DC DEVELOPER CERTIFICATION

SUCCEED AT THE FIRST ATTEMPT!

https://developercertification.com

Questions and Answers Demo PDF

CompTIA

CAS-003 Exam

CompTIA Advanced Security Practitioner Exam

Questions & Answers
Demo

Version: 28.0

Question: 1

An attacker exploited an unpatched vulnerability in a web framework, and then used an application service account that had an insecure configuration to download a rootkit The attacker was unable to obtain root privileges Instead the attacker then downloaded a crypto-currency mining program and subsequently was discovered The server was taken offline, rebuilt, and patched. Which of the following should the security engineer suggest to help prevent a similar scenario in the future?

A. Remove root privileges from the application service account
B. Implement separation of duties.
C. Properly configure SELinux and set it to enforce.
D. Use cron to schedule regular restarts of the service to terminate sessions.
E. Perform regular uncredentialed vulnerability scans

Answer: E

Question: 2

An engineer wants to assess the OS security configurations on a company's servers. The engineer has downloaded some files to orchestrate configuration checks When the engineer opens a file in a text editor, the following excerpt appears:

```
<?xml version="1.0" encoding="UTF-8"?>
<cdf:Benchmark id="server-check" resolved="0" xml:lang="en">
        ...
        xsi:schemaLocation="http://checklists.nist.gov/xccdf/1.1" xccdf-1.1.xsd
        ...
</cdf:Benchmark>
```

Which of the following capabilities would a configuration compliance checker need to support to interpret this file?

A. Nessus
B. Swagger file
C. SCAP
D. Netcat
E. WSDL

Answer: A

Question: 3

A Chief Information Security Officer (CISO) has created a survey that will be distributed to managers of mission-critical functions across the organization The survey requires the managers to determine how long their respective units can operate in the event of an extended IT outage before the organization suffers monetary losses from the outage To which of the following is the survey question related? (Select TWO)

A. Risk avoidance
B. Business impact
C. Risk assessment
D. Recovery point objective
E. Recovery time objective
E. Mean time between failures

Answer: B, D

Question: 4

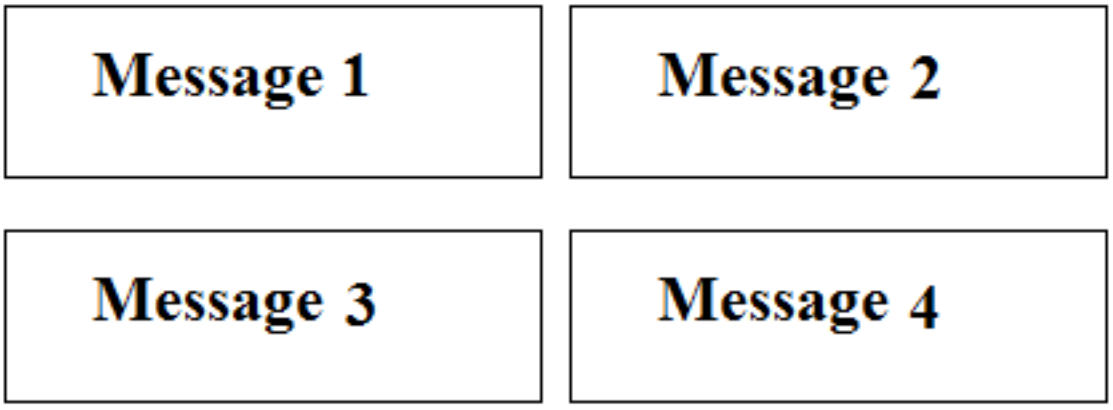
Following a recent security incident on a web server the security analyst takes HTTP traffic captures for further investigation The analyst suspects certain jpg files have important data hidden within them. Which of the following tools will help get all the pictures from within the HTTP traffic captured to a specified folder?

A. tshark
B. memdump
C. nbtstat
D. dd

Answer: A

Question: 5

Click on the exhibit buttons to view the four messages.



Message 1

Send

To:

Cc:

Subject: Security Escalation for ProjectX

I am escalating a security issue for ProjectX, which is an initiative to deliver exciting banking features to customers, with an initial release scheduled for next week.

The project had oroginally planned to implement storage-level encryption of customer details, but it is unable to deliver this security control in time for next week's launch. The impact will be minimized if the project agres on a post-launch mitigation date for this security control, as well as implementing detective controls in the interim (i.e., additional staff performing log monitoring of all calls to the storage module).

Is leadership willing to accept this project risk or are additional details needed to be able to reach a decision?

Message 2

Send

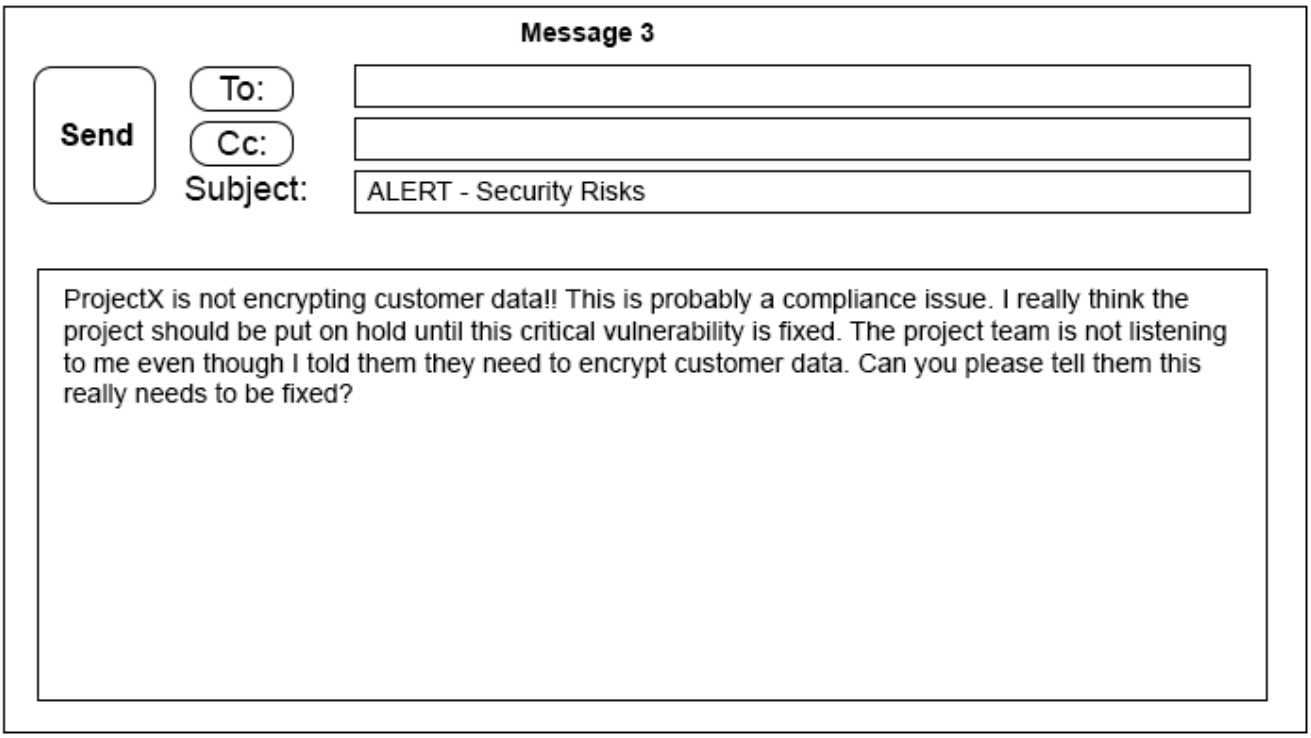
To:

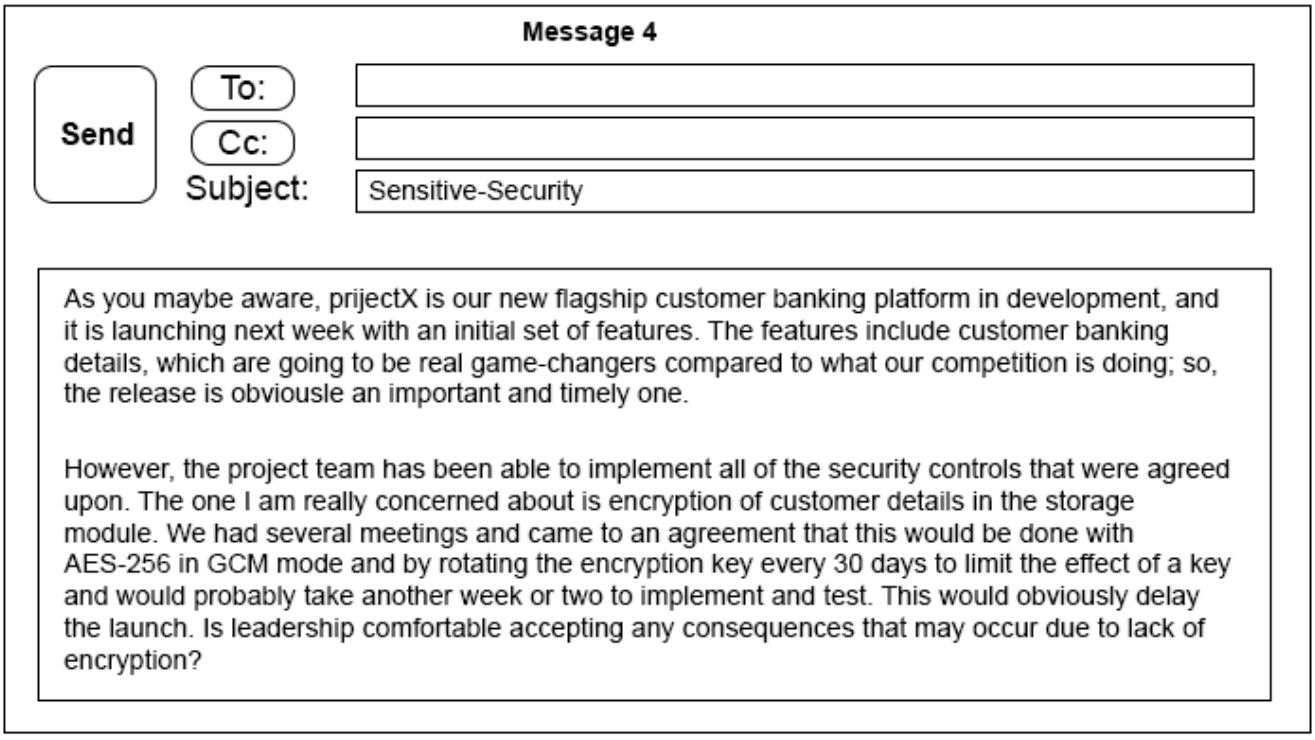
Cc:

Subject: Security Vulnerability for ProjectX

It has come to my attention that ProjectX has a security vulnerability. The storage module does not encrypt sensitive customer details, and this could lead to a data breach, resulting in negative media attention.

My recommendation is to delay the launch until this security control is implemented. Do you concur?





A security architect is working with a project team to deliver an important service that stores and processes customer banking details. The project, internally known as ProjectX, is due to launch its first set of features publicly within a week, but the team has not been able to implement encryption-at-rest of the customer records. The security architect is drafting an escalation email to senior leadership.
Which of the following BEST conveys the business impact for senior leadership?

A. Message 1
B. Message 2
C. Message 3
D. Message 4

Answer: D

Question: 6

A software development firm wants to validate the use of standard libraries as part of the software development process Each developer performs unit testing prior to committing changes to the code repository. Which of the following activities would be BEST to perform after a commit but before the creation of a branch?

A. Static analysis
B. Heuristic analysis
C. Dynamic analysis
D. Web application vulnerability scanning
E. Penetration testing

Answer: A

Question: 7

A company's human resources department recently had its own shadow IT department spin up ten VMs that host a mixture of differently labeled data types (confidential and restricted) on the same VMs Which of the following cloud and visualization considerations would BEST address the issue presented in this scenario?

A. Vulnerabilities associated with a single platform hosting multiple data types on VMs should have been considered
B. Vulnerabilities associated with a single server hosting multiple data types should have been considered.
C. Type 1vs Type 2 hypervisor approaches should have been considered
D. Vulnerabilities associated with shared hosting services provided by the IT department should have been considered.

Answer: B

Question: 8

An internal penetration tester finds a legacy application that takes measurement input made in a text box and outputs a specific string of text related to industry requirements. There is no documentation about how this application works, and the source code has been lost. Which of the following would BEST allow the penetration tester to determine the input and output relationship?

A. Running an automated fuzzer
B. Constructing a known cipher text attack
C. Attempting SQL injection commands
D. Performing a full packet capture
E. Using the application in a malware sandbox

Answer: A

Question: 9

An organization is facing budget constraints The Chief Technology Officer (CTO) wants to add a new marketing platform but the organization does not have the resources to obtain separate servers to run the new platform. The CTO recommends running the new marketing platform on a virtualized video-conferencing server because video conferencing is rarely used The Chief Information Security Officer (CISO) denies this request Which of the following BEST explains the reason why the CISO has not approved the request?

A. Privilege escalation attacks
B. Performance and availability
C. Weak DAR encryption
D. Disparate security requirements

Answer: D

Question: 10

A company is implementing a new secure identity application, given the following requirements
• The cryptographic secrets used in the application must never be exposed to users or the OS
• The application must work on mobile devices.
• The application must work with the company's badge reader system
Which of the following mobile device specifications are required for this design? (Select TWO).

A. Secure element
B. Biometrics
C. UEFI
D. SEAndroid
E. NFC
F. HSM

Answer: B, E

https://developercertification.com