SY0-601 Q&As

CompTIA Security+ 2021

Pass CompTIA SY0-601 Exam with 100% Guarantee

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

https://www.certbus.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

An organization is concerned about hackers potentially entering a facility and plugging in a remotely accessible Kali Linux box.

Which of the following should be the first lines of defense against such an attack? (Select TWO).

A. MAC filtering

B. Zero Trust segmentation

C. Network access control

D. Access control vestibules

E. Guards

F. Bollards

Correct Answer: BD

QUESTION 2

An organization needs to implement more stringent controls over administrator/root credentials and service accounts. Requirements for the project include:

1.

Check-in/checkout of credentials

2.

The ability to use but not know the password

3.

Automated password changes

4.

Logging of access to credentials

Which of the following solutions would meet the requirements?

A. OAuth 2.0

B. Secure Enclave

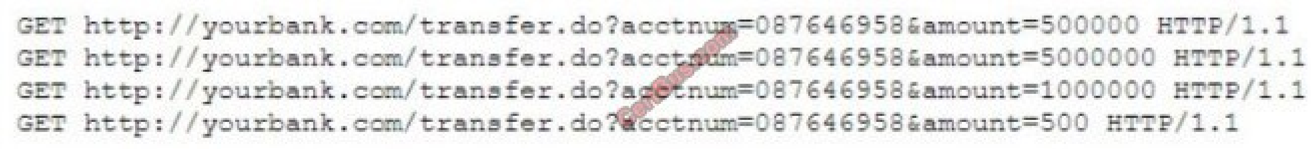
C. A privileged access management system

D. An OpenID Connect authentication system

Correct Answer: D

QUESTION 3

A security analyst is reviewing the output of a web server log and notices a particular account is attempting to transfer large amounts of money:



```
GET http://yourbank.com/transfer.do?acctnum=087646958&amount=500000 HTTP/1.1
GET http://yourbank.com/transfer.do?acctnum=087646958&amount=5000000 HTTP/1.1
GET http://yourbank.com/transfer.do?acctnum=087646958&amount=1000000 HTTP/1.1
GET http://yourbank.com/transfer.do?acctnum=087646958&amount=500 HTTP/1.1
```

Which of the following types of attack is MOST likely being conducted?

A. SQLi

B. CSRF

C. Session replay

D. API

Correct Answer: C

QUESTION 4

An analyst is trying to identify insecure services that are running on the internal network After performing a port scan the analyst identifies that a server has some insecure services enabled on default ports Which of the following BEST describes the services that are currently running and the secure alternatives for replacing them\\' (Select THREE)

A. SFTP FTPS

B. SNMPv2 SNMPv3

C. HTTP, HTTPS

D. TFTP FTP

E. SNMPv1, SNMPv2

F. Telnet SSH

G. TLS, SSL

H. POP, IMAP

I. Login, rlogin

Correct Answer: BCF

QUESTION 5

The SIEM at an organization has detected suspicious traffic coming a workstation in its internal network. An analyst in the SOC the workstation and discovers malware that is associated with a botnet is installed on the device A review of the logs on the workstation reveals that the privileges of the local account were escalated to a local administrator. To which of the following groups should the analyst report this real-world event?

A. The NOC team

B. The vulnerability management team

C. The CIRT

D. The read team

Correct Answer: A

QUESTION 6

A company just implemented a new telework policy that allows employees to use personal devices for official email and file sharing while working from home. Some of the requirements are:

1.

Employees must provide an alternate work location (i.e., a home address)

2.

Employees must install software on the device that will prevent the loss of proprietary data but will not restrict any other software from being installed.

Which of the following BEST describes the MDM options the company is using?

A. Geofencing, content management, remote wipe, containerization, and storage segmentation

B. Content management, remote wipe, geolocation, context-aware authentication, and containerization

C. Application management, remote wipe, geofencing, context-aware authentication, and containerization

D. Remote wipe, geolocation, screen locks, storage segmentation, and full-device encryption

Correct Answer: D

QUESTION 7

An attacker is attempting to exploit users by creating a fake website with the URL users. Which of the following social-engineering attacks does this describe?

A. Information elicitation

B. Typo squatting

C. Impersonation

D. Watering-hole attack

Correct Answer: D

QUESTION 8

The Chief Security Officer (CSO) at a major hospital wants to implement SSO to help improve in the environment patient data, particularly at shared terminals. The Chief Risk Officer (CRO) is concerned that training and guidance have been provided to frontline staff, and a risk analysis has not been performed. Which of the following is the MOST likely cause of the CRO\\'s concerns?

A. SSO would simplify username and password management, making it easier for hackers to pass guess accounts.

B. SSO would reduce password fatigue, but staff would still need to remember more complex passwords.

C. SSO would reduce the password complexity for frontline staff.

D. SSO would reduce the resilience and availability of system if the provider goes offline.

Correct Answer: D

QUESTION 9

A large industrial system\\'s smart generator monitors the system status and sends alerts to third-party maintenance personnel when critical failures occur. While reviewing the network logs the company\\'s security manager notices the generator\\'s IP is sending packets to an internal file server\\'s IP. Which of the following mitigations would be BEST for the security manager to implement while maintaining alerting capabilities?

A. Segmentation

B. Firewall whitelisting

C. Containment

D. isolation

Correct Answer: A

QUESTION 10

An organization\\'s help desk is flooded with phone calls from users stating they can no longer access certain websites. The help desk escalates the issue to the security team, as these websites were accessible the previous day. The security analysts run the following command: ipconfig /flushdns, but the issue persists. Finally, an analyst changes the DNS server for an impacted machine, and the issue goes away. Which of the following attacks MOST likely occurred on the original DNS server?

A. DNS cache poisoning

B. Domain hijacking

C. Distributed denial-of-service

D. DNS tunneling

Correct Answer: B

QUESTION 11

During an asset inventory, several assets, supplies, and miscellaneous items were noted as missing. The security manager has been asked to find an automated solution to detect any future theft of equipment. Which of the following would be BEST to implement?

A. Badges

B. Fencing

C. Access control vestibule

D. Lighting

E. Cameras

Correct Answer: C

QUESTION 12

A company has determined that if its computer-based manufacturing is not functioning for 12 consecutive hours, it will lose more money that it costs to maintain the equipment. Which of the following must be less than 12 hours to maintain a positive total cost of ownership?

A. MTBF

B. RPO

C. RTO

D. MTTR

Correct Answer: C

QUESTION 13

An organization routes all of its traffic through a VPN Most users are remote and connect into a corporate datacenter that houses confidential information There is a firewall at the Internet border followed by a DIP appliance, the VPN server and the datacenter itself. Which of the following is the WEAKEST design element?

A. The DLP appliance should be integrated into a NGFW.

B. Split-tunnel connections can negatively impact the DLP appliance\\'s performance

C. Encrypted VPN traffic will not be inspected when entering or leaving the network

D. Adding two hops in the VPN tunnel may slow down remote connections

Correct Answer: C

QUESTION 14

Which of the following BEST describes the method a security analyst would use to confirm a file that is downloaded from a trusted security website is not altered in transit or corrupted using a verified checksum?

A. Hashing

B. Salting

C. Integrity

D. Digital signature

Correct Answer: A

QUESTION 15

A local coffee shop runs a small WiFi hot-spot for its customers that utilizes WPA2-PSK. The coffee shop would like to stay current with security trends and wants to implement WPA3 to make its WiFi even more secure.

Which of the following technologies will the coffee shop MOST likely use in place of PSK?

A. WEP

B. MSCHAP

C. WPS

D. SAE

Correct Answer: A

Submit A Ticket

100%