CIT 285: Ethical Hacking

This course is an introduction to hacking tools, techniques, and incident handling. Areas of instruction include an evolution of hacking and penetration testing; the basics of cryptology for information security; foot printing; vulnerability scanning and exploit; wireless, web, and database attacks; malware and system exploit; traffic analysis; incident response; and defensive technologies and controls. In this course, the students will learn how to discover vulnerabilities, how to attack and defend systems, how to respond to attacks, and how to identify and design controls to prevent future attacks. This course prepares students to pass the EC-Council Certified Ethical Hacker certification exam. Pre or co-requisites: CIS 115, or permission of the instructor. Three lecture hours per week. Instructional Support Fee applies. Gen. Ed. Competencies Met: Critical Thinking, Ethical Dimensions, Information Literacy, and Scientific Reasoning and Discovery.

Course Student Learning Outcomes

1. Explain the history and current state of hacking and penetration testing, including ethical and legal implications. 2. Describe fundamental TCP/IP concepts, networking technologies, and their known vulnerabilities. 3. Identify common information-gathering tools and techniques to stage system attacks. 4. Identify security controls and defensive technologies to mitigate common types of malware, threats, and vulnerabilities exploited by hackers. 5. Perform system hacking, web attacks, and database attacks against IT systems. 6. Perform network traffic analysis, sniffing, and incident handling using appropriate tools and methods

Credits: 3

Program: Computer Information Technology