19CSE335	ETHICAL HACKING	L-T-P-C: 3-0-0-3

Pre-Requisite(s):19MAT115 Discrete Mathematics, 19CSE102 Computer Programming, **19CSE331** Cryptography

Course Objectives

- This course introduces the concepts of Ethical Hacking and gives opportunity to learn about different tools and techniques in Ethical hacking and security.

Course Outcomes

CO1: Understand and apply the core concepts related to malware and software vulnerabilities and their causes
CO2: Appreciate the Cyber Laws and ethics behind hacking and vulnerability disclosure
CO3: Exploit the vulnerabilities related to data and storage systems using state of the art tools and technologies
CO4: Exploit the vulnerabilities related to computer system and networks using state of the art tools and technologies

CO-PO Mapping

PO/ PSO / CO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2
CO1	1	1	1										3	2
CO2	1	2	2	1									3	2
CO3	1	2	2	2	2			2					3	2
CO4	3	3	2	2	2	2		2					3	2

Syllabus

Unit 1
Introduction: Understanding the importance of security, Concept of ethical hacking and essential Terminologies- Threat, Attack, Vulnerabilities, Target of Evaluation, Exploit.

Unit 2
Phases involved in hacking: Foot printing, Scanning, System Hacking, Session Hijacking. Buffer Overflows: Significance of Buffer Overflow Vulnerability, Why Programs/Applications are vulnerable. Reasons for Buffer Overflow Attacks. Methods of ensuring that buffer overflows are trapped. Sniffers: Active and passive sniffing. ARP poisoning and countermeasures. Man in the middle attacks, Spoofing and Sniffing attacks. Sniffing countermeasures. SQL Injection: Attacking SQL Servers, Sniffing, Brute Forcing and finding Application Configuration Files, Input validation attacks. Preventive Measures. Web Application Threats, Web Application Hacking, Cross Site Scripting / XSS Flaws / Countermeasures Correct Web Application Set-up.

Unit 3
Web Application Security: Core Defence Mechanisms. Handling User Access, Authentication, Session Management, Access Control. Web Application Technologies: HTTP Protocol, Requests, Responses and Methods. Encoding schemes. Server side functionality technologies (Java, ASP, PHP). Attacking Authentication: Attacking Session Management, Design Flaws in Authentication Mechanisms Attacking Forgotten Password Functionality, attacking Password change functions. Countermeasures to authentication attacks. Attacking other users: Reflected XSS Vulnerabilities, Stored XSS Vulnerabilities, DOM-Based XSS Vulnerabilities, HTTP Header Injection. Countermeasures to XSS.

Text Book(s)

Patrick Engebretson. The Basics of Hacking and Penetration Testing, Elsevier; 2013.
Graves K. Ceh: Official certified ethical hacker review guide: Exam 312-50. John Wiley & Sons; 2007..

Reference(s)

Ali S, Heriyanto T. BackTrack 4: Assuring Security by Penetration Testing: Master the Art of Penetration Testing with BackTrack. Packt Publishing Ltd; 2011 Apr 14.
Khare R. Network Security and Ethical Hacking. Luniver Press; 2006.

Evaluation Pattern:

Assessment	Internal	External
Periodical 1 (P1)	15	
Periodical 2 (P2)	15	
*Continuous Assessment (CA)	20	
End Semester		50

*CA – Can be Quizzes, Assignment, Projects, and Reports