INT244:SECURING COMPUTING SYSTEMS

L:0 T:0 P:4 Credits:3

Course Outcomes: Through this course students should be able to

- identify the basic concept, fundamentals and practice of penetration testing
- analyze various vulnerabilities and security flaws in the operating systems, web servers, network equipment's and to be able to patch them
- distinguish and compare legal and illegal techniques used by hackers, specific types of attacks and their countermeasures

Unit I

Introduction to Ethical Hacking : Hacking Evolution, What Is an Ethical Hacker?, Ethical hacking and Penetration testing, Hacking methodologies

System Fundamentals : Fundamental of computer networks, Exploring TCP/IP ports, Understanding network devices, Proxies, Firewall and Network Security, Knowing Operating Systems(Windows, Mac, Android and Linux)

Cryptography : History of cryptography, Symmetric cryptography, Asymmetric cryptography, Understanding Hashing, Issues with cryptography, Application of cryptography(IPsec, PGP, SSl)

Unit II

Footprinting : What is Footprinting, Threats Introduced by Footprinting, The Footprinting process, Using (Search engine, Google hacking, Social networking and Financial services) Information gathering

Scanning : What is Scanning, Types of Scans, Family tree of Scans, OS fingerprinting, Countermeasure, Vulnerability Scanning and Using Proxies

Unit III

Enumeration : What is Enumeration, Windows Enumeration, Enumeration with SNMP, LDAP and Directory Service Enumeration, SMTP Enumeration

System Hacking : What is System Hacking, Password cracking, Authentication on Microsoft Platforms, Executing Applications

Malware : Malware and the law, Categories of Malware(Viruses, worms, spyware, Adware, Scareware Ransomware and Trojans), Overt and Covert Channels

Unit IV

Sniffers : Understanding Sniffers, Using a Sniffer, Switched network Sniffing, MAC Flooding, ARP Poisoning, MAC Spoofing, Port Mirror and SPAN Port, Detecting Sniffing Attacks

Social Engineering : What is Social Enginnering, Social Engineering Phases, Commonly Employed Threats, Identity Theft

Denial of Service : Understanding DoS, Understanding DDoS, DoS Tools, DDoS Tools, DoS Pen-Testing Considerations

Unit V

Session Hijacking : Understanding Session Hijacking, Exploring Defensive Strategies, Network Session Hijacking

Web Servers and Applications : Exploring the Client-Server Relationship, The client and the server, Vulnerabilities of Web Servers and Application, Testing Web Application

SQL Injection : Introducing SQL Injection, Databases and Their Vulnerabilities, Anatomy of a SQL Injection Attack, Altering Data with a SQL Injection Attack, Evading Detection Mechanisms, SQL Injection Countermeasures

Unit VI

Hacking Wi-Fi and Bluetooth : What Is a Wireless Network, A Close Examination of Threats, Hacking Bluetooth

Mobile Device Security : Mobile OS Models and Architectures, Goals of Mobile Security, Device Security Models, Countermeasures

Cloud Technologies and Security : What Is the Cloud, Threats to Cloud Security, Cloud Computing Attacks, Testing Security in the Cloud

Text Books:

1. CEH V9: CERTIFIED ETHICAL HACKER - VERSION 9 STUDY GUIDE by SEAN-PHILIP ORIYANO, SYBEX

References:

1. MASTERING KALI LINUX FOR ADVANCED PENETRATION TESTING by VIJAY KUMAR VELU, PACKT PUBLISHING