POWERED BY CYBER SKYLINE

The National Cyber League
A Community Where Cybersecurity Is a Passion

Jacob Suveges
jacobsuveges45@gmail.com

NCL Spring 2024 Individual Game Scouting Report

Dear Jacob Suveges,

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.

HANDS-ON SKILLS ASSESSMENT CYBER SKYLINE VERIFIED SCORE REPORT

To validate this report, please access: cyberskyline.com/report/EWTV464VGQ1T

CompTIA

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

NATIONAL RANK

455TH PLACE OUT OF 7406

PERCENTILE

94TH

YOUR TOP CATEGORIES

CRYPTOGRAPHY	LOG ANALYSIS	ENUMERATION & EXPLOITATION
98TH PERCENTILE	96TH PERCENTILE	96TH PERCENTILE

68.1%
ACCURACY

Average: 67.4%

cyberskyline.com/report
ID: EWTV464VGQ1T

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.

455 TH PLACE OUT OF 7406
NATIONAL RANK

94th National Percentile

1980 POINTS OUT OF 3000
PERFORMANCE SCORE

Average: 948.1 Points

68.1% ACCURACY

Average: 67.4%

71.8% COMPLETION

Average: 37.5%

Cryptography

280 POINTS OUT OF 370

100.0% ACCURACY

COMPLETION: 85.7%

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

Enumeration & Exploitation

110 POINTS OUT OF 300

100.0% ACCURACY

COMPLETION: 60.0%

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

Forensics

110 POINTS OUT OF 300

57.1% ACCURACY

COMPLETION: 50.0%

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

Log Analysis

220 POINTS OUT OF 300

83.3% ACCURACY

COMPLETION: 88.2%

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

245 POINTS OUT OF 300

70.0% ACCURACY

COMPLETION: 87.5%

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

Open Source Intelligence

230 POINTS OUT OF 430

93.3% ACCURACY

COMPLETION: 56.0%

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

185 POINTS OUT OF 300

66.7% ACCURACY

COMPLETION: 61.5%

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

Scanning & Reconnaissance

200 POINTS OUT OF 300

40.0% ACCURACY

COMPLETION: 71.4%

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 300

38.5% 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.

Cryptography Module

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

196 TH PLACE OUT OF 7406
NATIONAL RANK

280 POINTS OUT OF 370
PERFORMANCE SCORE

100.0%
ACCURACY

85.7%
COMPLETION

98th National Percentile

Average: 184.5 Points

Average: 78.8%

Average: 57.6%

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)

80 POINTS OUT OF 80

100.0% 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

100.0% ACCURACY

COMPLETION: 100.0%

Analyze and decode a x509 certificate used for public key cryptography

Love's the AES (Hard)

10 POINTS OUT OF 100

100.0% ACCURACY

COMPLETION: 33.3%

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.

336 TH PLACE OUT OF 7406
NATIONAL RANK

96th National Percentile

110 POINTS OUT OF 300
PERFORMANCE SCORE

Average: 96.8 Points

100.0%
ACCURACY

Average: 74.6%

60.0%
COMPLETION

Average: 44.9%

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

100.0% 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.

836 TH PLACE OUT OF 7406
NATIONAL RANK

89th National Percentile

110 POINTS OUT OF 300
PERFORMANCE SCORE

Average: 102.5 Points

57.1%
ACCURACY

Average: 49.6%

50.0%
COMPLETION

Average: 39.8%

Lost (Easy)

100 POINTS OUT OF 100

50.0% ACCURACY

COMPLETION: 100.0%

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

Backdoor (Medium)

10 POINTS OUT OF 100

100.0% ACCURACY

COMPLETION: 33.3%

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

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.

302 ND PLACE OUT OF 7406
NATIONAL RANK

96 th National Percentile

220 POINTS OUT OF 300
PERFORMANCE SCORE

Average: 123.4 Points

83.3%
ACCURACY

Average: 68.3%

88.2%
COMPLETION

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)

100 POINTS OUT OF 100

88.9% ACCURACY

COMPLETION: 100.0%

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

Buffed (Hard)

20 POINTS OUT OF 100

33.3% ACCURACY

COMPLETION: 33.3%

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.

453 RD PLACE OUT OF 7406
NATIONAL RANK

94 th National Percentile

245 POINTS OUT OF 300
PERFORMANCE SCORE

Average: 138.2 Points

70.0%
ACCURACY

Average: 54.3%

87.5%
COMPLETION

Average: 53.3%

Shell (Easy)

100 POINTS OUT OF 100

75.0% ACCURACY

COMPLETION: 100.0%

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

Missing (Medium)

100 POINTS OUT OF 100

100.0% ACCURACY

COMPLETION: 100.0%

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

Route (Hard)

45 POINTS OUT OF 100

50.0% ACCURACY

COMPLETION: 66.7%

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.

1946 TH PLACE OUT OF 7406
NATIONAL RANK

74th National Percentile

230 POINTS OUT OF 430
PERFORMANCE SCORE

Average: 246.9 Points

93.3%
ACCURACY

Average: 67.9%

56.0%
COMPLETION

Average: 60.9%

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 | 100.0% 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)

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

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

Password Cracking Module

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

624 TH PLACE OUT OF 7406
NATIONAL RANK

185 POINTS OUT OF 300
PERFORMANCE SCORE

66.7%
ACCURACY

61.5%
COMPLETION

92nd National Percentile

Average: 91.5 Points

Average: 88.0%

Average: 38.1%

Hashing (Easy)

15 POINTS OUT OF 15 | 100.0% 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)

30 POINTS OUT OF 30 | 27.3% ACCURACY | COMPLETION: 100.0%

Crack Windows NTLM password hashes using rainbow tables

Pattern (Medium)

45 POINTS OUT OF 45 | 100.0% ACCURACY | COMPLETION: 100.0%

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

PDF (Medium)

50 POINTS OUT OF 50 | 100.0% ACCURACY | COMPLETION: 100.0%

Crack the insecure password for a protected PDF file

Wordlist (Hard)

30 POINTS OUT OF 75 | 100.0% ACCURACY | COMPLETION: 40.0%

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

Scanning & Reconnaissance Module

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

554 TH PLACE OUT OF 7406
NATIONAL RANK

200 POINTS OUT OF 300
PERFORMANCE SCORE

40.0%
ACCURACY

71.4%
COMPLETION

93 rd National Percentile

Average: 136.9 Points

Average: 66.6%

Average: 50.5%

Port Scan (Easy)

100 POINTS OUT OF 100

100.0% ACCURACY

COMPLETION: 100.0%

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

Foreign (Medium)

100 POINTS OUT OF 100

25.0% ACCURACY

COMPLETION: 100.0%

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.

356 TH PLACE OUT OF 7406
NATIONAL RANK

300 POINTS OUT OF 300
PERFORMANCE SCORE

38.5%
ACCURACY

100.0%
COMPLETION

96 th National Percentile

Average: 108.2 Points

Average: 53.3%

Average: 46.1%

PiratePals (Easy)

100 POINTS OUT OF 100

30.0% 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)

100 POINTS OUT OF 100

50.0% 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)

100 POINTS OUT OF 100

100.0% ACCURACY

COMPLETION: 100.0%

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