COMS-164: INTRODUCTION TO CYBERSECURITY: ETHICAL HACKING

Effective Term
Fall 2025

CC Approval
10/04/2024

AS Approval
10/24/2024

BOT Approval
11/21/2024

COCI Approval
04/23/2025

SECTION A - Course Data Elements

CB04 Credit Status
Credit - Degree Applicable

Discipline

Minimum Qualifications	And/Or
Computer Service Technology (Any Degree and Professional Experience)	

Subject Code
COMS - Computer Studies
Course Number
164

Department
Computer Studies (COMS)

Division
Career Education and Workforce Development (CEWD)

Full Course Title
Introduction to Cybersecurity: Ethical Hacking

Short Title
Introduction to Cybersecurity

CB03 TOP Code
0702.00 - *Computer Information Systems

CB08 Basic Skills Status
NBS - Not Basic Skills

CB09 SAM Code
C - Clearly Occupational

Rationale
Building Cybersecurity certificates per industry request. Please articulate to ITIS 164

SECTION B - Course Description

Catalog Course Description

This course introduces the network security specialist to the various methodologies for attacking a network. Students will be introduced to the concepts, principles, and techniques, supplemented by hands-on exercises, for attacking and disabling a network within the context of properly securing a network. The course will emphasize network attack methodologies with an emphasis on student use of network attack techniques and tools and appropriate defenses and countermeasures. Students will receive course content information through a variety of methods: lectures and demonstration of hacking tools will be used in addition to a virtual environment. Students will experience a hands-on practical approach to penetration testing measures and ethical hacking.

SECTION C - Conditions on Enrollment

Open Entry/Open Exit

No

Repeatability

Not Repeatable

Grading Options

Letter Grade or Pass/No Pass

Allow Audit

Yes

Requisites

Advisory Prerequisite(s)

Completion of COMS-190 with a minimum grade of C.

SECTION D - Course Standards

Is this course variable unit?

No

Units

3.00

Lecture Hours

54

Outside of Class Hours

108

Total Contact Hours

54

Total Student Hours

162

Distance Education Approval

Is this course offered through Distance Education?

Yes

Online Delivery Methods

DE Modalities	Permanent or Emergency Only?
Entirely Online	Permanent
Hybrid	Permanent

SECTION E - Course Content

Student Learning Outcomes

	Upon satisfactory completion of the course, students will be able to:
1.	Understand concepts of cybersecurity, network security, risk assessment, disaster recovery, threat assessment, computer forensics, privacy, and ethics as they relate to security, law, civil compliance, and criminal activity.

Course Objectives

	Upon satisfactory completion of the course, students will be able to:
1.	Defend a computer and a LAN against a variety of different types of security attacks using a number of hands-on techniques.
2.	Practice and use safe techniques on the World Wide Web.
3.	Describe the tools and methods a "hacker" uses to break into a computer or network.

Course Content

1. Ethical Hacking Overview
2. TCP/IP Concepts Review
3. Network and Computer Attacks
4. Footprinting and Social Engineering
5. Port Scanning
6. Enumeration
7. Programming for Security Professionals
8. Embedded Operating Systems
9. Linux Operating System Vulnerabilities
10. Hacking Web Servers
11. Hacking Wireless Networks
12. Cryptography
13. Protecting Networks with Security Devices

Methods of Instruction

Methods of Instruction

Types	Examples of learning activities
Activity	Evaluation will include hands-on projects and a combination of examinations, presentations, discussions, or problem-solving assignments.

Instructor-Initiated Online Contact Types

Announcements/Bulletin Boards
Chat Rooms
Discussion Boards
E-mail Communication
Video or Teleconferencing

Student-Initiated Online Contact Types

Discussions

Course design is accessible

Yes

Methods of Evaluation

Methods of Evaluation

Types	Examples of classroom assessments
Exams/Tests	Evaluation will include hands-on projects and a combination of examinations, presentations, discussions, or problem-solving assignments.

Assignments

Reading Assignments
Read articles about the tools and methods a "hacker" uses to break into a computer or network.

Writing Assignments
Describe the tools and methods a "hacker" uses to break into a computer or network.

Other Assignments
Defend a computer and a LAN against a variety of different types of security attacks using a number of hands-on techniques.

SECTION F - Textbooks and Instructional Materials

Material Type
Textbook

Author
Simpson, M. T., Backman, K. & Corley, J.

Title
Hands-On Ethical Hacking and Network Defense

Edition/Version
4th Edition

Publisher
Cengage Learning

Year
2022

Rationale
Per descriptor ITIS suggestion

ISBN #
978-0357509760

Course Codes (Admin Only)

ASSIST Update
Yes

C-ID Approval Dates

C-ID Descriptor	Approval Date
N/A	

CB00 State ID
CCC000652093

CB10 Cooperative Work Experience Status
N - Is Not Part of a Cooperative Work Experience Education Program

CB11 Course Classification Status
Y - Credit Course

CB13 Special Class Status
N - The Course is Not an Approved Special Class

CB23 Funding Agency Category
Y - Not Applicable (Funding Not Used)

CB24 Program Course Status
Program Applicable

Allow Pass/No Pass
Yes

Only Pass/No Pass
No