COURSE OUTLINE: CYB302 - ETHICAL HACKING

Prepared: IT Studies
Approved: Martha Irwin, Dean, Business and Information Technology

Course Code: Title	CYB302: ETHICAL HACKING
Program Number: Name	2198: CYBERSECURITY 5911: CYBERSECURITY
Department:	PPP triOS
Academic Year:	2024-2025
Course Description:	Viewed from a Canadian perspective, this course introduces students to what and who ethical hackers are and how they are different from non-ethical hackers . The course explores why ethical hacking is essential for protecting data from cyber-attacks. This course covers the procedures used to assess the attack surface of an organization, as well as perform a penetration test and vulnerability assessment.
Total Credits:	5
Hours/Week:	5
Total Hours:	70
Prerequisites:	There are no pre-requisites for this course.
Corequisites:	There are no co-requisites for this course.
Vocational Learning Outcomes (VLO's) addressed in this course: **Please refer to program web page for a complete listing of program outcomes where applicable.**	**2198 - CYBERSECURITY** VLO 5 Comply with existing industry policies, regulations, and ethics for information systems and information technology security solutions to ensure industry expectations and standards are met or exceeded VLO 6 Analyze security risks to organizations and business processes to mitigate risk in compliance with industry standards VLO 8 Implement and conduct penetration testing to identify and exploit an organization's network system vulnerability VLO 9 Perform various types of cyber analysis to detect actual security incidents and suggest solutions **5911 - CYBERSECURITY** VLO 5 Comply with existing industry policies, regulations, and ethics for information systems and information technology security solutions to ensure industry expectations and standards are met or exceeded. VLO 6 Analyze security risks to organizations and business processes to mitigate risk in compliance with industry standards. VLO 8 Implement and conduct penetration testing to identify and exploit an organization's network system vulnerability. VLO 9 Perform various types of cyber analysis to detect actual security incidents and suggest solutions.

Essential Employability Skills (EES) addressed in this course:

EES 1 Communicate clearly, concisely and correctly in the written, spoken, and visual form that fulfills the purpose and meets the needs of the audience.

EES 2 Respond to written, spoken, or visual messages in a manner that ensures effective communication.

EES 4 Apply a systematic approach to solve problems.

EES 5 Use a variety of thinking skills to anticipate and solve problems.

EES 6 Locate, select, organize, and document information using appropriate technology and information systems.

EES 7 Analyze, evaluate, and apply relevant information from a variety of sources.

EES 9 Interact with others in groups or teams that contribute to effective working relationships and the achievement of goals.

EES 10 Manage the use of time and other resources to complete projects.

Course Evaluation:

Passing Grade: 50%, D

A minimum program GPA of 2.0 or higher where program specific standards exist is required for graduation.

Other Course Evaluation & Assessment Requirements:

A+ = 90-100%
A = 80-89%
B = 70-79%
C = 60-69%
D = 50-59%
F < 50%

Students are expected to be present to write all tests in class, unless otherwise specified. If a student is unable to write a test due to illness or a legitimate emergency, that student must contact the professor prior to class and provide reasoning. Should the student fail to contact the professor, the student shall receive a grade of zero on the test.

If a student is not present 10 minutes after the test begins, the student will be considered absent and will not be given the privilege of writing the test.
Students exhibiting academic dishonesty during a test will receive an automatic zero. Please refer to the College Academic Dishonesty Policy for further information.

In order to qualify to write a missed test, the student shall have:
a.) attended at least 75% of the classes to-date.
b.) provide the professor an acceptable explanation for his/her absence.
c.) be granted permission by the professor.

NOTE: The missed test that has met the above criteria will be an end-of-semester test.

Labs / assignments are due on the due date indicated by the professor. Notice by the professor will be written on the labs / assignments and verbally announced in advance, during class.

Labs and assignments that are deemed late will have a 10% reduction per academic day to a maximum of 5 academic days at 50% (excluding weekends and holidays). Example: 1 day late - 10% reduction, 2 days late, 20%, up to 50%. After 5 academic days, no late assignments and labs will be accepted. If you are going to miss a lab / assignment deadline due to circumstances beyond your control and seek an extension of time beyond the due date, you must contact your professor in advance of the deadline with a legitimate reason that is acceptable.

It is the responsibility of the student who has missed a class to contact the professor immediately to obtain the lab / assignment. Students are responsible for doing their own work. Labs / assignments that are handed in and are deemed identical or near identical in content may constitute academic dishonesty and result in a zero grade.

Students are expected to be present to write in-classroom quizzes. There are no make-up options for missed in-class quizzes.

Students have the right to learn in an environment that is distraction-free, therefore, everyone is expected to arrive on-time in class. Should lectures become distracted due to students walking in late, the professor may deny entry until the 1st break period, which can be up to 50 minutes after class starts or until that component of the lecture is complete.

The total overall average of test scores combined must be 50% or higher in order to qualify to pass this course. In addition, combined tests, Labs / Assignments total grade must be 50% or higher.

Books and Required Resources:

CompTIA PenTest+ Study Guide by Seidl/Chapple
Publisher: Sybex (Wiley) Edition: 2
ISBN: 978-1-119-82381-0

Course Outcomes and Learning Objectives:

Course Outcome 1	**Learning Objectives for Course Outcome 1**
Assess planning and scoping best practices.	PLANNING AND SCOPING 1.1 Compare and contrast governance, risk, and compliance concepts. 1.2 Explain the importance of scoping and organizational/customer requirements. 1.3 Demonstrate an ethical hacking mindset by maintaining professionalism and integrity.
Course Outcome 2	**Learning Objectives for Course Outcome 2**
Determine how to leverage information to prepare for system exploitation after gathering information, scanning vulnerabilities, and analyzing results.	INFORMATION GATHERING AND VULNERABILITY SCANNING 2.1 Perform passive reconnaissance. 2.2 Perform active reconnaissance. 2.3 Analyze the results of a reconnaissance exercise. 2.4 Perform vulnerability scanning.
Course Outcome 3	**Learning Objectives for Course Outcome 3**
Perform ethical hacking by exploiting various vulnerabilities and implement post-exploitation techniques.	ATTACKS AND EXPLOITS 3.1 Research attack vectors and perform network attacks. 3.2 Research attack vectors and perform wireless attacks. 3.3 Research attack vectors and perform application-based attacks. 3.4 Research attack vectors and perform attacks on cloud technologies. 3.5 Explain common attacks and vulnerabilities against specialized systems. 3.6 Perform a social engineering or physical attack. 3.7 Perform post-exploitation techniques.

Course Outcome 4	Learning Objectives for Course Outcome 4
Use penetration testing tools in various scenarios to gather information and analyze output.	TOOLS AND CODE ANALYSIS 4.1 Explain the basic concepts of scripting and software development. 4.2 Analyze a script or code sample for use in a penetration test. 4.3 Explain use cases of different tools during the phases of a penetration test.

Course Outcome 5	Learning Objectives for Course Outcome 5
Write a report that adheres to best practices for recommending mitigation strategies in the aftermath of penetration testing.	REPORTING AND COMMUNICATION 5.1 Compare and contrast important components of written reports. 5.2 Analyze the findings and recommend the appropriate remediation within a report. 5.3 Explain the importance of communication during the penetration testing process.5.4 Explain post-report delivery activities.

Evaluation Process and Grading System:

Evaluation Type	Evaluation Weight
Final Exam	30%
Lab Assignments	48%
Professional Performance	10%
Quizzes	12%

Date: June 16, 2024

Addendum: Please refer to the course outline addendum on the Learning Management System for further information.