

Computer Networking & Cyber Security Syllabus

Instructor:	Tabitha Senty
E-Mail:	tabitha.senty@district196.org
Office Hours:	By appointment
Grade Level:	11 th & 12 th
Course Date:	August 28, 2024 – Jun 5, 2025
Location:	AVHS M223
Prerequisite:	None

Course Description:

This course offers an in-depth introduction to both computer networking and cybersecurity. Students will explore the architecture, structure, functions, components, and models of networks, gaining a solid foundation in IP addressing, internet principles, media, and operations. The curriculum then broadens to cover essential cybersecurity fundamentals, including risk management, security policies, common threats, countermeasures, and the ethical implications of cybersecurity practices. Students will learn and implement best practices in access control, password management, network security, and incident response. By the end of the course, students will be capable of building and configuring simple Local Area Networks (LANs), setting up routers and switches, and implementing IP addressing schemes. A portion of each trimester will be dedicated to career exploration in Networking and Cybersecurity, with students also participating in a Cyber Society, where they will apply critical thinking, problem-solving, and teamwork skills to real-world cybersecurity scenarios, including vulnerability assessment and threat mitigation.

Course Objectives:

This course aims to prepare students for the industry certification exams, with class exercises and assessments designed to mirror these certifications. Students' will need to prepare for examinations outside of class. Class exercises and testing will be similar to those found on one or more of these certification examinations.

- Understand and differentiate between various types of networks and topologies.
- Identify and explain the functions of network hardware components.
- Demonstrate comprehensive knowledge of the OSI model and its application to network hardware.
- Recognize different network cabling types and protocols.
- Explore various network architectures and services.
- Understand the fundamentals of network administration and management.
- Discuss software used in network management.
- Identify components of Wide Area Networks (WANs) and internet networking.
- Use network testing equipment effectively.
- Analyze the cybersecurity landscape, including emerging threats and vulnerabilities.
- Understand the roles and motivations of major threat actors in cyberattacks.
- Evaluate different cyberattack methods and techniques, including DDoS, WiFi exploits, social engineering, and advanced persistent threats (APTs).
- Distinguish between compliance and security in network environments.
- Describe perimeter-based and Zero Trust network security models.
- Compare virtualized and physical data center security measures.
- Discuss cloud computing security and its effects on organizational networks.
- Evaluate various network security devices, such as firewalls, VPNs, intrusion detection/prevention systems (IDS/IPS), and more.
- Understand the basics of cryptography, including encryption methods, PKI, certificates, and digital signatures.
- Explore advanced malware research and its role in enhancing network protection.
- Examine security considerations for mobile, IoT, and cloud-based connection technologies.
- Develop strategies for risk assessment, threat modeling, and vulnerability management.
- Learn the principles of incident response, including detection, containment, eradication, and recovery.
- Explore the ethical and legal implications of cybersecurity practices, including data privacy, intellectual property, and regulatory compliance.

Grading

Please note, **all quizzes will need to be completed by 11:59 pm on the due date assigned.** The lab due dates will be communicated in class and posted in Schoology. If you miss a quiz, lab, etc., I will work with you to determine the best solution for the tardy assignment/lab/assessment. If the grade item is not completed after a reasonable attempt have been made, the student will

receive a zero for the graded item until it has been turned in. **There will be no late work allowed after final unit assessments.**

Grade Point Values

A	= 4.0	D-	= 0.7
A-	= 3.7	F	= 0.0
B+	= 3.3	I	= Course work has not been completed due to serious illness/extended absences.
B	= 3.0	NG	= No Grade
B-	= 2.7	NC	= No Credit
C+	= 2.3		
C	= 2.0		
C-	= 1.7		
D+	= 1.3		
D	= 1.0		

Articulated College Credit Agreement:

Students successfully completing this course, with an 80% or higher may have the opportunity to earn Articulated College Credit from a post-secondary institution. Please contact the course instructor for more information regarding articulation agreements and participating colleges and universities.

Technical Skills Assessment

Students enrolled in this course will complete project based assessments throughout this course to ensure that he/she has met the course content goals. Students will also complete a technical skills assessment that will ensure that they have met the course learning outcomes. This exam will also be a student's benchmark test to determine qualifications to sit for the industry recognized certification examination.