Luke Leveque
lileve01@louisville.edu

NCL Fall 2024 Team Game Scouting Report

Dear Luke Leveque (Team "UofL Team Pear"),

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/3Q2XQ2AHK6PE

Congratulations for your participation in the NCL Fall 2024 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

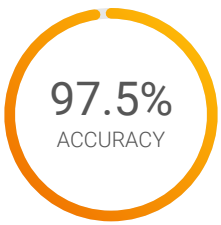
NCL FALL 2024 TEAM GAME

EXPERIENCED STUDENTS RANK
12TH PLACE OUT OF 532

PERCENTILE
98TH

YOUR TOP CATEGORIES

CRYPTOGRAPHY	FORENSICS	NETWORK TRAFFIC ANALYSIS
100TH PERCENTILE	100TH PERCENTILE	99TH PERCENTILE



Average: 72.7%

cyberskyline.com/report
ID: 3Q2XQ2AHK6PE

Luke Leveque
lileve01@louisville.edu

NCL Fall 2024 Team Game

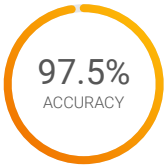
The NCL Team Game is designed for student players nationwide to compete in realtime in the categories listed below. The Team Game promotes camaraderie and evaluates the collective technical cybersecurity skills of the team members.

12 TH PLACE OUT OF 532
EXPERIENCED STUDENTS RANK

2850 POINTS OUT OF 3100
PERFORMANCE SCORE

98th Experienced Students Percentile

Average: 1850.2 Points



Average: 72.7%

Average: 66.5%

Cryptography

310 POINTS OUT OF 310

100.0% ACCURACY

COMPLETION: 100.0%

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

Enumeration & Exploitation

210 POINTS OUT OF 300

100.0% ACCURACY

COMPLETION: 88.9%

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

Forensics

400 POINTS OUT OF 400

100.0% ACCURACY

COMPLETION: 100.0%

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

Log Analysis

350 POINTS OUT OF 350

95.0% 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

300 POINTS OUT OF 300

100.0% ACCURACY

COMPLETION: 100.0%

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

Open Source Intelligence

390 POINTS OUT OF 390

95.5% 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

280 POINTS OUT OF 340

100.0% ACCURACY

COMPLETION: 89.3%

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

Scanning & Reconnaissance

310 POINTS OUT OF 310

90.9% 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

200 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.

Luke Leveque
lileve01@louisville.edu

Cryptography Module

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

2 ND PLACE OUT OF 532
EXPERIENCED STUDENTS RANK

310 POINTS OUT OF 310
PERFORMANCE SCORE

100.0% ACCURACY

100.0% COMPLETION

100th Experienced Students Percentile

Average: 175.0 Points

Average: 60.2%

Average: 66.0%

Bases (Easy)

45 POINTS OUT OF 45

100.0% ACCURACY

COMPLETION: 100.0%

Decode messages that have been encoded one or more times using different number bases.

Shady Shapes (Easy)

50 POINTS OUT OF 50

100.0% ACCURACY

COMPLETION: 100.0%

Decode a morse code message encoded using shapes for dots and dashes.

Jefferson (Easy)

60 POINTS OUT OF 60

100.0% ACCURACY

COMPLETION: 100.0%

Find and use the correct Jefferson cipher wheel to decode a message.

Secure Flag Share (Medium)

80 POINTS OUT OF 80

100.0% ACCURACY

COMPLETION: 100.0%

Perform a known plaintext attack on an XOR-encrypted message.

Scheming (Hard)

75 POINTS OUT OF 75

100.0% ACCURACY

COMPLETION: 100.0%

Perform a known plaintext attack on a homophonic cipher.

Luke Leveque
lileve01@louisville.edu

Enumeration & Exploitation Module

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

17 TH PLACE OUT OF 532
EXPERIENCED STUDENTS RANK

210 POINTS OUT OF 300
PERFORMANCE SCORE

100.0% ACCURACY

88.9% COMPLETION

97th Experienced Students Percentile

Average: 162.5 Points

Average: 72.7%

Average: 66.8%

Break-Fast (Easy)

100 POINTS OUT OF 100

100.0% ACCURACY

COMPLETION: **100.0%**

Analyze a Ruby script and bypass its insecure implementation of AES and XOR cryptography.

Trojan (Medium)

100 POINTS OUT OF 100

100.0% ACCURACY

COMPLETION: **100.0%**

Decompile and explore a Powershell file that has been compiled to a Windows executable file.

Industry Guidelines (Hard)

10 POINTS OUT OF 100

100.0% ACCURACY

COMPLETION: **50.0%**

Find a vulnerability in a custom architecture VM and exploit it.

Forensics Module

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

2 ND PLACE OUT OF 532
EXPERIENCED STUDENTS RANK

400 POINTS OUT OF 400
PERFORMANCE SCORE

100.0% ACCURACY

100.0% COMPLETION

100th Experienced Students Percentile

Average: 269.0 Points

Average: 71.9%

Average: 60.2%

Registry (Easy)

100 POINTS OUT OF 100

100.0% ACCURACY

COMPLETION: **100.0%**

Explore a Windows registry file to identify system information.

Jammed (Medium)

200 POINTS OUT OF 200

100.0% ACCURACY

COMPLETION: **100.0%**

Fixed a corrupted header in a zip file to extract lost information.

Dump (Hard)

100 POINTS OUT OF 100

100.0% ACCURACY

COMPLETION: **100.0%**

Explore a memory dump using analysis tools like Volatility to extract information from running programs.

Luke Leveque
lileve01@louisville.edu

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.

10 TH PLACE OUT OF 532
EXPERIENCED STUDENTS RANK

350 POINTS OUT OF 350
PERFORMANCE SCORE

99th Experienced Students Percentile

Average: 308.5 Points

95.0% ACCURACY

Average: 71.0%

100.0% COMPLETION

Average: 89.0%

Web (Easy)

110 POINTS OUT OF 110

100.0% ACCURACY

COMPLETION: 100.0%

Analyze an access log from a WordPress site to identify trends.

Activity (Medium)

120 POINTS OUT OF 120

100.0% ACCURACY

COMPLETION: 100.0%

Analyze a log of JSON data and identify trends of device activity on a network.

Monitor (Hard)

120 POINTS OUT OF 120

85.7% ACCURACY

COMPLETION: 100.0%

Analyze a Sysmon log to calculate statistics and network trends.

Network Traffic Analysis Module

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

6 TH PLACE OUT OF 532
EXPERIENCED STUDENTS RANK

300 POINTS OUT OF 300
PERFORMANCE SCORE

99th Experienced Students Percentile

Average: 232.7 Points

100.0% ACCURACY

Average: 77.4%

100.0% COMPLETION

Average: 88.6%

Stream'n (Easy)

100 POINTS OUT OF 100

100.0% ACCURACY

COMPLETION: 100.0%

Extract a transmitted file from a packet capture.

Net (Medium)

100 POINTS OUT OF 100

100.0% ACCURACY

COMPLETION: 100.0%

Analyze a packet capture to inspect the behavior of a load balancer.

Testing (Hard)

100 POINTS OUT OF 100

100.0% ACCURACY

COMPLETION: 100.0%

Extract data that was exfiltrated from a network using the reserved bits of a TCP header.

Luke Leveque
lileve01@louisville.edu

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.

47 TH PLACE OUT OF 532
EXPERIENCED STUDENTS RANK

390 POINTS OUT OF 390
PERFORMANCE SCORE

95.5% ACCURACY

100.0% COMPLETION

92nd Experienced Students Percentile

Average: 329.1 Points

Average: 82.9%

Average: 91.5%

Rules of Conduct (Easy)

25 POINTS OUT OF 25

100.0% ACCURACY

COMPLETION: 100.0%

Introductory challenge on acceptable conduct during NCL.

Van Life (Easy)

125 POINTS OUT OF 125

100.0% ACCURACY

COMPLETION: 100.0%

Apply OSINT techniques to identify and track the locations of vehicles using VINs.

Airport (Medium)

70 POINTS OUT OF 70

100.0% ACCURACY

COMPLETION: 100.0%

Determine the geolocation of an image solely by analyzing visual clues, without relying on metadata.

Nostalgia (Medium)

70 POINTS OUT OF 70

75.0% ACCURACY

COMPLETION: 100.0%

Conduct reconnaissance on a website by performing a WHOIS lookup.

Insider Threat (Hard)

100 POINTS OUT OF 100

100.0% ACCURACY

COMPLETION: 100.0%

Conduct a reverse image search to find sources or profiles that match an AI-generated person.

Luke Leveque
lileve01@louisville.edu

Password Cracking Module

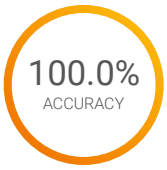
Identify types of password hashes and apply various techniques to efficiently determine plaintext passwords.

17 TH PLACE OUT OF 532
EXPERIENCED STUDENTS RANK

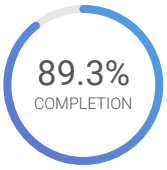
280 POINTS OUT OF 340
PERFORMANCE SCORE

97th Experienced Students Percentile

Average: 155.7 Points



Average: 89.8%



Average: 53.6%

Hashing (Easy)

15 POINTS OUT OF 15

100.0% ACCURACY

COMPLETION: 100.0%

Generate password hashes for MD4, Whirlpool, and SHA512.

Common Passwords (Easy)

30 POINTS OUT OF 30

100.0% ACCURACY

COMPLETION: 100.0%

Crack MD5 password hashes for common passwords .

Windows (Easy)

30 POINTS OUT OF 30

100.0% ACCURACY

COMPLETION: 100.0%

Crack Windows NTLM password hashes that may not be found in common rainbow tables.

Combination (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.

PDF (Medium)

50 POINTS OUT OF 50

100.0% ACCURACY

COMPLETION: 100.0%

Crack the insecure password for a protected PDF file.

Wordlist (Hard)

50 POINTS OUT OF 65

100.0% ACCURACY

COMPLETION: 83.3%

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

Prog Rock (Hard)

60 POINTS OUT OF 105

100.0% ACCURACY

COMPLETION: 75.0%

Create a custom wordlist to crack passwords by creating permutations based on password complexity requirements.

Luke Leveque
lileve01@louisville.edu

Scanning & Reconnaissance Module

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

24 TH PLACE OUT OF 532
EXPERIENCED STUDENTS RANK

310 POINTS OUT OF 310
PERFORMANCE SCORE

90.9% ACCURACY

100.0% COMPLETION

96th Experienced Students Percentile

Average: 235.7 Points

Average: 63.0%

Average: 82.8%

Storytime (Easy)

100 POINTS OUT OF 100

100.0% ACCURACY

COMPLETION: 100.0%

Perform a scan on an FTP server and access shared files.

Vuln Recon (Medium)

110 POINTS OUT OF 110

100.0% ACCURACY

COMPLETION: 100.0%

Scan a system and identify vulnerable services and their associated CVEs.

Feed (Hard)

100 POINTS OUT OF 100

75.0% ACCURACY

COMPLETION: 100.0%

Perform a remote scan of an insecurely configured MQTT server and access its sensitive information.

Web Application Exploitation Module

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

13 TH PLACE OUT OF 532
EXPERIENCED STUDENTS RANK

200 POINTS OUT OF 300
PERFORMANCE SCORE

100.0% ACCURACY

66.7% COMPLETION

98th Experienced Students Percentile

Average: 136.6 Points

Average: 91.8%

Average: 45.5%

Service Up (Easy)

100 POINTS OUT OF 100

100.0% ACCURACY

COMPLETION: 100.0%

Bypass user-agent filtering in a web application to leek sensitive information.

Flag Dispenser (Medium)

100 POINTS OUT OF 100

100.0% ACCURACY

COMPLETION: 100.0%

Exploit a flaw with a custom session checksum.

Book (Hard)

0 POINTS OUT OF 100

0.0% ACCURACY

COMPLETION: 0.0%

Perform an XML injection attack and bypass input sanitization on a web application.