C|PENT V2 Exam Blueprint

EC-Council

Building A Culture Of Security

Domain	Sub Domain	No of Questions	Weightage
1. Penetration Testing Methodologies, Scoping, and Engagement	• Principles and Objectives of Penetration Testing • Penetration Testing Methodologies and Frameworks • Best Practices and Guidelines for Penetration Testing • Role of Artificial Intelligence in Penetration Testing • Role of Penetration Testing in Compliance with Laws, Acts, and Standards • Key Elements Required to Respond to Penetration Testing RFPs • Drafting Effective Rules of Engagement (ROE) • Legal and Regulatory Considerations Critical to Penetration Testing • Resources and Tools for Successful Penetration Testing • Strategies to Effectively Manage Scope Creep	7	13%
2. Information Gathering and Attack Surface Mapping	• Collecting Open-source Intelligence (OSINT) on Target's Domain Name • Collecting OSINT about Target Organization on the Web • Perform OSINT on Target's Employees • Open Source Intelligence (OSINT) using Automation Tools • Attack Surface Mapping • Social Engineering Penetration Testing Concepts • Off-Site Social Engineering Penetration Testing • On-Site Social Engineering Penetration Testing • Document Findings with Countermeasure Recommendations	7	13%
3. Web Application and API Penetration Testing	• Techniques to Evaluate Firewall Security Implementations • Techniques to Evaluate IDS Security Implementations • Techniques to Evaluate the Security of Routers • Techniques to Evaluate the Security of Switches	7	14%

4. Perimeter Defense Evasion Techniques	• Techniques to Evaluate Firewall Security Implementations • Techniques to Evaluate IDS Security Implementations • Techniques to Evaluate the Security of Routers • Techniques to Evaluate the Security of Switches	6	12%
5. Endpoint Exploitation, Privilege Escalation, and Lateral Movement	• Techniques to Perform Reconnaissance on a Windows Target • Techniques to Perform Vulnerability Assessment and Exploit Verification • Methods to Gain Initial Access to Windows Systems • Techniques to Perform Enumeration with User Privilege • Techniques to Perform Privilege Escalation • Post-Exploitation Activities • Architecture and Components of Active Directory • Active Directory Reconnaissance • Active Directory Enumeration • Exploit Identified Active Directory Vulnerabilities • Role of Artificial Intelligence in AD Penetration Testing Strategies • Linux Exploitation and Penetration Testing Methodologies • Linux Reconnaissance and Vulnerability Scanning • Techniques to Gain Initial Access to Linux Systems • Linux Privilege Escalation Techniques • Advanced Lateral Movement Techniques • Advanced Pivoting and Tunneling Techniques to Maintain Access	7	13%
6. Reverse Engineering and Binary Exploitation	• Concepts and Methodology for Analyzing Linux Binaries • Methodologies for Examining Windows Binaries • Buffer Overflow Attacks and Exploitation Methods • Concepts, Methodologies, and Tools for Application Fuzzing	6	11%

7. IoT Penetration Testing	• Fundamental Concepts of IoT Pen Testing • Information Gathering and Attack Surface Mapping • Analyze IoT Device Firmware • In-depth Analysis of IoT Software • Assess the Security of IoT Networks and Protocols • Post-Exploitation Strategies and Persistence Techniques • Comprehensive Pen Testing Reports	6	11%
8. Reporting and Post Testing Actions	• Purpose and Structure of a Penetration Testing Report • Essential Components of a Penetration Testing Report • Phases of a Pen Test Report Writing • Skills to Deliver a Penetration Testing Report Effectively • Post-Testing Actions for Organizations	7	13%