Nicholas Malamud
nickfromsd@gmail.com

NCL Spring 2023 Team Game Scouting Report

Dear Nicholas Malamud (Team "c0ug4rs"),

Thank you for participating in the National Cyber League (NCL) 2023 Spring 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 2023 Spring Season had 7,820 students/players and 533 faculty/coaches from more than 450 two- and four-year schools & 250 high schools across all 50 U.S. states registered to play. The Individual Game Capture the Flag (CTF) event took place from March 31 through April 2. The Team Game CTF event took place from April 14 through April 16. 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/FFQVM63T18CN

Congratulations for your participation in the NCL 2023 Spring 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 2023 SPRING TEAM GAME

EXPERIENCED STUDENTS RANK
16TH PLACE OUT OF 316

PERCENTILE
95TH

YOUR TOP CATEGORIES

OPEN SOURCE INTELLIGENCE	WEB APPLICATION EXPLOITATION	CRYPTOGRAPHY
100TH PERCENTILE	99TH PERCENTILE	99TH PERCENTILE

Average: 73.1%

cyberskyline.com/report
ID: FFQVM63T18CN

Nicholas Malamud
nickfromsd@gmail.com

NCL Spring 2023 Team Game

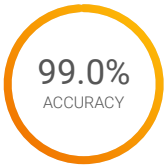
The NCL Team Game is designed for student players nationwide to compete in realtime in the categories listed below. The Team Game promotes camaraderie and evaluates the collective technical cybersecurity skills of the team members.

16 TH PLACE OUT OF 316
EXPERIENCED STUDENTS RANK

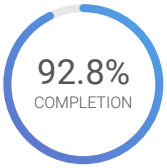
95th Experienced Students Percentile

2510 POINTS OUT OF 3000
PERFORMANCE SCORE

Average: 1508.8 Points



Average: 73.1%



Average: 60.3%

Cryptography

355 POINTS OUT OF 355

100.0% ACCURACY

COMPLETION: 100.0%

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

Enumeration & Exploitation

200 POINTS OUT OF 300

100.0% ACCURACY

COMPLETION: 83.3%

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

Forensics

230 POINTS OUT OF 300

100.0% ACCURACY

COMPLETION: 88.9%

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

Log Analysis

300 POINTS OUT OF 300

95.2% ACCURACY

COMPLETION: 100.0%

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

315 POINTS OUT OF 365

100.0% ACCURACY

COMPLETION: 94.1%

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

Open Source Intelligence

350 POINTS OUT OF 350

100.0% ACCURACY

COMPLETION: 100.0%

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

210 POINTS OUT OF 330

100.0% ACCURACY

COMPLETION: 82.4%

Try your hand at cracking these passwords.

Scanning & Reconnaissance

300 POINTS OUT OF 300

100.0% ACCURACY

COMPLETION: 100.0%

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

Web Application Exploitation

150 POINTS OUT OF 300

100.0% ACCURACY

COMPLETION: 66.7%

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.

Nicholas Malamud
nickfromsd@gmail.com

Cryptography Module

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

5 TH PLACE OUT OF 316
EXPERIENCED STUDENTS RANK

99th Experienced Students Percentile

355 POINTS OUT OF 355
PERFORMANCE SCORE

Average: 189.5 Points

100.0% ACCURACY

Average: 75.0%

100.0% COMPLETION

Average: 68.6%

TOP NICE WORKROLES
Security Control Assessor
Secure Software Assessor
Exploitation Analyst
Cyber Operator
Security Architect

Decoding 1 (Easy)

30 POINTS OUT OF 30

100.0% ACCURACY

COMPLETION: 100.0%

Obtain plaintext from messages encoded with common number bases

Decoding 2 (Easy)

30 POINTS OUT OF 30

100.0% ACCURACY

COMPLETION: 100.0%

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

Decoding 3 (Easy)

30 POINTS OUT OF 30

100.0% ACCURACY

COMPLETION: 100.0%

Obtain the plaintext of a message using a keypad cipher

Decoding 4 (Medium)

50 POINTS OUT OF 50

100.0% ACCURACY

COMPLETION: 100.0%

Decrypt an AES encrypted message with a known password

PGP (Medium)

50 POINTS OUT OF 50

100.0% ACCURACY

COMPLETION: 100.0%

Decrypt a PGP message and encrypt a PGP message using provided keys

Beep Boop (Medium)

65 POINTS OUT OF 65

100.0% ACCURACY

COMPLETION: 100.0%

Analyze an audio file and decode a message that is encoded with dual-tone multi-frequency signaling

AutoCrypt (Hard)

100 POINTS OUT OF 100

100.0% ACCURACY

COMPLETION: 100.0%

Analyze a cryptographic scheme and find the vulnerability in an autokey cipher to decrypt the message

Nicholas Malamud
nickfromsd@gmail.com

Enumeration & Exploitation Module

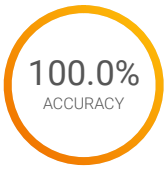
Identify actionable exploits and vulnerabilities and use them to bypass the security measures in code and compiled binaries.

19 TH PLACE OUT OF 316
EXPERIENCED STUDENTS RANK

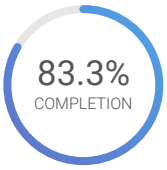
94th Experienced Students Percentile

200 POINTS OUT OF 300
PERFORMANCE SCORE

Average: 119.3 Points



Average: 79.8%



Average: 61.7%

TOP NICE WORKROLES
Cyber Operator
Target Developer
Exploitation Analyst
Software Developer
Systems Security Analyst

Shinny Stone (Easy)

100 POINTS OUT OF 100
100.0% ACCURACY
COMPLETION: 100.0%

Analyze Ruby source code to decrypt a message that was encrypted using AES

Vault (Medium)

100 POINTS OUT OF 100
100.0% ACCURACY
COMPLETION: 100.0%

Extract and analyze a compiled Python file from a macOS mach-o binary

Crypto Coincidence (Hard)

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

Analyze a compiled C binary and bypass its custom encryption and packing

Forensics Module

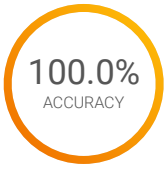
Utilize the proper tools and techniques to analyze, process, recover, and/or investigate digital evidence in a computer-related incident.

26 TH PLACE OUT OF 316
EXPERIENCED STUDENTS RANK

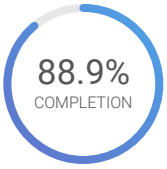
92nd Experienced Students Percentile

230 POINTS OUT OF 300
PERFORMANCE SCORE

Average: 163.3 Points



Average: 76.0%



Average: 57.4%

TOP NICE WORKROLES
Cyber Defense Forensics Analyst
Cyber Crime Investigator
Cyber Defense Incident Responder
Cyber Defense Analyst

Stacked (Easy)

100 POINTS OUT OF 100
100.0% ACCURACY
COMPLETION: 100.0%

Find and extract hidden files within an image using tools like binwalk

Hidden (Medium)

100 POINTS OUT OF 100
100.0% ACCURACY
COMPLETION: 100.0%

Extract hidden information from a macOS .DS_STORE file

Memory (Hard)

30 POINTS OUT OF 100
100.0% ACCURACY
COMPLETION: 66.7%

Analyze a Linux memory dump using tools like Volatility to extract encryption keys from a Vim buffer and decrypt an in-memory encrypted file

Nicholas Malamud
nickfromsd@gmail.com

Log Analysis Module

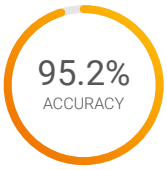
Utilize the proper tools and techniques to establish a baseline for normal operation and identify malicious activities using log files from various services.

15 TH PLACE OUT OF **316**
EXPERIENCED STUDENTS RANK

96th Experienced Students Percentile

300 POINTS OUT OF 300
PERFORMANCE SCORE

Average: 205.4 Points



Average: 71.6%

Average: 73.8%

TOP NICE WORKROLES
Cyber Defense Analyst
Systems Security Analyst
All-Source Analyst
Cyber Defense Forensics Analyst
Data Analyst

PGP (Easy) Analyze clear-signed documents to verify their authenticity using PGP keys	100 POINTS OUT OF 100	100.0% ACCURACY	COMPLETION: 100.0%
Iptables (Medium) Analyze a iptables log file to identify network traffic patterns	100 POINTS OUT OF 100	100.0% ACCURACY	COMPLETION: 100.0%
Flight Record (Hard) Parse a binary encoded drone flight record file and extract its fields	100 POINTS OUT OF 100	88.9% ACCURACY	COMPLETION: 100.0%

Network Traffic Analysis Module

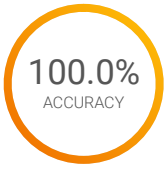
Identify malicious and benign network traffic to demonstrate an understanding of potential security breaches.

16 TH PLACE OUT OF **316**
EXPERIENCED STUDENTS RANK

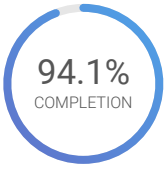
95th Experienced Students Percentile

315 POINTS OUT OF 365
PERFORMANCE SCORE

Average: 212.9 Points



Average: 57.9%



Average: 66.4%

TOP NICE WORKROLES
Cyber Defense Analyst
All-Source Analyst
Cyber Defense Incident Responder
Target Network Analyst
Cyber Operator

Attack (Easy) Analyze a network packet capture to identify an ARP spoofing attack	100 POINTS OUT OF 100	100.0% ACCURACY	COMPLETION: 100.0%
Chunked (Easy) Analyze a wireless network packet capture to extract information from the broadcast packets	65 POINTS OUT OF 65	100.0% ACCURACY	COMPLETION: 100.0%
Lighting (Medium) Analyze a network packet capture to identify the IOT protocol and decode its communications	100 POINTS OUT OF 100	100.0% ACCURACY	COMPLETION: 100.0%
Covert Exfiltration (Hard) Reassemble a multi-part HTTP file download from a network packet capture	50 POINTS OUT OF 100	100.0% ACCURACY	COMPLETION: 66.7%

Nicholas Malamud
nickfromsd@gmail.com

Open Source Intelligence Module

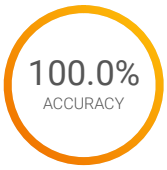
Utilize publicly available information such as search engines, public repositories, social media, and more to gain in-depth knowledge on a topic or target.

3 RD PLACE OUT OF **316**
EXPERIENCED STUDENTS RANK

350 POINTS OUT OF 350
PERFORMANCE SCORE

100th Experienced Students Percentile

Average: 288.1 Points



Average: 77.3%

Average: 89.7%

TOP NICE WORKROLES
Systems Security Analyst
Target Developer
System Administrator
Research & Development Specialist
Cyber Intel Planner

Rules of Conduct (Easy)

25 POINTS OUT OF 25

100.0% ACCURACY

COMPLETION: **100.0%**

Introductory challenge on acceptable conduct during NCL

Network Info (Easy)

50 POINTS OUT OF 50

100.0% ACCURACY

COMPLETION: **100.0%**

Extract WiFi network information out of a QR code

Message in Stone (Medium)

75 POINTS OUT OF 75

100.0% ACCURACY

COMPLETION: **100.0%**

Identify the ancient esoteric alphabet used to hide a secret message

Restaurant WiFi (Medium)

100 POINTS OUT OF 100

100.0% ACCURACY

COMPLETION: **100.0%**

Identify the guest WiFi password using openly available information

Vantage Point (Hard)

100 POINTS OUT OF 100

100.0% ACCURACY

COMPLETION: **100.0%**

Geolocate a photo without GPS metadata

Nicholas Malamud
nickfromsd@gmail.com

Password Cracking Module

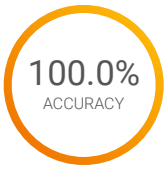
Try your hand at cracking these passwords.

34 TH PLACE OUT OF 316
EXPERIENCED STUDENTS RANK

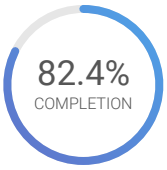
90th Experienced Students Percentile

210 POINTS OUT OF 330
PERFORMANCE SCORE

Average: 162.2 Points



Average: 93.6%



Average: 64.2%

TOP NICE WORKROLES
Cyber Operator
Exploitation Analyst
Systems Security Analyst
Cyber Defense Incident Responder
Cyber Crime Investigator

Cracking 1 (Easy)

30 POINTS OUT OF 30

100.0% ACCURACY

COMPLETION: 100.0%

Crack MD5 password hashes

Cracking 2 (Easy)

30 POINTS OUT OF 30

100.0% ACCURACY

COMPLETION: 100.0%

Crack Windows NTLM password hashes using rainbow tables

Cracking 3 (Medium)

45 POINTS OUT OF 45

100.0% ACCURACY

COMPLETION: 100.0%

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

Cracking 4 (Hard)

75 POINTS OUT OF 75

100.0% ACCURACY

COMPLETION: 100.0%

Crack salted MD5 password hashes

Cracking 5 (Hard)

30 POINTS OUT OF 150

100.0% ACCURACY

COMPLETION: 40.0%

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

Nicholas Malamud
nickfromsd@gmail.com

Scanning & Reconnaissance Module

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

6 TH PLACE OUT OF 316
EXPERIENCED STUDENTS RANK

99th Experienced Students Percentile

300 POINTS OUT OF 300
PERFORMANCE SCORE

Average: 204.3 Points

100.0% ACCURACY

Average: 95.7%

100.0% COMPLETION

Average: 69.7%

TOP NICE WORKROLES
- Vulnerability Assessment Analyst
- Target Network Analyst
- Cyber Operations Planner
- Target Developer
- Security Control Assessor

Docker (Easy)

100 POINTS OUT OF 100

100.0% ACCURACY

COMPLETION: 100.0%

Extract metadata information from a Docker container image

Call to Action (Medium)

100 POINTS OUT OF 100

100.0% ACCURACY

COMPLETION: 100.0%

Scan and extract information data from a Redis database

Database (Hard)

100 POINTS OUT OF 100

100.0% ACCURACY

COMPLETION: 100.0%

Scan and extract information data from a MongoDB database

Web Application Exploitation Module

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

5 TH PLACE OUT OF 316
EXPERIENCED STUDENTS RANK

99th Experienced Students Percentile

150 POINTS OUT OF 300
PERFORMANCE SCORE

Average: 83.8 Points

100.0% ACCURACY

Average: 77.8%

66.7% COMPLETION

Average: 37.0%

TOP NICE WORKROLES
- Cyber Operator
- Software Developer
- Exploitation Analyst
- Systems Security Analyst
- Database Administrator

Never Winter Bank (Easy)

100 POINTS OUT OF 100

100.0% ACCURACY

COMPLETION: 100.0%

Exploit a bug in the parseInt function of older JavaScript web runtimes

WebAuthn (Medium)

20 POINTS OUT OF 100

100.0% ACCURACY

COMPLETION: 50.0%

Exploit an improperly configured WebAuthn login scheme

File Server v2 (Hard)

30 POINTS OUT OF 100

100.0% ACCURACY

COMPLETION: 50.0%

Exploit a race condition to download a restricted file during server operations