

How NCL Skill Categories Align to the NSA Centers of Academic Excellence in Cyber Defense (CAE-CD) Knowledge Units (KUs)

The National Cyber League (NCL), powered by Cyber Skyline, helps colleges achieve their CAE designation through alignment of nine NCL cybersecurity skills categories to outcomes specified in CAE-CD Knowledge Units. NCL also aligns with NIST NICE Cybersecurity Workforce categories and CompTIA Security Certifications. Visit nationalcyberleague.org for details on getting students involved in the NCL Games.

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


























NCL CATEGORY	NSA CAE-CD KNOWLEDGE UNIT	KNOWLEDGE UNITS - OUTCOMES MET
 Open Source Intelligence	Cyber Threats (CTH)	Leverage open source intelligence to identify threats and threat actors, along with the TTPs such as those listed in the MITRE ATT&CK Framework.
 Open Source Intelligence	Cyber Threats (CTH)	Identify the specific TTPs, CVEs, or general software vulnerability used in an attack or malware threat.
 Cryptography	Basic Cryptography (BCY)	Identify cryptographic schemes and use cases.
 Cryptography	Basic Cryptography (BCY)	Identify symmetric vs. asymmetric encryption schemes.
 Cryptography	Basic Cryptography (BCY)	Identify encryption and signing algorithms that are being used.
 Cryptography	Basic Cryptography (BCY)	Identify strengths and weaknesses in certain cryptographic schemes.
 Cryptography	Advanced Cryptography (ACR)	Perform symmetric and asymmetric encryption/decryption.
 Cryptography	Advanced Cryptography (ACR)	Identify cryptographic security controls placed on a system.
 Cryptography	Advanced Cryptography (ACR)	Identify properties of SSL, VPN, data storage, hashing, PKI, etc.
 Log Analysis	Basic Scripting and Programming (BSP)	Use scripting languages to analyze log files.
 Log Analysis	Basic Scripting and Programming (BSP)	Use scripting languages to automate repetitive tasks.
 Log Analysis	Basic Scripting and Programming (BSP)	Write advanced scripts and conditional parsing strategies.
 Log Analysis	Basic Scripting and Programming (BSP)	Use programming languages to parse, interpret, manipulate, and aggregate log data.
 Log Analysis	Fraud Prevention and Management (FPM)	Identify the elements of a fraudulent transaction or network request.
 Log Analysis	Fraud Prevention and Management (FPM)	Leverage existing and custom tools to identify evidence of fraud.
 Network Traffic Analysis	Basic Networking (BNW)	Identify components of the OSI model.
 Network Traffic Analysis	Basic Networking (BNW)	Identify CIDR network and constraints.
 Network Traffic Analysis	Basic Networking (BNW)	Trace network packet captures and data flow.
 Network Traffic Analysis	Basic Networking (BNW)	Dissect network packet captures using tools such as Wireshark and tcpdump.
 Network Traffic Analysis	Basic Networking (BNW)	Perform host discovery and service scanning using tools such as nmap.
 Network Traffic Analysis	Basic Networking (BNW)	Identify network vulnerabilities and misconfigurations based on network data.

How NCL Skill Categories Align to the NSA CAE-CD Knowledge Units (cont.)

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



NCL CATEGORY	NSA CAE-CD KNOWLEDGE UNIT	KNOWLEDGE UNITS - OUTCOMES MET
 Network Traffic Analysis	Network Defense (NDF)	Analyze network traffic to determine network topography and design.
 Network Traffic Analysis	Network Defense (NDF)	Analyze network traffic to determine firewall and IDS/IPS behavior.
 Network Traffic Analysis	Network Defense (NDF)	Interpret network traffic to determine security practices in place.
 Network Traffic Analysis	Network Defense (NDF)	Examine network traffic to identify attacks and threats.
 Network Traffic Analysis	Advanced Network Technology and Protocols (ANT)	Parse and process novel or custom protocols without a native Wireshark dissector.
 Network Traffic Analysis	Advanced Network Technology and Protocols (ANT)	Identify vulnerabilities in novel or custom protocols and attempt to exploit them.
 Network Traffic Analysis	Advanced Network Technology and Protocols (ANT)	Create tools, scripts, or configuration settings to parse and dissect novel or custom protocols.
 Network Traffic Analysis	Intrusion Detection/Prevention Systems (IDS)	Analyze network traffic to identify network intrusion attempts.
 Network Traffic Analysis	Intrusion Detection/Prevention Systems (IDS)	Leverage existing and custom tools to detect malware on the network.
 Network Traffic Analysis	Network Forensics (NWF)	Leverage tools such as Wireshark to conduct packet analysis and dissection.
 Network Traffic Analysis	Network Forensics (NWF)	Perform deep packet inspection (DPI) to identify forensic evidence, malicious traffic, or indicators of compromise.
 Network Traffic Analysis	Network Technology and Protocols (NTP)	Dissect and analyze layer 2 protocols such as Ethernet.
 Network Traffic Analysis	Network Technology and Protocols (NTP)	Dissect IPv4 and IPv6 data to determine source and destination.
 Network Traffic Analysis	Network Technology and Protocols (NTP)	Analyze network traffic to determine network vulnerabilities.
 Network Traffic Analysis	Network Technology and Protocols (NTP)	Identify packet replay attacks and timing attacks in network traffic.
 Network Traffic Analysis	Network Technology and Protocols (NTP)	Leverage tools such as Wireshark, tcpdump, and Network Miner.
 Network Traffic Analysis	Network Technology and Protocols (NTP)	Leverage Aircrack-ng to crack WEP WiFi password.
 Forensics	Device Forensics (DVF)	Identify common mechanisms for device forensics and storage of forensic data.
 Forensics	Digital Forensics (DFS)	Use common digital forensics tools.
 Forensics	Digital Forensics (DFS)	Leverage existing and custom tools to retrieve, analyze, and process forensic data.
 Forensics	Host Forensics (HOF)	Identify data and elements that can be extracted from various computing devices and operating systems.
 Forensics	Host Forensics (HOF)	Leverage existing and common tools to extract forensic data.
 Forensics	Media Forensics (MEF)	Identify or repair corrupted files through hash verification and file recovery mechanisms.

How NCL Skill Categories Align to the NSA CAE-CD Knowledge Units (cont.)

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



NCL CATEGORY	NSA CAE-CD KNOWLEDGE UNIT	KNOWLEDGE UNITS - OUTCOMES MET
 Web Application Exploitation	Databases (DAT)	Identify various different databases being used in a web application.
 Web Application Exploitation	Databases (DAT)	Identify the parts in which a database is powering a web application.
 Web Application Exploitation	Databases (DAT)	Identify and exploit common SQL injection and noSQL injection vulnerabilities.
 Web Application Exploitation	Database Management Systems (DMS)	Identify various different databases being used in a web application.
 Web Application Exploitation	Database Management Systems (DMS)	Identify the role of the database in the web application and any potential vulnerabilities.
 Web Application Exploitation	Database Management Systems (DMS)	Exploit SQL vulnerabilities to inject arbitrary SQL commands into the database.
 Web Application Exploitation	Database Management Systems (DMS)	Identify protections and remediation mechanisms present in the database system.
 Web Application Exploitation	Database Management Systems (DMS)	Identify database models and structures present in the database system.
 Web Application Exploitation	Database Management Systems (DMS)	Design a database to temporarily store information relevant for a proof of concept attack.
 Web Application Exploitation	Web Application Security (WAS)	Intelligently identify web application security flaws by interacting with the web application and exploiting it to gain access to an exfiltrate sensitive information.
 Web Application Exploitation	Web Application Security (WAS)	Identify issues in the development process that may lead to security vulnerabilities and exploit them.
 Web Application Exploitation	Web Application Security (WAS)	Identify secure aspects of the web application to eliminate possible vulnerabilities.
 Scanning & Reconnaissance	Cloud Computing (CCO)	Identify the various services being used from a cloud provider.
 Scanning & Reconnaissance	Cloud Computing (CCO)	Identify vulnerabilities and attack surfaces against a cloud service.
 Scanning & Reconnaissance	IA Architectures (IAA)	Scan vulnerabilities on various architectures and operating systems.
 Scanning & Reconnaissance	IA Architectures (IAA)	Identify secure and insecure elements of a given application.
 Scanning & Reconnaissance	Operating Systems Hardening (OSH)	Scan an operating system for vulnerable or insecure settings, ports, or applications.
 Scanning & Reconnaissance	Operating Systems Hardening (OSH)	Demonstrate a proof of concept exploit to patch a system against scanned vulnerabilities.
 Scanning & Reconnaissance	Operating Systems Theory (OST)	Interface with a machine's file system, IO, interfaces to perform regular functionalities or to exploit a security vulnerability.
 Scanning & Reconnaissance	Vulnerability Analysis (VLA)	Scan for software vulnerabilities using common tools.
 Scanning & Reconnaissance	Vulnerability Analysis (VLA)	Map out all possible attack surfaces against a target system.
 Scanning & Reconnaissance	Vulnerability Analysis (VLA)	Perform vulnerability analysis and root cause analysis to pinpoint specific CVEs.
 Scanning & Reconnaissance	Vulnerability Analysis (VLA)	Identify patches and workarounds available for CVEs.

How NCL Skill Categories Align to the NSA CAE-CD Knowledge Units (cont.)

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











NCL CATEGORY	NSA CAE-CD KNOWLEDGE UNIT	KNOWLEDGE UNITS - OUTCOMES MET
Enumeration & Exploitation	Operating System Concepts (OSC)	Identify how software interacts with the operating system through reverse engineering.
Enumeration & Exploitation	Operating System Concepts (OSC)	Examine software source code and binaries to identify security issues on the target operating system.
Enumeration & Exploitation	Algorithms (ALG)	Create simple scripts to iterate and sort data.
Enumeration & Exploitation	Advanced Algorithms (AAL)	Create advanced and custom scripts to retrieve, process, and interpret big data problems.
Enumeration & Exploitation	Data Structures (DST)	Analyze and interpret common data structures in software source code and binaries.
Enumeration & Exploitation	Data Structures (DST)	Identify potential vulnerabilities, shortcomings, or advantages of a particular data structure.
Enumeration & Exploitation	Data Structures (DST)	Leverage common data structures to exploit or fix a software vulnerability.
Enumeration & Exploitation	Data Structures (DST)	Create data structures to aid in the above tasks.
Enumeration & Exploitation	Industrial Control Systems (ICS)	Identify ICS protocols and applications.
Enumeration & Exploitation	Industrial Control Systems (ICS)	Identify various ICS devices and endpoints.
Enumeration & Exploitation	Industrial Control Systems (ICS)	Identify readable and writable ICS devices.
Enumeration & Exploitation	Industrial Control Systems (ICS)	Scan and identify for ICS vulnerabilities.
Enumeration & Exploitation	Industrial Control Systems (ICS)	Identify various different ICS protocols - e.g., Modbus, BACnet, CAN bus.
Enumeration & Exploitation	Linux System Administration (LSA) & Operating Systems Administration (OSA) & Windows System Administration (WSA)	Demonstrate basic proficiency of Linux command line capabilities such as user management.
Enumeration & Exploitation	LSA, OSA and WSA (see above)	Change user password and password policies.
Enumeration & Exploitation	LSA, OSA and WSA (see above)	View basic Linux system logs.
Enumeration & Exploitation	LSA, OSA and WSA (see above)	Leverage basic Linux tools to access backups.
Enumeration & Exploitation	LSA, OSA and WSA (see above)	Interact with package managers such as apt or yum.
Enumeration & Exploitation	LSA, OSA and WSA (see above)	Audit security logs such as syslog, auth.log, etc.
Enumeration & Exploitation	LSA, OSA and WSA (see above)	Change user password and password policies.
Enumeration & Exploitation	Low Level Programming (LLP)	Reverse engineer compiled C binaries and identify syscalls and interpret assembly instructions.
Enumeration & Exploitation	Low Level Programming (LLP)	Analyze syscalls and assembly instructions to identify security vulnerabilities and advantages.

How NCL Skill Categories Align to the NSA CAE-CD Knowledge Units (cont.)

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



NCL CATEGORY	NSA CAE-CD KNOWLEDGE UNIT	KNOWLEDGE UNITS - OUTCOMES MET
 Enumeration & Exploitation	Secure Programming Practices (SPP)	Review source code to identify specific lines of code where vulnerabilities are introduced.
 Enumeration & Exploitation	Secure Programming Practices (SPP)	Identify specific lines where insecure programming practices or function calls/APIs were used.
 Enumeration & Exploitation	Secure Programming Practices (SPP)	Identify language-specific vulnerabilities such as language specific deserialization mechanisms.
 Enumeration & Exploitation	Secure Programming Practices (SPP)	Audit open source code to identify vulnerabilities in libraries.
 Enumeration & Exploitation	Software Reverse Engineering (SRE)	Decompile software binaries to identify vulnerabilities, malware behavior, or evasive techniques.
 Enumeration & Exploitation	Software Security Analysis (SSA)	Leverage software analysis techniques such as memory analysis, static analysis, or security scanning.
 Enumeration & Exploitation	Software Security Analysis (SSA)	Perform software source code or binary analysis using existing and custom tools such as gdb, IDA, or Ghidra.
 Enumeration & Exploitation	Penetration Testing (PTT)	Intelligently identify application security flaws by interacting with the target system and exploiting it to gain access to and exfiltrate sensitive information.