COURSE OUTLINE: CYB302 - ETHICAL HACKING

Prepared: IT Studies
Approved: Corey Meunier, Chair, Technology and Skilled Trades

Course Code: Title	CYB302: ETHICAL HACKING
Program Number: Name	5911: CYBERSECURITY
Department:	PPP triOS
Academic Year:	2021-2022
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:	75
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.**	**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:	OTHER EVALUATION CONSIDERATIONS 1. In order to pass this course, the student must obtain an overall test/quiz average of 50% or better, as well as, an overall assignment average of 50% or better. A student who is not present to write a particular test/quiz, and does not notify the professor beforehand of their intended absence, may be subject to a zero grade on that test/quiz. 2. There will be no supplemental or make-up quizzes/tests in this course unless there are extenuating circumstances. 3. Assignments must be submitted by the due date according to the specifications of the professor. Late assignments will normally be given a mark of zero. Late assignments will only be marked at the discretion of the professor in cases where there were extenuating circumstances. 4. Any assignment/projects submissions, deemed to be copied, will result in a zero grade being assigned to all students involved in that particular incident. 5. It is the responsibility of the student to ask the professor to clarify any assignment requirements. 6. The professor reserves the right to modify the assessment process to meet any changing needs of the class. Attendance: Sault College is committed to student success. There is a direct correlation between academic performance and class attendance, therefore, for the benefit of all its constituents, all students are encouraged to attend all of their scheduled learning and evaluation sessions. This implies arriving on time and remaining for the duration of the scheduled session. It is the departmental policy that once the classroom door has been closed, the learning process has begun. Late arrivers may not be granted admission to the room.
Books and Required Resources:	CompTIA PenTest+ Study Guide by Mike Chapple Publisher: Sybex (Wiley) ISBN: 978-1-119-50424-5

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 Outline the importance of planning for an engagement. 1.2 Review key legal concepts. 1.3 Examine the importance of scoping an engagement properly. 1.4 Explore the key aspects of compliance-based assessments.
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	INFORMATION GATHERING AND VULNERABILITY IDENTIFICATION 2.1 Conduct information gathering using appropriate techniques for various vulnerability scenarios. 2.2 Perform a vulnerability scan.

	analyzing results	2.3 Analyze vulnerability scan results. 2.4 Outline the process of leveraging information to prepare for exploitation. 2.5 Evaluate weaknesses related to specialized systems.
	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 Examine social engineering attacks. 3.2 Exploit network-based vulnerabilities for various scenarios. 3.3 Exploit wireless and RF-based vulnerabilities. 3.4 Exploit application-based vulnerabilities. 3.5 Exploit local host vulnerabilities. 3.6 Evaluate physical security attacks related to facilities. 3.7 Implement 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	PENETRATION TESTING TOOLS 4.1 Use Nmap to conduct information gathering exercises. 4.2 Examine various use cases of tools. 4.3 Evaluate tool output or data related to a penetration test. 4.4 Analyze a basic script (limited to Bash, Python, Ruby, and PowerShell).
	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 Adopt best practices in post-penetration testing report writing. 5.2 Explain post-report delivery activities. 5.3 Recommend mitigation strategies for discovered vulnerabilities following penetration testing. 5.4 Explain the importance of communication during the penetration testing process

Evaluation Process and Grading System:

Evaluation Type	Evaluation Weight
Final Exam	60%
Lab Work and Quizzes	30%
Professional Performance	10%

Date: June 30, 2022

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