UE19CSXXX: ETHICALHACKING
(2-0-0-2-2)

Course Introduction: This course will allow students to learn about ethical hacking, students are expected to be very hands on and they will have opportunity to learn and use industry leading tools.

Course Objectives:

- Understand various cyber threats and Vulnerabilities.
- Understand and apply various security tools and techniques.
- Understand the concept of Ethical hacking.

Course Outcomes:

At the end of this course, the student will be able to:

- Be able to Identify potential cyber threats and vulnerability.
- Be able to use appropriate tools to exploit the vulnerabilities.
- Be able to prepare a comprehensive report and present the finding.

Pre-Requisite: Students should have strong foundation in Computer network security, Software security, Cryptography, Web security. Students should be interested in doing hands on.

Course Content:

Unit 1:

Introduction to ethical hacking, basic concepts – network, protocols.

6 Hours

Unit 2:

Usage of tools eg – Wireshark, Nmap, Nessus, DNS and email security

6 Hours

Unit 3:

Cryptography, Steganography application

5 Hours

Unit 4:

Password cracking, phishing attack, malware, wifi hacking, D - Dos

5 Hours

Unit 5:

Web application security – using kali, metas, burp

6 Hours

- Giving hands on experience for relevant topics in the form of Lab or Assignment

- Relevant cyber security Case for undergraduate students are discussed.

Tools/ Languages: Kali, Metasploit, Wireshark, burp suite, aircrack-ng, Hashcat, steghide, exiftool, pyton, Nessus,nmap, sqlmap, owasp Zap.

Text Book:
1: No prescribed text book

Reference Book(s):
1: No text book