SY0-501 Q&As

CompTIA Security+ Certification Exam

Pass CompTIA SY0-501 Exam with 100% Guarantee

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

https://www.pass4itsure.com/sy0-501.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

Joe, an employee, asks a coworker how long ago Ann started working at the help desk. The coworker expresses surprise since nobody named Ann works at the help desk. Joe mentions that Ann called several people in the customer service department to help reset their passwords over the phone due to unspecified "server issues".

Which of the following has occurred?

A. Social engineering

B. Whaling

C. Watering hole attack

D. Password cracking

Correct Answer: A

QUESTION 2

Which of the following implements two-factor authentication?

A. A phone system requiring a PIN to make a call

B. At ATM requiring a credit card and PIN

C. A computer requiring username and password

D. A datacenter mantrap requiring fingerprint and iris scan

Correct Answer: B

QUESTION 3

A security administrator learns that PII, which was gathered by the organization, has been found in an open forum. As a result, several C-level executives found their identities were compromised, and they were victims of a recent whaling

attack.

Which of the following would prevent these problems in the future? (Select TWO).

A. Implement a reverse proxy.

B. Implement an email DLP.

C. Implement a spam filter.

D. Implement a host-based firewall.

E. Implement a HIDS.

Correct Answer: BC

QUESTION 4

A security engineer is installing a WAF to protect the company\\'s website from malicious web requests over SSL. Which of the following is needed to meet the objective?

A. A reverse proxy

B. A decryption certificate

C. A split-tunnel VPN

D. Load-balanced servers

Correct Answer: B

By deploying a WAF in front of a web application, a shield is placed between the web application and the Internet. While a proxy server protects a client machine\\'s identity by using an intermediary, a WAF is a type of reverse-proxy, protecting

the server from exposure by having clients pass through the WAF before reaching the server.

A WAF operates through a set of rules often called policies. These policies aim to protect against vulnerabilities in the application by filtering out malicious traffic. The value of a WAF comes in part from the speed and ease with which policy

modification can be implemented, allowing for faster response to varying attack vectors; during a DDoS attack, rate limiting can be quickly implemented by modifying WAF policies.

QUESTION 5

A large financial services firm recently released information regarding a security breach within its corporate network that began several years before. During the time frame in which the breach occurred, indicators show an attacker gained administrative access to the network through a file download from a social media site and subsequently installed it without the user\\'s knowledge. Since the compromise, the attacker was able to take command and control of the computer systems anonymously while obtaining sensitive corporate and personal employee information.

Which of the following methods did the attacker MOST likely use to gain access?

A. A bot

B. A fileless virus

C. A logic bomb

D. A RAT

Correct Answer: A

QUESTION 6

A Chief Information Security Officer (CISO) for a school district wants to enable SSL to protect all of the public- facing servers in the domain. Which of the following is a secure solution that is the MOST cost effective?

A. Create and install a self-signed certificate on each of the servers in the domain.

B. Purchase a load balancer and install a single certificate on the load balancer.

C. Purchase a wildcard certificate and implement it on every server.

D. Purchase individual certificates and apply them to the individual servers.

Correct Answer: B

QUESTION 7

A technician is recommending preventive physical security controls for a server room. Which of the following would the technician MOST likely recommend? (Choose two.)

A. Geofencing

B. Video surveillance

C. Protected cabinets

D. Mantrap

E. Key exchange

F. Authorized personnel signage

Correct Answer: CD

QUESTION 8

A third-party penetration testing company was able to successfully use an ARP cache poison technique to gain root access on a server. The tester successfully moved to another server that was not in the original network. Which of the following is the MOST likely method used to gain access to the other host?

A. Backdoor

B. Pivoting

C. Persistance

D. Logic bomp

Correct Answer: B

QUESTION 9

An email systems administrator is configuring the mail server to prevent spear phishing attacks through email messages. Which of the following refers to what the administrator is doing?

A. Risk avoidance

B. Risk mitigation

C. Risk transference

D. Risk acceptance

Correct Answer: A

QUESTION 10

A network technician discovered the usernames and passwords used for network device configuration have been compromised by a user with a packet sniffer. Which of the following would secure the credentials from sniffing?

A. Implement complex passwords

B. Use SSH for remote access

C. Configure SNMPv2 for device management

D. Use TFTP to copy device configuration

Correct Answer: B

QUESTION 11

An organization prefers to apply account permissions to groups and not individual users, but allows for exceptions that are justified. Some systems require a machine-to-machine data exchange and an associated account to perform this data exchange. One particular system has data in a folder that must be modified by another system. No user requires access to this folder; only the other system needs access to this folder. Which of the following is the BEST account management practice?

A. Create a service account and apply the necessary permissions directly to the service account itself

B. Create a service account group, place the service account in the group, and apply the permissions on the group

C. Create a guest account and restrict the permissions to only the folder with the data

D. Create a generic account that will only be used for accessing the folder, but disable the account until it is needed for the data exchange

E. Create a shared account that administrators can use to exchange the data, but audit the shared account activity

Correct Answer: A

QUESTION 12

A Chief Security Officer (CSO) has been unsuccessful in attempts to access the website for a potential partner (www.example.net). Which of the following rules is preventing the CSO from accessing the site? Blocked sites: *.nonews.com, *.rumorhasit.net, *.mars?

A. Rule 1: deny from inside to outside source any destination any service smtp

B. Rule 2: deny from inside to outside source any destination any service ping

C. Rule 3: deny from inside to outside source any destination {blocked sites} service http-https

D. Rule 4: deny from any to any source any destination any service any

Correct Answer: C

QUESTION 13

A contracting company recently completed its period of performance on a government contract and would like to destroy all information associated with contract performance. Which of the following is the best NEXT step for the company to take?

A. Consult data disposition policies in the contract.

B. Use a pulper or pulverizer for data destruction

C. Retain the data for a period no more than one year

D. Burn hard copies containing Pll or PHI.

Correct Answer: A

QUESTION 14

Although a web enabled application appears to only allow letters in the comment field of a web form, malicious user was able to carry a SQL injection attack by sending special characters through the web comment field. Which of the following has the application programmer failed to implement?

A. Revision control system

B. Client side exception handling

C. Server side validation

D. Server hardening

Correct Answer: C

QUESTION 15

Which of the following could an attacker use to overwrite instruction pointers in order to execute malicious code?

A. Memory leak

B. SQL injection

C. Resource exhaustion

D. Buffer overflow

Correct Answer: D