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

QUESTION 1

A security analyst is responding to an alert from the SIEM. The alert states that malware was discovered on a host and was not automatically deleted. Which of the following would be BEST for the analyst to perform?

A. Add a deny-all rule to that host in the network ACL

B. Implement a network-wide scan for other instances of the malware.

C. Quarantine the host from other parts of the network

D. Revoke the client\\'s network access certificates

Correct Answer: C

QUESTION 2

A security assessment determines DES and 3DES at still being used on recently deployed production servers. Which of the following did the assessment identify?

A. Unsecme protocols

B. Default settings

C. Open permissions

D. Weak encryption

Correct Answer: D

DES stands for Data Encryption Standard hence why the answer is encryption as its still using a weak/old encryption standard.

QUESTION 3

The spread of misinformation surrounding the outbreak of a novel virus on election day led to eligible voters choosing not to take the risk of going the polls. This is an example of:

A. prepending

B. an influence campaign.

C. A watering-hole attack

D. intimidation

E. information elicitation.

Correct Answer: B

From Chapter 1 Social Engineering Techniques Influence Campaigns Influence campaigns involve the use of collected information and selective publication of material to key individuals in an attempt to alter perceptions and change people\\'s minds on a topic. One can engage in an influence campaign against a single person, but the effect is limited. Influence campaigns are even more powerful when used in conjunction with social media to spread influence through influencer propagation. Influencers are people who have large followings of people who read what they post, and in many cases act in accordance or agreement. This results in an amplifying mechanism, where single pieces of disinformation can be rapidly spread and build a following across the Internet.

QUESTION 4

A Chief Security Officer (CSO) is concerned about the volume and integrity of sensitive information that is exchanged between the organization and a third party through email. The CSO is particularly concerned about an unauthorized party who is intercepting information that is in transit between the two organizations.

Which of the following would address the CSO\\'s concerns?

A. SPF

B. DMARC

C. SSL

D. DKIM

E. TLS

Correct Answer: E

DKIM (DomainKeys Identified Mail) is a protocol that allows an organization to take responsibility for transmitting a message by signing it in a way that mailbox providers can verify. DKIM record verification is made possible through cryptographic authentication. Transport Layer Security (TLS) encrypts data sent over the Internet to ensure that eavesdroppers and hackers are unable to see what you transmit which is particularly useful for private and sensitive information such as passwords, credit card numbers, and personal correspondence

---

QUESTION 5

Which of the following provides guidelines for the management and reduction of information security risk?

A. CIS

B. NIST CSF

C. ISO

D. PCI DSS

Correct Answer: B

QUESTION 6

A company is switching to a remote work model for all employees. All company and employee resources will be in the cloud. Employees must use their personal computers to access the cloud computing environment. The company will manage the operating system. Which of the following deployment models is the company implementing?

A. CYOD

B. MDM

C. COPE

D. VDI

Correct Answer: D

According to Professor Messer\\'s video1, VDI stands for Virtual Desktop Infrastructure and it is a deployment model where employees use their personal computers to access a virtual machine that runs the company\\'s operating system and applications.

In the scenario described, the company is implementing a virtual desktop infrastructure (VDI) deployment model [1]. This allows employees to access the cloud computing environment using their personal computers, while the company manages the operating system. The VDI model is suitable for remote work scenarios because it provides secure and centralized desktop management, while allowing employees to access desktops from any device.

QUESTION 7

Multiple beaconing activities to a malicious domain have been observed. The malicious domain is hosting malware from various endpoints on the network. Which of the following technologies would be best to correlate the activities between the different endpoints?

A. Firewall

B. SIEM

C. IPS

D. Protocol analyzer

Correct Answer: B

SIEM stands for Security Information and Event Management, which is a technology that collects, analyzes, and correlates data from multiple sources, such as firewall logs, IDS/IPS alerts, network devices, applications, and endpoints. SIEM provides real-time monitoring and alerting of security events, as well as historical analysis and reporting for compliance and forensic purposes. A SIEM technology would be best to correlate the activities between the different endpoints that are beaconing to a malicious domain. A SIEM can detect the malicious domain by comparing it with threat intelligence feeds or known indicators of compromise (IOCs). A SIEM can also identify the endpoints that are communicating with the malicious domain by analyzing the firewall logs and other network traffic data. A SIEM can alert the security team of the potential compromise and provide them with relevant information for investigation and remediation. A security analyst reviews web server logs and notices the following line:

104.35. 45.53 [22/May/2020:07 : 00:58 +0100] "GET . UNION ALL SELECT user login, user _ pass, user email from wp users---- HTTP/I.I" 200 1072 http://www.example.com/wordpress/wp--admin/

QUESTION 8

A user enters a password to log in to a workstation and is then prompted to enter an authentication code. Which of the following MFA factors or attributes are being utilized in the authentication process? (Select TWO).

A. Something you know

B. Something you have

C. Somewhere you are

D. Someone you are

E. Something you are

F. Something you can do

Correct Answer: AB

This is yet another poorly worded question, obviously the password is something you know, the authentication code is extremely vague. If you are like me you were looking for the option that this isn\\'t MFA or two options of "something you know". But it is up to us to suss out that an authentication code can come from a item you have such as a phone or phob etc.....

QUESTION 9

A company is designing the layout of a new datacenter so it will have an optimal environmental temperature Which of the following must be included? (Select TWO)

A. An air gap

B. A cold aisle

C. Removable doors

D. A hot aisle

E. An loT thermostat

F. A humidity monitor

Correct Answer: BD

Hot aisle/cold aisle refers to a layout design especially for data warehouses or datacenters where huge servers and computing equipment are kept and data is stored. The purpose of the hot aisle/cold aisle scheme is to manage air flow in data centers, consequently lowering the energy, cooling and management cost inside data centers

---

QUESTION 10

A cybersecurity department purchased o new PAM solution. The team is planning to randomize the service account credentials of the Windows server first. Which of the following would be the BEST method to increase the security on the Linux server?

A. Randomize the shared credentials

B. Use only guest accounts to connect.

C. Use SSH keys and remove generic passwords

D. Remove all user accounts.

Correct Answer: C

(Use SSH keys and remove generic passwords.) seems like the better answer because it involves authentication. https://jumpcloud.com/blog/what-are-ssh-keys Using a guest account does nothing for security.

QUESTION 11

An incident analyst finds several image files on a hard disk. The image files may contain geolocation coordinates. Which of the following best describes the type of information the analyst is trying to extract from the image files?

A. Log data

B. Metadata

C. Encrypted data

D. Sensitive data

Correct Answer: B

QUESTION 12

After a recent security breach, a security analyst reports that several administrative usernames and passwords are being sent via cleartext across the network to access network devices over port 23. Which of the following should be implemented so all credentials sent over the network are encrypted when remotely accessing and configuring network devices?

A. SSH

B. SNMPv3

C. SFTP

D. Telnet

E. FTP

Correct Answer: A

SSH (22)

Port 23 (Telnet) and Port 22 (SSH) are network protocols used to remotely access and manage systems however telnet does not encrypt the connection so captured traffic appears in cleartext whereas an ssh connection would be encrypted.

========================

SNMP (Simple Network Management Protocol) - is a protocol for collecting and organizing information about managed devices on networks. Devices that typically support SNMP include servers/desktops, routers, switches, etc.

SFTP (Secure File Transfer Protocol) is a secure file transfer protocol that uses SSH encryption to securely sending and receiving file transfers.

FTP (File Transfer Protocol) - For file transfers

QUESTION 13

An administrator is experiencing issues when trying to upload a support file to a vendor A pop-up message reveals that a payment card number was found in the file, and the file upload was Mocked. Which of the following controls is most likely causing this issue and should be checked FIRST?

A. DLP

B. Firewall rule

C. Content filter

D. MDM

E. Application allow list

Correct Answer: A

DLP - Data Loss Prevention uses exact data matching or regex matching

in this case a regex rule for detecting credit card numbers could be in place that is actively blocking the upload of the document Regex for detecting and Amex Card: ^3[47][0-9]{13}$

Source https://stackoverflow.com/questions/9315647/regex-credit-card-number-tests

---

QUESTION 14

A security analyst is concerned about critical vulnerabilities that have been detected on some applications running inside containers Which of the following is the BEST remediation strategy?

A. Update the base container image and redeploy the environment

B. Include the containers in the regular patching schedule for servers

C. Patch each running container individually and test the application

D. Update the host in which the containers are running

Correct Answer: A

In the scenario, the vulnerabilities found were critical meaning that patches would need to be applied immediately.

The options to patch the containers (B andC) could work, however, patching would likely take months, seeing how this vulnerability is critical, neither would address the concern\\'s urgency.

The option to update the host (D) also could work, however, the scenario specified that the vulnerabilities have been detected only on some applications and not on the host itself. While a container runs on a host machine, it does not mean they share the same vulnerabilities. So updating the host would likely not patch the vulnerabilities that were found in the containers.

Out of the given options, the option to update on the base container image would 1.) addresses where the vulnerabilities were found and what needs to be updated and 2.) addresses the urgency to patch the critical vulnerability.

QUESTION 15

Which of the following types of disaster recovery plan exercises requires the least interruption to IT operations?

A. Parallel

B. Full-scale

C. Tabletop

D. Simulation

Correct Answer: C