

# CSIT 242: PENETRATION TESTING FUNDAMENTALS

---

## 1. Course Information

**Subject**

CSIT - Computer Science/ Information Technology

**Course Number**

242

**School**

Science, Technology, Engineering, Mathematics

**Course Title**

Penetration Testing Fundamentals

## 2. Hours

**Semester Hours**

3

**Lecture**

3

**Lab**

0

**Practicum**

0

## 3. Catalog Description

**For display in the online catalog**

Penetration testing fundamentals assesses the most up-to-date penetration testing, vulnerability assessment, and management skills necessary to determine the resiliency of the network against attacks. It will cover fundamental methodologies, techniques, tools to identify vulnerabilities, exploit, assess security risk to networks, operating systems, and applications.

## 4. Requisites

**Prerequisites**

CSIT 165

**Corequisites**

CSIT 185

## 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 provides the required training in Cybersecurity programs of study and helps students prepare for the fundamental of penetration testing.

## 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

Raritan Valley CC

#### Course Title

Ethical Hacking and Penetration Testing

#### Course Number

NTWK290

#### Number of Credits

3

#### Institution

County College of Morris

#### Course Title

Ethical Hacking and Systems Defense Course

#### Course Number

CMP243

#### Number of Credits

3

## Transferability of Course

### Georgian Court University

Course Code, Title, and Credits	Transfer Category	If non-transferable; select status
EC Elective Credit	Elective	

**Kean University**

Course Code, Title, and Credits	Transfer Category	If non-transferable; select status
FEX 2000	Free Elective	

**Monmouth University**

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

**Rowan University**

Course Code, Title, and Credits	Transfer Category	If non-transferable; select status
CST 03215, Penetration Testing Fundamentals, 3	Major	

**Rutgers - New Brunswick, Mason Gross School of the Arts**

Course Code, Title, and Credits	Transfer Category	If non-transferable; select status
		Unable to determine status

**Stockton University**

Course Code, Title, and Credits	Transfer Category	If non-transferable; select status
CSISEC Computer Science & Info Systems Elective 4	Computer Science Elective	

**10. Course Learning Outcomes****Learning Outcomes**

Students who successfully complete this course will be able to:	
CLO1	Describe the fundamentals of penetration testing and vulnerability management.
CLO2	Describe the history, development, and principles of cybersecurity.
CLO3	Identify key (vs. secondary) risk elements faced by computer network systems.
CLO4	Assess the current security landscape, including the nature of the threat, the general status of common vulnerabilities, and the likely consequences of security failures.
CLO5	Analyze security components within organizational context: identity and access management, data protection, security operations.
CLO6	Create a plan for the third-party risk assessments.

**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)
T01	1.Planning a Pen Test 2.Rules of Engagement 3.Resources and Budgets 4.Impact and Constraints 5.Support Resources	Reading, Class discussion	Quiz/ Exam	CLO1, CLO2
T02	1. Legal Groundwork 2. Scope Considerations 3. Project Strategy and Risk 4. Scope Vulnerabilities 5. Compliance-Based Assessments	Reading, Class discussion	Quiz/ Exam	CLO3

T03	1. Scanning and Enumeration 2. Scanning and Demo 3. Packet Investigation 4. Packet Inspection Demo 5. Application and Open-Source Resources	Reading, Class discussion	Quiz/ Exam	CLO2, CLO3
T04	1. Vulnerability Scanning 2. Vulnerability Scanning Demo 3. Target Considerations 4. Nmap Timing and Performance Options 5. Prioritization of Vulnerabilities 6. Common Attack Techniques	Reading, Class discussion	Quiz/ Exam	CLO4
T05	1. Credential Attacks 2. Weaknesses in Specialized Systems 3. Remote Social Engineering 4. Spear Phishing Demo 5. In-Person Social Engineering 6. Network-Based Exploits 7. FTP Exploit Demo 8. Man-in-the-Middle Exploits 9. Wireless Exploits 10. Application Exploits, Part 1	Reading, Class discussion	Quiz/ Exam	CLO4, CLO5
T06	1. SQL Injection Demo 2. Application Exploits, Part 2 3. Application Exploits, Part 3 4. Cross-Site Scripting Demo 5. Code Vulnerabilities 6. Local Host Vulnerabilities 7. Privilege Escalation (Linux) 8. Privilege Escalation (Windows) 9. Misc. Privilege Escalation 10. Misc. Local Host Vulnerabilities 11. Physical Security 12. Post-Exploitation Techniques	Reading, Class discussion	Quiz/ Exam	CLO5, CLO6
T07	1. Persistence and Stealth 2. Nmap Scoping and Output Options 3. Pen Testing Toolbox 4. Using Kali Linux 5. Scanners and Credential Tools 6. Code Cracking Tools 7. Open-Source Research Tools 8. Wireless and Web Pen Testing Tools 9. Remote Access Tools 10. Analyzers and Mobile Pen Testing Tools	Reading, Class discussion	Quiz/ Exam	CLO5, CLO6
T08	1. Other Pen Testing Tools 2. Using Scripting in Pen Testing 3. Bash Scripting Basics 4. Bash Scripting Techniques 5. PowerShell Scripts	Reading, Class discussion	Quiz/ Exam	CLO4, CLO5, CLO6

T09	1. Ruby Scripts 2. Python Scripts 3. Scripting Languages Comparison 4. Writing Reports 5. Post Report Activities 6. Mitigation Strategies 7. Communication	Reading, Class discussion	Quiz/ Exam	CLO4, CLO5 ,CLO6
-----	--	---------------------------	------------	------------------

## 12. Methods of Instruction

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

Class lecture, presentations, discussions, lab assignments/exercises, case studies, and projects.

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

Information

**Communication-Written and Oral**

Yes

**Related Course Learning Outcome**

CLO1-CLO6

**Related Outline Component**

T01-T09

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

N/A

---



---



---

**Technological Competency**

Yes

**Related Course Learning Outcome**

CLO1-CLO6

**Related Outline Component**

T01-T09

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

N/A

---



---



---



---



---



---

**Independent/Critical Thinking**

Yes

**Related Course Learning Outcome**

CLO1-CLO6

**Related Outline Component**

T01-T09

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

N/A

## **14. Needs**

**Instructional Materials (text etc.):**

Appropriate textbook(s) will be selected. Please contact the department for current adoptions.

**Technology Needs:**

N/A

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

N/A

**Facility Needs:**

N/A

**Library needs:**

N/A

## **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**

Board of Trustees Approval Date: March 17, 2023