Kore Infotech
Intelligent IT Solutions
Passionate People

Advanced Cyber Security

This intensive, hands-on course equips security practitioners with the tools, techniques and mindset needed to identify, exploit, and defend against modern threats. Over 40 hours you'll build a lab, perform reconnaissance, scanning and vulnerability analysis, execute and analyze system-level attacks (including malware, sniffing, session hijacking and privilege escalation), and practise countermeasures for social engineering, DoS/DDoS, web and cloud threats.

The curriculum covers defensive topics too — hardening web servers and applications, securing wireless and cloud environments, and evading/defeating organizational defences (IDS/IPS, firewalls, honeypots) so you understand attacker techniques and can design effective protections. Realistic labs, tool usage (OSINT, Shodan, scanners, exploitation utilities) and remediation workflows prepare you to assess, report and remediate risks in production-like environments.

Who Should Attend This Course:
IT professionals, system administrators, network engineers, and aspiring ethical hackers who want to advance their skills in identifying, exploiting, and defending against real-world cyber threats.

Pre-Requisites: Good understanding of Cyber Security Fundamentals is required.

Course Duration: This course will be conducted over a period of 5 Days (9.30 am to 5.30 pm)

Objectives:

1. Build and configure a secure lab environment (client/server VMs) for testing and analysis.
2. Explain core information security concepts, attack vectors and phases of an attack.
3. Conduct reconnaissance and footprinting (OSINT, Google Hacking, Shodan) and apply countermeasures.
4. Perform network scanning, live host discovery, port & service enumeration and OS/banner fingerprinting.
5. Enumerate services (NetBIOS, DNS etc.) and mitigate enumeration risks.
6. Run and analyze vulnerability scans and plan remediation for hosts, networks and virtual environments.
7. Demonstrate system-level attacks: password cracking, privilege escalation, code execution and evidence clearing.
8. Identify, analyze and defend against malware (viruses, worms, trojans, ransomware).
9. Detect and mitigate network sniffing attacks (ARP/DNS poisoning, MAC flooding, DHCP attacks).
10. Recognize social engineering techniques (phishing, impersonation) and implement practical countermeasures.
11. Understand DoS/DDoS attack methods and defensive strategies.
12. Explain session hijacking techniques for web and network clients and apply mitigation measures.
13. Describe how IDS/IPS, firewalls and honeypots work and how attackers attempt to evade them.
14. Identify and remediate common web server and web application vulnerabilities (including OWASP Top 10).
15. Assess cloud security fundamentals, risks and hardening techniques for cloud deployments.
16. Perform SQL injection testing (including blind and advanced techniques) and implement defenses.
17. Evaluate wireless security, attack methodologies (including Bluetooth) and apply wireless protection measures.

Kore Infotech
Intelligent IT Solutions
Passionate People

Course Content

1. **Understanding Security Attacks**
   - 1.1. How to Build a Lab for Security Tasks
   - 1.2. Installing and Configuring Client and Server VMs
   - 1.3. Information Security Overview
   - 1.4. Security Threats and Attack Vectors
   - 1.5. Attack Types, Concepts and Phases
   - 1.6. Information Security Controls

2. **Reconnaissance/Footprinting**
   - 2.1. What is Reconnaissance/ Footprinting?
   - 2.2. What to Look For?
   - 2.3. OSINT and Web spider
   - 2.4. Using Google Hacking and Shodan
   - 2.5. Reconnaissance Countermeasures

3. **Scanning Networks**
   - 3.1. Overview and Types of Scanning
   - 3.2. Finding "Live" Systems Open Ports
   - 3.3. Banner Grabbing and OS Fingerprinting
   - 3.4. Vulnerability Scanning and Drawing Out the Network
   - 3.5. Anomysing through Proxies and VPN

4. **Enumeration**
   - 4.1. What is Enumeration?
   - 4.2. Enumeration via Defaults & NetBIOS
   - 4.3. Enumeration via DNS
   - 4.4. Countermeasures for Enumeration

5. **Vulnerability Analysis**
   - 5.1. Incorporating Vulnerability Scans
   - 5.2. Analyzing Vulnerability Scans
   - 5.3. Remediating Host Vulnerabilities
   - 5.4. Remediating Network Vulnerabilities
   - 5.5. Remediating Virtual Environment Vulnerabilities

6. **System Hacking**
   - 6.1. Understanding System Security Attacks
   - 6.2. Phase 1: Cracking Passwords
   - 6.3. Phase 2: Escalating Privileges
   - 6.4. Phase 3: Executing Applications
   - 6.5. Phase 4: Clearing Logs and Evidence

7. **Malware**
   - 7.1. Introduction to Malware
   - 7.2. Types of Malwares
   - 7.3. Malware Infections
   - 7.4. Virus, Worms, Trojan and Ransomware
   - 7.5. Detecting Malware
   - 7.6. Countermeasures

8. **Sniffing**
   - 8.1. Sniffing
   - 8.2. DHCP Assaults
   - 8.3. MAC Flooding Attacks
   - 8.4. ARP Poisoning
   - 8.5. DNS Poisoning
   - 8.6. Countermeasures

9. **Social Engineering**
   - 9.1. What is Social Engineering?
   - 9.2. Phishing and Spear Phishing Attacks
   - 9.3. Identity Theft and Impersonation
   - 9.4. Sensitive Data Stealing
   - 9.5. Social Engineering Countermeasures

10. **DoS and DDoS**
    - 10.1. What is Denial of Service Attacks?
    - 10.2. Attacking Techniques
    - 10.3. Tools and Services
    - 10.4. Defending Against DoS Attacks

11. **Session Hijacking**
    - 11.1. Understanding Session Hijacking
    - 11.2. Hijacking Sessions in Web Applications
    - 11.3. Network and Client Level Session Hijacking
    - 11.4. Automating Session Hijack Attacks
    - 11.5. Mitigating the Risk of Session Hijacking

12. **Evading IDS, Firewalls, and Honeypots**
    - 12.1. Understanding Organizational Defenses
    - 12.2. Firewalls
    - 12.3. IDS and IPS
    - 12.4. Honeypots

13. Protecting Web Servers
- 13.1. OWASP Top 10
- 13.2. Understanding Web Servers Techniques
- 13.3. Discovering Risks in Web Servers
- 13.4. Web Server Misconfiguration
- 13.5. Managing and Hardening Web Servers

14. Protecting Web Applications
- 14.1. Attacking Web Applications
- 14.2. Tampering of Untrusted Data
- 14.3. Attacks Against Identity Management and Access Controls
- 14.4. Countermeasures

15. Cloud Security
- 15.1. Cloud Computing Concepts
- 15.2. Organizational Security Considerations
- 15.3. Cloud Computing Risks
- 15.4. Cloud Computing Security Strengths
- 15.5. Hardening the Cloud

16. Database Assessment
- 16.1. Why SQL Injection Matters?
- 16.2. The Mechanics of SQL Injection Attacks
- 16.3. Blind SQL Injection
- 16.4. Advanced SQL Injection Concepts
- 16.5. Automating Attacks
- 16.6. Defending Against Attacks

17. Wireless Network Protection
- 17.1. Insights into Wireless
- 17.2. Encryption in Wireless
- 17.3. Threats from Wireless
- 17.4. The Methodology of Attacking Wireless
- 17.5. Attacking Bluetooth