INT244:SECURING COMPUTING SYSTEMS

L:2 T:0 P:2 Credits:3

Course Outcomes: Through this course students should be able to

CO1 :: describe the basic concepts of operating systems, cryptography and ethical hacking

CO2 :: discuss various methods of performing footprinting and scanning the target systems

CO3 :: illustrate the process of enumerating and compromising a target system

CO4 :: examine the usage of sniffers, social engineering techniques and denial of service attacks for compromising the target

CO5 :: analyze the functionality of session hijacking, web applications and SQL injection in testing the security of target

CO6 :: understand the process of identifying the threats to WiFi, Bluetooth, mobile devices, cloud services and SOC and SIEM solutions

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, Introduction to SIEM and SOC Solutions

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

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

List of Practicals / Experiments:

List of practical's/ experiment

- Foot-printing: Demonstration of the process of active and active and passive information gathering using search engines, GHDB and Netcraft
- Scanning: Demonstration of port, network and vulnerability scanning with the help of Nmap, Nessus and Rapid7 and AngryIP
- Enumeration: Demonstration of windows, Linux enumeration and network protocol enumeration with the help of inbuilt utilities and open-source tools
- System Hacking: Demonstration of offline and online password cracking with the help of dictionary, brute force and hybrid attack and generating rainbow tables
- Sniffing: Demonstration of network sniffing with the help of packet sniffers such as Wireshark, Tcpdump and Dsniff and understand the data that is being sniffed by the respective tools
- Denial of Service: Demonstration of various Dos attacks such as Service Request Floods, ICMP Flooding, Smurf and Fraggle Attacks using different tools
- SQL Injection: Demonstration of various types of SQL injection with the help of different tools

Text Books:

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

References:

1. CERTIFIED ETHICAL HACKER (CEH) V11 312-50 EXAM GUIDE by DALE MEREDITH, PACKT PUBLISHING