## **CYBR 467: Ethical Hacking (3 credits)**

This Ethical Hacking course introduces students to the principles and practices of ethical hacking, starting with an overview of the field and its significance in cybersecurity. Key topics include Footprinting, Reconnaissance, Network Scanning, Enumeration, and System Hacking, with practical insights into Sniffing, Social Engineering, and Denial-of-Service attacks. Advanced modules cover Evading IDS, Firewalls, Honeypots, Hacking Web Applications, SQL Injections, and Wireless Network vulnerabilities.  ***(****Prerequisite****:*** *CYBR 362****)***

**Course Learning Outcomes:**

By the end of the course, students will be able to:

A1. Demonstrate critical knowledge and understanding in various ethical hacking areas.

A2. Apply appropriate specialized ethical hacking methods, practices, techniques, tools, and strategies in diverse complex cybersecurity scenarios.

B1. Critically analyze information and concepts within complex ethical hacking scenarios, including the critical analysis of system vulnerabilities.

B2. Effectively communicate findings in ethical hacking investigations through comprehensive formal reports or presentations, highlighting potential security breaches and mitigation strategies.

**Course Learning Materials:**

* The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy by Patrick Engebretson (2013).
* Ethical Hacking: A Comprehensive Beginner's Guide to Learn and Master Ethical Hacking by Jack Jones (2020).
* CEH Certified Ethical Hacker All-in-One Exam Guide, Fourth Edition by Matt Walker (2019).

**Course Content:**

1. Introduction to ethical hacking
2. Footprinting and reconnaissance
3. Scanning networks
4. Enumeration
5. System hacking
6. Sniffing
7. Malware threats
8. Social engineering
9. Denial of service attacks
10. Evading IDS, Firewalls, and Honeypots
11. Hacking Web and Applications
12. SQL Injections
13. Session hijacking
14. Hacking web servers and applications