CompTIA SecurityX Practice Test (Sample)

Study Guide

BY EXAMZIFY

Everything you need from our exam experts!

Notice: Examzify makes every reasonable effort to obtain accurate, complete, and timely information about this product from reliable sources.

Table of Contents

Introduction

Preparing for a certification exam can feel overwhelming, but with the right tools, it becomes an opportunity to build confidence, sharpen your skills, and move one step closer to your goals. At Examzify, we believe that effective exam preparation isn’t just about memorization, it’s about understanding the material, identifying knowledge gaps, and building the test-taking strategies that lead to success.

This guide was designed to help you do exactly that.

Whether you’re preparing for a licensing exam, professional certification, or entry-level qualification, this book offers structured practice to reinforce key concepts. You’ll find a wide range of multiple-choice questions, each followed by clear explanations to help you understand not just the right answer, but why it’s correct.

The content in this guide is based on real-world exam objectives and aligned with the types of questions and topics commonly found on official tests. It’s ideal for learners who want to:

- **Practice answering questions under realistic conditions,**
- **Improve accuracy and speed,**
- **Review explanations to strengthen weak areas, and**
- **Approach the exam with greater confidence.**

We recommend using this book not as a stand-alone study tool, but alongside other resources like flashcards, textbooks, or hands-on training. For best results, we recommend working through each question, reflecting on the explanation provided, and revisiting the topics that challenge you most.

Remember: successful test preparation isn’t about getting every question right the first time, it’s about learning from your mistakes and improving over time. Stay focused, trust the process, and know that every page you turn brings you closer to success.

Let’s begin.

How to Use This Guide

This guide is designed to help you study more effectively and approach your exam with confidence. Whether you're reviewing for the first time or doing a final refresh, here’s how to get the most out of your Examzify study guide:

1. Start with a Diagnostic Review

Skim through the questions to get a sense of what you know and what you need to focus on. Your goal is to identify knowledge gaps early.

2. Study in Short, Focused Sessions

Break your study time into manageable blocks (e.g. 30 – 45 minutes). Review a handful of questions, reflect on the explanations.

3. Learn from the Explanations

After answering a question, always read the explanation, even if you got it right. It reinforces key points, corrects misunderstandings, and teaches subtle distinctions between similar answers.

4. Track Your Progress

Use bookmarks or notes (if reading digitally) to mark difficult questions. Revisit these regularly and track improvements over time.

5. Simulate the Real Exam

Once you're comfortable, try taking a full set of questions without pausing. Set a timer and simulate test-day conditions to build confidence and time management skills.

6. Repeat and Review

Don’t just study once, repetition builds retention. Re-attempt questions after a few days and revisit explanations to reinforce learning. Pair this guide with other Examzify tools like flashcards, and digital practice tests to strengthen your preparation across formats.

There’s no single right way to study, but consistent, thoughtful effort always wins. Use this guide flexibly, adapt the tips above to fit your pace and learning style. You've got this!

Questions

1. **Which term refers to the use of electronics and computer-controlled devices to take control of processes?**

   A. Automation

   B. Bootstrap

   C. Traffic

   D. Erros

2. **Which control approach enforces policies based on conditions or rules without considering individual user identity?**

   A. Discretionary Access Control

   B. Mandatory Access Control

   C. Attribute-Based Access Control

   D. Rule-Based Access Control

3. **Which term describes taking CI/CD further with automated production deployment?**

   A. Continuous Deployment

   B. Continuous Integration

   C. CI/CD

   D. Sandbox

4. **Which system monitors traffic, reports on it, and blocks or responds to suspicious activity?**

   A. SIEM Systems

   B. Network Intrusion Detection/Prevention System (NIDS/NIPS)

   C. SNMP Manager

   D. Break and Inspect

5. **The heart of the operating system is:**

   A. BIOS

   B. Middleware

   C. UEFI

   D. Kernel

6. Residual risk is the risk that remains after which step of the risk treatment process?

A. After incident response

B. After risk transfer

C. After mitigation actions

D. After escalation

7. Which event is used primarily for basic training of team members?

A. Tabletop Exercise

B. Walkthrough

C. Checklist

D. Threat Researchers

8. Which term describes large or complex data sets that traditional data processing applications cannot sufficiently handle?

A. Cryptocurrency

B. Big Data

C. Blockchain

D. Distributed Consensus

9. Which concept allows multiple parties to jointly compute a function over their inputs while keeping those inputs private?

A. It encrypts all communications using quantum keys.

B. It updates firmware on mobile devices.

C. It creates methods for parties to jointly compute a function over their inputs while keeping those inputs private.

D. It provides virtual reality simulations

10. Which component ensures that only authorized users can access sensitive resources?

A. Boundary Control

B. Access Control

C. Cryptography

D. DMZ

Answers

1. **A**
2. **D**
3. **A**
4. **B**
5. **D**
6. **C**
7. **B**
8. **B**
9. **C**
10. **B**

Explanations

1. Which term refers to the use of electronics and computer-controlled devices to take control of processes?

A. Automation

B. Bootstrap

C. Traffic

D. Erros

Automation is the use of electronics and computer-controlled devices to take control of processes. It brings sensors, actuators, and control software together so machines can perform tasks, monitor conditions, and adjust operations without human intervention, delivering consistent, efficient, and scalable results in things like manufacturing, utilities, and IT workflows. Bootstrap is about starting up a system, not ongoing control. Traffic refers to data moving across a network, not controlling processes. Erros isn’t a relevant term here (likely a misspelling of errors).

2. Which control approach enforces policies based on conditions or rules without considering individual user identity?

A. Discretionary Access Control

B. Mandatory Access Control

C. Attribute-Based Access Control

D. Rule-Based Access Control

This question tests how access decisions are driven by policy rules rather than who the user is. Rule-Based Access Control makes decisions by evaluating a set of conditions or rules—such as time of day, source IP address, or network zone—and grants or denies access based on those rules. The user’s identity isn’t the deciding factor; the rules themselves control the outcome. That’s why this model best fits “policies based on conditions or rules without considering individual user identity.” By contrast, other models tie access to identity or roles (owner permissions in Discretionary Access Control, security labels in Mandatory Access Control, user attributes in Attribute-Based Access Control, or user roles in Role-Based Access Control), which means the user or their identity does influence access decisions.

3. Which term describes taking CI/CD further with automated production deployment?

A. Continuous Deployment

B. Continuous Integration

C. CI/CD

D. Sandbox

Automated production deployment means every change that passes automated tests is pushed directly into the live environment without human intervention. This describes Continuous Deployment. It sits after the broader CI/CD pipeline and specifically automates releasing to production. Continuous Integration focuses on frequently merging and validating code; CI/CD covers the whole pipeline, but doesn’t by itself specify automatic production release. Continuous Delivery is the idea that code can be released to production at any time, but may require a manual trigger to actually deploy. A sandbox is just a separate testing environment, not a deployment approach.

4. Which system monitors traffic, reports on it, and blocks or responds to suspicious activity?

A. SIEM Systems

B. Network Intrusion Detection/Prevention System (NIDS/NIPS)

C. SNMP Manager

D. Break and Inspect

Network intrusion detection and prevention systems monitor traffic in real time, report findings, and can block or respond to suspicious activity. This type of system watches network packets for signs of attack or unusual behavior, then raises alerts to notify administrators. If it's in prevention mode, it also takes action to stop threats—dropping malicious packets, resetting connections, or enforcing rules to block the attacker. That combination of monitoring, reporting, and active response is what sets it apart. SIEM systems collect and analyze logs from many sources and provide alerts and dashboards, but they don't typically inspect live traffic or block traffic on the wire by themselves. A SNMP Manager handles device management and monitoring, not security-focused traffic analysis. Break and Inspect isn't a standard security control used to describe a system that monitors, reports, and blocks traffic.

5. The heart of the operating system is:

A. BIOS

B. Middleware

C. UEFI

D. Kernel

The kernel is the central piece of an operating system. It manages all hardware resources—CPU time, memory, devices—and provides core services to software through system calls. It handles process scheduling, memory management, and inter-process communication, and it runs with the highest privileges to protect and isolate applications. This abstraction layer lets programs run without needing to know the specifics of the hardware. Firmware like BIOS or UEFI runs before the OS is loaded, initializing hardware and loading the kernel, but they aren't the ongoing heart of the system once it's up. Middleware sits above the OS to connect applications, not to manage core OS resources. So the kernel is the component that truly anchors the operating system's operation.

6. Residual risk is the risk that remains after which step of the risk treatment process?

A. After incident response

B. After risk transfer

C. After mitigation actions

D. After escalation

Residual risk is the risk that remains after mitigation actions are in place. In the risk treatment process you first assess the inherent risk and then apply controls to reduce it. Once those controls are implemented, you evaluate what's left—that leftover risk is the residual risk. It's this remaining level that you decide whether to accept, or you add more safeguards to bring it down further. For example, patching vulnerabilities and tightening access reduce overall risk, but there may still be some threat from unknown exploits or insider actions. That leftover risk is what you manage next, rather than the risks present before any controls. This concept isn't tied to incident response (which deals with handling active incidents), risk transfer (which shifts risk to another party), or escalation (which raises the issue to higher authority).

7. Which event is used primarily for basic training of team members?

A. Tabletop Exercise

B. Walkthrough

C. Checklist

D. Threat Researchers

Walkthroughs are instructional events where a facilitator guides learners through a process step by step. This format lets team members observe the exact actions, see the proper sequence, and ask questions as they perform tasks under supervision. Because basic training focuses on building familiarity with routine procedures and how to execute them, a walkthrough provides hands-on exposure and immediate feedback — ideal for foundational skills. In contrast, a tabletop exercise is discussion-based and centers on decision-making and coordination during a hypothetical scenario, not the hands-on steps. A checklist is a reference tool used to verify that steps are completed, not an instructional activity by itself. Threat researchers refers to a role rather than a training method.

8. Which term describes large or complex data sets that traditional data processing applications cannot sufficiently handle?

A. Cryptocurrency

B. Big Data

C. Blockchain

D. Distributed Consensus

Big data describes data sets that are too large or complex for traditional data processing tools to handle efficiently. This challenge often involves the three Vs: volume (massive amounts of data), velocity (rapid data inflow requiring real-time or near-real-time processing), and variety (diverse data types and formats, including unstructured data). Traditional systems are typically designed for smaller, structured data and batch processing, so they struggle with storage, processing speed, and integration when faced with big data. To manage these demands, organizations use scalable, distributed storage and processing frameworks that can run across many machines, enabling timely analysis and insights from vast datasets. The other terms relate to different concepts: cryptocurrency is a digital currency, blockchain is a distributed ledger technology, and distributed consensus is a method for agreeing on state in a distributed system; none describe the overarching challenge of handling extremely large or complex data sets.

9. Which concept allows multiple parties to jointly compute a function over their inputs while keeping those inputs private?

A. It encrypts all communications using quantum keys.

B. It updates firmware on mobile devices.

C. It creates methods for parties to jointly compute a function over their inputs while keeping those inputs private.

D. It provides virtual reality simulations

Secure multi-party computation lets multiple parties jointly compute a function over their inputs while keeping those inputs private. No single participant reveals their raw data; only the final result is learned. Techniques like secret sharing, garbled circuits, and homomorphic encryption enable performing the calculation on encrypted or split data, so privacy is preserved throughout the process. For example, several organizations can compute a shared statistic without exposing their individual records. The other options describe protecting data in transit, updating software, or running simulations, which don’t address private collaborative computation.

10. Which component ensures that only authorized users can access sensitive resources?

A. Boundary Control

B. Access Control

C. Cryptography

D. DMZ

Access control is the mechanism that enforces who can do what with which resources. It starts with authenticating a user to confirm identity, then authorizing actions based on policies, roles, or attributes to grant or deny access. This direct enforcement is what prevents unauthorized users from reaching sensitive resources, by checking permissions before allowing actions like read, write, or execute. Tools and models such as access control lists, role-based access control, and attribute-based access control implement these policies at the point where access decisions are made. Boundary control governs traffic between networks and isn't focused on individual user privileges; cryptography secures data but doesn't determine who may access resources; a DMZ is a network zone for publicly accessible services and does not enforce internal resource access rights.

Next Steps

Congratulations on reaching the final section of this guide. You've taken a meaningful step toward passing your certification exam and advancing your career.

As you continue preparing, remember that consistent practice, review, and self-reflection are key to success. Make time to revisit difficult topics, simulate exam conditions, and track your progress along the way.

If you need help, have suggestions, or want to share feedback, we’d love to hear from you. Reach out to our team at hello@examzify.com.

Or visit your dedicated course page for more study tools and resources:

https://comptiasecurityx.examzify.com

We wish you the very best on your exam journey. You've got this!