SY0-601 Q&As

CompTIA Security+

Pass CompTIA SY0-601 Exam with 100% Guarantee

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

https://www.leads4pass.com/sy0-601.html

100% Passing Guarantee
100% Money Back Assurance

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

Instant Download After Purchase
100% Money Back Guarantee
365 Days Free Update
800,000+ Satisfied Customers

QUESTION 1

A security analyst was asked to evaluate a potential attack that occurred on a publicly accessible section of the company\\'s website The malicious actor posted an entry in an attempt to trick users into cltckmg the following:

```
https://www.c0mpt1a.com/contact-us/%3Fname%3D%3Cscript%3Ealert(document.cookie)%3C%2Fscript%3E
```

Which of the following was MOST likely observed?

A. DLL injection

B. Session replay

C. SOLI

D. XSS

Correct Answer: D

URL Structure: The URL starts with "https://www.c0mpt1a.com/contact-us/," which is a typical URL structure for a website\\'s contact page. This part appears normal.

Query Parameter: Following the "/", there is a query parameter represented as "?name=". Query parameters in a URL are often used to pass data to a web application.

Payload: After the "name=" query parameter, there is a URL-encoded string: "%3Cscript%3Ealert(document.cookie)%3C%2Fscript%3E". Let\\'s decode and analyze this payload step by step:

"%3C" represents "".

So, "%3Cscript%3E" is "", and "%3C%2Fscript%3E" is "" in HTML.

Between the "" and "" tags, there is JavaScript code: "alert(document.cookie)".

QUESTION 2

A security analyst discovers several .jpg photos from a cellular phone during a forensics investigation involving a compromised system. The analyst runs a forensics tool to gather file metadata. Which of the following would be part of the images if all the metadata is still intact?

A. The GPS location

B. When the file was deleted

C. The total number of print jobs

D. The number of copies made

Correct Answer: A

A security analyst discovers several .jpg photos from a cellular phone during a forensics investigation involving a compromised system. The analyst runs a forensics tool to gather file metadata.

QUESTION 3

A company was recently breached, Part of the company\\'s new cybersecurity strategy is to centralize the logs from all security devices. Which of the following components forwards the logs to a central source?

A. Log enrichment

B. Log aggregation

C. Log parser

D. Log collector

Correct Answer: D

Log collectors are pieces of software that function to gather data from multiple independent sources and feed it into a unified source such as a SIEM. Log aggregation is the process of combining logs together. This is done to allow different formats from different systems to work together.

QUESTION 4

The marketing department at a retail company wants to publish an internal website to the internet so it is reachable by a limited number of specific, external service providers in a secure manner. Which of the following configurations would be BEST to fulfil this requirement?

A. NAC

B. ACL

C. WAF

D. NAT

Correct Answer: B

QUESTION 5

A report delivered to the Chief Information Security Officer (CISO) shows that some user credentials could be exfilltrated. The report also indicates that users tend to choose the same credentials on different systems and applications. Which of the following policies should the CISO use to prevent someone from using the exfilltrated credentials?

A. MFA

B. Lockout

C. Time-based logins

D. Password history

Correct Answer: A

The CISO should use MFA (multi-factor authentication) to prevent someone from using the exfiltrated credentials.

MFA is a security measure that requires multiple forms of authentication to access a system or data. MFA typically involves the use of two or more of the following factors: something the user knows (e.g. a password or PIN), something the user has (e.g. a security token or smart card), or something the user is (e.g. a biometric characteristic). By requiring multiple forms of authentication, MFA helps to prevent unauthorized access to a system or data, even if a user\\'s credentials are exfiltrated. The report delivered to the CISO indicates that some user credentials could be exfiltrated, and that users tend to choose the same credentials on different systems and applications. This means that if an attacker were to obtain a user\\'s credentials, they could potentially use them to gain access to multiple systems or applications. MFA would help to prevent this by requiring additional forms of authentication, making it more difficult for an attacker to gain access to a system or data.

QUESTION 6

A security architect is implementing a new email architecture for a company. Due to security concerns, the Chief Information Security Officer would like the new architecture to support email encryption, as well as provide for digital signatures. Which of the following should the architect implement?

A. TOP

B. IMAP

C. HTTPS D. S/MIME

Correct Answer: D

QUESTION 7

A network administrator is concerned about users being exposed to malicious content when accessing company cloud applications. The administrator wants to be able to block access to sites based on the AUP. The users must also be protected because many of them work from home or at remote locations, providing on- site customer support. Which of the following should the administrator employ to meet these criteria?

A. Implement NAC.

B. Implement an SWG.

C. Implement a URL filter.

D. Implement an MDM.

Correct Answer: B

What is SWG in cyber security?

" A secure web gateway (SWG) protects users from web-based threats in addition to applying and enforcing corporate acceptable use policies. Instead of connecting directly to a website, a user accesses the SWG, which is then responsible

for connecting the user to the desired website and performing functions such as URL filtering, web visibility, malicious content inspection, web access controls and other security measures."

This hits all the points.

QUESTION 8

one of the attendees starts to notice delays in the connection. and the HTTPS site requests are reverting to HTTP. Which of the following BEST describes what is happening?

A. Birthday collision on the certificate key

B. DNS hyacking to reroute traffic

C. Brute force to the access point

D. A SSUTLS downgrade

Correct Answer: D

QUESTION 9

The cost of removable media and the security risks of transporting data have become too great for a laboratory. The laboratory has decided to interconnect with partner laboratories to make data transfers easier and more secure.

The Chief Security Officer (CSO) has several concerns about proprietary data being exposed once the interconnections are established.

Which of the following security features should the network administrator implement to prevent unwanted data exposure to users in partner laboratories?

A. VLAN zoning with a file-transfer server in an external-facing zone

B. DLP running on hosts to prevent file transfers between networks

C. NAC that permits only data-transfer agents to move data between networks

D. VPN with full tunneling and NAS authenticating through the Active Directory

Correct Answer: A

The labs are not part of the network so data access/loss controls within the network will not solve the issue. Network design (segmentation) with a FS accessible to the labs solves better as only authorised data is stored and no access to internal network/data. Of course other security measures for data at rest and in transit will be applied to FS i.e firewalls, VPN to authenticate and secure connections from the labs but the issue here is what data are they allowed access

QUESTION 10

An administrator identifies some locations on the third floor of the building that have a poor wireless signal Multiple users confirm the incident and report it is not an isolated event. Which of the following should the administrator use to find the areas with a poor or non-existent wireless signal?

A. Heat map

B. Input validation

C. Site survey

D. Embedded systems

Correct Answer: C

To find the areas with a poor or non-existent wireless signal, the administrator should conduct a wireless site survey. A wireless site survey is a process of planning and designing a wireless network by surveying the physical location to understand the RF (radio frequency) characteristics and signal propagation in the area.

During a site survey, the administrator uses specialized tools and equipment to measure the wireless signal strength at various locations within the building. The data collected is then used to create a heat map, which visually represents the signal coverage and strength across the surveyed area. This heat map helps identify areas with poor or weak signal strength and allows the administrator to make informed decisions about the placement of wireless access points or other necessary adjustments to improve wireless coverage and performance.

QUESTION 11

An audit Identified Pll being utilized In the development environment of a critical application. The Chief Privacy Officer (CPO) Is adamant that this data must be removed; however, the developers are concerned that without real data they cannot perform functionality tests and search for specific data. Which of the following should a security professional implement to BEST satisfy both the CPO\\'s and the development team\\'s requirements?

A. Data anonymlzallon

B. Data encryption

C. Data masking

D. Data tokenization

Correct Answer: C

Data masking refers to modifying data to hide the original content. The primary reason to do so is to protect sensitive information such as PII. The process retains usable data but converts it to inauthentic data.

QUESTION 12

The process of passively gathering information prior to launching a cyberattack is called:

A. tailgating.

B. reconnaissance.

C. pharming

D. prepending

Correct Answer: B

QUESTION 13

A security analyst needs to produce a document that details how a security incident occurred, the steps that were taken for recovery, and how future incidents can be avoided. During which of the following stages of the response process will this activity take place?

A. Recovery

B. Identification

C. Lessons learned

D. Preparation

Correct Answer: C

Lessons learned or remediation step is the final phase of the incident response. It examines and documents how well the team responded, discovers what caused the incident, and determines how the incident can be avoided in the future.

==========

Phases of the Incident Response Plan:

1.

Preparation - Preparing for an attack and how to respond

2.

Identification - Identifying the threat

3.

Containment - Containing the threat

4.

Eradication - Removing the threat

5.

Recovery - Recovering affected systems

6.

Lessons Learned - Evaluating the incident response, see where there can be improvements for a future incident.

QUESTION 14

A network administrator needs to build out a new datacenter, with a focus on resiliency and uptime. Which of the following would BEST meet this objective? (Choose two.)

A. Dual power supply

B. Off-site backups

C. Automatic OS upgrades

D. NIC teaming

E. Scheduled penetration testing

F. Network-attached storage

Correct Answer: AB

Dual PS keeps the servers up / a DRS will conform to the question of resiliency: Site Resiliency Resiliency of a site should include consideration of sites used to continue operations. Site resiliency considerations can be connected to the idea of restoration sites and their availability. Related to the location of backup storage is where the restoration services will be located. If the organization has suffered physical damage to its facility, having offsite data storage is only part of the solution. This data will need to be processed somewhere, which means that computing facilities similar to those used in normal operations are required. These sites are referred to as recovery sites. The recovery problem can be approached in a number of ways, including hot sites, warm sites, and cold sites.

https://searchdatacenter.techtarget.com/definition/resiliency

QUESTION 15

While reviewing the wireless router, a systems administrator of a small business determines someone is spoofing the MAC address of an authorized device. Given the table below:

Hostname	IP address	MAC	MAC filter
PC1	192.168.1.20	00:1E:1B:43:21:B2	On
PC2	192.168.1.23	31:1C:3C:13:25:C4	Off
PC3	192.168.1.25	20:A2:22:45:11:D2	On
UNKNOWN	192.168.1.21	12:44:B2:FF:A1:22	Off

Which of the following should be the administrator\\'s NEXT step to detect if there is a rague system without impacting availability?

A. Conduct a ping sweep.

B. Physically check each system.

C. Deny Internet access to the "UNKNOWN" hostname.

D. Apply MAC filtering.

Correct Answer: A

NEED FOR PING SWEEP

Ping sweep is used for various purposes, such as improving and maintaining network security. It can also be used to:

Discover active IP addresses on the network

Ensure IP addresses on the network match the documentation

Detect rogue devices connected to the network

Latest SY0-601 Dumps SY0-601 VCE Dumps SY0-601 Practice Test