CompTIA Security+ (SY0-601) Exam Dumps 2022

SkillCertPro offers real exam questions for practice for all major IT certifications.

- For a full set of 650+ questions. Go to https://skillcertpro.com/product/comptia-security-sy0-601-exam-questions/
- SkillCertPro offers detailed explanations to each question which helps to understand the concepts better.
- It is recommended to score above 85% in SkillCertPro exams before attempting a real exam.
- SkillCertPro updates exam questions every 2 weeks.
- You will get life time access and life time free updates
- SkillCertPro assures 100% pass guarantee in first attempt.

Below are the free 10 sample questions

Question 1:

A member of the company asks for a financial transfer by sending an encrypted message to the financial administrator. An attacker eavesdrops on this message, captures it, and is now in a position to resend it. Because it's an authentic message that has simply been resent, the message is already correctly encrypted and looks legitimate to the financial administrator. Then the financial administrator is likely to respond to this new request, that response could include sending a large sum of money to the attacker's bank account.

Which of the following type of attack does the scenario describe?

A. SSL Stripping

B. Replay attack

C. Improper Input Handling

D. Pass the hash attack

Answer: B

Explanation:

A replay attack occurs when a cybercriminal eavesdrops on secure network communication, intercepts it, and then fraudulently delays or resends it to misdirect the receiver into doing what the hacker wants. The added danger of replay attacks is that a hacker doesn't even need advanced skills to decrypt a message after capturing it from the network. The attack could be successful simply by resending the whole thing.

Improper Input Handling is incorrect as it is the term used to describe functions such as validation, sanitization, filtering, or encoding and/or decoding of input data. Improper Input Handling is a leading cause of critical vulnerabilities that exist in today's systems and applications.

The root cause of Improper Input Handling is the application trusting, rather than validating, data inputs. One of the key aspects of input handling is validating that the input satisfies certain criteria. All inputs should be considered untrusted as they can come from a variety of mechanisms and be transferred in various formats.

A Pass-the-Hash (PtH) attack is incorrect as it is a technique whereby an attacker captures a password hash (as opposed to the password characters) and then simply passes it through for authentication and potentially lateral access to other networked systems.

The threat actor doesn't need to decrypt the hash to obtain a plain text password. PtH attacks exploit the authentication protocol, as the password's hash remains static for every session until the password is rotated. Attackers commonly obtain hashes by scraping a system's active memory and other techniques.

SSL Stripping or an SSL Downgrade Attack is incorrect as it is an attack used to circumvent the security enforced by SSL certificates on HTTPS-enabled websites. In other words, SSL stripping is a technique that downgrades your connection from secure HTTPS to insecure HTTP and exposes you to eavesdropping and data manipulation.

Question 2:

Which of the following cryptographic technique will you use to validate the authenticity and integrity of a message or digital document?

A. Hashing

B. Salting

C. Digital signatures

D. Key stretching

Answer: C

Explanation:

Digital signature is correct. A digital signature is a mathematical technique used to validate the authenticity and integrity of a message, software or digital document. As the digital equivalent of a handwritten signature or stamped seal, a digital signature offers far more inherent security, and it is intended to solve the problem of tampering and impersonation in digital communications.

Key stretching is incorrect. Key stretching algorithms take a relatively insecure value, such as a password, and manipulates it in a way that makes it stronger and more resilient to threats like dictionary attacks.

Hashing is incorrect. Hashing is the practice of using an algorithm to map data of any size to a fixed length. This is called a hash value (or sometimes hash code or hash sums or even a hash digest if you're feeling fancy). Hashing is meant to verify that a file or piece of data hasn't been altered.

Salting is incorrect. Salting is a random string of data used to modify a password hash. Salt can be added to the hash to prevent a collision by uniquely identifying a user's password, even if another user in the system has selected the same password. Salt can also be added to make it more difficult for an attacker to break into a system by using password hash-matching strategies because adding salt to

a password hash prevents an attacker from testing known dictionary words across the entire system.

Question 3:

Which of the following options allows your application to interact with an external service using a simple set of commands rather than having to create complex processes yourself?

A. Micro service

B. Containers

C. Thin Client

D. API

Answer: D

Explanation:

API is correct. An API, or Application Programming Interface, allows your application to interact with an external service using a simple set of commands. Rather than having to create complex processes yourself, you can use APIs to access the underlying services of another application which can save you time and resources.

Many applications that you use every day rely on APIs in some capacity to function, since there are APIs for almost every category imaginable.

Thin Client is incorrect. Thin clients function as regular PCs, but lack hard drives and typically do not have extra I/O ports or other unnecessary features. Since they do not have hard drives, thin clients do not have any software installed on them. Instead, they run programs and access data from a server.

Thin clients can be a cost-effective solution for businesses or organizations that need several computers that all do the same thing.

Microservice is incorrect. A microservice architectural pattern is a modular application development technique that organizes loosely coupled services. Microservice architecture is like an assembly line, where every service has a specialized role. Together, the services create a complete application.

These services can be independently deployed and tend to serve a specific purpose. For example, an eCommerce website might have a service for customer information, a service for payments, and a service for shipping logistics.

Containers is incorrect. Containers are a solution to the problem of how to get the software to run reliably when moved from one computing environment to another. A container is a standard unit of software that packages up code and all its dependencies so the application runs quickly and reliably from one computing environment to another.

Question 4:

Which of the following part(s) of the Authentication, Authorization, and Accounting (AAA) is responsible for measuring the resources a user consumes during access to a system?

A. Accounting

B. Authentication

C. Authorization

D. Authentication & Authorization

Answer: A

Explanation:

The correct answer is Accounting.

Authentication, Authorization and Accounting is the term for intelligently controlling access to computer resources, enforcing policies, auditing usage, and providing the information necessary to bill for services.

As the first process, authentication provides a way of identifying a user, typically by having the user enter a valid user name and valid password before access is granted.

Following authentication, a user must gain authorization for doing certain tasks. After logging into a system, for instance, the user may try to issue commands. The authorization process determines whether the user has the authority to issue such commands.

The final plank in the AAA framework is accounting, which measures the resources a user consumes during access. This can include the amount of system time or the amount of data a user has sent and/or received during a session.

Question 5:

Your company migrates its infrastructure to the public cloud because of the advantages the cloud offers. Which of the following options are considered advantages for using public cloud services? (Choose all that apply.)

A. Full-control

B. Near-unlimited scalability

C. High reliability

D. Lower costs

E. No maintenance

F. Secure data

Answer: B, C, D, E

Explanation:

Public clouds are the most common way of deploying cloud computing. The cloud resources like servers and storage are owned and operated by a third-party cloud service provider and delivered over the Internet. With a public cloud, all hardware, software, and other supporting infrastructure is owned and managed by the cloud provider.

Advantages of public clouds:

1. Lower costs—no need to purchase hardware or software, and you pay only for the service you use.

2. No maintenance—your service provider provides the maintenance.

3. Near-unlimited scalability—on-demand resources are available to meet your business needs.

4. High reliability—a vast network of servers ensures against failure.

Disadvantages of public clouds:

1. Loss of Control-When you outsource your technology to the public cloud, it's out of your hands.

2. Insecure Data-When you entrust your data and applications to the public cloud, you have no real assurances that they will be safe.

- For a full set of 650+ questions. Go to
- https://skillcertpro.com/product/comptia-security-sy0-601-exam-questions/
- SkillCertPro offers detailed explanations to each question which helps to understand the concepts better.
- It is recommended to score above 85% in SkillCertPro exams before attempting a real exam.
- SkillCertPro updates exam questions every 2 weeks.
- You will get life time access and life time free updates
- SkillCertPro assures 100% pass guarantee in first attempt.

Question 6:

Cloud backup is a strategy for sending a copy of files or database to a secondary server which is usually hosted by a third-party service provider, for preservation in case of equipment failure or catastrophe. (True/False)

A. TRUE

B. FALSE

Answer: A

Explanation:

TRUE.

Cloud backup, also known as online backup or remote backup, is a strategy for sending a copy of a physical or virtual file or database to a secondary, off-site location for preservation in case of equipment failure or catastrophe.

The secondary server and storage systems are usually hosted by a third-party service provider, who charges the backup customer a fee based on storage space or capacity used, data transmission bandwidth, number of users, number of servers or number of times data is accessed.

Question 7:

Which of the following products using Software as a Service cloud model? (Choose all that apply.)

A. Slack

B. Google Compute Engine

C. Dropbox

D. AWS EC2

E. Mail Chimp

F. Google Apps

Answer: A, C, E, F

Explanation:

SaaS platforms make software available to users over the internet, usually for a monthly subscription fee. With SaaS, you don't need to install and run software applications on your computer (or any computer). Everything is available over the internet when you log in to your account online.

SaaS platforms are:

1. Available over the internet.

2. Hosted on a remote server by a third-party provider.

3. Scalable, with different tiers for small, medium, and enterprise-level businesses.

4. Inclusive, offering security, compliance, and maintenance as part of the cost.

Products using SaaS cloud models are:

1. Google Apps

2. Dropbox

3. Mail Chimp

4. Slack

The rest options are using the Infrastructure as a Service (IaaS) cloud model.

Question 8:

Asymmetrical encryption uses a single key that needs to be shared among the people who need to receive the message while symmetric encryption uses a pair of a public key and a private key to encrypt and decrypt messages when communicating. (True/False)

A.TRUE

B. FALSE

Answer: B

Explanation:

False.

Symmetric encryption uses a single key that needs to be shared among the people who need to receive the message.

It's a simple technique, and because of this, the encryption process can be carried out quickly.

It's mostly used when large chunks of data need to be transferred.

The secret key is shared. Consequently, the risk of compromise is higher.

Asymmetrical encryption uses a pair of a public key and a private key to encrypt and decrypt messages when communicating.

It's a much more complicated process than symmetric key encryption, and the process is slower.

It's used in smaller transactions, primarily to authenticate and establish a secure communication channel prior to the actual data transfer.

The private key is not shared, and the overall process is more secure as compared to symmetric encryption.

Question 9:

Recently the physical network adapter card from your company's server broke. As a result, your co-workers couldn't access important resources for hours. You have been instructed to implement a solution to eliminate this from happening again in the event of a network adapter failure.

Which of the following solutions will you implement to meet the requirement?

A. PDU

B. UPS

C. Power generator

D. NIC teaming

Answer: D

Explanation:

Network interface card teaming is correct. NIC (Network Interface Card) teaming, also known as Load Balancing/Failover (LBFO) in the Microsoft world, is a mechanism that enables multiple physical network adapter cards in the same physical host/server to be bound together and placed into a "team" in the form of a single logical NIC. The connected network adapters, shown as one or more virtual adapters. These virtual network adapters provide fast performance and fault tolerance in the event of a network adapter failure.

UPS is incorrect. An uninterruptible power supply (UPS) is a device that allows a computer to keep running for at least a short time when the primary power source is lost. UPS devices also provide protection from power surges.

PDU is incorrect. A PDU, or Power Distribution Unit, is a device used in data centers to control and distribute electric power. The most basic form of a PDU is a

large power strip without surge protection. This is designed to provide standard electrical outlets for use within a variety of settings that don't require monitoring or remote access capabilities.

Power generator is incorrect. A power generator is, as its name implies, a device capable of generating energy. This is responsible for converting any type of energy (e.g. chemical, mechanical, etc.) into electrical energy.

Question 10:

You have been tasked to find a way to transform a plain text sensitive file into a non-readable form and send it through the web. Which of the following technique will you use to send the file through the web and only authorized parties can understand the information?

A. Data masking

B. Encryption

C. Tokenization

D. Data at rest

Answer: B

Explanation:

Encryption is correct. Encryption is the process of using an algorithm to transform plain text information into a non-readable form called ciphertext. An algorithm and an encryption key are required to decrypt the information and return it to its original plain text format. Today, SSL encryption is commonly used to protect information as it's transmitted on the Internet.

In other words, Encryption is a way of scrambling data so that only authorized parties can understand the information. In technical terms, it is the process of

converting plaintext to ciphertext. In simpler terms, encryption takes readable data and alters it so that it appears random. Encryption requires the use of an encryption key: a set of mathematical values that both the sender and the recipient of an encrypted message know.

Data masking is incorrect. Data masking is a method of creating a structurally similar but inauthentic version of an organization's data that can be used for purposes such as software testing and user training. The purpose is to protect the actual data while having a functional substitute for occasions when the real data is not required.

Overall, the primary function of masking data is to protect sensitive, private information in situations where it might be visible to someone without clearance to the information.

Tokenization is incorrect. Tokenization is the process of turning a meaningful piece of data, such as an account number, into a random string of characters called a token that has no meaningful value if breached. Tokens serve as a reference to the original data, but cannot be used to guess those values. That's because, unlike encryption, tokenization does not use a mathematical process to transform sensitive information into the token.

There is no key or algorithm that can be used to derive the original data for a token. Instead, tokenization uses a database, called a token vault, which stores the relationship between the sensitive value and the token. The real data in the vault is then secured, often via encryption.

Data at rest is incorrect. Data at rest is data that is not actively moving from device to device or network to network such as data stored on a hard drive, laptop, flash drive, or archived/stored in some other way. Data protection at rest aims to secure inactive data stored on any device or network. While data at rest is sometimes considered to be less vulnerable than data in transit, attackers often find data at rest a more valuable target than data in motion.

- For a full set of 650+ questions. Go to
- https://skillcertpro.com/product/comptia-security-sy0-601-exam-questions/
- SkillCertPro offers detailed explanations to each question which helps to understand the concepts better.
- It is recommended to score above 85% in SkillCertPro exams before attempting a real exam.
- SkillCertPro updates exam questions every 2 weeks.
- You will get life time access and life time free updates
- SkillCertPro assures 100% pass guarantee in first attempt.

SKILLCERTPRO
IT CERTIFICATION TRAININGS

Search for products...

All Courses

Prepare and pass your IT certification in 1st attempt

We offer World Class Trainings and Practice Tests Everything you need to prepare and quickly pass the tough certification exams in the first Attempt!

Why Skillcertpro ?

- **Real Exam Question taken from Previous Exams**
- **Online Mock Exam (Just like a real exam)**
- **Up to Date Questions. All Practice Sets updated every 2 weeks.**
- **Life time access & Life time free updates**
- **100% Pass Guarantee in First attempt.**
- **60 Day No Questions Asked Money-back Guarantee (If you fail your money will be refunded back)**
- **24/7 Chat & Email Support**

Browser our Practice Tests →