We All Soar Together

Secrets to winning cyber competitions

Matt Boehnke

Cyber Security
Assistant Professor, Cyber Security

Email: mboehnke@columbiabasin.edu
Office hours: Zoom online

CBC
Columbia Basin College

CBC CySER

- CyberHawks
- Competitions
- National Cyber League
- Community Outreach/ Internships
- Questions?

Cyber Security Program

- Started 2014
- Degree Pathways
  - Short Term or 1 year Certifications
  - 2 year AAS;
  - BAS in Cyber Security
  - *Added BAS in Information Technology (2020)
  - Working on: data analytics/ cloud services
- Graduates: 4 - 2015, 28 - 2017 (600% increase)
- Over 85% job placement; average salary: $65,000

CERTIFIED AS A NATIONAL CENTER OF ACADEMIC EXCELLENCE (CAE2Y)

Designation is certified by the National Security Agency (NSA) and the U.S. Department of Homeland Security due to the college's proof of commitment to excellence in the field of Information Assurance and Cyber Defense Education.

Columbia Basin College

Cyber Security Division

CYBERHAWKS

"Vigilance, quick thinking pays off for CBC cybersecurity students"

TCH, April 15, 2016

Cyber Competitions

- Started years ago
- Computer security challenges are available for every level of expertise
- Many are hosted through colleges and government agencies and supported/sponsored by industry leading organizations.
- As part of a team or as a single person or the competition places you in a team.

Cyber Competitions

- The exercises involved in the competition allow you to test your current knowledge and learn new skills in realistic situations.
- Very advanced and competitive challenges often offer high-value prizes
- Help competitors develop and advance their skill set to a higher degree than standard education alone.

Competition

- Pre Event
- Before start – Last minute prep
- Competition Days
- Post Event Analysis
- Curriculum Integration

"Don't Forget the Basic 13"

Dwayne Williams, National CCDC Director, CCDC post

Competition – Pre Event

"Don't Forget the Basic 13"

Dwayne Williams, National CCDC Director, CCDC post

- Yearly Schedule
- Build off other competitions
- Rehearse Historical data
- Integration with Advisory Groups
- Mentoring and Developing leads

Competition – Before Start

- Planning, Planning, Planning
- Rules of Engagement
- Rehearse Daily events (Injects)
- Walkthrough contingency plans

"Don't Forget the Basic 13"

Dwayne Williams, National CCDC Director, CCDC post

National Cyber League

NCL Vision

- To prepare the next generation of cybersecurity professionals.

NCL Mission

- Prepare the next generation of cybersecurity professionals by providing high school and college students, as well as their coaches, an online, safe platform of real-world cybersecurity challenges.
- Virtual training ground features a competitive process and a supportive community, helping students develop, improve and validate their cybersecurity skills.
- Students' progress and strengths are validated through their individual Scouting Reports and team rankings, enabling HR teams and recruiters to easily determine the students' fit for open positions.

NCL - Background

- In 2011, a group of cybersecurity-focused academics from several public agencies
- Important to reduce barriers and excite young people to participate. Students would have easy access, no matter what their age, skill level or location.
- One of the earliest e-Sports
- Simulate real-life cyberthreats in a safe environment
- Growing population - more than 13,000 students of all ages, representing over 650 colleges and high schools across the U.S. - participates each year in the biannual competition.

NCL - Background

- Run by Cyber Skyline, Inc., collaborating with the National Cyber League, Inc., a 501(c)3 non-profit founded in May 2011. The founding members of NCL are:
  - Cyber Security Privacy and Research Institute (CSPRI) - George Washington University
  - Center for Systems Security and Information Assurance (CSSIA)
  - CyberWatch West (Now NCYTE Center)
  - Mid-Pacific Information and Communication Technologies (MPICT) Center
  - National CyberWatch Center

NCL – Why It Works

- FOR STUDENTS
- FOR FACULTY AND COACHES
- FOR EMPLOYERS
- FOR THE COUNTRY

NCL – How It Works

Beginner

- Open Source Intelligence
- Log Analysis
- Cryptography

Intermediate

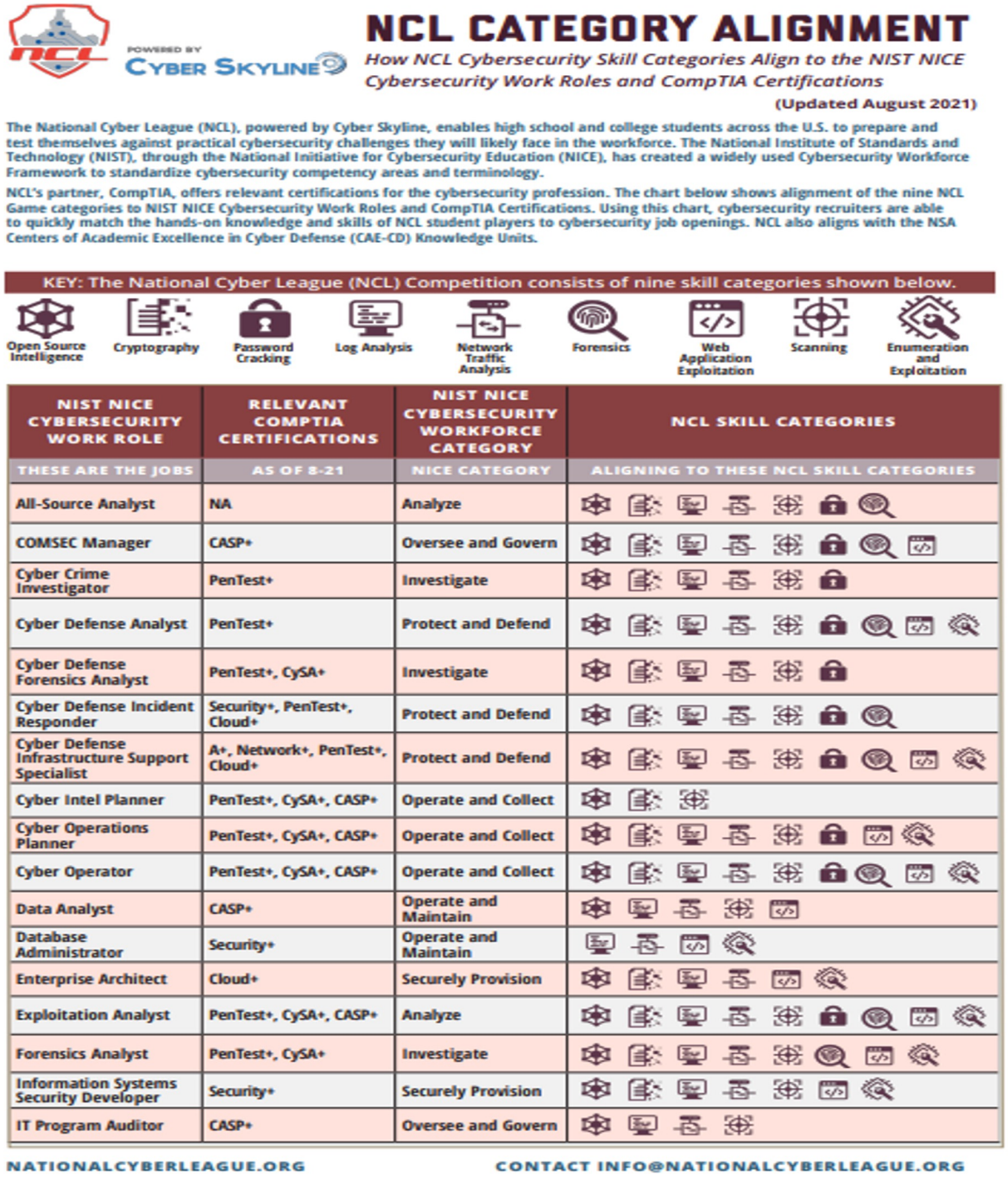
- Password Cracking
- Network Traffic Analysis
- Web Application Exploitation
- Scanning

Advanced

- Enumeration & Exploitation
- Forensics

- Soft Skills/ Social Engineering
- Lessons Learned

Competition



POWERED BY CYBER SKYLINE

NCL CATEGORY ALIGNMENT

How NCL Cybersecurity Skill Categories Align to the NIST NICE Cybersecurity Work Roles and CompTIA Certifications

(Updated August 2021)

The National Cyber League (NCL), powered by Cyber Skyline, enables high school and college students across the U.S. to prepare and test themselves against practical cybersecurity challenges they will likely face in the workforce. The National Institute of Standards and Technology (NIST), through the National Initiative for Cybersecurity Education (NICE), has created a widely used Cybersecurity Workforce Framework to standardize cybersecurity competency areas and terminology.

NCL's partner, CompTIA, offers relevant certifications for the cybersecurity profession. The chart below shows alignment of the nine NCL Game categories to NIST NICE Cybersecurity Work Roles and CompTIA Certifications. Using this chart, cybersecurity recruiters are able to quickly match the hands-on knowledge and skills of NCL student players to cybersecurity job openings. NCL also aligns with the NSA Centers of Academic Excellence in Cyber Defense (CAE-CD) Knowledge Units.

KEY: The National Cyber League (NCL) Competition consists of nine skill categories shown below.

Open Source Intelligence · Cryptography · Password Cracking · Log Analysis · Network Traffic Analysis · Forensics · Web Application Exploitation · Scanning · Enumeration and Exploitation

NIST NICE CYBERSECURITY WORK ROLE	RELEVANT COMPTIA CERTIFICATIONS	NIST NICE CYBERSECURITY WORKFORCE CATEGORY	NCL SKILL CATEGORIES
THESE ARE THE JOBS	AS OF 8-21	NICE CATEGORY	ALIGNING TO THESE NCL SKILL CATEGORIES
All-Source Analyst	NA	Analyze	● ● ● ● ● ● ●
COMSEC Manager	CASP+	Oversee and Govern	● ● ● ● ● ● ● ●
Cyber Crime Investigator	PenTest+	Investigate	● ● ● ● ● ●
Cyber Defense Analyst	PenTest+	Protect and Defend	● ● ● ● ● ● ● ● ●
Cyber Defense Forensics Analyst	PenTest+, CySA+	Investigate	● ● ● ● ● ●
Cyber Defense Incident Responder	Security+, PenTest+, Cloud+	Protect and Defend	● ● ● ● ● ● ●
Cyber Defense Infrastructure Support Specialist	A+, Network+, PenTest+, Cloud+	Protect and Defend	● ● ● ● ● ● ● ● ●
Cyber Intel Planner	PenTest+, CySA+, CASP+	Operate and Collect	● ● ●
Cyber Operations Planner	PenTest+, CySA+, CASP+	Operate and Collect	● ● ● ● ● ● ● ●
Cyber Operator	PenTest+, CySA+, CASP+	Operate and Collect	● ● ● ● ● ● ● ● ●
Data Analyst	CASP+	Operate and Maintain	● ● ● ● ●
Database Administrator	Security+	Operate and Maintain	● ● ● ●
Enterprise Architect	Cloud+	Securely Provision	● ● ● ● ● ●
Exploitation Analyst	PenTest+, CySA+, CASP+	Analyze	● ● ● ● ● ● ● ● ●
Forensics Analyst	PenTest+, CySA+	Investigate	● ● ● ● ● ● ● ●
Information Systems Security Developer	Security+	Securely Provision	● ● ● ● ● ● ●
IT Program Auditor	CASP+	Oversee and Govern	● ● ● ●

NATIONALCYBERLEAGUE.ORG

CONTACT INFO@NATIONALCYBERLEAGUE.ORG

Competition

How NCL Skill Categories Align to the NIST NICE Cybersecurity Work Roles and Comp-TIA Certifications (cont.)

KEY: The National Cyber League (NCL) Competition consists of nine skill categories shown below.

Open Source Intelligence | Cryptography | Password Cracking | Log Analysis | Network Traffic Analysis | Forensics | Web Application Exploitation | Scanning | Enumeration and Exploitation

NIST NICE CYBERSECURITY WORK ROLE	RELEVANT COMPTIA CERTIFICATIONS	NIST NICE CYBERSECURITY WORKFORCE CATEGORY	NCL SKILL CATEGORIES
THESE ARE THE JOBS	AS OF 8-21	NICE CATEGORY	ALIGNING TO THESE NCL SKILL CATEGORIES
Language Analyst	NA	Analyze	
Network Operations Specialist	Cloud+, Security+	Operate and Maintain	
Partner Integration Planner	PenTest+, CySA+, CASP+	Operate and Collect	
Privacy Compliance Manager	NA	Oversee and Govern	
Requirements Planner	CASP+	Securely Provision	
Research & Development Specialist	PenTest+	Securely Provision	
Secure Software Assessor	Security+	Securely Provision	
Security Architect	CASP+	Securely Provision	
Security Controls Assessor	Security+, PenTest+, CySA+	Securely Provision	
Software Developer	Security+	Securely Provision	
Systems Administrator	Cloud+	Operate and Maintain	
Systems Developer	Security+	Securely Provision	
Systems Security Analyst	CySA+	Operate and Maintain	
Target Analyst	NA	Analyze	
Target Developer	NA	Analyze	
Technical Support Specialist	PenTest+, CySA+, CASP+	Operate and Maintain	
Testing and Evaluation Specialist	Network+, Security+, PenTest+, CySA+	Securely Provision	
Vulnerability Analyst	PenTest+	Protect and Defend	

Competition – Open Source Intel

- Help the police extract information using publicly available data and tools.
- Challenge yourself during the NCL games to find answers on a topic or target, using search engines, public repositories, social media, and more.
- By gathering publicly available information about a particular target, attackers can profile potential victims to find vulnerabilities.
- Without actively engaging the target, an attacker can use the intelligence to build a threat model and develop a plan of attack.
- Targeted cyber attacks, like military attacks, begin with reconnaissance, and the first stage of digital reconnaissance is passively acquiring intel without alerting the target.

Competition - Log Analysis

- Logs hold a ton of information.
- Using logs to learn what's happened. Analyze the logs to figure out what the hackers have been up to.
- Establish a baseline for normal operation and identify malicious activities through log files from various services.
- Computers, networks and other IT systems generate records call audit trail records or logs that document system activities.
- Process helps businesses comply with security policies, audits or regulations, comprehend system troubleshoots, and understand online user behavior.

Competition - Cryptography

- Information is key
- Learn how to identify techniques used to encrypt or obfuscate messages
- Leverage tools to extract the plain text.
- Magic Bytes point the way

Competition – Password Cracking

- Passwords are the keys to our digital lives.
- Consumers, companies, governments and institutions routinely get hacked through various means, and user authentication databases get leaked or breached.
- Identify types of password hashes and apply various techniques to efficiently determine plain text passwords.
- Having comprehensive password cracking expertise arms cybersecurity workers to improve security.
- They can implement better cyber awareness and password creation practices, while identifying the source of attacks more quickly.

Competition - Network Traffic Analysis

- Determine what happened and exactly when it happened by looking at network traffic capture.
- Use the NCL games to identify malicious and benign network traffic and demonstrate your understanding of potential security breaches.
- NTA the process of intercepting, recording and analyzing network traffic communication patterns in order to detect and respond to security threats.
- It’s an effective tool to make extracting data harder for the hackers, and it helps companies detect cyber threats with a higher degree of certainty, so they can eliminate security threats more quickly.

Competition – Web App Exploitation

owasp.org/ OWASP Top 10

1. Injections
2. Broken Authentication
3. Sensitive Data Exposure
4. XML External Entities (XXE)
5. Broken Access Control
6. Security Misconfigurations
7. Cross-Site Scripting (XSS)
8. Insecure Deserialization
9. Using components with known vulnerabilities
10. Insufficient Logging and Monitoring

Competition - Scanning

- Before you catch the hackers, you need to find them.
- Use the NCL games to put your tracking skills to the test and find out what the hackers are up to.
- Practice and apply the proper tools to gain intelligence about a hacker's potential target including its services and potential vulnerabilities.
- All a hacker needs is just one vulnerability to gain a foothold in a network!
- Networks (including any device with an IP address) should be scanned at least monthly to identify and remediate vulnerabilities.
- People running a scan should have a background in networking, knowledge on scanning tools, and understand a wide range of vulnerabilities and ways they can be exploited.
- Careers

Competition - Enumeration & Exploitation

- Hacking isn't just for the bad guys.
- Use the NCL games to break hackers' software and secure your own programs.
- Identify actionable exploits and vulnerabilities
- Use them to bypass the security measures in code and compiled binaries.

Competition - Forensics

- Practicing digital forensics is more important than ever to ensure that data and evidence from a breach is securely preserved, analyzed and processed.
- Challenge yourself to become a digital Sherlock and investigate computer-related crimes and evidence!
- Forensics techniques can uncover important data that was lost or damaged in a breach.
- You'll have the tools to identify critical pieces of evidence for unearthing the adversary or determining exactly what was stolen in an incident.

Competition - soft skills

- Help Desk
- Critical Thinking Skills
- Explain a complicated CS issue, in a professional, respectful way

Competition - Post Event Analysis

- After Action Review
- Documentation
- Every voice matters
- Scouting Reports

CBC Internships

- Pacific Northwest National Labs (PNNL)
- Amazon

- Department of Energy/Ecology
  - Office of River Protection
  - Hanford Laboratory Management & Integration
  - Bechtel National, Inc (BNI)
  - Washington River Protection Solutions LLC (WRPS)
  - DOE Richland Operations Office
  - Hanford Mission Integration Solutions
  - HPM Corporation (HPMC)
  - CH2M Remediation Company
  - Mission Support Alliance (MSA)

- State Agencies
  - Department of Commerce/Port of Benton
  - WA ST Office of Chief Information Officer
  - Energy Northwest (Nuclear/Solar/Wind)

- Regional
  - City of Richland- Solar/ Battery Storage
  - Darklight
  - Marcraft
  - Port of Kennewick (Ransomware 2020)
  - Port of Pasco
  - Port of Benton

Questions

Hands-on Exercise

CBC Columbia Basin College

Thank you

We All Soar Together