CSIT 240: ETHICAL HACKING: HACKER TECHNIQUES AND TOOLS

1. Course Information

Subject
CSIT - Computer Science/ Information Technology

Course Number
240

School
Science, Technology, Engineering, Mathematics

Course Title
Ethical Hacking: Hacker Techniques and Tools

2. Hours

Semester Hours
3

Lecture
3

Lab
0

Practicum
0

3. Catalog Description

For display in the online catalog
This course explores the fundamental concepts of hacker techniques and tools which are used in the field of Ethical Hacking. Topics to be covered include the planning, sanctioning, assurance and execution of an ethical hack, including an understanding of the critical categories of attack techniques that would be used. The course will also review the various software, application, network, and platform vulnerabilities that would be the focus of the attacks. Lab activities will provide students with practical experiences in ethical hacking. Open lab time is required.

4. Requisites

Prerequisites
CSIT 200 with a grade of C or higher.

5. Course Type

Course Fee Code
3

Course Type for Perkins Reporting
vocational (approved for Perkins funding)

6. Justification

Describe the need for this course
This course will be a requirement toward a Cybersecurity Certificate of Completion as part of a curriculum designed to address the “Cyber Threats (CT)” Knowledge Unit requirement for OCC qualification as a National Center of Academic Excellence in Cyber Defense (CAE-CD). It will also prepare the student to test to for certification by the EC-Council as a Certified Ethical Hacker (CEH). The CEH certification is recognized for the DoD's computer network defense Service Providers (CND-SP’s), a specialized personnel classification within the United States Department of Defense’s information assurance workforce.

7. General Education

Will the college submit this course to the statewide General Education Coordinating Committee for approval as a course, which satisfies a general education requirement?

No

If the course does not satisfy a general education requirement, which of the following does it satisfy:

Program-specific requirement

8. Consistency with the Vision and Mission Statements, the Academic Master Plan, and the strategic initiatives of the College

Please describe how this course is consistent with Ocean County College's current Vision Statement, Mission Statement, Academic Master Plan, and the strategic initiatives of the College:

	Add item
1	Demonstrating the college's commitment to offer comprehensive educational programs that develop intentional learners of all ages. (Mission Statement)
2	Seeking to ensure that students will thrive in an increasingly diverse and complex world. (Vision Statement)
3	Preparing students for successful transfer to other educational institutions and/or for entrance into the workforce. (Academic Master Plan)
4	Seeking to empower students through the mastery of intellectual and Practical Skills. (Academic Master Plan)
5	Challenging students to transfer information into knowledge and knowledge into action. (Academic Master Plan)

9. Related Courses at Other Institutions

Comparable Courses at NJ Community Colleges

Institution

Brookdale CC

Course Title

Hacker Techniques, Tools, and Incident Handling

Course Number

NETW238

Number of Credits

3

Institution

Rowan College at Burlington County

Course Title

Ethical Hacking Fundamentals

Course Number

CIS-218

Number of Credits

3

Institution

County College of Morris

Course Title

Ethical Hacking and Systems Defense

Course Number

CMP-243

Number of Credits
3

Institution
Essex County College

Course Title
Network Defense and Countermeasures

Course Number
CSC 226

Number of Credits
4

Institution
Hudson County CC

Course Title
Ethical Hacking

Course Number
CSC 245

Number of Credits
3

Institution
Mercer County CC

Course Title
Ethical Hacking

Course Number
NET 245

Number of Credits
3

Institution
Raritan Valley CC

Course Title
Ethical Hacking and Penetration Testing

Course Number
NTWK 290

Number of Credits
3

Transferability of Course

Georgian Court University

Course Code, Title, and Credits	Transfer Catagory	If non-transferable; select status
EC 56 Elective - 3 Credits	Elective	

Kean University

Course Code, Title, and Credits	Transfer Catagory	If non-transferable; select status
CPSX1003 - Computer Science Free Elective or TECHX2002 - Technology Elective - 3 Credits	Elective	

Monmouth University

Course Code, Title, and Credits	Transfer Catagory	If non-transferable; select status
CS002 - 200 Level Computer Science Elective - 3 Credits	Elective	

Rowan University

Course Code, Title, and Credits	Transfer Catagory	If non-transferable; select status
Elective, EC, 3 cr.	Elective	

Rutgers - New Brunswick, Mason Gross School of the Arts

Course Code, Title, and Credits	Transfer Catagory	If non-transferable; select status
		Will not transfer

Stockton University

Course Code, Title, and Credits	Transfer Catagory	If non-transferable; select status
CSISEC - Computer Science and Information Systems Elective - 3 Credits	Elective	

If not transferable to any institution, explain:

Rutgers: Students who take this course as a part of an AA or AS degree can receive Elective credit

10. Course Learning Outcomes

Learning Outcomes

	Students who successfully complete this course will be able to:
CLO1	Develop a plan for an ethical hack for proposal and review by parties responsible for protecting corporate systems.
CLO2	Specify the skills, tools and techniques required for ethical hacking.
CLO3	List various avenues of attacks including the categories of compromise, the critical assets, the elements of a system, cloud platforms and the system lifecycle which covers when attacks can occur.
CLO4	Classify details of the various attack vulnerabilities including software, authentication, network, denial of service, platform, and social engineering vulnerabilities.
CLO5	Demonstrate ways to avoid detection during an ethical hacking exercise.
CLO6	Leverage resources from the various Hacker networks, forums and information resources.

11. Topical Outline

(include as many themes/skills as needed)

	Major Themes/ Skills	Assignments (Recommended but not limited to)	Assessments (Recommended but not limited to)	Course Learning Outcome(s)
TO1	Being an Ethical Hacker 1) The Demand for Ethical Hacking 2) The Dangers and Penalties for Unethical Hacking 3) Contracting and Planning the Ethical Hack 4) Creating a Monster – Case Study: The Morris Worm	Hands-on, Lab exercises	Exam	CL01

TO2	Avenues of Attack 1) Categories of Compromise 2) Critical Assets 3) The Elements of a System 4) Cloud (ETSI NFV) Architecture Elements	Hands-on, Lab exercises	Exam	CL01, CL02
TO3	Attack Categories 1) Software Vulnerabilities 2) Authentication Vulnerabilities 3) Network Vulnerabilities 4) Denial of Service Vulnerabilities 5) Client Platform Vulnerabilities 6) Covert Channels 7) Social Engineering	Hands-on, Lab exercises	Lab assignment	CL01, CL03
TO4	Avoiding Detection 1) Logs and Audit Trails, 2) Intrusion Detection Systems, 3) Caller ID, 4) Establishing E-mail Accounts, 5) Bots and Zombies, 6) Honeypots, 7) Security Operations Centers.	Hands-on, Lab exercises	Exam	CL01, CL04
TO5	Hacker Networks and Information Sources 1) Computer Emergency Response Team (CERT) 2) Certified Ethical Hacker (CEH) Certification (http://eccouncil.org) 3) Google's Bug Hunter University 4) Hacktivity	Hands-on, Lab exercises	Exam	CL01, CL05

12. Methods of Instruction

In the structuring of this course, what major methods of instruction will be utilized?

o Class lecture
o Discussion
o Demonstrations
o Lab assignments
o Programs and online presentations

13. General Education Goals Addressed by this Course (this section is to fulfill state requirements)

Information

_____

_____

_____

Technological Competency

Yes

Related Course Learning Outcome

CL01-CL01

Related Outline Component

TO1-TO5

Assessment of General Education Goal (Recommended but not limited to)

Exam, Project

_____

_____

_____

_____

_____

_____

_____

Independent/Critical Thinking
Yes

Related Course Learning Outcome
CL01, CL03

Related Outline Component
TO1-TO5

Assessment of General Education Goal (Recommended but not limited to)
Exam, Project

14. Needs

Instructional Materials (text etc.):
Appropriate textbooks and/or Open Educational Resources will be selected. Class notes, presentations, software and online materials.

Technology Needs:
College Portal and/or College Distance Learning Platform and/or Textbook or Instructor Website.

Human Resource Needs (Presently Employed vs. New Faculty):
Presently Employed Faculty.

Facility Needs:
Laboratory classrooms equipped with computer workstations. Isolated network and computers to demonstrate cybersecurity principles, security and attacks. Podium computer similarly equipped plus the ability to present audio-video presentations to the class.

Library needs:
None

15. Grade Determinants

The final grade in the course will be the cumulative grade based on the following letter grades or their numerical equivalents for the course assignments and examinations

A: Excellent

B+: Very Good

B: Good

C+: Above Average

C: Average

D: Below Average

F: Failure

I: Incomplete

R: Audit

For more detailed information on the Ocean County College grading system, please see Policy #5154.

16. Board Approval

History of Board approval dates
New course board approved: February 25, 2021