ETHICAL HACKING
(NEW SYLLABUS)

Credits : 3 **Semester: V**
Course Code : CE21502 **No. of Lecture Hours: 45**

Objectives:

- To get familiarize with the essential terms in Hacking and Various phases of attacks
- To provide the details on Law and Punishment for Hacking.
- To explain the maintenance of access gained through hacking and the techniques used to avoid the traces of attacks in order to escape from the legal Punishment by a malicious hacker

Course Outcomes:
CO1: **Explain** essential terminology and phases of hacking
CO2: **Analyze** how to perform reconnaissance in various organizations
CO3: **Identify** different types of scanning methods
CO4: **Explain** the maintenance of access gained through hacking
CO5: **Design** techniques used to avoid the traces of attacks in order to escape from the legal Punishment by a malicious hacker.

UNIT – I		**9Hrs**
1.	Ethical Hacking concepts and essential terminology	2
2.	Different phases involved in an exploit by a Hacker	2
3.	Overview of Attacks and Identification of Exploit Categories	2
4.	Legal implications of Hacking.	1
5.	Hacking, Law and Punishment	2

UNIT-II		**9Hrs**
1.	Essential Terms : Threat, Vulnerability and Attack	2
2.	Elements of Security : Reconnaissance, Active & Passive reconnaissance	2
3.	Foot printing, Internet Foot printing: Determining the scope of your activities	2
4.	Get Proper Authorization and Publicly Available Information	1
5.	DNS Interrogation and Network Reconnaissance	2

UNIT-III		**9Hrs**
1.	Scanning :Network Ping Sweeps, Determine which services are running, Scan types	2
2.	Identifying TCP and UDP services Running, Unix/Linux-based Port Scanning Strobe	2
3.	UDP_scan , Netcat Windows-based port scanners WUPS	2
4.	Detecting the Operating system, Active stack Fingerprinting, Passive stack fingerprinting	2
5.	Passive Signatures, Basic Banner Grabbing: Telnet and Netcat	1

UNIT-IV	**9Hrs**
1. Gaining Access, Hacking Windows, Privilege Escalation	2
2. Extracting and Cracking Passwords, Grabbing the Password Hashes	2
3. Dumping Cached Passwords, Remote Control and Back doors,	1
4. Command-line Remote control Tools, Port Redirection:Fpipe	2
5. Data-Driven Attacks, Buffer Overflow Attacks, DNS Cache Poisoning	2

UNIT-V	**9Hrs**
1. Trojans, Social Engineering and Maintaining Access	1
2. Rootkits and Back Doors, Kernel Modification, File/Directory hiding	2
3. Process Hiding, port hiding, Registry Key/value Hiding, User/group hiding	2
4. Keystroke Loggers ,service hiding and hacker defender, Bots and Zombies	2
5. Covering Tracks, Disabling Auditing, Clearing Event Log, Log clearing in UNIX	2

ESSENTIAL READING

1. Mc Clure, Stuart, Scambray, Joel and Kurtz, George. 2009. **Hacking Exposed.**7thEdition.New Delhi: McGraw Hill.

SUGGESTED READING

1. Engerbrestson, Patrick. 2011.**Basics of Hacking and Penetration**.Syngress
2. Walker, Matt.2012. C**ertified Ethical Hacker All-in-One**.McGraw Hill.