Dear Student Player,

Congratulations on a great NCL Individual Game!

National Cyber League (NCL)

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. The NCL is a next-generation learning and gaming environment using high-fidelity and scenario-based challenges from Cyber Skyline. The challenges are designed around industry recognized and performance-based exam objectives to further develop student skills. Learn more about the NCL at www.nationalcyberleague.org. If you have any questions regarding the information in this report please inquire at info@nationalcyberleague.org.

NCL Season

The NCL Season was designed to develop and validate player knowledge and skills in preparation for further learning, career readiness, industry certifications, and other cybersecurity competitions. Hosted challenges in the NCL Gymnasium were made available to all players and coaches and aligned to the games. The games were designed around performance-based exam objectives of the CompTIA Security+™ certification and the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework published by the National Institute of Standards and Technology (NIST).

The NCL Season began with the Preseason round to group players into one of three competition brackets based on skill level: Gold (top 15% of all players nationally - 665 players), Silver (the next 35% of all players nationally - 1540 players) or Bronze (the next 50% of all players nationally - 2193 players). Players who did not participate in the Preseason were not bracketed or ranked. This made the Individual Game more engaging by grouping players with similar knowledge and skill levels.

At the beginning of the NCL Season, 5900 students/players and 415 faculty/coaches from more than 460 two- and four-year schools across all 50 U.S. states registered to play.

The Individual Game Capture the Flag (CTF) event took place from April 3 through April 5. The Team Game CTF event took place from April 17 through April 19. The games were conducted in real-time for students across the country.

The NCL Season was powered by Cyber Skyline's cloud-based skills evaluation platform. Cyber Skyline hosted the scenario-driven cybersecurity challenges for all players to compete and track their progress in real-time.

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

Thank you for your participation in the NCL 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. Dan Manson
NCL Commissioner
NCL Scouting Report

What follows is a customized NCL Scouting Report of your performance in the NCL Individual Game. We hope you find it to be valuable in both confirming your skills and identifying areas for improvement. In addition, the NCL Scouting Report can be used as part of any job application, as it provides an external validation of skills as demonstrated in competitive gameplay based on industry-recognized certification exam and framework objectives.

The following definitions apply to your performance across a range of cybersecurity scenarios:

- **National Rank**: overall place with respect to all players, across all Brackets
- **Bracket Rank**: overall place within the Bracket
- **Performance Score**: total points earned; the higher the score, the higher the ranking
- **Accuracy**: percentage of flag submissions that were correct (total flag captures divided by total flag attempts).
- **Completion**: percentage of possible flags submitted (total flag captures divided by total possible flags).

The following are the categories of cybersecurity scenarios that you were evaluated against:

1. **Cryptography**
   - Identify techniques used to encrypt or obfuscate messages and leverage tools to extract the plaintext.
2. **Enumeration and Exploitation**
   - Identify actionable exploits and vulnerabilities and use them to bypass the security measures in code and compiled binaries.
3. **Log Analysis**
   - Utilize the proper tools and techniques to establish a baseline for normal operation and identify malicious activities using log files from various services.
4. **Network Traffic Analysis**
   - Identify malicious and benign network traffic to demonstrate an understanding of potential security breaches.
5. **Open Source Intelligence**
   - Utilize publicly available information such as search engines, public repositories, social media, and more to gain in-depth knowledge on a topic or target.
6. **Password Cracking**
   - Identify types of password hashes and apply various techniques to efficiently determine plaintext passwords.
7. **Scanning**
   - Identify and use the proper tools to gain intelligence about a target including its services and potential vulnerabilities.
8. **Web Application Exploitation**
   - Identify actionable exploits and vulnerabilities and use them to bypass the security measures in online services.
9. **Wireless Access Exploitation**
   - Identify the security posture of wireless networks from network captures.

NCL Preseason

2ND PLACE
OUT OF 5379
NATIONAL RANK

1760 POINTS OUT OF 1760
PERFORMANCE SCORE

96.1% ACCURACY

100.0% COMPLETION

Based on Preseason performance, **Student Player** was placed into the **Gold Bracket** for the Individual Game.
The National Cyber League
Where Cybersecurity is a Passion

Student Player
student@nationalcyberleague.org

NCL 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.

<table>
<thead>
<tr>
<th>Category</th>
<th>Points</th>
<th>Accuracy</th>
<th>Completion</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cryptography</td>
<td>390</td>
<td>100.0%</td>
<td>100.0%</td>
</tr>
<tr>
<td>Enumeration and Exploitation</td>
<td>350</td>
<td>92.3%</td>
<td>100.0%</td>
</tr>
<tr>
<td>Log Analysis</td>
<td>400</td>
<td>100.0%</td>
<td>100.0%</td>
</tr>
<tr>
<td>Network Traffic Analysis</td>
<td>350</td>
<td>95.8%</td>
<td>100.0%</td>
</tr>
<tr>
<td>Open Source Intelligence</td>
<td>260</td>
<td>95.5%</td>
<td>100.0%</td>
</tr>
<tr>
<td>Password Cracking</td>
<td>255</td>
<td>100.0%</td>
<td>89.5%</td>
</tr>
<tr>
<td>Scanning</td>
<td>200</td>
<td>90.9%</td>
<td>90.9%</td>
</tr>
<tr>
<td>Web Application Exploitation</td>
<td>350</td>
<td>100.0%</td>
<td>100.0%</td>
</tr>
<tr>
<td>Wireless Access Exploitation</td>
<td>155</td>
<td>80.0%</td>
<td>92.3%</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Task</th>
<th>Points</th>
<th>Accuracy</th>
<th>Completion</th>
</tr>
</thead>
<tbody>
<tr>
<td>Decoding 1 (Easy)</td>
<td>30</td>
<td>100.0%</td>
<td>100.0%</td>
</tr>
<tr>
<td>Decoding 2 (Easy)</td>
<td>25</td>
<td>100.0%</td>
<td>100.0%</td>
</tr>
<tr>
<td>Decoding 3 (Easy)</td>
<td>25</td>
<td>100.0%</td>
<td>100.0%</td>
</tr>
<tr>
<td>Decoding 4 (Medium)</td>
<td>30</td>
<td>100.0%</td>
<td>100.0%</td>
</tr>
<tr>
<td>Decoding 5 (Hard)</td>
<td>50</td>
<td>100.0%</td>
<td>100.0%</td>
</tr>
<tr>
<td>Decoding 6 (Hard)</td>
<td>80</td>
<td>100.0%</td>
<td>100.0%</td>
</tr>
<tr>
<td>Steg (Easy)</td>
<td>45</td>
<td>100.0%</td>
<td>100.0%</td>
</tr>
<tr>
<td>Image (Medium)</td>
<td>50</td>
<td>100.0%</td>
<td>100.0%</td>
</tr>
<tr>
<td>Docx (Hard)</td>
<td>55</td>
<td>100.0%</td>
<td>100.0%</td>
</tr>
</tbody>
</table>

The National Cyber League
Where Cybersecurity is a Passion

Student Player
student@nationalcyberleague.org

Learn more at nationalcyberleague.org | Verify this report at cyberskyline.com/report/SAMPLE
Enumeration and Exploitation Module

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

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.
Network Traffic Analysis Module
Identify malicious and benign network traffic to demonstrate an understanding of potential security breaches.

ARP (Easy)  
Points: 60  
Accuracy: 100.0%  
Completion: 100.0%

TFTP (Easy)  
Points: 95  
Accuracy: 100.0%  
Completion: 100.0%

DHCP (Medium)  
Points: 95  
Accuracy: 87.5%  
Completion: 100.0%

CAN Bus (Hard)  
Points: 100  
Accuracy: 100.0%  
Completion: 100.0%

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.

Rules of Conduct (Easy)  
Points: 15  
Accuracy: 100.0%  
Completion: 100.0%

WHOIS (Easy)  
Points: 50  
Accuracy: 100.0%  
Completion: 100.0%

Tax Purposes (Easy)  
Points: 60  
Accuracy: 100.0%  
Completion: 100.0%

Caucus Report (Medium)  
Points: 85  
Accuracy: 87.5%  
Completion: 100.0%

Geolocation (Hard)  
Points: 50  
Accuracy: 100.0%  
Completion: 100.0%
Password Cracking Module

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

<table>
<thead>
<tr>
<th>Task</th>
<th>Points</th>
<th>Accuracy</th>
<th>Completion</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hashing (Easy)</td>
<td>30</td>
<td>100.0%</td>
<td>100.0%</td>
</tr>
<tr>
<td>Cracking 1 (Easy)</td>
<td>45</td>
<td>100.0%</td>
<td>100.0%</td>
</tr>
<tr>
<td>Cracking 2 (Easy)</td>
<td>45</td>
<td>100.0%</td>
<td>100.0%</td>
</tr>
<tr>
<td>Cracking 3 (Medium)</td>
<td>60</td>
<td>100.0%</td>
<td>100.0%</td>
</tr>
<tr>
<td>Cracking 4 (Hard)</td>
<td>35</td>
<td>100.0%</td>
<td>60.0%</td>
</tr>
<tr>
<td>Zip (Medium)</td>
<td>40</td>
<td>100.0%</td>
<td>100.0%</td>
</tr>
</tbody>
</table>

Scanning Module

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

<table>
<thead>
<tr>
<th>Task</th>
<th>Points</th>
<th>Accuracy</th>
<th>Completion</th>
</tr>
</thead>
<tbody>
<tr>
<td>Git (Easy)</td>
<td>75</td>
<td>100.0%</td>
<td>100.0%</td>
</tr>
<tr>
<td>Worksmart (Medium)</td>
<td>25</td>
<td>100.0%</td>
<td>66.7%</td>
</tr>
<tr>
<td>Who's There? (Hard)</td>
<td>100</td>
<td>50.0%</td>
<td>100.0%</td>
</tr>
</tbody>
</table>
Web Application Exploitation Module

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

<table>
<thead>
<tr>
<th>Module</th>
<th>Points out of</th>
<th>Accuracy</th>
<th>Completion</th>
</tr>
</thead>
<tbody>
<tr>
<td>Election Hacking (Easy)</td>
<td>105</td>
<td>100.0%</td>
<td>100.0%</td>
</tr>
<tr>
<td>MetroGov (Medium)</td>
<td>115</td>
<td>100.0%</td>
<td>100.0%</td>
</tr>
<tr>
<td>GregsList (Hard)</td>
<td>130</td>
<td>100.0%</td>
<td>100.0%</td>
</tr>
</tbody>
</table>

Wireless Access Exploitation Module

Identify the security posture of wireless networks from network captures.

<table>
<thead>
<tr>
<th>Module</th>
<th>Points out of</th>
<th>Accuracy</th>
<th>Completion</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cracking 1 (Easy)</td>
<td>70</td>
<td>62.5%</td>
<td>100.0%</td>
</tr>
<tr>
<td>Cracking 2 (Medium)</td>
<td>60</td>
<td>100.0%</td>
<td>100.0%</td>
</tr>
<tr>
<td>Cracking 3 (Hard)</td>
<td>25</td>
<td>100.0%</td>
<td>75.0%</td>
</tr>
</tbody>
</table>