

SY 2026-2027 SYLLABUS

C Cubed Training — Cybersecurity Fall 2026 First Semester Syllabus

Course Overview

This course introduces students to cybersecurity through hands-on challenges, investigation, competition, and problem solving. Students will work with Windows, Linux, and Windows Server systems while learning cryptography, password security, social engineering, OSINT, web concepts, quantum computing, and digital investigation skills.

A major component of the semester is **CyberPatriot preparation and competition**. Students will progressively move from introductory system-hardening exercises to Windows, Linux, networking, PowerShell, Server Manager, and Windows Server activities.

Semester Learning Goals

By the end of the semester, students should be able to recognize and work with common number and encoding systems including binary, hexadecimal, decimal, Base64, octal, and ASCII; explain basic cryptographic and steganographic concepts; recognize phishing and other social-engineering techniques; use advanced search and OSINT techniques responsibly; identify fundamental HTTP and web-security concepts; apply password, account-permission, and network-security best practices; perform introductory Windows, Linux, and Windows Server security tasks; and explain introductory quantum-computing concepts such as qubits, superposition, and entanglement.

Students will demonstrate these skills through Owl Sector challenges, CyberPatriot images, games, investigations, practice rounds, and a semester final challenge.

Semester Schedule

Week	Dates	Primary Instruction	CyberPatriot / Applied Work
1	Aug. 10–16	Welcome, course introduction, computer setup; personal vs. competition computing	Windows 11: forensics questions, password complexity, account permissions
2	Aug. 17–23	Binary, hexadecimal, decimal, Base64 and octal; binary history and arithmetic	Ubuntu Linux: forensics, passwords and account permissions
3	Aug. 24–30	Steganography, EXIF and metadata; understanding internet-connected devices	No CyberPatriot practice
4	Aug. 31–Sept. 6	Rail Fence and octal codes; password hygiene; introduction to hashing	Training Game 1 — Windows 11 plus network-security settings
5	Sept. 7–13	Introduction to quantum computing: qubits, superposition and entanglement; ASCII and everyday coding	Training Game 1 — Linux Mint plus network-security settings
6	Sept. 14–20	Quantum Computing Level 1; social engineering, phishing and variants	Windows Server 2022: PowerShell, Server Manager and Windows Admin Center
7	Sept. 21–27	Cryptography/steganography review; HTTP methods and responses; security concepts	Training Game 1 — student choice of image

Week	Dates	Primary Instruction	CyberPatriot / Applied Work
8	Sept. 28–Oct. 4	General cybersecurity skills through the Percy Jackson challenge series	Training Game 1 — student choice of image
9	Oct. 5–11	Google “Dorking”: refining and pinpointing search results	CyberPatriot Practice Round 1 — Windows 11
10	Oct. 12–18	Open Source Intelligence (OSINT)	Practice Round 1 — Linux Mint
11	Oct. 19–25	Cryptography and encoding review	CyberPatriot Game 1
12	Oct. 26–Nov. 1	CyberScare 2026	CyberScare activities
13	Nov. 2–8	Open-source research	Training Round 2 — Windows Server 2022
14	Nov. 9–15	Quantum-computing concepts and review	CyberPatriot Game 2
15	Nov. 16–22	Steganography challenge and Google research challenge	Training Round 2 — Windows Server 2022
—	Nov. 23–29	Thanksgiving Break — No Classes	—
16	Nov. 30–Dec. 6	Quantum-computing review and next steps	Training Round 2 — choice of image
17	Dec. 7–13	Quantum computing: qubits, superposition and entanglement	CyberPatriot Game 2
18	Dec. 14–20	Semester Final Challenge	Training Round 2 — choice of image

Instructional Approach

This is a hands-on course. Students will learn concepts and then apply them through challenges rather than relying primarily on lectures or traditional worksheets. Activities include Owl Sector missions, CyberPatriot competition images, research investigations, cryptography exercises, web-based games, system-hardening tasks, and collaborative problem solving.

The course intentionally revisits several topics—particularly **cryptography, quantum computing, Windows/Linux security, and research skills**—so students encounter them first at an introductory level and later apply them in more difficult situations.

Student Expectations

Students are expected to participate actively, work responsibly with cybersecurity tools, document their work when requested, collaborate appropriately with teammates, and follow ethical cybersecurity practices. Students should understand that the goal is not simply to obtain the correct answer, but to develop the ability to explain **how and why** they reached it.

Cybersecurity techniques taught in class are to be used only on systems, accounts, challenges, and resources for which students have permission.

Assessment

Rather than relying heavily on traditional tests, student progress will be evaluated through **participation, successful completion of hands-on challenges, demonstrated cybersecurity skills, CyberPatriot preparation and competition performance, research/investigation activities, and the Semester Final Challenge**.

The final challenge will require students to draw upon skills developed throughout the semester rather than simply memorizing terminology.

Special Schedule Notes

The source schedule notes that **Florence has no class on Labor Day**, the **Pueblo team has no class during Week 7**, and several CyberPatriot competition weeks require altered meeting days for Colorado Springs and Florence. It also lists the **Peak Cyber Summit visit on Wednesday, September 9 at 10:00 a.m. at the Antlers Hotel in Colorado Springs**, open to everyone.

For the full annual calendar, including competition dates and events, please visit:

<https://www.ccubedtraining.com/parents.html>