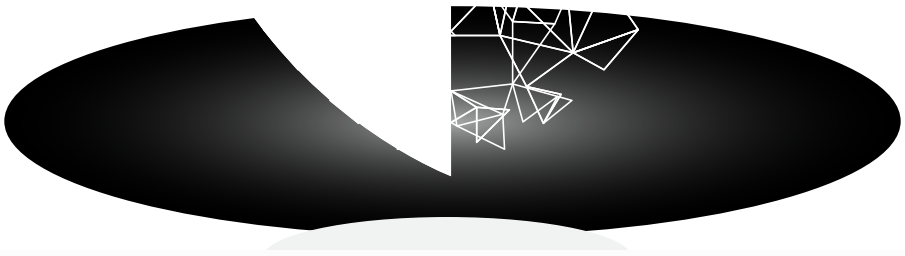
EC-Council



Certified Penetration Testing Professional (CPENT) Exam Blueprint v1

Certified Penetration Testing Professional

Exam Blueprint

(Version 1)

S. No.	Domain	Sub Domain	Domain %
1	Penetration Testing Methodologies, Scoping and Engagement	1.1 Overview of Penetration Testing	5%
		1.2 Penetration Testing Types	
		1.3 Penetration Testing Process	
		1.4 Penetration Testing Methodology	
		1.5 Ethics of a Penetration Tester	
		1.6 Collecting the Penetration Testing Requirements	
		1.7 Preparing Response Requirements for Proposal Submission	
		1.8 Drafting Timeline and Quote for Penetration Testing	
		1.9 Creating Rules of Engagement (ROE)	
		1.10 Estimating the Timeline for the Engagement	
		1.11 Identifying the Resources Required for the Penetration Testing	
		1.12 Handling Legal Issues in Penetration Testing Engagement	
		1.13 Preparing Penetration Testing Team	
		1.14 Preparing a Penetration Testing Test Plan	
		1.15 Obtaining Permissions for Penetration Testing	
		1.16 Handling Scope Creeping During Pen Testing	

2	Information Gathering	2.1 OSINT through World Wide Web (WWW)	7%
		2.2 OSINT through Website Analysis	
		2.3 OSINT through DNS Interrogation	
		2.4 OSINT Tools/Frameworks/Scripts	
		2.5 Social Engineering Penetration Testing Concepts	
		2.6 Social Engineering Penetration Testing using E-mail Attack Vector	
		2.7 Social Engineering Penetration Testing using Telephone Attack Vector	
		2.8 Social Engineering Penetration Testing using Physical Attack Vector	
		2.9 Creating a Social Engineering Penetration Testing Report	
3	Network Penetration Testing	3.1 Overview of External Penetration Testing	45%
		3.2 Port Scanning on Target	
		3.3 OS and Service Fingerprinting on Target	
		3.4 Conducting Vulnerability Research	
		3.5 Exploit Verification	
		3.6 Overview of Internal Penetration Testing	
		3.7 Footprinting on Internal Network	
		3.8 Network Scanning on Internal Network	
		3.9 OS and Service Fingerprinting on Internal Network	
		3.10 Various Enumeration Techniques for Internal Network	
		3.11 Vulnerability Assessment/ Scanning	
		3.12 Windows Exploitation	
		3.13 Unix/Linux Exploitation	
		3.14 Testing Interwork Network against Various Types of Attacks	
		3.15 Automating Internal Network Penetration Test Effort	
		3.16 Post Exploitation activities	

		3.17 Testing Interwork Network Using Advanced Tips and Techniques	
		3.18 Assessing Firewall Security Implementation	
		3.19 Assessing IDS Security Implementation	
		3.20 Assessing Security of Routers	
		3.21 Assessing Security of Switches	
4	Web Application Penetration Testing	4.1 Overview of Web Application Penetration Testing	16%
		4.2 Discovering Web Application Default Content	
		4.3 Discovering Web Application Hidden Content	
		4.4 Web Vulnerability Scanning	
		4.5 Testing for SQL Injection Vulnerabilities	
		4.6 Testing for XSS Vulnerabilities	
		4.7 Testing for Parameter Tampering	
		4.8 Testing for Weak Cryptography Vulnerabilities	
		4.9 Testing for Security Misconfiguration Vulnerabilities	
		4.10 Testing for Client-Side Attack	
		4.11 Testing for Broken the Authentication and Authorization Vulnerabilities	
		4.12 Testing for Broken Session Management Vulnerabilities	
		4.13 Testing for Web Services Vulnerabilities	
		4.14 Testing for Business Logic Flaws	
		4.15 Testing for Web Server Vulnerabilities	
		4.16 Testing for Thick Clients Vulnerabilities	
		4.17 Testing for Wordpress	
5	Wireless and IoT Penetration Testing	5.1 Overview of Wireless Penetration Testing	4%
		5.2 Wireless Local Area Network (WLAN) Penetration Testing	
		5.3 RFID Penetration Testing	
		5.4 NFC Penetration Testing	

		5.5 Understanding IoT Attacks and Threats	
		5.6 IoT Penetration Testing	
6	Industrial Controls and Cloud Penetration Testing	6.1 Understanding OT/SCADA Concepts	7%
		6.2 Overview of Modbus	
		6.3 ICS and SCADA Penetration Testing	
		6.4 Understanding Cloud Computing Security and Concerns	
		6.5 Understanding the Scope of Cloud Pen Testing	
		6.6 Cloud Penetration Testing	
		6.7 AWS Specific Penetration Testing	
		6.8 Azure Specific Penetration Testing	
		6.9 Google Cloud Platform Specific Penetration Testing	
7	Binary Analysis and Exploitation	7.1 Overview of Binary Coding Concepts	11%
		7.2 Understanding Binary Analysis Methodology	
8	Reporting and Post Testing Actions	8.1 Overview of Penetration Testing Report	5%
		8.2 Understanding the Different Phases of Report Development	
		8.3 Understanding various Components of Penetration Testing Report	
		8.4 Analyzing Penetration Testing Report	
		8.5 Overview of Penetration Testing Report Delivery	
		8.6 Understanding Post Testing Actions	