

Ethical Hacking

Duration: 5 Days

Description

Throughout the 5-day training, participants practically address the point of view of cyber attackers, the tools and techniques they use. At the end of this period, it is aimed to gain the knowledge and skills to detect and exploit the vulnerabilities of systems, networks and applications.

Delegates will learn

- Introduction to Ethical Hacking
- Gathering Information
- Vulnerability Detection
- System Security
- Network Security
- Threat Analysis and Risk Management
- Application Security
- Social Engineering Attacks

Outline

Introduction to Ethical Hacking

- Introduction to information security
- principles of information security
- Privacy
- integrity and accessibility triangle
- Challenges of security
- Types of cyber-attackers
- Integrated security approach
- Gradual security approach
- Infiltration testing methodologies
- Hacking cycle

Gathering Information

- System detection

- Whois queries
- DNS queries
- Finding targets
- Scan types
- Port scanning
- Google hacking
- Open source intelligence techniques
- Information gathering tools

Vulnerability Detection

- Determination of vulnerability at network level
- Determination of vulnerability at system level
- Determination of application vulnerabilities

System Security

- Password cracking attacks
- Vulnerability scanning tools
- Metasploit usage
- Other vulnerability/abuse detection methods
- Cache overflow attacks
- Malware
- DNS tunneling
- Ensuring system security
- Client firewall (host firewall/Host IPS)
- Antiviruses
- Patch management

Network Security

- Network principles
- Scanning networks
- Open ports
- Working protocols
- Monitoring network traffic
- Wireshark usage
- Vulnerability detection
- Local network attacks
- Firewalls
- IPS/IDS
- Secure network design

Threat Analysis and Risk Management

- Threat detection methods
- Risk management approach
- Assessment of technical impact
- Assessment of business impacts
- Determination of vulnerability management processes

Application Security

- Application structures
- Determination of attack points
- Tools to be used in tests
- OWASP Top 10
- OWASP test methodology
- Application test methodology
- Disengagement attacks
- Understanding of application architecture
- Source code analysis techniques

Social Engineering Attacks

- Social engineering principles
- Signs of social engineering attack
- Use of Social Engineering Toolkit
- Phishing attacks
- Information gathering techniques for social engineering

Prerequisites

There are no prerequisites