

Subject Code	Subject Name	Credits
26CS103	ETHICAL HACKING	4

Course Objectives:

1. To understand and analyse Information security threats and counter measures
2. To perform security auditing & testing
3. To understand issues relating to ethical hacking

Learning Objectives:

On successful completion of the course, students will be able to:

1. To study & employ network defense measures

Unit 1 - Overview(12 hrs.):

Programming Overview – Exploitation – Cryptology – Social Engineering – Software Vulnerabilities – Malware – Firewalls – Virus

Unit 2 - Types of Hacking (12 hrs.):

How Hackers Hack – Hacking Windows – Wireless Hacking – Network Hacking – Web Hacking – Password Hacking

Unit 3 - Types of Cyber Attacks (12 hrs.):

Input Validation Attacks – Buffer Overflow Attacks – Privacy Attacks – Denial of Service Attacks – IoT Attacks

Unit 4 - Prevention and Ethics (12 hrs.):

Penetration Testing – Secure OS – Hacker Code of Ethics

Unit 5 - Cyber Threats (12 hrs.):

Cyber War – Cyber Terror – Cyber Crime

Reference Books:

1. Hacking: Digital Media and Technological Determinism By Tim Jordan
2. An Unofficial Guide to Ethical Hacking By Ankit Fadia
3. Hacking the Hacker: Learn From the Experts Who Take Down Hackers By Roger A. Grimes
4. Hacking, 2nd Edition: The Art of Exploitation By Jon Erickson
5. Hacking: Be a Hacker with Ethics By Harsh Bothra

