Washtenaw Community College Comprehensive Report

CSS 200 Introduction to Network Security - Security+
Effective Term: Spring/Summer 2020

Course Cover

Division: Business and Computer Technologies
Department: Computer Science & Information Technology
Discipline: Computer Systems Security
Course Number: 200
Org Number: 13400
Full Course Title: Introduction to Network Security - Security+
Transcript Title: Intro to Network Security
Is Consultation with other department(s) required: No
Publish in the Following: College Catalog , Time Schedule , Web Page
Reason for Submission: Three Year Review / Assessment Report
Change Information:
Consultation with all departments affected by this course is required.
Course description
Pre-requisite, co-requisite, or enrollment restrictions
Outcomes/Assessment
Objectives/Evaluation
Other:
Rationale: Syllabus update.
Proposed Start Semester: Fall 2019
Course Description: In this course, students learn the fundamentals of network security. Topics to be covered include understanding security measures and threats, techniques and tools for testing and securing systems, legal and ethical issues, basic intrusion detection and incident response methods. Many of the topics required for the CompTIA Security+ certification will be covered. This course helps students prepare for the CompTIA Security+ Certification. The student is expected to have a basic knowledge of Linux, Windows, working at the command line of any operating system and networking.

Course Credit Hours

Variable hours: No
Credits: 4
Lecture Hours: Instructor: 60 **Student:** 60
Lab: Instructor: 0 **Student:** 0
Clinical: Instructor: 0 **Student:** 0

Total Contact Hours: Instructor: 60 **Student:** 60
Repeatable for Credit: NO
Grading Methods: Letter Grades
Audit
Are lectures, labs, or clinicals offered as separate sections?: NO (same sections)

College-Level Reading and Writing

College-level Reading & Writing

College-Level Math

Level 1

Requisites

Level II Prerequisite
CIS 121 minimum grade "C"

General Education

General Education Area 7 - Computer and Information Literacy
Assoc in Arts - Comp Lit
Assoc in Applied Sci - Comp Lit
Assoc in Science - Comp Lit

Request Course Transfer

Proposed For:

Student Learning Outcomes

1. Identify and troubleshoot common cyber security threats, attacks and vulnerabilities.

Assessment 1

Assessment Tool: Outcome-related questions on the departmentally-developed multiple-choice final exam
Assessment Date: Fall 2022
Assessment Cycle: Every Three Years
Course section(s)/other population: All sections
Number students to be assessed: All students
How the assessment will be scored: Departmentally-developed answer key
Standard of success to be used for this assessment: 70% of the students assessed will score 70% or higher
Who will score and analyze the data: Department faculty

Assessment 2

Assessment Tool: Capstone lab
Assessment Date: Fall 2022
Assessment Cycle: Every Three Years
Course section(s)/other population: All sections
Number students to be assessed: Random sample of 50% of all students with a minimum of 1 full section
How the assessment will be scored: Departmentally-developed rubric
Standard of success to be used for this assessment: 70% of the students assessed will score 70% or higher
Who will score and analyze the data: Department faculty

2. Utilize cryptography to ensure confidentiality and integrity in networked systems.

Assessment 1

Assessment Tool: Outcome-related questions on the departmentally-developed multiple-choice final exam
Assessment Date: Fall 2022
Assessment Cycle: Every Three Years
Course section(s)/other population: All sections
Number students to be assessed: All students
How the assessment will be scored: Departmentally-developed answer key
Standard of success to be used for this assessment: 70% of the students assessed will score 70% or higher
Who will score and analyze the data: Department faculty

Assessment 2

Assessment Tool: Capstone lab

Assessment Date: Fall 2022
Assessment Cycle: Every Three Years
Course section(s)/other population: All sections
Number students to be assessed: Random sample of 50% of all students with a minimum of 1 full section
How the assessment will be scored: Departmentally-developed rubric
Standard of success to be used for this assessment: 70% of the students assessed will score 70% or higher
Who will score and analyze the data: Department faculty

3. Implement and administer a secure network architecture to ensure confidentiality, integrity and availability.
   Assessment 1
   Assessment Tool: Outcome-related questions on the departmentally-developed multiple-choice final exam
   Assessment Date: Fall 2022
   Assessment Cycle: Every Three Years
   Course section(s)/other population: All sections
   Number students to be assessed: All students
   How the assessment will be scored: Departmentally-developed answer key
   Standard of success to be used for this assessment: 70% of the students assessed will score 70% or higher
   Who will score and analyze the data: Department faculty
   Assessment 2
   Assessment Tool: Capstone lab
   Assessment Date: Fall 2022
   Assessment Cycle: Every Three Years
   Course section(s)/other population: All sections
   Number students to be assessed: Random sample of 50% of all students with a minimum of 1 full section
   How the assessment will be scored: Departmentally-developed rubric
   Standard of success to be used for this assessment: 70% of the students assessed will score 70% or higher
   Who will score and analyze the data: Department faculty

4. Analyze and interpret output from electronic devices and applications in a network to ensure security.
   Assessment 1
   Assessment Tool: Outcome-related questions on the departmentally-developed multiple-choice final exam
   Assessment Date: Fall 2022
   Assessment Cycle: Every Three Years
   Course section(s)/other population: All sections
   Number students to be assessed: All students
   How the assessment will be scored: Departmentally-developed answer key
   Standard of success to be used for this assessment: 70% of the students assessed will score 70% or higher
   Who will score and analyze the data: Department faculty
   Assessment 2
   Assessment Tool: Capstone lab
   Assessment Date: Fall 2022
   Assessment Cycle: Every Three Years
   Course section(s)/other population: All sections
   Number students to be assessed: Random sample of 50% of all students with a minimum of 1 full section

How the assessment will be scored: Departmentally-developed rubric
Standard of success to be used for this assessment: 70% of the students assessed will score 70% or higher
Who will score and analyze the data: Department faculty

5. Install, configure and manage identity and access services to ensure confidentiality and integrity.

Assessment 1

Assessment Tool: Outcome-related questions on the departmentally-developed multiple-choice final exam
Assessment Date: Fall 2022
Assessment Cycle: Every Three Years
Course section(s)/other population: All sections
Number students to be assessed: All students
How the assessment will be scored: Departmentally-developed answer key
Standard of success to be used for this assessment: 70% of the students assessed will score 70% or higher
Who will score and analyze the data: Department faculty

Assessment 2

Assessment Tool: Capstone lab
Assessment Date: Fall 2022
Assessment Cycle: Every Three Years
Course section(s)/other population: All sections
Number students to be assessed: Random sample of 50% of all students with a minimum of 1 full section
How the assessment will be scored: Departmentally-developed rubric
Standard of success to be used for this assessment: 70% of the students assessed will score 70% or higher
Who will score and analyze the data: Department faculty

6. Evaluate the cyber security posture of an organization to ensure business continuity and reduce risk.

Assessment 1

Assessment Tool: Outcome-related questions on the departmentally-developed multiple-choice final exam
Assessment Date: Fall 2022
Assessment Cycle: Every Three Years
Course section(s)/other population: All sections
Number students to be assessed: All students
How the assessment will be scored: Departmentally-developed answer key
Standard of success to be used for this assessment: 70% of the students assessed will score 70% or higher
Who will score and analyze the data: Department faculty

Assessment 2

Assessment Tool: Capstone lab
Assessment Date: Fall 2022
Assessment Cycle: Every Three Years
Course section(s)/other population: All sections
Number students to be assessed: Random sample of 50% of all students with a minimum of 1 full section
How the assessment will be scored: Departmentally-developed rubric
Standard of success to be used for this assessment: 70% of the students assessed will score 70% or higher
Who will score and analyze the data: Department faculty

Course Objectives

1. Define and explain the challenges of securing information.

2. Identify the types of threat actors, malware and attacks that are common today.
3. Describe how to defend against cyber based attacks.
4. List and describe cryptographic functions.
5. Explain how to implement cryptography to ensure the confidentiality and integrity of data.
6. Describe the different types of networking-based attacks.
7. List the different types of network security devices and how they can be used to enhance security.
8. Describe and implement secure network architectures.
9. Perform essential testing of network security systems.
10. Develop best practices for configuring network operating system services to provide optimum security.
11. Define application security.
12. List the steps for securing a client device.
13. Explain how physical security can be used for protection.
14. Explain the risks associated with mobile devices and how to secure the devices.
15. Describe different types of embedded systems and IoT devices and how to secure them.
16. Describe the different types of authentication credentials.
17. List the account management procedures for securing passwords.
18. Describe how to manage access through account management.
19. Describe how to implement access control based on best practices.
20. Explain the different types of identity and access services.
21. Explain the differences between vulnerability scanning and penetration testing and why each is important.
22. Describe the techniques for practicing data privacy and security.
23. Describe how to achieve fault tolerance.
24. Describe forensics and incident response procedures.
25. List strategies for reducing risk.

New Resources for Course

Course Textbooks/Resources

Textbooks

Mark Ciampa. *CompTIA Security+ Guide to network Security Fundamentals*, 6th ed. Cengage/MindTap, 2018, ISBN: 1-337-28878-0.

Manuals

Periodicals

Software

MindTap for CompTIA Security+ Guide to Network Security Fundamentals. Cengage, 2018 ed. this is included with textbook access.

NetLabs. WCC, Sec+ V3 ed. WCC provided NetLab access for completion of labs.

Equipment/Facilities

Reviewer	Action	Date
Faculty Preparer:		
Cyndi Millns	*Faculty Preparer*	*Aug 15, 2019*
Department Chair/Area Director:		
Khaled Mansour	*Recommend Approval*	*Aug 15, 2019*
Dean:		
Eva Samulski	*Recommend Approval*	*Aug 19, 2019*
Curriculum Committee Chair:		
Lisa Veasey	*Recommend Approval*	*Dec 09, 2019*

Assessment Committee Chair:		
Shawn Deron	*Recommend Approval*	*Dec 17, 2019*
Vice President for Instruction:		
Kimberly Hurns	*Approve*	*Dec 18, 2019*

Washtenaw Community College Comprehensive Report

CSS 200 Introduction to Network Security - Security+
Effective Term: Spring/Summer 2016

Course Cover

Division: Business and Computer Technologies
Department: Computer Instruction
Discipline: Computer Systems Security
Course Number: 200
Org Number: 13400
Full Course Title: Introduction to Network Security - Security+
Transcript Title: Intro to Network Security
Is Consultation with other department(s) required: No
Publish in the Following: College Catalog , Time Schedule , Web Page
Reason for Submission: Course Change
Change Information:

Consultation with all departments affected by this course is required.
Course title
Course description
Pre-requisite, co-requisite, or enrollment restrictions

Rationale: Update to course description and prerequisites to accurately reflect skills necessary for success and course content.
Proposed Start Semester: Spring/Summer 2016
Course Description: In this course, students learn the fundamentals of network security. Topics to be covered include understanding security measures, techniques for securing systems, legal issues, basic intrusion detection and recovery methods. Many of the topics required for the Security+ certification will be covered. This course prepares the student of the CompTIA Security+ Certification. The student is expected to have a basic knowledge of Linux, Windows, working at the command line of any Operating System and networking. The title of this course was previously Computer Security II.

Course Credit Hours

Variable hours: No
Credits: 4
Lecture Hours: Instructor: 60 **Student:** 60
Lab: Instructor: 0 **Student:** 0
Clinical: Instructor: 0 **Student:** 0

Total Contact Hours: Instructor: 60 **Student:** 60
Repeatable for Credit: NO
Grading Methods: Letter Grades
Audit
Are lectures, labs, or clinicals offered as separate sections?: NO (same sections)

College-Level Reading and Writing

College-level Reading & Writing

College-Level Math

Level 1

Requisites

Level II Prerequisite
CIS 121 minimum grade "C"
and
Level II Prerequisite
CNT 201 minimum grade "C"

General Education

General Education Area 7 - Computer and Information Literacy
Assoc in Arts - Comp Lit
Assoc in Applied Sci - Comp Lit
Assoc in Science - Comp Lit

Request Course Transfer

Proposed For:

Student Learning Outcomes

1. Identify current techniques for securing operating systems and networks.
   Assessment 1
   Assessment Tool: Department created final exam - short answer/multiple choice questions
   Assessment Date: Winter 2017
   Assessment Cycle: Every Three Years
   Course section(s)/other population: Random sample of a minimum of two sections of CSS 200 over the three-year period
   Number students to be assessed: all
   How the assessment will be scored: answer key
   Standard of success to be used for this assessment: 70% of the students will score 70% or higher.
   Who will score and analyze the data: departmental faculty

2. Test systems and identify basic vulnerabilities.
   Assessment 1
   Assessment Tool: Laboratory reports
   Assessment Date: Winter 2017
   Assessment Cycle: Every Three Years
   Course section(s)/other population: Random sample of a minimum of two sections of CSS 200 over the three-year period
   Number students to be assessed: all
   How the assessment will be scored: departmentally-developed rubric
   Standard of success to be used for this assessment: 70% of the students will score 70% or higher.
   Who will score and analyze the data: departmental faculty

3. Identify legal, privacy and ethical issues regarding computer usage.
   Assessment 1
   Assessment Tool: Department created final exam - short answer/multiple choice questions
   Assessment Date: Winter 2017
   Assessment Cycle: Every Three Years
   Course section(s)/other population: Random sample of a minimum of two sections of CSS 200 over the three-year period
   Number students to be assessed: all
   How the assessment will be scored: answer key
   Standard of success to be used for this assessment: 70% of the students will score 70% or higher.

Who will score and analyze the data: departmental faculty

4. Set up basic intrusion detection systems.

Assessment 1

Assessment Tool: Laboratory reports
Assessment Date: Winter 2017
Assessment Cycle: Every Three Years
Course section(s)/other population: Random sample of a minimum of two sections of CSS 200 over the three-year period
Number students to be assessed: all
How the assessment will be scored: departmentally-developed rubric
Standard of success to be used for this assessment: 70% of the students will score 70% or higher.
Who will score and analyze the data: departmental faculty

Course Objectives

1. List basic security concepts.
2. Explain basic techniques for security systems.
3. Perform essential testing of security systems.
4. List legal, privacy and ethical issues.
5. Explain and perform basic intrusion detection.
6. Explain and perform basic recovery methods.
7. Explain and perform basic encryption.
8. Explain and perform basic physical, logical and administrative security.
9. Explain and perform basic intrusion detection and firewall implementation.
10. Explain concepts of general security awareness.

New Resources for Course

Course Textbooks/Resources

Textbooks
Manuals
Periodicals
Software

Equipment/Facilities

Reviewer	Action	Date
Faculty Preparer:		
Michael Galea	*Faculty Preparer*	*Nov 23, 2015*
Department Chair/Area Director:		
John Trame	*Recommend Approval*	*Dec 04, 2015*
Dean:		
Kimberly Hurns	*Recommend Approval*	*Dec 12, 2015*
Curriculum Committee Chair:		
Kelley Gottschang	*Recommend Approval*	*Jan 20, 2016*
Assessment Committee Chair:		
Michelle Garey	*Recommend Approval*	*Jan 25, 2016*
Vice President for Instruction:		
Michael Nealon	*Approve*	*Jan 25, 2016*