# CYBR C242: ETHICAL HACKING & AI DRIVEN PENETRATION TESTING (PENTEST+)

| Item | Value |
|---|---|
| Curriculum Committee Approval Date | 10/27/2023 |
| Top Code | 070800 - Computer Infrastructure and Support |
| Units | 3 Total Units |
| Hours | 54 Total Hours (Lecture Hours 54) |
| Total Outside of Class Hours | 0 |
| Course Credit Status | Credit: Degree Applicable (D) |
| Material Fee | No |
| Basic Skills | Not Basic Skills (N) |
| Repeatable | No |
| Grading Policy | Standard Letter (S),<br>• Pass/No Pass (B) |

## Course Description

This course covers the fundamentals of planning and scoping security assessments, understanding legal and compliance requirements, conducting vulnerability scans, and performing penetration tests using industry-standard and AI-driven tools and methodologies. Students will explore how AI enhances penetration testing by automating threat detection, prioritizing vulnerabilities, and simulating advanced attack scenarios. They will learn to create detailed reports with proposed remediation strategies and actionable recommendations, effectively communicating findings to management. Hands-on exercises provide practical experience, building the technical skills needed for roles such as Vulnerability Tester and Network Security Operations Specialist. The course also prepares students for the CompTIA PenTest+ certification exam. ADVISORY: IT C128, CYBR C132, and CYBR C230. Transfer Credit: CSU.

## Course Level Student Learning Outcome(s)

1. Given a scenario, plan and scope an assessment to find security vulnerabilities.
2. Demonstrate the use of AI-driven security tools and techniques to perform vulnerability scanning and penetration testing.
3. Analyze penetration test results to develop a report that provides practical recommendations for management.

## Course Objectives

- 1. Describe the penetration testing process, including planning and scoping the assessment, information gathering, and identifying vulnerabilities.
- 2. Demonstrate the use of appropriate tools and techniques to perform vulnerability scanning and penetration testing.
- 3. Describe appropriate reporting techniques to communicate test results to management.
- 4. Explain the importance of planning an engagement.
- 5. Explain how to enumerate information about an application or network using appropriate techniques.
- 6. Provide a method for analyzing the results of reconnaissance and enumeration activities.
- 7. Demonstrate how to conduct an attack and exploits.
- 8. Demonstrate the use of tool output to identify vulnerabilities.

## Lecture Content

Planning and Scoping Explain the importance of planning for an engagement Explain key legal concepts Explain the importance of scoping an engagement properly Explain the key aspects of compliance-based assessments Information Gathering and Vulnerability Identification Conduct information gathering using appropriate techniques Perform a vulnerability scan Analyze vulnerability scan results Explain the process of leveraging information to prepare for exploitation Explain weaknesses related to specialized systems  Attacks and Exploits Compare and contrast social engineering attacks Exploit various system-based vulnerabilities Summarize physical security attacks related to facilities Perform post-exploitation techniques Penetration Testing Tools Use Nmap to conduct information gathering exercises Compare and contrast various use cases of tools Analyze tool output or data related to a penetration test Analyze a basic script Reporting and Communication Use report writing and handling best practices Explain post-report delivery activities Recommend mitigation strategies for discovered vulnerabilities Explain the importance of communication during the penetration testing process

## Lab Content

Conduct information gathering using appropriate techniques for scanning, enumeration, packet crafting, and packet inspection Perform vulnerability scans; credentialed vs. uncredentialed Exploit network-based vulnerabilities; name resolution, man-in-the-middle, virtual local area network (VLAN) hopping Exploit wireless network vulnerabilities; evil twin, deauthentication, and fragmentation Exploit application-based vulnerabilities; injections, authentication, and cross-site scripting Analyze data to effectively report results to management

## Method(s) of Instruction

- Lecture (02)
- DE Live Online Lecture (02S)
- DE Online Lecture (02X)
- Lab (04)
- DE Live Online Lab (04S)
- DE Online Lab (04X)

## Instructional Techniques

This course will utilize a combination of lecture, hands-on guided laboratory assignments, classroom/discussion student interactions, problem solving, quizzes, tests, and troubleshooting assignments to achieve the goals and objectives of this course. All instructional methods are consistent across all modalities.

## Reading Assignments

A. Review and research the importance of planning for an engagement.B. Read the process of leveraging information to prepare for exploitation.C. Read various vulnerabilities for network-based systems, wireless and RF-based systems, application-based systems, and local hosts.

## Writing Assignments

A. Write a report to compare and contrast various use cases of tools. B. Complete documentation to analyze tool output or data related to a penetration test. C. Write a report to summarize the analysis of a basic script.

## Out-of-class Assignments

A. Complete hands-on lab to perform vulnerability scans. B. Complete hands-on lab to perform post-exploitation techniques. C. Conduct research based on a given scenario to find practical recommendations for management.

## Demonstration of Critical Thinking

Students will assess scenarios to scope and plan an assessment. A written report will be completed after penetration testing to provide practical recommendations.

## Required Writing, Problem Solving, Skills Demonstration

Students will scan for and assess vulnerabilities to determine network risks. A report will be written to communicate the findings and provide remediation solutions for management.

## Eligible Disciplines

Computer information systems (computer network installation, microcomputer ...: Any bachelors degree and two years of professional experience, or any associate degree and six years of professional experience. Computer service technology: Any bachelors degree and two years of professional experience, or any associate degree and six years of professional experience.

## Textbooks Resources

1. Required Nutting, R. CompTIA PenTest+ Certification All-in-One Exam Guide (Exam PT0-001), 1st ed. McGraw-Hill Education, 2018

## Other Resources

1. Coastline Library 2. White papers, security reports, and articles are available at no charge to all students at multiple sites as recommended by the instructor.