SY0-401 Q&As

CompTIA Security+ Certification

Pass CompTIA SY0-401 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.lead4pass.com/SY0-401.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by CompTIA Official Exam Center

QUESTION 1

Users have reported receiving unsolicited emails in their inboxes, often times with malicious links embedded. Which of the following should be implemented in order to redirect these messages?

A. Proxy server

B. Spam filter

C. Network firewall

D. Application firewall.

Correct Answer: B

QUESTION 2

A security researcher wants to reverse engineer an executable file to determine if it is malicious. The file was found on an underused server and appears to contain a zero-day exploit. Which of the following can the researcher do to determine if the file is malicious in nature?

A. TCP/IP socket design review

B. Executable code review

C. OS Baseline comparison

D. Software architecture review

Correct Answer: C

Zero-Day Exploits begin exploiting holes in any software the very day it is discovered. It is very difficult to respond to a zero-day exploit. Often, the only thing that you as a security administrator can do is to turn off the service. Although this can be a costly undertaking in terms of productivity, it is the only way to keep the network safe. In this case you want to check if the executable file is malicious. Since a baseline represents a secure state is would be possible to check the nature of the executable file in an isolated environment against the OS baseline.

QUESTION 3

Several departments in a corporation have a critical need for routinely moving data from one system to another using removable storage devices. Senior management is concerned with data loss and the introduction of malware on the network. Which of the following choices BEST mitigates the range of risks associated with the continued use of removable storage devices?

A. Remote wiping enabled for all removable storage devices

B. Full-disk encryption enabled for all removable storage devices

C. A well defined acceptable use policy

D. A policy which details controls on removable storage use

Correct Answer: D

Removable storage is both a benefit and a risk and since not all mobile devices support removable storage, the company has to has a comprehensive policy which details the controls of the use of removable s to mitigate the range of risks that are associated with the use of these devices.

QUESTION 4

Ann, a security administrator is hardening the user password policies. She currently has the following in place.

Passwords expire every 60 days

Password length is at least eight characters Passwords must contain at least one capital letter and one numeric character

Passwords cannot be reused until the password has been changed eight times

She learns that several employees are still using their original password after the 60-day forced change. Which of the following can she implement to BEST mitigate this?

A. Lower the password expiry time to every 30days instead of every 60 days

B. Require that the password contains at least one capital, one numeric, and one special character

C. Change the re-usage time from eight to 16 changes before a password can be repeated

D. Create a rule that users can only change their passwords once every two weeks

Correct Answer: D

QUESTION 5

A user has unknowingly gone to a fraudulent site. The security analyst notices the following system change on the user\\'s host:

Old `hosts\\' file:

127.0.0.1 localhost

New `hosts\\' file:

127.0.0.1 localhost

5.5.5.5 www.comptia.com

Which of the following attacks has taken place?

A. Spear phishing

B. Pharming

C. Phishing

D. Vishing

Correct Answer: B

We can see in this question that a fraudulent entry has been added to the user\\'s hosts file. This will point the URL: www.comptia.com to 5.5.5.5 instead of the correct IP address. Similar in nature to e-mail phishing, pharming seeks to obtain personal or private (usually financial related) information through domain spoofing. Rather than being spammed with malicious and mischievous e-mail requests for you to visit spoof Web sites which appear legitimate, pharming \\'poisons\\' a DNS server (or hosts file) by infusing false information into the DNS server, resulting in a user\\'s request being redirected elsewhere. Your browser, however will show you are at the correct Web site, which makes pharming a bit more serious and more difficult to detect. Phishing attempts to scam people one at a time with an e-mail while pharming allows the scammers to target large groups of people at one time through domain spoofing.

QUESTION 6

A new application needs to be deployed on a virtual server. The virtual server hosts a SQL server that is used by several employees. Which of the following is the BEST approach for implementation of the new application on the virtual server?

A. Take a snapshot of the virtual server after installing the new application and store the snapshot in a secure location.

B. Generate a baseline report detailing all installed applications on the virtualized server after installing the new application.

C. Take a snapshot of the virtual server before installing the new application and store the snapshot in a secure location.

D. Create an exact copy of the virtual server and store the copy on an external hard drive after installing the new application.

Correct Answer: C

Snapshots are backups of virtual machines that can be used to quickly recover from poor updates, and errors arising from newly installed applications. However, the snapshot should be taken before the application or update is installed.

QUESTION 7

Which of the following hardware based encryption devices is used as a part of multi-factor authentication to access a secured computing system?

A. Database encryption

B. USB encryption

C. Whole disk encryption

D. TPM

Correct Answer: D

Trusted Platform Module (TPM) is a hardware-based encryption solution that is embedded in the system\\'s motherboard and is enabled or disable in BIOS. It helps with hash key generation and stores cryptographic keys, passwords, or certificates.

QUESTION 8

The data backup window has expanded into the morning hours and has begun to affect production users. The main bottleneck in the process is the time it takes to replicate the backups to separate severs at the offsite data center. Which of the following uses of deduplication could be implemented to reduce the backup window?

A. Implement deduplication at the network level between the two locations

B. Implement deduplication on the storage array to reduce the amount of drive space needed

C. Implement deduplication on the server storage to reduce the data backed up

D. Implement deduplication on both the local and remote servers

Correct Answer: B

QUESTION 9

An administrator is configuring a network for all users in a single building. Which of the following design elements would be used to segment the network based on organizational groups? (Select two)

A. NAC

B. NAT

C. Subnetting

D. VLAN

E. DMZ

F. VPN

Correct Answer: BC

QUESTION 10

A certificate used on an ecommerce web server is about to expire. Which of the following will occur if the certificate is allowed to expire?

A. The certificate will be added to the Certificate Revocation List (CRL).

B. Clients will be notified that the certificate is invalid.

C. The ecommerce site will not function until the certificate is renewed.

D. The ecommerce site will no longer use encryption.

Correct Answer: B

A similar process to certificate revocation will occur when a certificate is allowed to expire. Notification will be sent out to

clients of the invalid certificate. The process of revoking a certificate begins when the CA is notified that a particular certificate needs to be revoked. This must be done whenever the private key becomes known. The owner of a certificate can request that it be revoked at any time, or the administrator can make the request.

QUESTION 11

Which of the following are unique to white box testing methodologies? (Select two)

A. Application program interface API testing

B. Bluesnarfing

C. External network penetration testing

D. Function, statement and code coverage

E. Input fuzzing

Correct Answer: AD

QUESTION 12

Which of the following controls can be implemented together to prevent data loss in the event of theft of a mobile device storing sensitive information? (Select TWO).

A. Full device encryption

B. Screen locks

C. GPS

D. Asset tracking

E. Inventory control

Correct Answer: AB

A: Device encryption encrypts the data on the device. This feature ensures that the data on the device cannot be accessed in a useable form should the device be stolen.

B: Screen locks are a security feature that requires the user to enter a PIN or a password after a short period of inactivity before they can access the system again. This feature ensures that if your device is left unattended or is lost or stolen, it will be difficult for anyone else to access your data or applications.

QUESTION 13

Environmental control measures include which of the following?

A. Access list

B. Lighting

C. Motion detection

D. EMI shielding

Correct Answer: D

Environmental controls include HVAC, Fire Suppression, EMI Shielding, Hot and Cold Aisles, Environmental monitoring as well as Temperature and Humidity controls.

QUESTION 14

An organization is working with a cloud services provider to transition critical business applications to a hybrid cloud environment. The organization retains sensitive customer data and wants to ensure the provider has sufficient administrative and logical controls in place to protect its data. In which of the following documents would this concern MOST likely be addressed?

A. Service level agreement

B. Interconnection security agreement

C. Non-disclosure agreement

D. Business process analysis

Correct Answer: A

QUESTION 15

During an office move a sever containing the employee information database will be shut down and transported to a new location. Which of the following would BEST ensure the availability of the employee database should happen to the server during the move?

A. The contents of the database should be encrypted; the encryption key should be stored off-site

B. A hash of the database should be taken and stored on an external drive prior to the move

C. The database should be placed on a drive that consists of a RAID array prior to the move

D. A backup of the database should be stored on an external hard drive prior to the move

Correct Answer: D

QUESTION 16

A system administrator wants to prevent password compromises from offline password attacks. Which of the following controls should be configured to BEST accomplish this task? (Select TWO)

A. Password reuse

B. Password length

C. Password complexity

D. Password history

E. Account lockouts

Correct Answer: CE

QUESTION 17

A network technician is on the phone with the system administration team. Power to the server room was lost and servers need to be restarted. The DNS services must be the first to be restarted. Several machines are powered off. Assuming each server only provides one service, which of the following should be powered on FIRST to establish DNS services?

A. Bind server

B. Apache server

C. Exchange server

D. RADIUS server

Correct Answer: A

BIND (Berkeley Internet Name Domain) is the most widely used Domain Name System (DNS) software on the Internet. It includes the DNS server component contracted for name daemon. This is the only option that directly involves DNS.

QUESTION 18

Having adequate lighting on the outside of a building is an example of which of the following security controls?

A. Deterrent

B. Compensating

C. Detective

D. Preventative

Correct Answer: A

QUESTION 19

Joe, the security administrator, sees this in a vulnerability scan report:

\\'The server 10.1..2.232 is running Apache 2.2.20 which may be vulnerabel to a mod_cgi exploit."

Joe verifies that mod_cgi module is not enabled on 10.1.2.232. This message is an example of

A. a threat

B. a risk

C. a false negative

D. afalse positive

Correct Answer: A

QUESTION 20

A security engineer is tasked with encrypting corporate email. Which of the following technologies provide the MOST complete protection? (Select TWO)

A. PGP/GPG

B. S/MIME

C. IPSEC

D. Secure POP3

E. IMAP

F. HMAC

Correct Answer: BF

QUESTION 21

Which of the following practices is used to mitigate a known security vulnerability?

A. Application fuzzing

B. Patch management

C. Password cracking

D. Auditing security logs

Correct Answer: B

Patch management is the process of maintaining the latest source code for applications and operating systems by applying the latest vendor updates. This helps protect a systems from new attacks and vulnerabilities that have recently become known.

QUESTION 22

A program displays:

ERROR: this program has caught an exception and will now terminate.

Which of the following is MOST likely accomplished by the program\\'s behavior?

A. Operating system\\'s integrity is maintained

B. Program\\'s availability is maintained

C. Operating system\\'s scalability is maintained

D. User\\'s confidentiality is maintained

Correct Answer: A

The purpose of error handling is to maintain the security and integrity of the system. Integrity is compromised when unauthorized modification occurs.

QUESTION 23

Ann, a security analyst, is preparing for an upcoming security audit. To ensure that she identifies unapplied security controls and patches without attacking or compromising the system, Ann would use which of the following?

A. Vulnerability scanning

B. SQL injection

C. Penetration testing

D. Antivirus update

Correct Answer: A

A vulnerability scan is the process of scanning the network and/or I.T. infrastructure for threats and vulnerabilities. The threats and vulnerabilities are then evaluated in a risk assessment and the necessary actions taken to resolve and vulnerabilities. A vulnerability scan scans for known weaknesses such as missing patches or security updates.

A vulnerability scan is the automated process of proactively identifying security vulnerabilities of computing systems in a network in order to determine if and where a system can be exploited and/or threatened. While public servers are important for communication and data transfer over the Internet, they open the door to potential security breaches by threat agents, such as malicious hackers. Vulnerability scanning employs software that seeks out security flaws based on a database of known flaws, testing systems for the occurrence of these flaws and generating a report of the findings that an individual or an enterprise can use to tighten the network\\'s security.

QUESTION 24

Which of the following is an important step in the initial stages of deploying a host-based firewall?

A. Selecting identification versus authentication

B. Determining the list of exceptions

C. Choosing an encryption algorithm

D. Setting time of day restrictions

Correct Answer: B

A host-based firewall is installed on a client system and is used to protect the client system from the activities of the user as well as from communication from the network or Internet. These firewalls manage network traffic using filters to block certain ports and protocols while allowing others to pass through the system.

QUESTION 25

Users report that they are unable to access network printing services. The security technician checks the router access list and sees that web, email, and secure shell are allowed. Which of the following is blocking network printing?

A. Port security

B. Flood guards

C. Loop protection

D. Implicit deny

Correct Answer: D

Implicit deny says that if you aren\\'t explicitly granted access or privileges for a resource, you\\'re denied access by default. The scenario does not state that network printing is allowed in the router access list, therefore, it must be denied by default.

QUESTION 26

RADIUS provides which of the following?

A. Authentication, Authorization, Availability

B. Authentication, Authorization, Auditing

C. Authentication, Accounting, Auditing

D. Authentication, Authorization, Accounting

Correct Answer: D

The Remote Authentication Dial In User Service (RADIUS) networking protocol offers centralized Authentication, Authorization, and Accounting (AAA) management for users who make use of a network service. It is for this reason that A, B, and C: are incorrect.

References: http://en.wikipedia.org/wiki/RADIUS

QUESTION 27

Establishing a published chart of roles, responsibilities, and chain of command to be used during a disaster is an example of which of the following?

A. Fault tolerance

B. Succession planning

C. Business continuity testing

D. Recovery point objectives

Correct Answer: B

Succession planning outlines those internal to the organization that has the ability to step into positions when they open. By identifying key roles that cannot be left unfilled and associating internal employees who can step into these roles, you can groom those employees to make sure that they are up to speed when it comes time for them to fill those positions.

QUESTION 28

Which of the following are restricted to 64-bit block sizes? (Select TWO).

A. PGP

B. DES

C. AES256

D. RSA

E. 3DES

F. AES

Correct Answer: BE

B: The Data Encryption Standard (DES) has been used since the mid-1970s. It was the primary standard used in government and industry until it was replaced by AES. It\\'s based on a 56-bit key and has several modes that offer security and integrity. It is now considered insecure because of the small key size.

E: Triple-DES (3DES) is a technological upgrade of DES. 3DES is still used, even though AES is the preferred choice for government applications. 3DES is considerably harder to break than many other systems, and it\\'s more secure than DES. It increases the key length to 168 bits (using three 56-bit DES keys).

QUESTION 29

Joe, the systems administrator, is setting up a wireless network for his team\\'s laptops only and needs to prevent other employees from accessing it. Which of the following would BEST address this?

A. Disable default SSID broadcasting.

B. Use WPA instead of WEP encryption.

C. Lower the access point\\'s power settings.

D. Implement MAC filtering on the access point.

Correct Answer: D

If MAC filtering is turned off, any wireless client that knows the values looked for (MAC addresses) can join the network. When MAC filtering is used, the administrator compiles a list of the MAC addresses associated with users\\' computers and enters those addresses. When a client attempts to connect and other values have been correctly entered, an additional check of the MAC address is done. If the address appears in the list, the client is allowed to join; otherwise, it is forbidden from doing so.

QUESTION 30

After a recent internal audit, the security administrator was tasked to ensure that all credentials must be changed within 90 days, cannot be repeated, and cannot contain any dictionary words or patterns. All credentials will remain enabled regardless of the number of attempts made. Which of the following types of user account options were enforced? (Select TWO).

A. Recovery

B. User assigned privileges

C. Lockout

D. Disablement

E. Group based privileges

F. Password expiration

G. Password complexity

Correct Answer: FG

Password complexity often requires the use of a minimum of three out of four standard character types for a password. The more characters in a password that includes some character type complexity, the more resistant it is to password-cracking techniques. In most cases, passwords are set to expire every 90 days.

QUESTION 31

A network consists of various remote sites that connect back to two main locations. Pete, the security administrator, needs to block TELNET access into the network. Which of the following, by default, would be the BEST choice to accomplish this goal?

A. Block port 23 on the L2 switch at each remote site

B. Block port 23 on the network firewall

C. Block port 25 on the L2 switch at each remote site

D. Block port 25 on the network firewall

Correct Answer: B

Telnet is a terminal-emulation network application that supports remote connectivity for executing commands and running applications but doesn\\'t support transfer of fi les. Telnet uses TCP port 23. Because it\\'s a clear text protocol and service, it should be avoided and replaced with SSH.

QUESTION 32

Matt, a security administrator, wants to configure all the switches and routers in the network in order to securely monitor their status. Which of the following protocols would he need to configure on each device?

A. SMTP

B. SNMPv3

C. IPSec

D. SNMP

Correct Answer: B

Explanation: Currently, SNMP is predominantly used for monitoring and performance management. SNMPv3 defines a secure version of SNMP and also facilitates remote configuration of the SNMP entities.

QUESTION 33

Which of the following is being tested when a company\\'s payroll server is powered off for eight hours?

A. Succession plan

B. Business impact document

C. Continuity of operations plan

D. Risk assessment plan

Correct Answer: C

Continuity of operations plan is the effort to ensure the continued performance of critical business functions during a wide range of potential emergencies.

QUESTION 34

The security department has implemented a new laptop encryption product in the environment. The product requires one user name and password at the time of boot up and also another password after the operating system has finished loading. This setup is using which of the following authentication types?

A. Two-factor authentication

B. Single sign-on

C. Multifactor authentication

D. Single factor authentication

Correct Answer: D

Single-factor authentication is when only one authentication factor is used. In this case, Something you know is being used as an authentication factor. Username, password, and PIN form part of Something you know.

QUESTION 35

Joe a computer forensic technician responds to an active compromise of a database server. Joe first collects information in memory, then collects network traffic and finally conducts an image of the hard drive. Which of the following procedures did Joe follow?

A. Order of volatility

B. Chain of custody

C. Recovery procedure

D. Incident isolation

Correct Answer: A

QUESTION 36

A company is exploring the option of letting employees use their personal laptops on the internal network. Which of the following would be the MOST common security concern in this scenario?

A. Credential management

B. Support ownership

C. Device access control

D. Antivirus management

Correct Answer: D

QUESTION 37

A security administrator needs to image a large hard drive for forensic analysis. Which of the following will allow for faster imaging to a second hard drive?

A. cp /dev/sda /dev/sdb bs=8k

B. tail -f /dev/sda > /dev/sdb bs=8k

C. dd in=/dev/sda out=/dev/sdb bs=4k

D. locate /dev/sda /dev/sdb bs=4k

Correct Answer: C

dd is a command-line utility for Unix and Unix-like operating systems whose primary purpose is to convert and copy files. dd can duplicate data across files, devices, partitions and volumes On Unix, device drivers for hardware (such as

hard disks) and special device files (such as /dev/zero and /dev/random) appear in the file system just like normal files; dd can also read and/or write from/to these files, provided that function is implemented in their respective driver. As a result, dd can be used for tasks such as backing up the boot sector of a hard drive, and obtaining a fixed amount of random data. The dd program can also perform conversions on the data as it is copied, including byte order swapping and conversion to and from the ASCII and EBCDIC text encodings. An attempt to copy the entire disk using cp may omit the final block if it is of an unexpected length; whereas dd may succeed. The source and destination disks should have the same size.

QUESTION 38

Which of the following algorithms has well documented collisions? (Select TWO).

A. AES

B. MD5

C. SHA

D. SHA-256

E. RSA

Correct Answer: BC

B: MD5 biggest weakness is that it does not have strong collision resistance, and thus it is no longer recommended for use.

C: SHA-1 (also known as SHA) is being retired from most government uses; the U.S. National Institute of Standards and Technology said, "Federal agencies should stop using SHA-1 for...applications that require collision resistance as soon

as practical, and must use the SHA-2 family of hash functions for these applications after 2010", though that was later relaxed.

Note: The hashing algorithm must have few or no collisions. This means that hashing two different inputs does not give the same output.

Cryptographic hash functions are usually designed to be collision resistant. But many hash functions that were once thought to be collision resistant were later broken. MD5 and SHA- 1 in particular both have published techniques more

efficient than brute force for finding collisions.

QUESTION 39

A company hired Joe, an accountant. The IT administrator will need to create a new account for

Joe. The company uses groups for ease of management and administration of user accounts.

Joe will need network access to all directories, folders and files within the accounting department.

Which of the following configurations will meet the requirements?

A. Create a user account and assign the user account to the accounting group.

B. Create an account with role-based access control for accounting.

C. Create a user account with password reset and notify Joe of the account creation.

D. Create two accounts: a user account and an account with full network administration rights.

Correct Answer: B

Role-based Access Control is basically based on a user\\'s job description. When a user is assigned a specific role in an environment, that user\\'s access to objects is granted based on the required tasks of that role. The IT administrator should, therefore, create an account with role-based access control for accounting for Joe.

QUESTION 40

A security analyst has been investigating an incident involving the corporate website. Upon investigation, it has been determined that users visiting the corporate website would be automatically redirected to a, malicious site. Further investigation on the corporate website has revealed that the home page on the corporate website has been altered to include an unauthorized item. Which of the following would explain why users are being redirected to the malicious site?

A. DNS poisoning

B. XSS

C. Iframe

D. Session hijacking

Correct Answer: B