CAP794:VULNERABILITY ASSESSMENT AND PENETRATION TESTING

Course Outcomes: Through this course students should be able to

CO1 :: understand the basic concept, fundamentals and practice of penetration testing

CO2 :: apply the working of hacking and cracking techniques, know vulnerabilities in existing software's

CO3 :: analyze legal and illegal techniques used by hackers and their counter measures

CO4 :: evaluate different and specific types of assaults and spoofing techinques

Unit I

Introduction to Vulnerability : computer security, Types of threats, Types of attack, Vulnerabilities, Major mail vulnerability, Server application vulnerabilities, Browser based vulnerabilities, Web application vulnerabilities, Web server vulnerabilities, Windows vulnerabilities

Unit II

Vulnerability Assessment : Incomplete mediation vulnerability, Race condition vulnerability, Time-to-check or time-to-use vulnerability, Undocumented access point vulnerability, Countermeasure, Malicious code attack, Malware, Voluntary introduction vulnerability, Unlimited privilege vulnerability countermeasure using detection tools

Unit III

Keys Vulnerability and Countermeasure : Key-logging attack, Data access threat, Data and reputation harm, Physical access vulnerability, Misplaced trust vulnerability, Insider's vulnerability, Weak authentication vulnerabilities, Countermeasure

Unit IV

Introduction to Penetration Testing : Impact of unethical hacking, Hacker communities, Introduction to reconnaissance, Social engineering, Dumpster diving, Internet foot-printing, Introduction to scanning, Types of scanning, Sniffer types, Sniffer operation, Sniffer program, Sniffer detection, Protecting against sniffer

Unit V

Encryption and Password Cracking : Introduction to Symmetric and asymmetric key encryption, decryption,Descriptions of popular ciphers, Attack on passwords, Password crackers Denial of Service Attack: Causes of DoS attack, Types of DoS attacks, Known DoS and DDoS attack

Unit VI

Spoofing and Session Hijacking : The process of IP spoofing attack, Types of spoofing, Spoofing tools, Prevention and mitigation, TCP session hijacking, Session hijacking tools, UDP hijacking, Prevention of session hijacking

Text Books:

1. COMPUTER SECURITY AND PENETRATION TESTING by ALFRED BASTA, NADINE BASTA AND MARY BRROWN, CENGAGE LEARNING, CENGAGE LEARNING

References:

1. ANALYZING COMPUTER SECURITY by CHARLES P. PFLEEGER SHARI LAWRENCE PFLEEGER, PEARSON