EXAM CRAM

# CompTIA® Security+ SY0-601

PEARSON IT CERTIFICATION

MARTY M. WEISS

# CompTIA® Security+ SY0-601 Exam Cram, Companion Website

Access interactive study tools on this book's companion website, including practice test software, Glossary, and Cram Sheet.

To access the companion website, simply follow these steps:

1. Go to **www.pearsonitcertification.com/register**.
2. Enter the print book ISBN: **9780136798675**.
3. Answer the security question to validate your purchase.
4. Go to your account page.
5. Click on the Registered Products tab.
6. Under the book listing, click on the Access Bonus Content link.

If you have any issues accessing the companion website, you can contact our support team by going to **http://pearsonitp.echelp.org**.

3. Your organization has been moving new applications from the testing environment directly to production, but lately there have been many issues. You have been asked to help mitigate these issues. Which of the following are the most appropriate? (Select two.)

   ❍ **A.** Move the code to both production environments to troubleshoot on one in case the other fails.

   ❍ **B.** Set up a parallel production environment.

   ❍ **C.** Set up a staging environment to closely match the production environment.

   ❍ **D.** Move the code to staging prior to moving it to production.

4. Your organization's development team wants to protect trade secrets and intellectual property. What should the team implement during the software development process to prevent software from being reverse engineered?

   ❍ **A.** Normalization

   ❍ **B.** Stored procedures

   ❍ **C.** Obfuscation and camouflage

   ❍ **D.** Automation and scripting

# Cram Quiz Answers

**Answer 1:** B. A false positive is a result that incorrectly indicates that a particular condition, such as a vulnerability, is present. Answer C is incorrect as a false negative is not identified but is missed. Answers A and D are incorrect and refer to the use of someone else's identity and a system that manages identity information, respectively.

**Answer 2:** A. Elasticity is the capacity to dynamically expand or reduce infrastructure resources by adjusting workloads to maximize resources. Answer B is incorrect as this is not the most specific answer. Scripting refers to automation, which elastic capabilities are likely to require. Answer C is incorrect. Continuous integration refers to the development process of continuous monitoring and merging. Answer D, while closely related to elasticity, is incorrect, as scalability refers to the ability to expand the amount of production from the current infrastructure without negatively impacting performance.

**Answer 3:** C and D. A staging environment is often implemented to reduce the risk of introducing issues upon deployment into the production environment. The code will be moved to production after being moved to staging. Answers A and B are incorrect. This would not be done in the application development process and is more akin to providing for redundancy.

**Answer 4:** C. Obfuscation, camouflage, and encryption are all often used in the software development process to prevent software from being reverse engineered. These practices protect the trade secrets and intellectual property of an organization. Answer A is incorrect. Normalization is the conversion of data to its anticipated, or "normal," value. Answer B is incorrect because stored procedures are combinations of precompiled SQL statements, stored in a database, that execute some task. Answer D is incorrect because automation and scripting greatly increase an organization's capability to detect and respond to threats. They combine machine learning with automation to respond to threats and maintain critical operations.

# What Next?

If you want more practice on this chapter's exam objective before you move on, remember that you can access all of the Cram Quiz questions on the Pearson Test Prep software online. You can also create a custom exam by objective with the Online Practice Test. Note any objective you struggle with and go to that objective's material in this chapter.

*This page intentionally left blank*

CHAPTER 12

# Authentication and Authorization Design

**This chapter covers the following official Security+ exam objective:**

- 2.4 Summarize authentication and authorization design concepts.

**Essential Terms and Components**

- authentication
- federation
- time-based one-time password (TOTP)
- HMAC-based one-time password (HOTP)
- false acceptance rate (FAR)
- false rejection rate (FRR)
- crossover error rate (CER)
- biometrics
- multifactor authentication (MFA)
- authentication, authorization, and accounting (AAA)

## Identification and Authentication, Authorization, and Accounting (AAA)

It is necessary to discern the differences between the actions *identification* and *authentication*, *authorization*, *and accounting* (*AAA*) because you will be tested on all these concepts. *Identification* occurs when a user or device presents information such as a username, a process ID, a smart card, or another unique identifier and claims an identity. *Authentication* is the process of validating an identity. It occurs when the user provides appropriate credentials, such as the correct password with a username. When identification through the presentation and acceptance of credentials is accomplished, the credentials must be measured against a list of all known credentials by the authentication service to determine *authorization* of the request before access rights during the session can be established. Authorization is based on security policy.

*Accounting* keeps track of the resources a user accesses by keeping a record of authentication and authorization actions. Accounting functions log session statistics and usage information, which can then be used for management tasks such as access control and resource utilization. Additional capabilities include billing, trend analysis, and capacity planning. Implementing the accounting component of AAA requires special server considerations.

These are the core components of AAA:

- The device that wants to access the network is known as the client.
- The policy enforcement point (PEP) is the authenticator. The PEP enforces the conditions of the client's access.
- The policy information point (PIP) holds data relevant to the decision on whether to grant access to the client.
- The policy decision point (PDP) is the crux of the AAA decision and is responsible for making the final decision about whether to grant access to the client.
- The accounting and reporting system tracks the client network usage and reports the "who, what, where, when, and why."
- Core AAA components are logical functions that can be combined and are not necessarily physical devices.

# Multifactor Authentication

A method for authenticating users must be designed and implemented properly for an organization to achieve established business goals and security control objectives. Several common factors are used for authentication: something you know, something you have, something you are, something you do, and somewhere you are. Authentication factors provide a means of implementing multifactor authentication. *Multifactor authentication* provides additional security because account access requires more than a password.

ExamAlert

Forms of authentication credentials can be generally broken into three basic categories, or factors, depending on what is required to identify the access requester:

- Something you know (passwords, account logon identifiers)
- Something you have (smart cards, synchronized shifting keys)
- Something you are (fingerprints, retinal patterns, hand geometry)

Additional categories, more appropriately known as attributes, include the following:

- Something you can do
- Somewhere you are
- Something you exhibit
- Someone you know

The most common form of authentication combines two “something you know” forms of authentication: a username and a password or passphrase. This form is easily implemented across many types of interfaces, including standard keyboards and assistive technology interfaces. If both values match the credentials associated within the authorization system’s database, the credentials can be authenticated and authorized for a connection.

An organization’s authentication needs are relative to the value assigned to a particular resource’s security. Additional authentication layers required for access increase both the administrative overhead necessary for management and the difficulty users have trying to reach needed resources. Consider, for example, the differences in authentication requirements for access to a high-security solution such as the Department of Energy’s power grid control network and those needed to access an unprivileged local account at a public kiosk. In the first scenario, to establish authentication for rightful access, the use of a combination of multiple biometric, token-based, and password form authentication credentials might be mandatory. You can also use these access methods with more complex forms of authentication, such as dedicated lines of communication, time-of-day restrictions, synchronized shifting-key hardware encryption devices, and redundant-path comparison. You use these to ensure that each account attempting to make an access request is properly identified. In the second scenario, authentication might be as simple as an automatic anonymous guest logon that all visitors share.

Different mechanisms for authentication provide different levels of identification, different security of data during the authentication exchange, and suitability to different authentication methods, such as wireless or dial-up network access requests.