CONCEPT

Penetration Testing and Ethical Hacking: Scoping, Methodology and Reporting

21 – 25 June 2027
London - Central London four-star

Penetration Testing and Ethical Hacking: Scoping, Methodology and Reporting

Ref: 380_13385 **Date:** 21 – 25 June 2027 **Location:** London - Central London four-star **Fees:** 23000 SAR

Introduction:

Penetration testing and ethical hacking engagements often fail their purpose before a single probe is sent: scopes miss critical assets, written authorisation is vague, rules of engagement ignore production risk, and reports list scanner output without business-rated findings or a retest plan. This Core Concept course trains security engineers, blue-team staff and IT auditors to run and commission authorised penetration tests using PTES, the OWASP Web Security Testing Guide and NIST SP 800-115, working in an isolated lab. Participants build a Penetration Test Engagement Pack covering authorisation, scope, test plan, CVSS-rated report and retest record.

Course Objectives:

- Prepare written authorisation, scope boundaries and rules of engagement that protect both the tested organisation and the testing team
- Plan an engagement against the PTES phases and NIST SP 800-115 planning, discovery, attack and reporting stages, choosing black, grey or white box coverage
- Execute reconnaissance, vulnerability analysis and web application test cases from the OWASP Web Security Testing Guide in a controlled lab
- Assess network, directory service and privilege escalation exposure at concept level and record evidence to a defensible standard
- Rate findings with CVSS v4.0 and write an executive and technical penetration test report with remediation guidance
- Manage third-party penetration testing suppliers, verify remediation through retesting and close findings in a tracked register

Target Audience:

- Security engineers who carry out internal vulnerability assessments and authorised penetration tests
- Blue-team and SOC staff who validate detection and response against simulated attacker activity
- IT auditors who review penetration test scope, evidence and findings as part of assurance work
- Security managers who commission external testing suppliers and own the findings register
- Infrastructure and application owners who approve test windows and remediate reported weaknesses

Course Outline:

Day 1: Authorised Testing Foundations, Legal Boundaries and Engagement Scoping

- Penetration Test Versus Vulnerability Scan Versus Red Team Exercise: Purpose and Depth
- Written Authorisation Letter, Legal Boundaries and Tester Code of Conduct
- PTES Pre-engagement Interactions: Scope Questionnaire, Asset Inventory and Exclusions
- Rules of Engagement: Test Windows, Production Safeguards, Stop Conditions and Escalation Contacts
- Black Box, Grey Box and White Box Coverage Selection and Current-State Testing Maturity Review

Day 2: Testing Methodologies and the Engagement Test Plan

- PTES Seven Sections from Intelligence Gathering to Post Exploitation
- NIST SP 800-115 Planning, Discovery, Attack and Reporting Stages
- OWASP Web Security Testing Guide Categories and WSTG Test Identifiers
- OSSTMM Operational Security Metrics as a Comparative Methodology
- Engagement Test Plan Build: Methodology Mapping, Test Cases and Traceability Matrix

Day 3: Reconnaissance, Vulnerability Analysis and Web Application Test Cases

- Passive and Active Intelligence Gathering: Public Footprint, DNS Records and Service Enumeration with Nmap
- Vulnerability Analysis Workflow: Scanner Output Validation and False Positive Elimination
- Lab: WSTG Authentication, Authorisation and Session Management Test Cases on a Training Application
- Lab: WSTG Input Validation, Business Logic and API Test Cases on a Training Application
- Evidence Capture Standards: Timestamped Screenshots, Request Logs and Tester Activity Journal

Day 4: Network, Directory Service and Privilege Escalation Concepts, Evidence and Risk Rating

- Internal Network Segmentation Testing and Exposed Management Services Review
- Directory Service Attack Paths: Weak Delegation, Stale Accounts and Excessive Group Rights
- Privilege Escalation Categories on Windows and Linux Hosts and Their Configuration Root Causes
- Evidence Handling, Data Minimisation and Secure Disposal of Test Artefacts
- CVSS v4.0 Base, Threat and Supplemental Metrics Applied to Test Findings

Day 5: Reporting, Supplier Oversight, Retesting and the Engagement Pack

- Penetration Test Report Structure: Executive Summary, Attack Narrative and Technical Findings
- Lab: Findings Write-Up with CVSS-BTE Scores and Remediation Guidance
- Third-Party Testing Supplier Selection: CREST Accreditation, Tester Competence and Statement of Work Review
- Remediation Verification Retest Plan and Findings Register Closure Criteria
- Penetration Test Engagement Pack Assembly and Peer Challenge Review

Skills You Will Gain:

- Engagement Scoping
- Rules of Engagement Drafting
- Web Application Test Case Execution
- Attack Surface Reconnaissance
- Vulnerability Validation
- Test Evidence Management
- CVSS Finding Severity Scoring
- Testing Supplier Oversight

Why Attend This Course:

- Leave with a Penetration Test Engagement Pack containing an authorisation letter, scope and rules of engagement, test plan, CVSS-rated report and retest record
- Work through WSTG test cases hands on in an isolated lab application rather than reading about attack categories
- Challenge supplier proposals and reports with a clear view of what a defensible test should cover and evidence
- Compare testing and assurance practice with security engineers, SOC staff and auditors from banking, energy, government services and technology organisations

Conclusion:

An authorised penetration test is only as useful as its scope, evidence and follow-through. The week moves from legal authorisation, scoping and rules of engagement, through PTES, NIST SP 800-115 and the OWASP Web Security Testing Guide, to reconnaissance, vulnerability validation and web application test cases in a lab. It then covers network, directory service and privilege escalation concepts, evidence handling and CVSS v4.0 rating, and closes with report writing, supplier oversight, retesting and a Penetration Test Engagement Pack for each participant.