

TestOut[®]

TestOut Security Pro - English 6.1.x

TEXTBOOK MAPPING

Objectives for CompTIA Security+ SY0-501 CompTIA Security+ Guide to Network Security Fundamentals, 6th Edition	TestOut Security Pro 6.1.x	CompTIA Security+ Guide to Network Security Fundamentals, 6th Edition
	<i>Author: TestOut</i>	<i>Author: Mark Ciampa</i>
	ISBN# 978-1-935080-44-2	ISBN#: 978-1-337-28878-1
	Sections	Chapters
1.0 Threats, Attacks, and Vulnerabilities		
1.1 Given a scenario, analyze indicators of compromise and determine the type of malware.	6.2, 7.1	2
1.2 Compare and contrast types of attacks	3.5, 4.3, 5.1, 5.2, 5.11, 6.2, 6.4, 7.2, 8.4, 9.4	2,3,5,8,11,15
1.3 Explain threat actor types and attributes	2.1	1
1.4 Explain penetration testing concepts	2.1, 5.1, 6.9, 6.13, 7.6	13
1.5 Explain vulnerability scanning concepts	6.9	13
1.6 Explain the impact associated with types of vulnerabilities	5.12, 6.1, 6.7, 7.7, 8.4	1,3,4,5,9,10
2.0 Technologies and Tools		
2.1 Install and configure network components, both hardware and software-based, to support organizational security.	5.3, 5.5, 5.7, 5.8, 5.9, 5.10, 5.12, 6.5, 6.7, 6.8, 6.9, 7.6, 7.8, 9.10, 9.11	4,6,7,8
2.2 Given a scenario, use appropriate software tools to assess the security posture of an organization.	2.5, 6.9, 6.10, 7.2	8,13,14
2.3 Given a scenario, troubleshoot common security issues.	5.5, 5.8, 5.12, 7.8, 9.11	15
2.4 Given a scenario, analyze and interpret output from security technologies.	5.5, 7.3, 8.6, 9.11	6,7,9
2.5 Given a scenario, deploy mobile devices securely.	3.8, 5.10, 7.11, 7.12	8,10,11
2.6 Given a scenario, implement secure protocols.	6.11, 9.10	4,5
2.7 Compare and contrast physical security and environmental controls.	4.1, 4.2, 4.4	N/A
3.0 Architecture and Design		
3.1 Explain use cases and purpose for frameworks, best practices and secure configuration guides.	2.2	1,15
3.2 Given a scenario, implement secure network architecture concepts.	4.3, 5.3, 5.4, 5.5, 5.6, 5.7, 5.8, 5.10, 6.1, 6.5, 6.6, 6.14, 6.15, 7.3	6,7,8,13
3.3 Given a scenario, implement secure systems design.	3.4, 6.2, 6.3, 6.9, 7.3, 7.4, 7.5, 7.6, 7.12, 8.6, 9.3	3,8,9,14
3.4 Explain the importance of secure staging deployment concepts.	8.6	9
3.5 Explain the security implications of embedded systems.	7.7	10
3.6 Summarize secure application development and deployment concepts.	3.6, 8.6	9
3.7 Summarize cloud and virtualization concepts.	6.14, 6.16, 7.13, 9.14	7
3.8 Explain how resiliency and automation strategies reduce risk.	9.12, 9.13	14,15
3.9 Explain the importance of physical security controls.	4.1, 4.4, 8.14	9,11,14
4.0 Identity and Access Management		
4.1 Compare and contrast identity and access management concepts.	2.3, 8.1, 8.2	11,12
4.2 Given a scenario, install and configure identity and access services.	6.11, 6.12	11
4.3 Given a Scenario, implement identity and access management controls.	8.1, 8.2, 8.3, 8.14	8,11,12
4.4 Given a scenario, differentiate common account management practices.	3.9, 6.2, 7.2, 7.4, 7.5, 7.9, 8.3, 8.8, 8.9, 8.11, 8.12, 8.13	11,12
5.0 Risk Management		
5.1 Explain the importance of policies, plans and procedures related to organizational security.	2.3, 3.1, 3.7, 3.9, 7.10, 9.3	12,15
5.2 Summarize business impact analysis concepts.	3.1, 9.12	14
5.3 Explain risk management processes and concepts.	3.1, 3.2, 3.3, 6.1, 6.13	1,15
5.4 Given a scenario, follow incident response procedures.	2.6	14
5.5 Summarize basic concepts of forensics.	2.6	14
5.6 Explain disaster recovery and continuity of operation concepts.	3.3, 9.12, 9.13	14
5.7 Compare and contrast various types of controls.	4.1	15
5.8 Given a scenario, carry out data security and privacy practices.	3.1, 9.1	12,13
6.0 Cryptography and PKI		
6.1 Compare and contrast basic concepts of cryptography.	2.4, 9.2, 9.3, 9.5, 9.6, 9.9	3,4,11
6.2 Explain cryptography algorithms and their basic characteristics.	9.3, 9.5, 9.6, 9.7, 9.9	3,4,11
6.3 Given a scenario, install and configure wireless security settings.	5.10, 5.12	8,12
6.4 Given a scenario, implement public key infrastructure.	7.10, 9.8	3,4