South Carolina Advanced Cybersecurity Syllabus

High School (165 Contact Hours)

Course Overview and Goals

In this course, students build on their foundational cybersecurity knowledge to explore complex concepts in data protection, secure communications, and threat defense. Through interactive lessons, hands-on coding, and investigative projects, students uncover how data is protected, communications verified, and cyber threats mitigated. They'll take on the roles of cryptographers, forensic analysts, and network architects as they tackle real-world security challenges and engineer creative solutions. With projects like building steganographic tools and crafting security policies, students gain both technical expertise and critical thinking skills for the digital age.

Learning Environment

The course utilizes a blended classroom approach. The content is a mix of web-based and physical activities. Each module of the course is broken down into lessons. Lessons are composed of short video tutorials, interactive learning pages, quizzes, explorations, simulations, and free-response prompts. Each module ends with a comprehensive quiz that assesses students' mastery of that module's material.

Programming Environment

In the programming and database modules, students modify and run programs in the browser using the CodeHS online editor. Students will be able to modify text-based programs in Python and SQL and simulate shell commands.

Prerequisites

This course is an advanced course for high school students. Students should take this course after successfully completing the Fundamentals of Cybersecurity (or equivalent) course.

Technology Requirements

To complete all activities and exercises in this course, students must have access to the 3rd party sites and tools listed here: Advanced Cybersecurity Course Links

More Information

Browse the content of this course at https://codehs.com/course/28176/overview

Course Breakdown

The full standards alignment can be found at https://codehs.com/standards/framework/south_carolina_advanced_cybersecurity/mapping/2225

Module 1: Advanced Cryptography (2 weeks / 10 hours)

In this module, students will deepen their understanding of modern cryptographic systems by exploring advanced concepts like public key encryption, hashing, digital certificates, and password salting. Through lessons, articles, code exercises, and creative assignments, they'll learn how encryption secures data, how

hashing algorithms are constructed and attacked, and how secure communications are verified and maintained online.

Objectives / Topics Covered	• Encryption Algorithms • Public Key Encryption • Hash Functions • Asymmetric Encryption • Digital Certificates

Example Assignments	• **Examining Public Key Cryptography**
	  ○ Students analyze how public key cryptography works and respond to questions about its real-world applications and limitations.
	• **Develop a Simple Hash Function**
	  ○ Students apply modulo arithmetic to design and test a basic hash function from scratch.
	• **Affine Cipher**
	  ○ Students work through an affine cipher to explore trapdoor functions used in asymmetric encryption.
	• **Become a Certificate Authority!**
	  ○ Students simulate the role of a certificate authority to understand how digital certificates are issued and validated in practice.

Module 2: Project: Steganography (1 week / 5 hours)

In this module, students will explore how steganography allows messages to be hidden in plain sight, often within images, text, or other media. Students will learn real-world applications of this practice, analyze encryption methods, and create their own image-based steganography projects. The module culminates in peer-to-peer decoding and reflection activities.

Objectives / Topics Covered	• Steganography • Data Hiding and Extraction • Encryption Algorithms • Peer Collaboration

Example Assignments	• **Encryption Algorithm Design**
	  ○ Students design an original steganography-based algorithm that hides text inside an image.
	• **Image Creation**
	  ○ Students implement their algorithm to produce an encoded image file.
	• **Partner Decode**
	  ○ Students exchange encoded images with a classmate and attempt to decode each other's hidden messages using only the partner's algorithm description.

Module 3: Networking Infrastructure (3 weeks / 15 hours)

In this module, students explore the foundational elements that make up digital communication systems, guiding students through the history, components, and security of computer networks. Students analyze network models, services, and tools, and simulate both theoretical and practical aspects of network design and security.

Objectives / Topics Covered	• Internet Evolution & Network Growth • Network Models & Architectures • Networking Services & Protocols • Network Security & Design • Cloud Computing & Virtualization

Example Assignments	• **Create a Subnet Network**
	  ○ Students design a subnet for a given organizational scenario, applying subnetting rules to assign valid IP address ranges.
	• **Wireshark Response**
	  ○ Students analyze captured network packets to identify traffic patterns and describe potential security concerns.
	• **Should ShopFast Move to the Cloud?**
	  ○ Students evaluate a business case for cloud migration and write a recommendation supported by evidence.
	• **Design and Defend a Town Network**
	  ○ Students design a complete network infrastructure for a town, justifying their topology and security choices.

Module 4: Advanced Networking (2 weeks / 10 hours)

In this module, students will explore and research network infrastructures and network security. They will demonstrate how to set up a virtual private network (VPN) and design and configure different types of networks. Students will also explain firewalls and how to initiate port scans.

Objectives / Topics Covered	• Advanced Devices • Environmental Controls • Protocols and Standards • Private Networks • Mobile Devices • Access Control

Example Assignments	• **Coffee Shop: Design an Intranet**
	  ○ Students design an intranet architecture for a small business, selecting appropriate network components and services.
	• **Biometric Data Debate**
	  ○ Students analyze the privacy and security trade-offs of biometric authentication and defend a position.
	• **Mobile Security Consultant**
	  ○ Students develop mobile device security recommendations for an organization adopting a BYOD policy.
	• **Applied AAA Security Framework**
	  ○ Students apply the authentication, authorization, and accounting framework to a realistic network access scenario.

Module 5: Project: The Inside Scoop on LANs (2 weeks / 10 hours)

In this project, students will create a "magazine" that explains key concepts about Local Area Networks (LANs), topologies, Ethernet standards, and LAN cabling. Students will research and present the information in a magazine-style layout with sections, images, and creative design.

Topics Covered	• LAN Methodologies • Network Topologies • Perimeter Networks (DMZ) • Ethernet Standards • LAN Cabling
Example Assignments	• **Magazine Submission** ○ Students compile all sections of their LAN magazine into a complete publication covering infrastructure design, topology comparisons, and security considerations.

Module 6: Threats and Security Principles (2-3 weeks / 10-15 hours)

In this module, students will explore foundational security concepts and apply them through real-world scenarios and simulations. They will learn to distinguish between threats, vulnerabilities, and exploits; investigate actual data breaches; evaluate ethical concerns; and examine how protocols and baseline security measures defend against attacks.

Objectives / Topics Covered	• Threats, Vulnerabilities & Exploits • Cyber Case Investigation • Security Breaches & Ethics • Security Baselines & Policies • Network Defenses & Protocols • Internet of Things (IoT) & Embedded Systems Security • Adversary Types & Social Engineering Psychology

Example Assignments	• **Attack Scenario Analysis**
	  ○ Students analyze a cyberattack scenario to identify the adversary type, attack methods used, and potential defensive countermeasures.
	• **Research: High Profile Breach**
	  ○ Students research a major real-world security breach and present findings on its causes, impact, and lessons learned.
	• **Mission: Network Defender**
	  ○ Students complete an interactive defense challenge, protecting a simulated network from a series of incoming attacks.
	• **Lab: Anti-virus Software Installation**
	  ○ Students install and configure anti-virus software in a simulated environment and document the process and results.

Module 7: Databases (2 weeks / 10 hours)

In this module, students will explore the fundamentals of SQL and relational databases, including structuring data into tables and writing basic SELECT queries with filters. They will then deepen their skills by practicing advanced filtering, sorting, and data presentation using logical operators, compound conditions, and clauses like ORDER BY and AS. Finally, students will learn how to join multiple tables to solve complex data problems and simulate real-world database scenarios.

Topics Covered	• Structuring Data in SQL • Basic Querying in SQL using SELECT • Filtering Queries in SQL using WHERE • Advanced Filters (BETWEEN, LIKE, IN) • Ordering Results using ORDER BY • Renaming Fields using AS • Joining Tables using JOIN • Databases & Cybersecurity • Data Privacy Laws (FERPA, PII)

Example Assignments	• **Your first SELECT statement**
	  ○ Students write and run their first SQL query to retrieve records from a database table.
	• **The Weasleys / The Potters**
	  ○ Students apply WHERE clauses to filter records by specific criteria in a themed dataset.
	• **List All Gryffindors**
	  ○ Students join two tables to retrieve cross-referenced data, combining student and house records.
	• **Personally Identifiable Information (PII) Response**
	  ○ Students analyze a database schema for PII and evaluate its handling against data protection standards.

Module 8: Cyber Defense (4-5 weeks / 20-25 hours)

In this module, students will investigate the various forms of cyberattacks and the methods used to carry them out. They will distinguish between threats, vulnerabilities, and exploits, analyze different types of malware and network attacks, and explore real-world prevention strategies.

Objectives / Topics Covered	• Network Attacks • Malware Types and Prevention • Common Network Attacks • Additional Attacks • Cross-Site Scripting • Internal Threats • Secure Application Development
Example Assignments	• **Spot the Scam** ○ Students examine real-world examples to identify phishing indicators and social engineering tactics. • **Create a Phishing Email**

	○ Students craft a phishing email from the attacker's perspective to understand how social engineering campaigns are constructed. ● **Operation Blackout** ○ Students analyze a simulated DDoS attack scenario and develop a coordinated response strategy. ● **XSS Reflection** ○ Students investigate a cross-site scripting vulnerability and explain its mechanism, potential impact, and mitigation approaches. ● **Bug Bounty Hunting** ○ Students research bug bounty programs and analyze a real vulnerability report submitted by an ethical hacker.

Module 9: Project: Digital Forensics (1 week / 5 hours)

In this project, students will step into the role of digital forensic investigators, using real-world techniques to analyze system logs, metadata, and image data. Through hands-on scenarios, they will learn how digital footprints can be uncovered and interpreted to solve cyber incidents, identify misuse, and verify or disprove claims in both criminal and non-criminal investigations.

Objectives / Topics Covered	● Network Log Analysis ● File Metadata Inspection ● Image Forensics via EXIF Data
Example Assignments	● **Network Logs Conclusion** ○ Students analyze network log evidence and write a forensic conclusion identifying suspicious activity and its likely source. ● **File Metadata Conclusion** ○ Students examine file metadata to reconstruct a timeline of events and identify a suspect. ● **Photo Exif Conclusion** ○ Students extract and analyze EXIF data from a photo using command-line tools to resolve a digital forensics case.

Module 10: Risk Management (2 weeks / 10 hours)

Students will demonstrate skills in conducting vulnerability scans and recognizing vulnerabilities in security systems. They will conduct a security audit and examine port scanning, packet sniffing, and proxy servers to discover exploits in a system. Students will recommend security measures to mitigate the vulnerabilities.

Objectives / Topics Covered	● Identifying Risks ● Assessing Risks ● Risk Response ● Security Frameworks ● Penetration Testing

Example Assignments	• **Malware Risk Assessment**
	  ○ Students assess the likelihood and impact of malware threats and document findings in a structured risk report.
	• **Defense in Depth Risk Mitigation**
	  ○ Students design a multi-layered mitigation strategy for a given risk scenario.
	• **Pen Test Simulation**
	  ○ Students complete a guided penetration test simulation, performing active reconnaissance and documenting exploited vulnerabilities in a report.
	• **Coffee Shop Consultant**
	  ○ Students complete a risk management project for a small business, working through asset identification, risk assessment, security controls, and defense-in-depth planning.

Module 11: Physical Security (2 weeks / 10 hours)

In this module, students examine the physical side of cybersecurity, learning how organizations layer controls to protect buildings, devices, and data. They explore security control types and functions, study real-world breaches like the 2013 Target attack, and investigate surveillance cameras, motion sensors, and entry logging as detection tools. Along the way, students apply defense-in-depth thinking to hands-on design challenges and grapple with the privacy and bias implications of facial recognition technology.

Objectives / Topics Covered	• CIA Triad and security controls • Defense in depth • Physical access controls • Surveillance and detection systems • Secure data destruction • Facial recognition ethics

Example Assignments	• **School Security Controls**
	  ○ Students evaluate physical and digital security controls at a school and recommend improvements based on observed gaps.
	• **Wipe Lab**
	  ○ Students follow a secure data destruction protocol to wipe a device and document each step of the process.
	• **Layered Defense Plan**
	  ○ Students design a physical security plan for a given scenario using multiple overlapping layers of protection.
	• **Entry Log Analysis**
	  ○ Students analyze an access entry log to identify unusual patterns and potential security concerns.

Module 12: Project: Put it in Writing! (2 weeks / 10 hours)

In this project, students will develop a training policy that informs employees on matters of network security and details the company policy on preventative measures employees should take.

Objectives / Topics Covered	• User Training • Incident Response Plans • Data Policy and Privacy • Change Management

Example Assignments	• **User Training Policy Development**
	  ○ Students draft a formal user training policy in response to a simulated employee negligence incident.
	• **Incident Response Plan**
	  ○ Students create an incident response plan and apply it to a simulated cyberattack scenario.
	• **Data Policy Development**
	  ○ Students write a data governance policy addressing licensing, breach response, and appropriate data handling.
	• **Change Management Plan**
	  ○ Students develop a change management plan for a proposed system update, anticipating risks and stakeholder impacts.

Module 13: Programming in Python (2 weeks / 10 hours)

In this module, students are introduced to the fundamentals of programming by learning how to write basic code in Python using print statements, variables, user input, and arithmetic expressions. They'll explore data types, string operations, comments, and the role of programming languages in creating interactive programs.

Objectives / Topics Covered	• Printing • Variables • Types • User Input • Converting Input Types • Arithmetic Expressions • String Operators • Comments • Programming Languages

Example Assignments	• **Introduce Yourself**
	  ○ Students write a program that accepts user input and displays a personalized greeting.
	• **Rectangle**
	  ○ Students calculate and display rectangle dimensions using mathematical and string operators.
	• **Recipe**
	  ○ Students apply string operators and formatting to produce a styled recipe output, incorporating a challenge-level extension.
	• **Programming and Cybersecurity**
	  ○ Students analyze how programming languages relate to cybersecurity practice and compare dynamically and statically typed languages.
	• **Debugging Exercises**
	  ○ Students identify and correct logic and syntax errors in provided

	Python programs.

Module 14: Decisions in Programming (2 weeks / 10 hours)

In this module, students expand their programming skills by working with Boolean values, logical and comparison operators, and if statements to create decision-making programs. They apply their understanding to secure coding practices and explore how programming decisions align with real-world cybersecurity policies and principles.

Objectives / Topics Covered	• If Statements • Boolean Values • Logical Operators • Comparison Operators • Floating Point Numbers • Shell Scripts

Example Assignments	• **Old Enough to Vote?**
	  ○ Students use comparison operators to determine eligibility based on user-entered age.
	• **Presidential Eligibility**
	  ○ Students apply logical operators to evaluate multiple conditions simultaneously for a complex eligibility check.
	• **Transaction**
	  ○ Students write a program with a challenge-level conditional structure to process a financial transaction.
	• **Shell Script Exercises**
	  ○ Students write and run shell scripts to automate tasks, connecting command-line skills to real-world cybersecurity workflows.
	• **Debugging Exercises**
	  ○ Students find and fix errors in programs involving conditionals and logical operators.

Module 15: Project: The Engineering Design Process (3 weeks / 15 hours)

In this project, students will learn the theory and practice of the engineering design process. This project allows students to think creatively about the applications of the concepts covered in the course and create something of personal value.

Topics Covered	• Design Thinking • Prototyping • Testing • Project Prep and Development
Example Assignments	• **User Interview** ○ Students conduct a structured interview to gather user perspectives on a cybersecurity problem.

	• **Create Your Survey and Gather Data**
	  ○ Students design and deploy a survey, then clean and analyze the resulting data to inform their design.
	• **Make Your Paper Prototypes!**
	  ○ Students build paper prototypes of their proposed solution based on brainstorming and user research.
	• **Test Prototype and Improve**
	  ○ Students conduct user testing sessions, document feedback, and iterate on their prototype to improve usability and effectiveness.

(Optional Module) Career and Workplace (10-15 hours)

Students explore computing career pathways, student organizations, certification opportunities, and workplace skills. They practice professional communication through resume writing and mock interviews, and learn essential personal safety practices in technology environments. Students taking more than one CodeHS course in their pathway may have already completed some of these activities in a previous course.

Topics Covered	• Computing careers • Student organizations • Certifications • Resume and interviewing • Workplace safety