INT245:PENETRATION TESTING

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

Course Outcomes: Through this course students should be able to

CO1 :: understand rules of engagement safely conducting the penetration testing exercise within an organization

CO2 :: identify various footprinting techniques to enumerate a target

CO3 :: apply a vulnerability scan strategy to detect, analyze and craft network traffic

CO4 :: demonstrate web application and mobile device exploitation using different attacks

CO5 :: explain different techniques use to conduct system hacking and launch exploit code to get remote access of a target

CO6 :: analyze different testing deliverables out of penetration testing reports and suggest post corrective actions

Unit I

Planning and Scoping : Introduction to penetration testing concepts, types of penetration testing, phases of penetration testing, Organizational pentesting,compliance requirements,pentesting standards, environmental considerations,rules of engagement

Unit II

Footprinting and Gathering Intelligence : discover a target, gather essential data, website information gathering, Information gathering, types of information gathering, open source intelligence (OSINT)

Human and Physical Vulnerabilities : exploiting human pysche, physical attacks,Social engineering

Unit III

Vulnerability Scan : scanning logical vulnerabilities,analyze scanning results,evade detection and covering tracks, Scanning tools, types of scans

Unit IV

Web Application Exploitation : OWASP top 10 vulnerabilities, session hijacking, Crafting Request Forgery attacks, SQL injection, identifying SQLi vulnerabilities, cross-site scripting (XSS) attacks, exploiting browser

Mobile Device Exploitation : Deployment Models, identifying vulnerabilities, attacks on mobile devices, social engineering attacks, hacking Bluetooth signal, exploiting with malware

Unit V

System Hacking and Post Exploitation : System hacking, password cracking, remote access tools, analyse exploit code, enumerating users and assets, reverse engineering, automating tasks using scripting, privilege escalation in windows and linux, maintaining persistence

Unit VI

Communication and Reporting : Communication path, communication triggers, reporting tools, identify report audience, report content, presentation of findings, define best practices for reports, recommending remediation, performing post-report delivery activities

List of Practicals / Experiments:

Gathering Information

- Gathering information using tools like theHarvester,
- Recon-ng
- Maltego
- FOCA
- shodan

Network discovery and security auditing

- Basic commands of Nmap

- Performing host and network scan using NSE scripts

Vulnerability-Scanning

- Assessing system and network vulnerabilities using vulnerability scanners like
- Nmap,Nikto and Nessus

Metasploit

- Introduction to the tool
- basic commands for searching, selection, parameter configurations and deployment of exploits
- Exploitation of Windows XP and windows 7

Password Cracking

- exploiting vulnerabilities using password cracking tools like hashcat
- john the ripper
- cain and abel

Web Application Penetration Testing

- Evaluating web application security using tools like OWASP ZAP (Zed Attack Proxy)
- Burpe Suite

Cross-Site-Scripting(XSS)

- Introduction to cross site scripting, identification of websites vulnerable to cross site scripting

XSS vulnerabilities-identification

- Identification of XSS vulnerabilities in the websites and the way they could be exploited

XSS-Exploitation

- Exploitation of XSS vulnerabilities using javascript

SQL Injection(SQLi)

- Introduction to SQL injection, Automated SQL injection using SQLmap

Manual SQL Injection(SQLi)

- Demonstration of manual SQL injection attacks

Text Books:

1. PENETRATION TESTING: A HANDS-ON INTRODUCTION TO HACKING by GEORGIA WEIDMAN, NO STARCH PRESS

References:

1. COMPTIA PENTEST+ STUDY GUIDE: EXAM PT0-002, 2ND EDITION by MIKE CHAPPLE, DAVID SEIDL, WILEY