DUMPS Expert

CompTIA

SY0-601

CompTIA Security+ Exam 2021

Version: Demo

[Total Questions: 467]

Web: www.dumpsexpert.com

Email: support@dumpsexpert.com

IMPORTANT NOTICE

Feedback

We have developed quality product and state-of-art service to ensure our customers interest. If you have any suggestions, please feel free to contact us at feedback@dumpsexpert.com

Support

If you have any questions about our product, please provide the following items:

- exam code
- screenshot of the question
- login id/email

please contact us at support@dumpsexpert.com and our technical experts will provide support within 24 hours.

Copyright

Question #:1

An.. that has a large number of mobile devices is exploring enhanced security controls to manage unauthorized access if a device is lost or stolen. Specifically, if mobile devices are more

than 3mi (4 8km) from the building, the management team would like to have the security team alerted and server resources restricted on those devices. Which of the following controls should the

organization implement?

A. Geofencing

B. Lockout

C. Near-field communication

D. GPS tagging.

Answer: A

Question #:2

The IT department’s on-site developer has been with the team for many years. Each time an application is released, the security team is able to identify multiple vulnerabilities. Which of the following would BEST help the team ensure the application is ready to be released to production?

A. Limit the use of third-party libraries.

B. Prevent data exposure queries.

C. Obfuscate the source code.

D. Submit the application to QA before releasing it.

Answer: D

Question #:3

Phishing and spear-phishing attacks have been occurring more frequently against a company’s staff. Which of the following would MOST likely help mitigate this issue?

A. DNSSEC and DMARC

B. DNS query logging

C. Exact mail exchanger records in the DNS

D. The addition of DNS conditional forwarders

Answer: C

Question #:4

The manager who is responsible for a data set has asked a security engineer to apply encryption to the data on a hard disk. The security engineer is an example of a:

A. data controller.

B. data owner

C. data custodian.

D. data processor

Answer: D

Question #:5

After reading a security bulletin, a network security manager is concerned that a malicious actor may have breached the network using the same software flaw. The exploit code is publicly available and has been reported as being used against other industries in the same vertical. Which of the following should the network security manager consult FIRST to determine a priority list for forensic review?

A. The vulnerability scan output

B. The IDS logs

C. The full packet capture data

D. The SIEM alerts

Answer: A

Question #:6

Which of the following are requirements that must be configured for PCI DSS compliance? (Select TWO).

A. Testing security systems and processes regularly

B. Installing and maintaining a web proxy to protect cardholder data

C. Assigning a unique ID to each person with computer access

D. Encrypting transmission of cardholder data across private networks

E. Benchmarking security awareness training for contractors

F. Using vendor-supplied default passwords for system passwords

Answer: B, D

Question #:7

A user must introduce a password and a USB key to authenticate against a secure computer, and authentication is limited to the state in which the company resides. Which of the following authentication concepts are in use?

A. Something you know, something you have, and somewhere you are

B. Something you know, something you can do, and somewhere you are

C. Something you are, something you know, and something you can exhibit

D. Something you have, somewhere you are, and someone you know

Answer: A

Question #:8

A company wants to modify its current backup strategy to minimize the number of backups that would need to be restored in case of data loss. Which of the following would be the BEST backup strategy to implement?

A. Incremental backups followed by differential backups

B. Full backups followed by incremental backups

C. Delta backups followed by differential backups

D. Incremental backups followed by delta backups

E. Full backups followed by differential backups

Answer: B

Question #:9

A user contacts the help desk to report the following:
Two days ago, a pop-up browser window prompted the user for a name and password after connecting to the corporate wireless SSID. This had never happened before, but the user entered the information as requested.

The user was able to access the Internet but had trouble accessing the department share until the next day.

The user is now getting notifications from the bank about unauthorized transactions.

Which of the following attack vectors was MOST likely used in this scenario?

A. Rogue access point

B. Evil twin

C. DNS poisoning

D. ARP poisoning

Answer: A

About dumpsexpert.com

dumpsexpert.com was founded in 2007. We provide latest & high quality IT / Business Certification Training Exam Questions, Study Guides, Practice Tests.

We help you pass any IT / Business Certification Exams with 100% Pass Guaranteed or Full Refund. Especially Cisco, CompTIA, Citrix, EMC, HP, Oracle, VMware, Juniper, Check Point, LPI, Nortel, EXIN and so on.

View list of all certification exams: All vendors

We prepare state-of-the art practice tests for certification exams. You can reach us at any of the email addresses listed below.

- Sales: sales@dumpsexpert.com
- Feedback: feedback@dumpsexpert.com
- Support: support@dumpsexpert.com

Any problems about IT certification or our products, You can write us back and we will get back to you within 24 hours.