

[Download Full Version SSCP Exam Dumps\(Updated in Feb/2023\)](#)

Biometrics (e.g. a fingerprint) or something you do (e.g. signature dynamics).

TIP FROM CLEMENT:

On the real exam you can expect to see synonyms and sometimes sub-categories under the main categories. People are familiar with Pin, Passphrase, Password as subset of Something you know.

However, when people see choices such as Something you do or Something you are they immediately get confused and they do not think of them as subset of Biometrics where you have Biometric implementation based on behavior and physiological attributes. So something you do falls under the Something you are category as a subset.

Something your do would be signing your name or typing text on your keyboard for example.

Strong authentication is simply when you make use of two factors that are within two different categories.

Reference(s) used for this question:

Shon Harris, CISSP All In One, Fifth Edition, pages 158-159

QUESTION 228

The controls that usually require a human to evaluate the input from sensors or cameras to determine if a real threat exists are associated with:

- A. Preventive/physical
- B. Detective/technical
- C. Detective/physical
- D. Detective/administrative

Correct Answer: C

Explanation:

Detective/physical controls usually require a human to evaluate the input from sensors or cameras to determine if a real threat exists.

Source: KRUTZ, Ronald L.& VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 36.

QUESTION 229

Which of the following would constitute the best example of a password to use for access to a system by a network administrator?

- A. holiday
- B. Christmas12
- C. Jenny
- D. GyN19Za!

Correct Answer: D

Explanation:

GyN19Za! would be the the best answer because it contains a mixture of upper and lower case characters, alphabetic and numeric characters, and a special character making it less vulnerable to password attacks.

All of the other answers are incorrect because they are vulnerable to brute force or dictionary attacks. Passwords should not be common words or names. The addition of a number to the end

[SSCP Exam Dumps](#) [SSCP PDF Dumps](#) [SSCP VCE Dumps](#) [SSCP Q&As](#)

<https://www.ensurepass.com/SSCP.html>

[Download Full Version SSCP Exam Dumps\(Updated in Feb/2023\)](#)

of a common word only marginally strengthens it because a common password attack would also check combinations of words:

Christmas23
Christmas123
etc...

QUESTION 230

The three classic ways of authenticating yourself to the computer security software are by something you know, by something you have, and by something:

- A. you need.
- B. non-trivial
- C. you are.
- D. you can get.

Correct Answer: C

Explanation:

This is more commonly known as biometrics and is one of the most accurate ways to authenticate an individual.

The rest of the answers are incorrect because they not one of the three recognized forms for Authentication.

QUESTION 231

What is the main focus of the Bell-LaPadula security model?

- A. Accountability
- B. Integrity
- C. Confidentiality
- D. Availability

Correct Answer: C

Explanation:

The Bell-LaPadula model is a formal model dealing with confidentiality.

The Bell-LaPadula Model (abbreviated BLP) is a state machine model used for enforcing access control in government and military applications. It was developed by David Elliott Bell and Leonard

J.LaPadula, subsequent to strong guidance from Roger R. Schell to formalize the U.S. Department of Defense (DoD) multilevel security (MLS) policy. The model is a formal state transition model of computer security policy that describes a set of access control rules which use security labels on objects and clearances for subjects. Security labels range from the most sensitive (e.g. "Top Secret"), down to the least sensitive (e.g., "Unclassified" or "Public").

The Bell-LaPadula model focuses on data confidentiality and controlled access to classified information, in contrast to the Biba Integrity Model which describes rules for the protection of data integrity. In this formal model, the entities in an information system are divided into subjects and objects.

The notion of a "secure state" is defined, and it is proven that each state transition preserves security by moving from secure state to secure state, thereby inductively proving that the system satisfies the security objectives of the model. The Bell-LaPadula model is built on the concept of a state machine with a set of allowable states in a computer network system. The transition from

[SSCP Exam Dumps](#) [SSCP PDF Dumps](#) [SSCP VCE Dumps](#) [SSCP Q&As](#)

<https://www.ensurepass.com/SSCP.html>

[Download Full Version SSCP Exam Dumps\(Updated in Feb/2023\)](#)

one state to another state is defined by transition functions.

A system state is defined to be "secure" if the only permitted access modes of subjects to objects are in accordance with a security policy. To determine whether a specific access mode is allowed, the clearance of a subject is compared to the classification of the object (more precisely, to the combination of classification and set of compartments, making up the security level) to determine if the subject is authorized for the specific access mode.

The clearance/classification scheme is expressed in terms of a lattice. The model defines two mandatory access control (MAC) rules and one discretionary access control (DAC) rule with three security properties:

The Simple Security Property - a subject at a given security level may not read an object at a higher security level (no read-up).

The -property (read "star"-property) - a subject at a given security level must not write to any object at a lower security level (no write-down). The -property is also known as the Confinement property.

The Discretionary Security Property - use of an access matrix to specify the discretionary access control.

The following are incorrect answers:

Accountability is incorrect. Accountability requires that actions be traceable to the user that performed them and is not addressed by the Bell-LaPadula model.

Integrity is incorrect. Integrity is addressed in the Biba model rather than Bell-Lapadula.

Availability is incorrect. Availability is concerned with assuring that data/services are available to authorized users as specified in service level objectives and is not addressed by the Bell-Lapadula model.

References:

CBK, pp. 325-326

AIO3, pp. 279 - 284

AIOv4 Security Architecture and Design (pages 333 - 336) AIOv5 Security Architecture and Design (pages 336 - 338)

Wikipedia at https://en.wikipedia.org/wiki/Bell-La_Padula_model

QUESTION 232

The Computer Security Policy Model the Orange Book is based on is which of the following?

- A. Bell-LaPadula
- B. Data Encryption Standard
- C. Kerberos
- D. Tempest

Correct Answer: A

Explanation:

The Computer Security Policy Model Orange Book is based is the Bell- LaPadula Model. Orange Book Glossary.

The Data Encryption Standard (DES) is a cryptographic algorithm. National Information Security Glossary.

TEMPEST is related to limiting the electromagnetic emanations from electronic equipment.

Reference:

[SSCP Exam Dumps](#) [SSCP PDF Dumps](#) [SSCP VCE Dumps](#) [SSCP Q&As](#)

<https://www.ensurepass.com/SSCP.html>

[Download Full Version SSCP Exam Dumps\(Updated in Feb/2023\)](#)

U.S. Department of Defense, Trusted Computer System Evaluation Criteria (Orange Book), DOD 5200.28-STD. December 1985 (also available here).

QUESTION 233

Which of the following was developed to address some of the weaknesses in Kerberos and uses public key cryptography for the distribution of secret keys and provides additional access control support?

- A. SESAME
- B. RADIUS
- C. KryptoKnight
- D. TACACS+

Correct Answer: A

Explanation:

Secure European System for Applications in a Multi-vendor Environment (SESAME) was developed to address some of the weaknesses in Kerberos and uses public key cryptography for the distribution of secret keys and provides additional access control support.

Reference:

TIPTON, Harold, Official (ISC)2 Guide to the CISSP CBK (2007), page 184.
ISC OIG Second Edition, Access Controls, Page 111

QUESTION 234

Which of the following statements pertaining to using Kerberos without any extension is false?

- A. A client can be impersonated by password-guessing.
- B. Kerberos is mostly a third-party authentication protocol.
- C. Kerberos uses public key cryptography.
- D. Kerberos provides robust authentication.

Correct Answer: C

Explanation:

Kerberos is a trusted, credential-based, third-party authentication protocol that uses symmetric (secret) key cryptography to provide robust authentication to clients accessing services on a network.

Because a client's password is used in the initiation of the Kerberos request for the service protocol, password guessing can be used to impersonate a client.

Here is a nice overview of HOW Kerberos is implement as described in RFC 4556:

1. Introduction

The Kerberos V5 protocol [RFC4120] involves use of a trusted third party known as the Key Distribution Center (KDC) to negotiate shared session keys between clients and services and provide mutual authentication between them.

The corner-stones of Kerberos V5 are the Ticket and the Authenticator. A Ticket encapsulates a symmetric key (the ticket session key) in an envelope (a public message) intended for a specific service. The contents of the Ticket are encrypted with a symmetric key shared between the service principal and the issuing KDC. The encrypted part of the Ticket contains the client principal name, among other items. An Authenticator is a record that can be shown to have been recently generated using the ticket session key in the associated Ticket. The ticket session key is

[SSCP Exam Dumps](#) [SSCP PDF Dumps](#) [SSCP VCE Dumps](#) [SSCP Q&As](#)

<https://www.ensurepass.com/SSCP.html>

[Download Full Version SSCP Exam Dumps\(Updated in Feb/2023\)](#)

known by the client who requested the ticket. The contents of the Authenticator are encrypted with the associated ticket session key. The encrypted part of an Authenticator contains a timestamp and the client principal name, among other items.

As shown in Figure 1, below, the Kerberos V5 protocol consists of the following message exchanges between the client and the KDC, and the client and the application service:

The Authentication Service (AS) Exchange

The client obtains an "initial" ticket from the Kerberos authentication server (AS), typically a Ticket Granting Ticket (TGT). The AS-REQ message and the AS-REP message are the request and the reply message, respectively, between the client and the AS.

The Ticket Granting Service (TGS) Exchange

The client subsequently uses the TGT to authenticate and request a service ticket for a particular service, from the Kerberos ticket-granting server (TGS). The TGS-REQ message and the TGS-REP message are the request and the reply message respectively between the client and the TGS.

The Client/Server Authentication Protocol (AP) Exchange

The client then makes a request with an AP-REQ message, consisting of a service ticket and an authenticator that certifies the client's possession of the ticket session key. The server may optionally reply with an AP-REP message. AP exchanges typically negotiate session-specific symmetric keys.

Usually, the AS and TGS are integrated in a single device also known as the KDC.

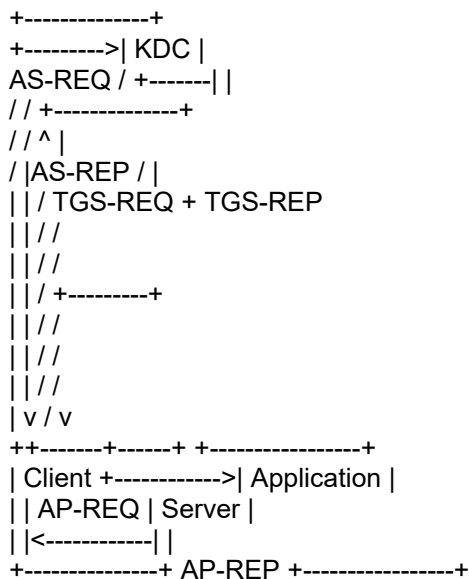


Figure 1: The Message Exchanges in the Kerberos V5 Protocol

In the AS exchange, the KDC reply contains the ticket session key, among other items, that is encrypted using a key (the AS reply key) shared between the client and the KDC. The AS reply key is typically derived from the client's password for human users. Therefore, for human users, the attack resistance strength of the Kerberos protocol is no stronger than the strength of their