22CSH402	ETHICAL HACKING	Semester	
PREREQUISITES	Category	PE	Credit 3

	Hours/Week	L	T	P	TH
		3	0	0	3

Course Learning Objectives

1	To understand the basics of computer based vulnerabilities.
2	To explore different foot printing, reconnaissance and scanning methods.
3	To expose the enumeration and vulnerability analysis methods.
4	To understand hacking options available in Web and wireless applications
5	To explore the options for network protection.
6	To practice tools to perform ethical hacking to expose the vulnerabilities.

UNIT I	INTRODUCTION	9	0	0	9

Ethical Hacking Overview - Role of Security and Penetration Testers .- Penetration-Testing Methodologies- Laws of the Land - Overview of TCP/IP- The Application Layer - The Transport Layer - The Internet Layer - IP Addressing .- Network and Computer Attacks - Malware – Protecting Against Malware Attacks.- Intruder Attacks - Addressing Physical Security

UNIT II	FOOT PRINTING, RECONNAISSANCE AND SCANNING NETWORKS	9	0	0	9

Footprinting Concepts - Footprinting through Search Engines, Web Services, Social Networking Sites, Website, Email - Competitive Intelligence - Footprinting through Social Engineering - Footprinting Tools - Network Scanning Concepts - Port-Scanning Tools - Scanning Techniques - Scanning Beyond IDS and Firewall

UNIT III	ENUMERATION AND VULNERABILITY ANALYSIS	9	0	0	9

Enumeration Concepts - NetBIOS Enumeration – SNMP, LDAP, NTP, SMTP and DNS Enumeration - Vulnerability Assessment Concepts - Desktop and Server OS Vulnerabilities - Windows OS Vulnerabilities - Tools for Identifying Vulnerabilities in Windows- Linux OS Vulnerabilities- Vulnerabilities of Embedded Oss

UNIT IV	SYSTEM HACKING	9	0	0	9

Hacking Web Servers - Web Application Components- Vulnerabilities - Tools for Web Attackers and Security Testers Hacking Wireless Networks - Components of a Wireless Network – Wardriving- Wireless Hacking - Tools of the Trade

UNIT V	NETWORK PROTECTION SYSTEMS	9	0	0	9

Access Control Lists. - Cisco Adaptive Security Appliance Firewall - Configuration and Risk Analysis Tools for Firewalls and Routers - Intrusion Detection and Prevention Systems - Network-Based and Host-Based IDSs and IPSs - Web Filtering - Security Incident Response Teams – Honeypots.

Total (45 L) =45 Periods

Text Books:

1	Michael T. Simpson, Kent Backman, and James E. Corley, Hands-On Ethical Hacking and Network Defense, Course Technology, Delmar Cengage Learning, 2010.
2	The Basics of Hacking and Penetration Testing - Patrick Engebretson, SYNGRESS, Elsevier, 2013.
3	The Web Application Hacker′s Handbook: Finding and Exploiting Security Flaws, Dafydd Stuttard and Marcus Pinto, 2011.

Reference Books:	
1	Black Hat Python: Python Programming for Hackers and Pentesters, Justin Seitz , 2014

Course Outcomes: Upon completion of this course, the students will be able to:		**Bloom's Taxonomy Level**
CO1	To express knowledge on basics of computer based vulnerabilities.	L1
CO2	To gain understanding on different foot printing, reconnaissance and scanning methods	L2
CO3	To demonstrate the enumeration and vulnerability analysis methods.	L1
CO4	To gain knowledge on hacking options available in Web and wireless applications.	L2
CO5	To acquire knowledge on the options for network protection	L1
	To use tools to perform ethical hacking to expose the vulnerabilities	L3

COURSE ARTICULATION MATRIX

COs/POs	**PO1**	**PO2**	**PO3**	**PO4**	**PO5**	**PO6**	**PO7**	**PO8**	**PO9**	**PO10**	**PO11**	**PO12**	**PSO1**	**PSO2**
CO 1	2	2	3	2	1	-	-	-	1	2	2	1	2	2
CO 2	1	2	1	2	1	-	-	-	2	2	1	1	2	2
CO 3	2	2	3	3	1	-	-	-	1	2	1	2	2	2
CO 4	2	1	1	2	1	-	-	-	1	3	3	3	2	2
CO 5	2	3	1	1	2	-	-	-	2	1	1	1	2	2
Avg	**1.8**	**2**	**1.8**	**2**	**1.2**	**-**	**-**	**-**	**1.4**	**2**	**1.6**	**1.6**	**2**	**2**

3 / 2 /1 - indicates strength of correlation (3- High, 2- Medium, 1- Low)