

Course Title	<b>ETHICAL HACKING</b>
Course Code	<b>CSC 403</b>
Course Purpose and Objectives	<p>The purpose of this course is to provide knowledge on ethical hacking. Students learn how to penetrate the computer systems, applications or networks to identify and exploit the security vulnerabilities that may lead to potential cyber threats and risks. This course provides practical knowledge and hands-on real-time concepts and penetration tools. In this course students will learn various hacking techniques and attacks. Additionally, tools and several techniques of penetration testing will be presented and/or demonstrated. Practical tasks will be assigned in order to improve the understanding of the theoretical background. For this purpose, students will learn how to exploit vulnerabilities and also how to protect system against attacks, for every stage of the penetration testing.</p>
Learning Outcomes	<ol style="list-style-type: none"> <li>1. Classify and analyze the stages which an ethical-hacker requires to apply in order to compromise a target system.</li> <li>2. Apply tools and techniques to carry out a penetration testing.</li> <li>3. Evaluate the security status of systems and suggest solutions for eliminating or removing security vulnerabilities.</li> <li>4. Discuss the legal aspects of performing ethical hacking and judge what is within and outside permitted activities.</li> </ol>
Course Content	<ul style="list-style-type: none"> <li>• Introduction to ethical hacking</li> <li>• Phases of hacking</li> <li>• Hacking windows</li> <li>• Wireless hacking</li> <li>• Evading firewall// ids and honeypots</li> <li>• Web application attacks</li> <li>• Cloud computing – IOT hacking</li> </ul>