NCL Fall 2022 Team Game Scouting Report

Dear Will Green (Team "SANS.edu Sentinels Team 2"),

Thank you for participating in the National Cyber League (NCL) 2022 Fall 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 2022 Fall Season had 7,690 students/players and 475 faculty/coaches from more than 470 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 October 21 through October 23. The Team Game CTF event took place from November 4 through November 6. 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/XXWWLD8L3P71

Congratulations for your participation in the NCL 2022 Fall Team Game! We hope you will continue to develop your knowledge and skills and make meaningful contributions as part of the Information Security workforce!
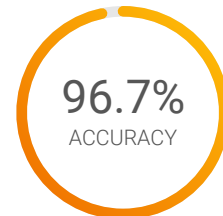
David Zeichick
NCL Commissioner

NATIONAL CYBER LEAGUE SCORE CARD

NCL 2022 FALL TEAM GAME

NATIONAL RANK
4TH PLACE
OUT OF 3926
PERCENTILE
100TH

YOUR TOP CATEGORIES

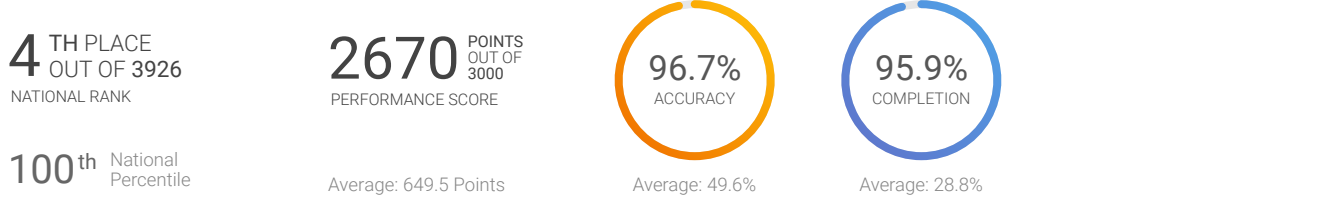| SCANNING & RECONNAISSANCE	OPEN SOURCE INTELLIGENCE	WEB APPLICATION EXPLOITATION
100TH PERCENTILE	100TH PERCENTILE	100TH PERCENTILE

96.7%
ACCURACY

Average: 49.6%

cyberskyline.com/report
ID: XXWWLD8L3P71

NCL Fall 2022 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.

4 TH PLACE OUT OF **3926**
NATIONAL RANK

100th National Percentile

2670 POINTS OUT OF 3000
PERFORMANCE SCORE

Average: 649.5 Points

96.7% ACCURACY
Average: 49.6%

95.9% COMPLETION
Average: 28.8%

Cryptography

310 POINTS OUT OF 310   **100.0%** ACCURACY   COMPLETION: **100.0%**

Information is key, but it's not going to be easy to get it. Decipher these hidden messages to learn what is really going on.

Enumeration & Exploitation

300 POINTS OUT OF 300   **100.0%** ACCURACY   COMPLETION: **100.0%**

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

Forensics

210 POINTS OUT OF 310   **90.0%** ACCURACY   COMPLETION: **90.0%**

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

Log Analysis

320 POINTS OUT OF 320   **89.5%** 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

250 POINTS OUT OF 370   **95.0%** ACCURACY   COMPLETION: **90.5%**

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

Open Source Intelligence

315 POINTS OUT OF 315   **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

335 POINTS OUT OF 360   **100.0%** ACCURACY   COMPLETION: **95.0%**

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

Scanning & Reconnaissance

315 POINTS OUT OF 315   **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

215 POINTS OUT OF 300   **100.0%** ACCURACY   COMPLETION: **83.3%**

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

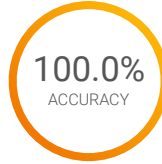Note: Survey module (100 points) was excluded from this report.

POWERED BY CYBER SKYLINE

POWERED BY
CYBER SKYLINE

Cryptography Module

Information is key, but it's not going to be easy to get it. Decipher these hidden messages to learn what is really going on.

4 TH PLACE
OUT OF **3926**
NATIONAL RANK

100 th National Percentile

310 POINTS OUT OF 310
PERFORMANCE SCORE

Average: 119.3 Points

100.0%
ACCURACY

Average: 78.6%

100.0%
COMPLETION

Average: 54.1%

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

Decoding 1 (Easy)

Identify the cipher scheme used and decrypt the data

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

Decoding 2 (Easy)

Identify the cipher scheme used and decrypt the data

| **20** POINTS OUT OF 20 | **100.0%** ACCURACY | COMPLETION: | **100.0%** |

Decoding 3 (Easy)

Identify the cipher scheme used and decrypt the data

| **35** POINTS OUT OF 35 | **100.0%** ACCURACY | COMPLETION: | **100.0%** |

Decoding 4 (Medium)

Identify the communication scheme used and decode the message

| **20** POINTS OUT OF 20 | **100.0%** ACCURACY | COMPLETION: | **100.0%** |

Decoding 5 (Medium)

Identify the cipher scheme used and decrypt the data

| **55** POINTS OUT OF 55 | **100.0%** ACCURACY | COMPLETION: | **100.0%** |

Problem (Medium)

Identify the steganography technique used and extract the hidden data

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

Magnetic (Hard)

Convert credit card magnetic stripe audio into numeric data

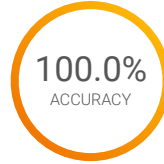| **100** POINTS OUT OF 100 | **100.0%** ACCURACY | COMPLETION: | **100.0%** |

POWERED BY
CYBER SKYLINE

Enumeration & Exploitation Module

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

5 TH PLACE
OUT OF **3926**
NATIONAL RANK

100th National Percentile

300 POINTS OUT OF 300
PERFORMANCE SCORE

Average: 52.0 Points

100.0% ACCURACY

Average: 51.7%

100.0% COMPLETION

Average: 27.7%

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

Channels (Easy)
100 POINTS OUT OF 100   **100.0%** ACCURACY   COMPLETION: **100.0%**

Analyze Go source code to identify its functionalities and vulnerabilities

Miner (Medium)
100 POINTS OUT OF 100   **100.0%** ACCURACY   COMPLETION: **100.0%**

Decompile a binary crypto-miner malware to identify its functionalities

Password Manager (Hard)
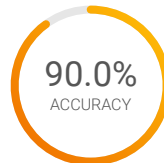**100** POINTS OUT OF 100   **100.0%** ACCURACY   COMPLETION: **100.0%**

Decompile and analyze a binary that implements a virtual machine (VM) for a custom instruction set architecture (ISA) and break the encryption to a custom password manager program
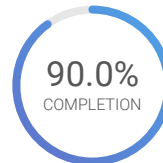
Forensics Module

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

16 TH PLACE
OUT OF **3926**
NATIONAL RANK

100th National Percentile

210 POINTS OUT OF 310
PERFORMANCE SCORE

Average: 106.1 Points

90.0% ACCURACY

Average: 57.8%

90.0% COMPLETION

Average: 26.7%

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

Blocked (Easy)
100 POINTS OUT OF 100   **100.0%** ACCURACY   COMPLETION: **100.0%**

Analyze a redacted PDF file to identify techniques to remove the redaction

Hiding (Medium)
0 POINTS OUT OF 100   **0.0%** ACCURACY   COMPLETION: **0.0%**

Identify the compressed data stream without header metadata

Unknown (Hard)
110 POINTS OUT OF 110   **88.9%** ACCURACY   COMPLETION: **100.0%**

Analyze a ZFS pool to extract hidden files and metadata

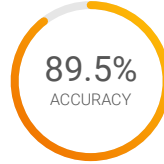POWERED BY CYBER SKYLINE

Will Green
will@willgreen.tech

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.

9TH PLACE
OUT OF **3926**
NATIONAL RANK

100th National Percentile

320 POINTS OUT OF 320
PERFORMANCE SCORE

Average: 63.6 Points

89.5% ACCURACY
Average: 26.9%

100.0% COMPLETION
Average: 23.6%

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

Cubes (Easy)
100 POINTS OUT OF 100 — **77.8%** ACCURACY — COMPLETION: **100.0%**
Analyze a DNS server log to identify potentially malicious domains

Lunch (Medium)
100 POINTS OUT OF 100 — **100.0%** ACCURACY — COMPLETION: **100.0%**
Analyze a web server log using MessagePack encoding and identify anomalies

Collection (Hard)
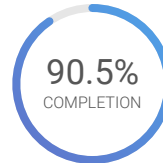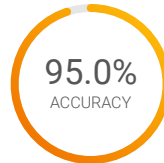**120** POINTS OUT OF 120 — **100.0%** ACCURACY — COMPLETION: **100.0%**
Analyze employee badge and motion sensor logs to compute outliers and identify anomalous behavior

Network Traffic Analysis Module

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

14TH PLACE
OUT OF **3926**
NATIONAL RANK

100th National Percentile

250 POINTS OUT OF 370
PERFORMANCE SCORE

Average: 111.9 Points

95.0% ACCURACY
Average: 41.6%

90.5% COMPLETION
Average: 46.4%

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

VPN (Easy)
100 POINTS OUT OF 100 — **90.0%** ACCURACY — COMPLETION: **100.0%**
Extract sensitive information transferred in a VPN packet capture

WiFi Cracking (Medium)
30 POINTS OUT OF 70 — **100.0%** ACCURACY — COMPLETION: **75.0%**
Identify vulnerable WiFi encryption scheme and crack the WiFi password

Kick Back (Medium)
100 POINTS OUT OF 100 — **100.0%** ACCURACY — COMPLETION: **100.0%**
Analyze the unencrypted IOT device traffic to extract personal information from a smart home packet capture

Extraction (Hard)
20 POINTS OUT OF 100 — **100.0%** ACCURACY — COMPLETION: **66.7%**
Identify and extract the hidden RTMP video stream transferred in a comprehensive packet capture

POWERED BY CYBER SKYLINE

POWERED BY
CYBER SKYLINE

The National Cyber League
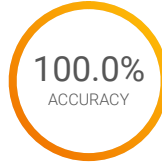A Community Where Cybersecurity Is a Passion

Will Green
will@willgreen.tech

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.

2 ND PLACE
OUT OF **3926**
NATIONAL RANK

100th National Percentile

315 POINTS OUT OF 315
PERFORMANCE SCORE

Average: 150.0 Points

100.0%
ACCURACY

Average: 49.7%

100.0%
COMPLETION

Average: 65.4%

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

Defense Acquisition (Easy)

45 POINTS OUT OF 45

100.0% ACCURACY

COMPLETION: 100.0%

Identify the common organizations responsible for purchases for the government

Vehicle (Easy)

50 POINTS OUT OF 50

100.0% ACCURACY

COMPLETION: 100.0%

Utilize reverse image search tools to identify the make and model of a vehicle

Targets (Medium)

45 POINTS OUT OF 45

100.0% ACCURACY

COMPLETION: 100.0%

Investigate an unknown number scheme to identify the IP address associated with the number

District (Medium)

50 POINTS OUT OF 50

100.0% ACCURACY

COMPLETION: 100.0%

Utilize Geographic Information System (GIS) to identify land plot and owner data

Tracking (Hard)

100 POINTS OUT OF 100

100.0% ACCURACY

COMPLETION: 100.0%

Investigate commonalities in the locations from a sequence of GPS coordinates to identify the potential next target location
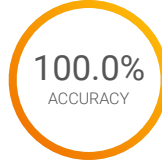
The National Cyber League
A Community Where Cybersecurity Is a Passion

Will Green
will@willgreen.tech

POWERED BY
CYBER SKYLINE

Password Cracking Module

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

5 TH PLACE
OUT OF **3926**
NATIONAL RANK

100th National Percentile

335 POINTS OUT OF 360
PERFORMANCE SCORE

Average: 123.5 Points

100.0% ACCURACY

Average: 87.0%

95.0% COMPLETION

Average: 39.5%

TOP NICE WORKROLES

Cyber Operator
Exploitation Analyst
Systems Security Analyst
Cyber Defense Incident Responder
Cyber Crime Investigator

Cracking 1 (Easy)

45 POINTS OUT OF 45 — **100.0%** ACCURACY — COMPLETION: **100.0%**

Crack MD5, SHA1, and SHA256 password hashes

Cracking 2 (Easy)

45 POINTS OUT OF 45 — **100.0%** ACCURACY — COMPLETION: **100.0%**

Crack Windows NTLM password hashes using rainbow tables

Cracking 3 (Medium)

60 POINTS OUT OF 60 — **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 100 — **100.0%** ACCURACY — COMPLETION: **83.3%**

Build a wordlist to crack passwords not found in common wordlists

PPTX (Medium)

50 POINTS OUT OF 50 — **100.0%** ACCURACY — COMPLETION: **100.0%**

Crack the password for a protected PowerPoint file

WiFi (Hard)

60 POINTS OUT OF 60 — **100.0%** ACCURACY — COMPLETION: **100.0%**

Crack the password hashes stored in a Linux wpa_supplicant.conf file
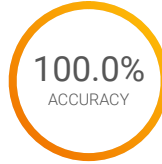
POWERED BY CYBER SKYLINE

Scanning & Reconnaissance Module

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

1 ST PLACE
OUT OF 3926
NATIONAL RANK

100th National Percentile

315 POINTS OUT OF 315
PERFORMANCE SCORE

Average: 33.4 Points

100.0% ACCURACY

Average: 19.0%

100.0% COMPLETION

Average: 9.3%

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

Catch Me If You Can (Easy)
100 POINTS OUT OF 100   **100.0%** ACCURACY   COMPLETION: **100.0%**

Scan the available UDP ports on a target system

Interstellar (Medium)
100 POINTS OUT OF 100   **100.0%** ACCURACY   COMPLETION: **100.0%**

Scan an InterPlanetary File System (IPFS) server and retrieve a file from the service

Tracker (Hard)
**115** POINTS OUT OF 115   **100.0%** ACCURACY   COMPLETION: **100.0%**

Scan and analyze the results from an UDP BitTorrent Tracker service

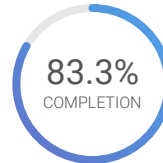## Web Application Exploitation Module

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

3 RD PLACE
OUT OF 3926
NATIONAL RANK

100th National Percentile

215 POINTS OUT OF 300
PERFORMANCE SCORE

Average: 59.4 Points

100.0% ACCURACY

Average: 38.0%

83.3% COMPLETION
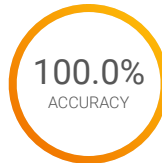
Average: 29.5%

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

Ticket Scalper (Easy)
100 POINTS OUT OF 100   **100.0%** ACCURACY   COMPLETION: **100.0%**

Exploit a ticket booking app by analyzing the partial logic in the browser side JavaScript code

Pesto's Pizza (Medium)
100 POINTS OUT OF 100   **100.0%** ACCURACY   COMPLETION: **100.0%**

Identify and exploit a PHP type juggling vulnerability to gain unauthorized access

Mercury Lotto (Hard)
15 POINTS OUT OF 100   **100.0%** ACCURACY   COMPLETION: **50.0%**

Identify and exploit a seeded random number generator by analyzing the deterministic server behavior