Program : **Diploma in Computer Engineering / Information Technology**	
Course Code : **5133B**	Course Title: **Ethical Hacking**
Semester : **5 / 5**	Credits: **4**
Course Category: **Program Elective**	
Periods per week: **4 (L:4 T:0 P:0)**	Periods per semester: **60**

Course Objective:

- Impart the concepts in ethical hacking.
- Introduce various network and system attacks, countermeasures and tools involved.
- Provide knowledge about current security issues in computer networks.

Course Prerequisites:

Topic	Course code	Course name	Semester
Digital fundamentals		Digital Computer Fundamentals	3
Basic programming concepts		Programming in C	3

Course Outcomes :

On completion of the course, the student will be able to:

COn	Description	Duration (Hours)	Cognitive Level
CO1	Summarize the concepts of hacking, Malwares, Network attacks and counter measures.	14	Understanding
CO2	Demonstrate foot printing and port scanning techniques using simple tools.	16	Understanding
CO3	Summarize operating systems and web Application Vulnerabilities.	15	Understanding
CO4	Outline counter measures for web application and wireless hacking	13	Understanding
	Series Test	2	

CO – PO Mapping

Course Outcomes	PO1	PO2	PO3	PO4	PO5	PO6	PO7
CO1	2				2		
CO2	2				2		
CO3	2				2		
CO4	2				2		

3-Strongly mapped, 2-Moderately mapped, 1-Weakly mapped

Course Outline

Module Outcomes	Description	Duration (Hours)	Cognitive Level
CO1	**Summarize the concepts of hacking, Malwares, Network attacks and counter measures.**		
M1.01	Describe the concepts of Hacking and Ethical Hacking.	2	Understanding.
M1.02	Identify various ethical issues related to hacking	2	Understanding
M1.03	Classify different malwares, their actions and methods for protection.	4	Understanding.
M1.04	Summarize Network attacks	4	Understanding
M1.05	Explain Counter measures for Network attacks	2	Understanding
Contents: Current security issues, Definition of hacking, ethical hacking and need. hacking-ethical issues, Penetration testing Malicious software – Viruses and types, Worms, Trojans programs, Spyware, Adware, protection methods, CIA triad, Network and system attacks - Denial of Service (DoS), Distributed Denial of Service (DDoS), Buffer overflow, Ping of death, Session Hijacking, Brute force attack, Man-in-the middle attack, Dictionary attack, Replay attack.			
CO2	**Demonstrate foot printing and port scanning techniques using simple tools**		
M2.01	Demonstrate foot printing and tools used for it	3	Applying
M2.02	Explain competitive intelligence methods	3	Understanding
M2.03	Illustrate Social Engineering Methods	4	Understanding

M2.04	Demonstrate port scanning, methods and tools	6	Applying
	Series Test – I	1	

Contents:

Foot printing - Web tools used for foot printing, Competitive intelligence-methods , DNS zone transfer - Social engineering - Shoulder surfing, Dumpster diving, Piggy backing, Phishing - Port scanning - Types of port scans, Port scanning tools - Nmap, Nessus, Ping sweeps and tools - Crafting IP packets & spoofing

CO3	**Summarize Operating systems and web Application Vulnerabilities.**		
M3.01	Summarize windows Vulnerable components	6	Understanding
M3.02	Explain methods for hardening windows	3	Understanding
M3.03	Summarize Linux OS vulnerabilities	3	Understanding
M3.04	Describe counter measures against Linux attacks	3	Understanding

Content:

Vulnerabilities in Windows, Linux Os, counter measures :

Windows vulnerable components - Windows file system, Windows RPC, NetBIOS, Server Message Block, common Internet File System, Null sessions, Web Services, Tools for identifying Windows vulnerabilities, Windows passwords and authentication, Hardening Windows systems, Linux OS vulnerabilities - Tools for identifying Linux vulnerabilities, Countermeasures against Linux attacks.

CO4	**Outline counter measures for web application and wireless hacking.**		
M4.01	Summarize web application and components	3	Understanding
M4.02	Explain web application vulnerabilities and counter measures	5	Understanding
M4.03	List wireless network components and its use	2	Understanding
M4.04	Summarize the counter measures for wireless attacks	3	Understanding
	Series Test – II	1	

Content :

Web server hacking - Web applications and their components - Web application vulnerabilities and countermeasures - Tools for web attackers and hackers Wireless hacking - Wireless network technology - Components of a wireless network – War driving - Tools for wireless hacking - Countermeasures against wireless attacks.

Text / Reference

T/R	Book Title/Author
T1	**Hands on Ethical Hacking and Network Defense**, 2nd Edition, Michael T Simpson, Kent Back man, James Coreley
R1	**Data and Computer Communications**- W. Stallings
R2	**Cryptography and Network Security: Principles and Practice**- W. Stallings

Online Resources

Sl.No	Website Link
1	http://uou.ac.in/foundation-course - Introduction to cyber security