CAP795:VULNERABILITY ASSESSMENT AND PENETRATION TESTING-LABORATORY

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 techniques.

List of Practicals / Experiments:

Vulnerability Assessment:

- •Vulnerabilities
- •Major mail vulnerability
- •Server application vulnerabilities
- •Browser based vulnerabilities
- •Web application vulnerabilities
- •Web server vulnerabilities
- •Windows vulnerabilities

Spoofing:

- •IP spoofing attack,
- •Spoofing tools

Sniffing and Scaning:

- •Sniffing the packet through wireshark
- •Scanning through nmap/zenmap
- •Port scanning
- •Host scanning
- •Scanning target to attack

Introduction to Penetration Testing:

- •Internet foot-printing
- •Sniffer operation
- •Sniffer program
- •Sniffer detection
- •Protecting against sniffer

Encryption and Password Cracking:

- •Symmetric and asymmetric key encryption
- •Descriptions of popular ciphers
- •Attack on passwords
- •Password crackers

Denial of Service Attack:

- •To demonstrate the causes of DoS attack
- •To demonstrate different types of DoS attacks

Text Books:

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

References:

References:

1. ANALYZING COMPUTER SECURITY by CHARLES P. PFLEEGER, SHARI LAWRENCE PFLEEGER, Pearson Education India