Exam Report: 8.2.7 Practice Questions

Date: 1/23/2020 4:15:40 pm
Time Spent: 14:39

Candidate: Garsteck, Matthew
Login: mGarsteck

Overall Performance

Your Score: 67%

Passing Score: 80%

View results by: ○ Objective Analysis ● Individual Responses

Individual Responses

Question 1: Correct

Which of the following is a password that relates to things that people know, such as a mother's maiden name or the name of a pet?

○ Dynamic

○ Pass phrase

○ One-time

➡ ● Cognitive

Explanation

Cognitive passwords relate to things that people know, such as a mother's maiden name or the name of a pet.

Dynamic passwords change upon each consecutive login. *One-time* passwords are only valid for a single use. A *pass phrase* is a password based on a phrase.

References

LabSim for Security Pro, Section 8.2.
[All Questions SecPro2017_v6.exm AUTH_01]

Question 2: Correct

What type of password is *maryhadalittlelamb*?

○ Static

○ Composition

○ Cognitive

➡ ● Pass phrase

Explanation

A *pass phrase* is a password based on a phrase, such as *maryhadalittlelamb*.

Cognitive passwords are passwords that relate to things that people know, such as a mother's maiden name or the name of a pet. A *static* password is created by a user and overseen by an administrator. *Composition* passwords are created by the system and are usually two or more unrelated words divided by symbols on the keyboard.

References

LabSim for Security Pro, Section 8.2.
[All Questions SecPro2017_v6.exm AUTH_02]

Question 3: Correct

Which of the following defines the *crossover error rate* for evaluating biometric systems?

○ The rate of people who are denied access that should be allowed access.

○ The rate of people who are given access that should be denied access.

○ The number of subjects or authentication attempts that can be validated.

➡ ● The point where the number of false positives matches the number of false negatives in a biometric system.

Explanation

The *crossover error rate*, or the *equal error rate*, is the point where the number of false positives matches the number of false negatives in a biometric system.

A *false negative* (or Type I error) occurs when a person who should be allowed access is denied access. A *false positive* (or Type II error) occurs when a person who should be denied access is allowed access. The *processing rate*, or *system throughput*, identifies the number of subjects or authentication attempts that can be validated.

References

LabSim for Security Pro, Section 8.2.
[All Questions SecPro2017_v6.exm AUTH_03]

▼ **Question 4:** Correct

Which of the following is the most common form of authentication?

➡ ● Password

○ Photo ID

○ Digital certificate on a smart card

○ Fingerprint

Explanation

Passwords are the most common form of authentication. Most secure systems require only a user name and password to provide users with access to the computing environment. Many forms of online intrusion attacks focus on stealing passwords. This makes using strong passwords very important. Without a strong password policy and properly trained users, the reliability of your security system is greatly diminished.

Photo ID, fingerprint, and digital certificate on a smart card are not the most common forms of authentication.

References

LabSim for Security Pro, Section 8.2.
[All Questions SecPro2017_v6.exm AUTH_16]

▼ **Question 5:** Correct

Which of the following is the strongest form of multi-factor authentication?

○ A password and a biometric scan

○ Two-factor authentication

○ Two passwords

➡ ● A password, a biometric scan, and a token device

Explanation

A password, a biometric scan, and a token device together are the strongest form of multi-factor authentication listed here. Multifactor authentication is any combination of two or more of the same or different authentication factors. The three common authentication factor types are Something You Know (such as a password), Something You Have (such as a smart card or a token device), and Something You Are (such as a biometric quality, like a fingerprint).

The other three options are all weaker forms of multi-factor authentication. A password and a biometric scan is a multi-factor authentication system, but it is also an example of two-factor authentication. Two-factor authentication is any combination of two or more different authentication factors. Two passwords is an example of multi-factor authentication, but since it uses two of the same type of factors, it is not a true two-factor authentication method.

References

LabSim for Security Pro, Section 8.2.
[All Questions SecPro2017_v6.exm AUTH_17]

▼ **Question 6:** Incorrect

Which of the following advantages can single sign-on (SSO) provide? (Select two.)

➡ ☑ Access to all authorized resources with a single instance of authentication

➡ □ The elimination of multiple user accounts and passwords for each individual

□ Secure remote access

□ Enhanced password complexity requirements

Explanation

A properly designed single sign-on (SSO) system can reduce human error and system administration time by providing access to all authorized resources with a single instance of authentication through a single set of user credentials.

Enhanced password complexity is not a direct function of SSO, although enhanced security may be achieved by eliminating multiple credentials for individual authentication and enforcing password complexity policies. SSO is not a replacement for sound security policies or properly configured systems. Implementation of an SSO system can be challenging, as all systems and applications must be capable of utilizing a common method of authentication.

References

LabSim for Security Pro, Section 8.2.
[All Questions SecPro2017_v6.exm AUTH_18]

▼ **Question 7:** Incorrect

Which of the following best describes *one-factor* authentication?

➡ ○ Multiple authentication credentials may be required, but they are all of the same type.

● ~~Only a single authentication credential is submitted.~~

○ Only Type 1 authentication credentials are accepted.

○ A user name without any additional credentials is accepted.

Explanation

One-factor authentication uses credentials of only one type, but may require multiple methods within the same type. For example, you might log in with just a password or use a password and answer a cognitive question (such as your mother's maiden name). One-factor authentication that uses multiple credentials of the same type is also sometimes called *strong* authentication.

One-factor authentication can use one or multiple credentials from any of the three authentication types. Supplying a user name does not provide authentication credentials, as the user name is used for identification, not authentication. Anonymous access occurs when only a user name is required.

References

LabSim for Security Pro, Section 8.2.
[All Questions SecPro2017_v6.exm AUTH_22]

▼ **Question 8:** Incorrect

Match the authentication factor types on the left with the appropriate authentication factor on the right. Each authentication factor type can be used more than once.

PIN

✓ Something You Know

Smart card

✓ Something You Have

Password

✓ Something You Know

Retina scan

~~Somewhere You Are~~ Something You Are

Fingerprint scan

✓ Something You Are

Hardware token

✓ Something You Have

Pass phrase

✓ Something You Know

Voice recognition

✓ Something You Are

Wi-Fi triangulation

✓ Somewhere You Are

Typing behaviors

~~Something You Are~~ Something You Do

Explanation

Something You Know authentication requires you to provide a password or some other data that you know. This is the weakest type of authentication. Examples of Something You Know authentication controls include:

- Passwords, codes, or IDs
- PINs
- Pass phrases (long, sentence-length passwords)

Something You Have (also called token-based authentication) is authentication based on something users have in their possession. Examples of Something You Have controls include:

- Swipe cards
- Photo IDs
- Smart cards
- Hardware tokens

Something You Are authentication uses a biometric system. A biometric system attempts to identify a person based on metrics or a mathematical representation of the subject's biological attribute. Biometric systems are the most expensive and least accepted system type, but are generally considered to be the most secure form of authentication. Common attributes used for biometric systems include:

- Fingerprints

- Hand topology (side view) or geometry (top-down view)
- Palm scans
- Retina scans
- Iris scans
- Facial scans
- Voice recognition

Somewhere You Are authentication (also known as geolocation) is a supplementary authentication factor that uses physical location to verify a user's identity. Examples of implementations include:

- An account is locked unless the user has passed through the building's entrance using an ID card.
- If the user is within RFID range of the workstation, authentication requests are allowed.
- GPS or Wi-Fi triangulation location data is used to determine a device's location. If the user and the device are in a specified location, authentication requests are allowed. If not, the device is locked.

Something You Do is a supplementary authentication factor that requires an action to verify a user's identity. Example implementations include:

- Analyzing a user's handwriting sample against a baseline sample before allowing authentication.
- Analyzing a user's typing behaviors against a baseline sample before allowing authentication.

References

LabSim for Security Pro, Section 8.2.
[All Questions SecPro2017_v6.exm AUTH_29]

Question 9: Incorrect

Which of the following are examples of single sign-on authentication solutions? (Select two.)

➡ ☑ Kerberos

➡ □ SESAME

□ Digital certificates

□ RADIUS

☑ ~~DIAMETER~~

□ Biometrics

Explanation

Kerberos and SESAME are single sign-on authentication solutions. A single sign-on authentication solution is a mechanism that allows a user to log in to a network once and then be able to roam the entire network without re-authenticating. This does not mean that the user is granted unlimited access to all of the resources within the network--it just means that the user is not required to re-authenticate each time he connects to a new system on the network as he accesses resources and performs activities he is authorized to perform.

Biometrics and digital certificates are used in authentication, but are not single sign-on authentication solutions. RADIUS and DIAMETER are centralized remote access authentication methods.

References

LabSim for Security Pro, Section 8.2.
[All Questions SecPro2017_v6.exm AUTH_06]

Question 10: Correct

Which of the following is an example of a single sign-on authentication solution?

○ RADIUS

○ Biometrics

➡ ● Kerberos

○

○ Digital certificates

Explanation

Kerberos is a single sign-on authentication solution. A single sign-on authentication solution is a mechanism that allows a user to log in to a network once and then roam the entire network without re-authenticating. This does not mean that the user is granted unlimited access to all of the resources within the network; it just means that as the user accesses resources and performs activities he is authorized to perform, he is not required to re-authenticate each time he connects to a new system on the network. Kerberos is only one example of a single sign-on solution. Others include directory services, scripting, thin clients, and SESAME.

Biometrics, RADIUS, and digital certificates are authentication mechanisms, but not single sign-on authentication solutions.

References

LabSim for Security Pro, Section 8.2.
[All Questions SecPro2017_v6.exm AUTH_14]

▼ **Question 11:** Incorrect

What is another term for the type of login credentials provided by a token device?

● ~~Two-factor authentication~~

○ Biometric

○ Mutual authentication

➡ ○ One-time password

Explanation

A token device provides a type of one-time password. There are several types of token devices. Generally, a token device requires you to enter a code or a PIN. The device then displays a code that you must enter into the login prompt. Some tokens are time-based so that the code provided by the token is only valid for a short period of time. Other tokens are challenge/response-based--the login prompt displays a challenge message that you enter into the token. The response from the token must match that expected by the secured system.

A token device may require the use of a biometric, or it may be involved in a mutual or two-factor authentication system.

References

LabSim for Security Pro, Section 8.2.
[All Questions SecPro2017_v6.exm AUTH_08]

▼ **Question 12:** Correct

Which of the following is stronger than any biometric authentication factor?

○ A 47-character password

➡ ● Two-factor authentication

○ A USB device hosting PKI certificates

○ A dynamic asynchronous token device without a PIN

Explanation

A two-factor authentication system is always stronger than a single authentication system, even if that single factor is a biometric.

When a single authentication factor is compared to other single authentication factors, they are all roughly the same in terms of strength of security protection. Thus, the single factors of a password, a non-PIN token device, and a USB drive with PKI certificates are all equally weak.

References

LabSim for Security Pro, Section 8.2.
[All Questions SecPro2017_v6.exm AUTH_09]

Question 13: Correct

Which of the following is **not** a form of biometric?

○ Fingerprint

➡ ● Token device

○ Retina scan

○ Face recognition

Explanation

A token device is not a form of biometric. Biometrics rely on personal characteristics (such as fingerprints, face recognition, or a retina scan) to prove identity.

A token device is an example of a Something You Have authentication factor. A token device is a small device that produces a response when a user types in a code or PIN. The response is along with your name and password to gain access to a secure system.

References

LabSim for Security Pro, Section 8.2.
[All Questions SecPro2017_v6.exm AUTH_26]

Question 14: Correct

What is the most important aspect of a biometric device?

➡ ● Accuracy

○ Throughput

○ Enrollment time

○ Size of the reference profile

Explanation

The most important aspect of a biometric device is accuracy. If an access control device is not accurate, it does not offer reliable security.

Enrollment time is how long it takes for a new user to be defined in the biometric database. Typically, an enrollment time less than two minutes is preferred. The size of the reference profile is irrelevant in most situations. Throughput is how many users a biometric device can scan and verify within a given time period. Typically, a throughput of 10 users per minute is preferred.

References

LabSim for Security Pro, Section 8.2.
[All Questions SecPro2017_v6.exm AUTH_27]

Question 15: Correct

Which of the following is a hardware device that contains identification information and can be used to control building access or computer logon?

○ Biometric

➡ ● Smart card

○ SSID

○ WAP

○ Security policy

Explanation

A smart card is a hardware device that contains identification information. Smart cards can contain a magnetic strip, radio frequency transmitter, or hardware contacts that allow it to interact with a smart card reader. The reader uses information on the card to allow or deny access.

A *biometric* is a physical characteristic of a human that can be scanned to control access. A WAP is a wireless access point. The SSID is the name of a wireless network. A security policy is a written document outlining the policies that are applied to create a secure network. In Windows, the Local Security policy is a collection of settings that control how the system behaves.

References

LabSim for Security Pro, Section 8.2.
[All Questions SecPro2017_v6.exm AUTH_28]