NCL Fall 2023 Team Game Scouting Report

Dear Ethan Brinks (Team "MTU Team 2"),

Thank you for participating in the National Cyber League (NCL) 2023 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 2023 Fall Season had 9,770 students/players and 591 faculty/coaches from more than 510 two- and four-year schools & 270 high schools across all 50 U.S. states registered to play. The Individual Game Capture the Flag (CTF) event took place from October 20 through October 22. The Team Game CTF event took place from November 3 through November 5. 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/74PXGK2HB8HA

Congratulations for your participation in the NCL 2023 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!

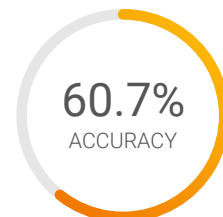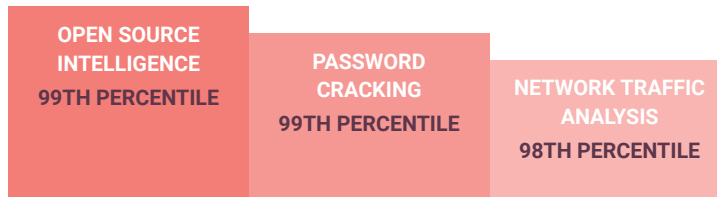Dr. David Zeichick
NCL Commissioner

NATIONAL CYBER LEAGUE SCORE CARD

NCL 2023 FALL TEAM GAME

YOUR TOP CATEGORIES

NATIONAL RANK
158TH PLACE OUT OF 4672

PERCENTILE
97TH

OPEN SOURCE INTELLIGENCE
99TH PERCENTILE

PASSWORD CRACKING
99TH PERCENTILE

NETWORK TRAFFIC ANALYSIS
98TH PERCENTILE

60.7%
ACCURACY

Average: 50.1%

cyberskyline.com/report
ID: 74PXGK2HB8HA

Learn more at nationalcyberleague.org | Get in touch with us via info@nationalcyberleague.org

POWERED BY
CYBER SKYLINE

The National Cyber League
A Community Where Cybersecurity Is a Passion

Ethan Brinks
erbrinks@mtu.edu

NCL Fall 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.

158 TH PLACE
OUT OF **4672**
NATIONAL RANK

97th National Percentile

1290 POINTS
OUT OF 3000
PERFORMANCE SCORE
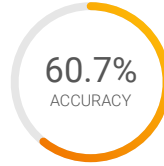
Average: 683.9 Points

60.7% ACCURACY

Average: 50.1%

58.2% COMPLETION

Average: 31.7%

Cryptography

140 POINTS OUT OF 335   **47.1%** ACCURACY   COMPLETION: **72.7%**

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

Enumeration & Exploitation

100 POINTS OUT OF 300   **100.0%** ACCURACY   COMPLETION: **33.3%**

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

Forensics

25 POINTS OUT OF 300   **66.7%** ACCURACY   COMPLETION: **16.7%**

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

Log Analysis

140 POINTS OUT OF 300   **50.0%** ACCURACY   COMPLETION: **72.2%**

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

240 POINTS OUT OF 360   **59.3%** ACCURACY   COMPLETION: **80.0%**

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

Open Source Intelligence

345 POINTS OUT OF 345   **59.5%** 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

100 POINTS OUT OF 360   **100.0%** ACCURACY   COMPLETION: **35.3%**

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

Scanning & Reconnaissance

90 POINTS OUT OF 300   **66.7%** ACCURACY   COMPLETION: **47.1%**

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

Web Application Exploitation

10 POINTS OUT OF 300   **33.3%** ACCURACY   COMPLETION: **20.0%**

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

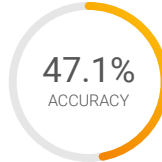Note: Survey module (100 points) was excluded from this report.

POWERED BY
CYBER SKYLINE

The National Cyber League
A Community Where Cybersecurity Is a Passion

Ethan Brinks
erbrinks@mtu.edu

Cryptography Module

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

257 TH PLACE OUT OF **4672**
NATIONAL RANK

95th National Percentile

140 POINTS OUT OF 335
PERFORMANCE SCORE

Average: 115.0 Points

47.1% ACCURACY

Average: 59.3%

72.7% COMPLETION

Average: 54.0%

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

Salad (Easy)
30 POINTS OUT OF 30 | **100.0%** ACCURACY | COMPLETION: 100.0%

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

Beep Beep (Easy)
30 POINTS OUT OF 30 | **100.0%** ACCURACY | COMPLETION: 100.0%

Analyze and obtain the plaintext for a message encoded with Morse code

Someone Cooked (Medium)
10 POINTS OUT OF 50 | **12.5%** ACCURACY | COMPLETION: 50.0%

Analyze and obtain the plaintext for a message with multiple layers of encoding

Roots (Medium)
50 POINTS OUT OF 50 | **100.0%** ACCURACY | COMPLETION: 100.0%

Interpret the Logo programming language to extract hidden information

Pretty Good Signature (Hard)
0 POINTS OUT OF 75 | **0.0%** ACCURACY | COMPLETION: 0.0%

Identify fraudulent emails through the use of PGP signature verification

Boomers (Hard)
20 POINTS OUT OF 100 | **50.0%** ACCURACY | COMPLETION: 50.0%

Decipher the plaintext for a message encrypted with a Sudoku cipher

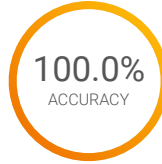POWERED BY
CYBER SKYLINE

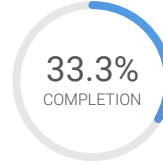## Enumeration & Exploitation Module

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

266 TH PLACE OUT OF **4672**
NATIONAL RANK

95th National Percentile

100 POINTS OUT OF 300
PERFORMANCE SCORE

Average: 58.8 Points

100.0% ACCURACY

Average: 54.4%

33.3% COMPLETION

Average: 33.2%

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

Espionage (Easy)

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

Be able to read and decipher OCaml Code and recognize bitwise operations

Bytecode (Medium)

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

Decompile and analyze the bytecode for Ruby to reverse engineer the authentication scheme

Journal (Hard)

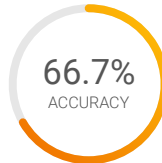**0** POINTS OUT OF 100 — **0.0%** ACCURACY — COMPLETION: **0.0%**

Reverse engineer a compiled binary and exploit a TOCTOU (Time-of-Check Time-of-Use) vulnerability to escalate user privileges
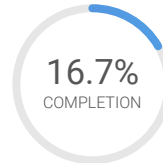
Forensics Module

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

237 TH PLACE OUT OF **4672**
NATIONAL RANK

95th National Percentile

25 POINTS OUT OF 300
PERFORMANCE SCORE

Average: 63.0 Points

66.7% ACCURACY

Average: 46.0%

16.7% COMPLETION

Average: 26.8%

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

Seek (Easy)

10 POINTS OUT OF 100 — **50.0%** ACCURACY — COMPLETION: **33.3%**

Identify tampered files on an NTFS file system through forensic analysis of the Master File Table

Art (Medium)

15 POINTS OUT OF 100 — **100.0%** ACCURACY — COMPLETION: **33.3%**

Reconstruct a file from a binary data stream by following the specification for a custom file format

The Book (Hard)

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

Analyze and search through a live Windows memory dump to extract the SQL database from memory

POWERED BY
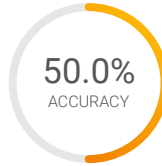CYBER SKYLINE

POWERED BY CYBER SKYLINE

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.

241 ST PLACE OUT OF **4672**
NATIONAL RANK

95th National Percentile

140 POINTS OUT OF 300
PERFORMANCE SCORE

Average: 111.8 Points

50.0% ACCURACY

Average: 42.2%

72.2% COMPLETION

Average: 49.7%

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

Wardriving (Easy)
100 POINTS OUT OF 100 | **40.9%** ACCURACY | COMPLETION: **100.0%**

Parse a wardriving log to identify WiFi and Bluetooth network beacons

Mobile (Medium)
10 POINTS OUT OF 100 | **100.0%** ACCURACY | COMPLETION: **20.0%**

Dissect an Android log to identify historic user activity on the device

Za (Hard)
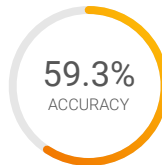**30** POINTS OUT OF 100 | **100.0%** ACCURACY | COMPLETION: **75.0%**

Analyze a Windows Sysmon log to identify the file that was covertly exfiltrated via DNS query packets
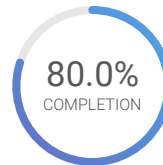
Network Traffic Analysis Module

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

128 TH PLACE OUT OF **4672**
NATIONAL RANK

98th National Percentile

240 POINTS OUT OF 360
PERFORMANCE SCORE

Average: 143.9 Points

59.3% ACCURACY

Average: 37.5%

80.0% COMPLETION

Average: 48.4%

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

Next Gen (Easy)
90 POINTS OUT OF 90 | **71.4%** ACCURACY | COMPLETION: **100.0%**

Analyze and identify the layout of an IPv6 network

The Webz (Medium)
100 POINTS OUT OF 100 | **75.0%** ACCURACY | COMPLETION: **100.0%**

Analyze Border Gateway Protocol (BGP) traffic to identify automatic route discovery mechanisms

Router (Medium)
30 POINTS OUT OF 70 | **50.0%** ACCURACY | COMPLETION: **50.0%**

Decrypt a WiFi packet capture and extract the contents of the network traffic

Looking Glass (Hard)
20 POINTS OUT OF 100 | **33.3%** ACCURACY | COMPLETION: **66.7%**

Analyze and extract raw H.264 video from a wireless Android screen recording

POWERED BY CYBER SKYLINE

The National Cyber League
A Community Where Cybersecurity Is a Passion

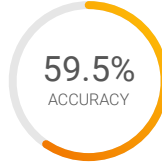Ethan Brinks
erbrinks@mtu.edu

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.

71 ST PLACE
OUT OF **4672**
NATIONAL RANK

99th National Percentile

345 POINTS OUT OF 345
PERFORMANCE SCORE

Average: 189.1 Points

59.5% ACCURACY

Average: 53.2%

100.0% COMPLETION

Average: 76.4%

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

Park (Easy)

45 POINTS OUT OF 45

50.0% ACCURACY

COMPLETION: **100.0%**

Extract EXIF metadata from a JPEG file to determine geolocation

X Marks the Spot (Easy)

60 POINTS OUT OF 60

53.8% ACCURACY

COMPLETION: **100.0%**

Identify characteristics of the 2020 Twitter hack from government reports

Reputation (Medium)

40 POINTS OUT OF 40

50.0% ACCURACY

COMPLETION: **100.0%**

Reverse lookup IP addresses to identify the name of the VPN service providers

Airport (Medium)

75 POINTS OUT OF 75

100.0% ACCURACY

COMPLETION: **100.0%**

Identify the geolocation of an image without the EXIF metadata

Gotta Go Fast (Hard)

100 POINTS OUT OF 100

40.0% ACCURACY

COMPLETION: **100.0%**

Analyze a series of locations to identify the commonality between them and extrapolate another likely target location
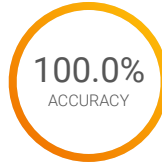
The National Cyber League
A Community Where Cybersecurity Is a Passion

Ethan Brinks
erbrinks@mtu.edu
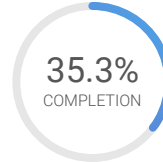
Password Cracking Module

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

74 TH PLACE OUT OF **4672**
NATIONAL RANK

99th National Percentile

100 POINTS OUT OF **360**
PERFORMANCE SCORE

Average: 44.4 Points

100.0%
ACCURACY

Average: 82.2%

35.3%
COMPLETION

Average: 18.2%

Hashing (Easy)

20 POINTS OUT OF **20**

100.0% ACCURACY

COMPLETION: 100.0%

Generate password hashes for MD5, SHA1, SHA256, and SHA512

International (Easy)

20 POINTS OUT OF **30**

100.0% ACCURACY

COMPLETION: 66.7%

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

WPA (Medium)

0 POINTS OUT OF **50**

0.0% ACCURACY

COMPLETION: 0.0%

Research and crack WiFi passwords saved in a wpa_supplicant.conf file

Monsters (Medium)

0 POINTS OUT OF **100**

0.0% ACCURACY

COMPLETION: 0.0%

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

Speakeasy (Medium)

0 POINTS OUT OF **60**

0.0% ACCURACY

COMPLETION: 0.0%

Build a wordlist or pattern rule to crack passwords with leet speak character replacements

Say My Name (Hard)

60 POINTS OUT OF **100**

100.0% ACCURACY

COMPLETION: 60.0%

Build a wordlist to crack passwords not found in common wordlists and augment with rules for special characters
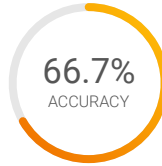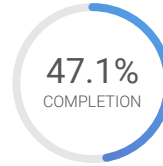
Scanning & Reconnaissance Module

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

174 TH PLACE OUT OF **4672**
NATIONAL RANK

97th National Percentile

90 POINTS OUT OF 300
PERFORMANCE SCORE

Average: 70.3 Points

66.7% ACCURACY

Average: 44.8%

47.1% COMPLETION

Average: 29.9%

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

Knock (Easy)

30 POINTS OUT OF 100 — **33.3%** ACCURACY — COMPLETION: **33.3%**

Run a TCP and UDP scan to identify running services and utilize port knocking to access a hidden service

SSH Server (Medium)

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

Utilize Public Key Infrastructure to generate valid SSH authentication certificates from a Certificate Authority

Academic Papers (Hard)

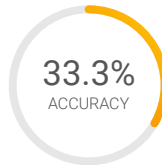**60** POINTS OUT OF 100 — **100.0%** ACCURACY — COMPLETION: **75.0%**

Analyze the history and metadata of a Docker image to identify information stored in the container

Web Application Exploitation Module

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

327 TH PLACE OUT OF **4672**
NATIONAL RANK

94th National Percentile

10 POINTS OUT OF 300
PERFORMANCE SCORE

Average: 32.6 Points

33.3% ACCURACY

Average: 39.8%

20.0% COMPLETION

Average: 26.0%

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

Secure Banking (Easy)

10 POINTS OUT OF 100 — **33.3%** ACCURACY — COMPLETION: **50.0%**

Identify the vulnerability that leaks an API token and utilize it in an account takeover attack

LowLine (Medium)

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

Exploit a known vulnerability in the JavaScript Lodash library (CVE-2021-23337) to extract sensitive server side data

Toms Fan Club v2 (Hard)

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

Analyze and conduct an assessment on a web application that uses a custom HTTP upgrade procedure