EC-Council

ECSA

EC-Council Certified Security Analyst

ECSA Exam Blueprint v2

S.No	Domain	Sub Domains	Weightage
1	**Penetration Testing Essential Concepts**	• Computer Network Fundamentals • Network Security Controls and Devices • Windows and Linux Security • Web Application and Web Server Architecture and Operations • Web Application Security Mechanisms • Information Security Attacks • Information Security Standards	20.72%
2	**Introduction to Penetration Testing Methodologies**	• Penetration Testing Process and Methodologies & Benefits • Types, Areas and Selection of Pentesting	5.63%
3	**Penetration Testing Scoping and Engagement Methodology**	• Penetration Testing Scoping and Rules and Engagement • Penetration Testing Engagement Contract and Preparation	5.38%
4	**Open-Source Intelligence (OSINT) Methodology**	• OSINT Through World Wide Web (WWW), Website Analysis, DNS Interrogation • Automating your OSINT Effort Using Tools/Frameworks/Scripts	4.80%
5	**Social Engineering Penetration Testing Methodology**	• Social Engineering Penetration Testing Techniques & Steps • Social Engineering Penetration testing using E	5.26%
6	**Network Penetration Testing Methodology – External**	• External Network Information & Reconnaissance • Scanning, and Exploitation	5.84%
7	**Network Penetration Testing Methodology – Internal**	• Internal Network Information Reconnaissance and Scanning • Internal Network Enumeration and Vulnerability Scanning • Local and Remote System Exploitation	8.62%
8	**Network Penetration Testing Methodology - Perimeter Devices**	• Firewall Security Assessment Techniques • iDs Security Assessment Techniques • Router and Switch Security Assessment Techniques	7.84%
9	**Web Application Penetration Testing Methodology**	• Web Application Content Discovery and Vulnerability Scanning • SQL Injection Vulnerability Penetration Testing • XSS, Parameter Tampering, Weak Cryptography, Security Misconfiguration and Client side scripting, vulnerabilities penetration techniques • Authentication, Authorization, session, Web Server Vulnerabilities Penetration Testing	11.30%

10	**Database Penetration Testing Methodology**	• Database Penetration Testing Techniques & Information Reconnaissance • Database Enumeration & Exploitation	5.10%
11	**Wireless Penetration Testing Methodology**	• WLAN Penetration Testing Techniques • RFID and NFC Penetration Testing Techniques • Mobile Device Penetration Testing Techniques • loT Penetration Testing Techniques	9.22%
12	**Cloud Penetration Testing Methodology**	• Cloud Specific Penetration Testing Techniques and Recommendations • Cloud Specific Penetration Testing Methods	4.65%
13	**Report Writing and Post Testing Actions**	• Penetration Testing Report Writing Process • Penetration Testing Reporting Formats	5.63%