medium)

95 POINTS
OUT OF 100

72.7%
ACCURACY

COMPLETION: **100.0%**

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

Buffered (Hard)

0 POINTS
OUT OF 100

0.0%
ACCURACY

COMPLETION: **0.0%**

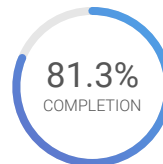
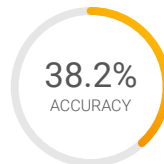
Parse a log of protobuf messages to extract key information

Network Traffic Analysis Module

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

583 RD PLACE
OUT OF 7406
NATIONAL RANK

220 POINTS
OUT OF 300
PERFORMANCE SCORE



93rd National
Percentile

Average: 138.2 Points

Average: 54.3%

Average: 53.3%

Shell (Easy)

100 POINTS
OUT OF 100

85.7%
ACCURACY

COMPLETION: **100.0%**

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

Missing (Medium)

30 POINTS
OUT OF 100

25.0%
ACCURACY

COMPLETION: **50.0%**

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

Route (Hard)

90 POINTS
OUT OF 100

26.3%
ACCURACY

COMPLETION: **83.3%**

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



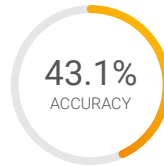


Open Source Intelligence Module

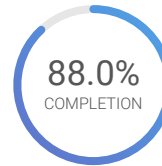
Utilize publicly available information such as search engines, public repositories, social media, and more to gain in-depth knowledge on a topic or target.

805 ^{TH PLACE}
OUT OF 7406
NATIONAL RANK

335 ^{POINTS}
OUT OF 430
PERFORMANCE SCORE



Average: 67.9%



Average: 60.9%

90th National
Percentile

Average: 246.9 Points

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

83.3%
ACCURACY

COMPLETION: **100.0%**

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

Exit Node (Easy)

90 ^{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)

90 ^{POINTS}
OUT OF 100

45.5%
ACCURACY

COMPLETION: **100.0%**

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

Plane (Hard)

25 ^{POINTS}
OUT OF 100

12.5%
ACCURACY

COMPLETION: **50.0%**

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





Password Cracking Module

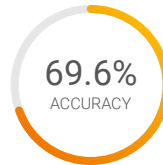
Identify types of password hashes and apply various techniques to efficiently determine plaintext passwords.

911 TH PLACE
OUT OF 7406
NATIONAL RANK

155 POINTS
OUT OF 300
PERFORMANCE SCORE

88th National
Percentile

Average: 91.5 Points



Average: 88.0%



Average: 38.1%

Hashing (Easy)

15 POINTS
OUT OF 15

75.0%
ACCURACY

COMPLETION: **100.0%**

Generate password hashes for MD5, SHA1, and SHA256

Rockyou (Easy)

15 POINTS
OUT OF 15

100.0%
ACCURACY

COMPLETION: **100.0%**

Crack MD5 password hashes for password found in the rockyou breach

Windows (Easy)

25 POINTS
OUT OF 30

50.0%
ACCURACY

COMPLETION: **100.0%**

Crack Windows NTLM password hashes using rainbow tables

Pattern (Medium)

40 POINTS
OUT OF 45

75.0%
ACCURACY

COMPLETION: **100.0%**

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

PDF (Medium)

45 POINTS
OUT OF 50

66.7%
ACCURACY

COMPLETION: **100.0%**

Crack the insecure password for a protected PDF file

Wordlist (Hard)

-5 POINTS
OUT OF 75

0.0%
ACCURACY

COMPLETION: **0.0%**

Build a wordlist to crack passwords not found in common wordlists

Complexity (Hard)

20 POINTS
OUT OF 70

66.7%
ACCURACY

COMPLETION: **28.6%**

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



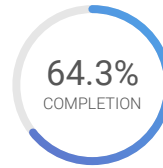
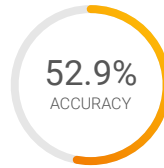


Scanning & Reconnaissance Module

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

834 TH PLACE
OUT OF 7406
NATIONAL RANK

155 POINTS
OUT OF 300
PERFORMANCE SCORE



89th National
Percentile

Average: 136.9 Points

Average: 66.6%

Average: 50.5%

Port Scan (Easy)

100 POINTS
OUT OF 100

83.3%
ACCURACY

COMPLETION: **100.0%**

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

Foreign (Medium)

55 POINTS
OUT OF 100

44.4%
ACCURACY

COMPLETION: **80.0%**

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%**

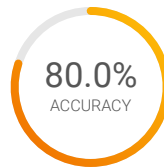
Scan an email server to enumerate user accounts

Web Application Exploitation Module

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

620 TH PLACE
OUT OF 7406
NATIONAL RANK

175 POINTS
OUT OF 300
PERFORMANCE SCORE



92nd National
Percentile

Average: 108.2 Points

Average: 53.3%

Average: 46.1%

PiratePals (Easy)

95 POINTS
OUT OF 100

75.0%
ACCURACY

COMPLETION: **100.0%**

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)

80 POINTS
OUT OF 100

100.0%
ACCURACY

COMPLETION: **100.0%**

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

