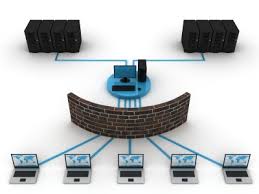
**Computer Networking III**

2022-2023 Course Syllabus

Instructor: Deborah Minassian, M.Ed.

Location: Room 257

[d.minassian@dover.k12.nh.us](mailto:d.minassian@dover.k12.nh.us)



**Course Description:**

CCNA Cyber Ops introduces the core security concepts and skills needed to monitor, detect, analyze and respond to cybercrime, cyberespionage, insider threats, advanced persistent threats, regulatory requirements, and other cybersecurity issues facing organizations. It emphasizes the practical application of the skills needed to maintain and ensure security operational readiness of secure networked systems. This course is eligible for Running Start credit.

**Classroom materials:**

Cisco Academy: <https://www.netacad.com>

**Goals and Objectives of this course:**

**Semester 1:**

**CCNA Cyber Operations**

* Install virtual machines to create a safe environment for implementing and analyzing cybersecurity threat events.
* Explain the role of the Cybersecurity Operations Analyst in the enterprise.
* Explain the Windows Operating System features and characteristics needed to support cybersecurity analyses.
* Explain the features and characteristics of the Linux Operating System.
* Analyze the operation of network protocols and services.
* Explain the operation of the network infrastructure.
* Classify the various types of network attacks.
* Use network monitoring tools to identify attacks against network protocols and services.
* Use various methods to prevent malicious access to computer networks, hosts, and data.
* Explain the impacts of cryptography on network security monitoring.
* Explain how to investigate endpoint vulnerabilities and attacks.
* Evaluate network security alerts.
* Analyze network intrusion data to identify compromised hosts and vulnerabilities.
* Apply incident response models to manage network security incidents.

**Semester 2:**

**Senior Project**

* Criteria and details will be distributed during Semester 1

**Certificates and Certifications available to students:**

**Certificates:**

Upon successful completion of Cyber Ops, students will earn a Certificate of Completion from Cisco Networking Academy. Certificates are not certifications, however, they demonstrate that you have completed the training and that you are competent with the material learned in the course.

**Certifications:**

This course aligns with the CCNA Cyber Ops certification. Candidates need to pass the 210-250 SECFND exam and the 210-255 SECOPS exam to achieve the CCNA Cyber Ops certification.

**Assessments:**

Graded assignments, testing, projects, and hands-on are evaluated as follows: Formative or Summative. Formative assessments determine how well you are grasping the concepts presented. This could be a vocabulary quiz on new terms introduced, or demonstration on your knowledge of CLI to perform a basic switch configuration. Summative assessments determine how well you have learned the concepts of the chapter(s). Summative assessments would include the Chapter exams, collaborative projects, or overall skill such as building a small LAN network.

**Late work:**

The Computer Networking Program is an Honors-level, Running Start program. What that means is that you can earn college credit and, if you desire, attempt several certifications. In keeping with the expectation that comes with earning college credit, you will submit all work on time.

**Formative assessments and other non-summative categories:**

Instructor will grade these assessments within one week after the due date. Students can re-submit work, **once**, within 5 days after receiving the initial grade. Work is due on the due date, unless negotiated in advance with the instructor. Work submitted late will receive the following score: Grace period of three days after due date; students will lose 10 points each day. On the third day, the highest score you will receive is a 70. Work turned in after three days will receive a grade of 50. If you are struggling with an assignment, please ask for help, attend flex, or arrange time on Wednesday afternoon.

Students must complete all labs, quizzes and exams to be eligible for a certificate of completion signed by the instructor and to receive running start credit.

**Summative assessments:**

Summative assessments are due on the date assigned. Mid-term and Final Exams are scheduled in advance. Students take exams on the day they are scheduled. Students, who are unable to take the exam as scheduled, must make alternative arrangements with the teacher.

Grading is as follows:

**Formative: 20%**

* Soft skills, professionalism, conduct
* Quizzes
* Labs
* Competency – demonstration of a particular skill

**Summative: 80%**

* Chapter Exams
* Projects
* Labs
* Competency – demonstration of combined set of skills

**Student Expectations: Whether we are in the classroom or online**

* Arrive on time, be prepared, ready to work, and learn.
* Professionalism. Dress, manners, and attitude. No hats or hoods, please.
* Attendance: In order to do well in this class, you need to present and able to participate. Students who know in advance of a tardy or absence, should discuss with the teacher.
* Follow all safety rules at ALL times.
* Complete all assignments and assessments as instructed. Packet Tracer labs will include screen shots of assessment items or other information as indicated by the instructor.
* Cheating will not be tolerated. Cheating is copying answers off of instructor answer sheets from the internet or using sources from the internet without citation. Students caught cheating will receive a grade of 0. You will not be able to resubmit work that has been plagiarized.
* Be respectful of one another.
* Raise your hand when asking or answering questions.
* Equipment, peripherals, devices, components and tools are in the classroom for all students to use. The altering or removing any equipment, peripherals, devices, components or tools without permission, is considered grounds for removal from the program.
* **Use of personal technology (smart phones, android devices, iPods, iPads or similar) are at the teacher’s discretion. Personal technology devices are out of sight and silenced unless the teacher provides explicit approval. Parents/guardians will be notified if their student is unable to follow this rule.**

**Course Outline:**

The following schedule of topics is preliminary and may be changed as the school year progresses. Students are expected to read assigned materials before it is covered in class.

**Semester I: Cyber Operations**

**Quarter 1: Quarter 2:**

|  |  |
| --- | --- |
| * Cybersecurity and the Security Ops Center | * Protecting the Network |
| * Windows Operating System | * Cryptograpy & the Public Key Infrastructure |
| * Linux Operating System | * Endpoint Security and Analysis |
| * Network Protocols and Services * Network Infrastructure * Principles of Network Security * Network Attacks | * Security Monitoring * Intrusion Data Analysis * Incident Response and Handling |

**Semester II: Senior Project**

|  |  |
| --- | --- |
|  |  |

Please sign and return this portion of the syllabus to acknowledge that you read this and agree to the terms of this document.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Student name Date

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Parent/Guardian name Date

**Semester I Schedule:**

|  |  |  |
| --- | --- | --- |
| Week (Estimation) | Lecture Topics | Assignments |
| 1 | Course Overview, Build Accounts  Syllabus  Cybersecurity and the Security Ops Center | Chapter 1  Quiz, Labs  Chapter Test |
| 2 |  |  |
| 3 | Windows Operating System | Chapter 2  Quiz, Labs  Chapter Test |
| 4 |  |  |
| 5 | Linux Operating System | Chapter 3  Quiz, Labs  Chapter Test |
| 6 |  |  |
| 7 | Network Protocols and Services | Chapter 4  Quiz, Labs  Chapter Test |
| 8 |  |  |
| 9 | Network Infrastructure | Chapter 5  Quiz, Labs  Chapter Test |
| 10 |  |  |
| 11 | Principles of Network Security | Chapter 6  Quiz, Labs  Chapter Test |
| 12 |  |  |
| 13 | Network Attacks | Chapter 7  Quiz, Labs  Chapter Test |
| 14 |  |  |
| 15 | Protecting the Network | Chapter 8  Quiz, Labs  Chapter Test |
| 16 |  |  |
| 17 | Cryptography & the Public Key Infrastructure | Chapter 9  Quiz, Labs  Chapter Test |
| 18 |  |  |
| 19 | Endpoint Security and Analysis | Chapter 10  Quiz, Labs  Chapter Test |
| 20 |  |  |
| 21 | Security Monitoring | Chapter 11  Quiz, Labs  Chapter Test |
| 22 |  |  |
| 23 | Intrusion Data Analysis | Chapter 12  Quiz, Labs  Chapter Test |
| 24 |  |  |
| 24 | Incident Response and Handling | Chapter 13  Quiz, Labs  Chapter Test |