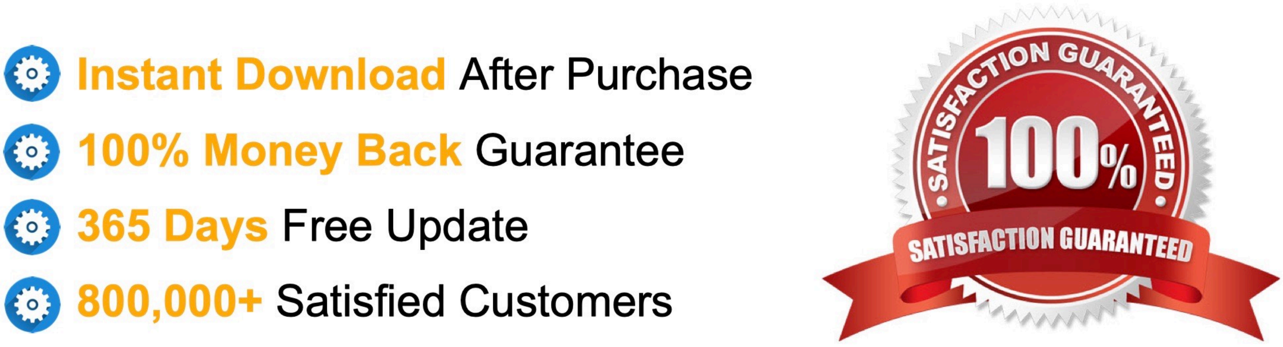
CS0-002 Q&As

CompTIA Cybersecurity Analyst (CySA+)

Pass CompTIA CS0-002 Exam with 100% Guarantee

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
SATISFACTION GUARANTEED
100%
SATISFACTION GUARANTEED

QUESTION 1

Which of the following are essential components within the rules of engagement for a penetration test? (Select TWO).

A. Schedule

B. Authorization

C. List of system administrators

D. Payment terms

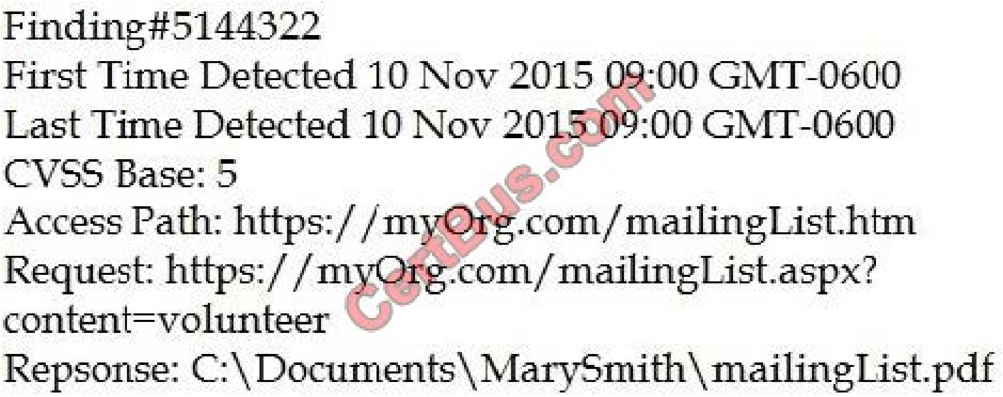
E. Business justification

Correct Answer: AB

QUESTION 2

An organization is attempting to harden its web servers and reduce the information that might be disclosed by potential attackers. A security analyst is reviewing vulnerability scan results from a recent web server scan.

Portions of the scan results are shown below:



```
Finding#5144322
First Time Detected 10 Nov 2015 09:00 GMT-0600
Last Time Detected 10 Nov 2015 09:00 GMT-0600
CVSS Base: 5
Access Path: https://myOrg.com/mailingList.htm
Request: https://myOrg.com/mailingList.aspx?
content=volunteer
Repsonse: C:\Documents\MarySmith\mailingList.pdf
```

Which of the following lines indicates information disclosure about the host that needs to be remediated?

A. Response: :\Documents\MarySmith\mailingList.pdf

B. Finding#5144322

C. First Time Detected 10 Nov 2015 09:00 GMT-0600

D. Access Path: http://myOrg.com/mailingList.htm

E. Request: GET http://myOrg.com/mailingList.aspx?content=volunteer

Correct Answer: A

QUESTION 3

A security analyst for a large pharmaceutical company was given credentials from a threat intelligence resources organisation for Internal users, which contain usernames and valid passwords for company accounts. Which of the following is the FIRST action the analyst should take as part of security operations monitoring?

A. Run scheduled antivirus scans on all employees\\' machines to look for malicious processes.

B. Reimage the machines of all users within the group in case of a malware infection.

C. Change all the user passwords to ensure the malicious actors cannot use them.

D. Search the event logs for event identifiers that indicate Mimikatz was used.

Correct Answer: C

QUESTION 4

A security analyst is assisting in the redesign of a network to make it more secure. The solution should be low cost, and access to the secure segments should be easily monitored, secured, and controlled. Which of the following should be implemented?

A. System isolation

B. Honeyport

C. Jump box

D. Mandatory access control

Correct Answer: C

QUESTION 5

A security administrator recently deployed a virtual honeynet. The honeynet is not protected by the company\\'s firewall, while all production networks are protected by a stateful firewall. Which of the following would BEST allow an external penetration tester to determine which one is the honeynet\\'s network?

A. Banner grab

B. Packet analyzer

C. Fuzzer

D. TCP ACK scan

Correct Answer: D

QUESTION 6

A security analyst is conducting a vulnerability assessment of older SCADA devices on the corporate network. Which of the following compensating controls is likely to prevent the scans from providing value?

A. Access control list network segmentation that prevents access to the SCADA devices inside the network.

B. Detailed and tested firewall rules that effectively prevent outside access of the SCADA devices.

C. Implementation of a VLAN that allows all devices on the network to see all SCADA devices on the network.

D. SCADA systems configured with `SCADA SUPPORT\\'=ENABLE

Correct Answer: B

QUESTION 7

A network appliance manufacturer is building a new generation of devices and would like to include chipset security improvements. Management wants the security team to implement a method to prevent security weaknesses that could be reintroduced by downgrading the firmware version on the chipset. Which of the following would meet this objective?

A. UEFI

B. A hardware security module

C. eFUSE

D. Certificate signed updates

Correct Answer: C

QUESTION 8

Which of the following is a best practice when sending a file/data to another individual in an organization?

A. When encrypting, split the file, and then compress each file.

B. Encrypt and then compress the file.

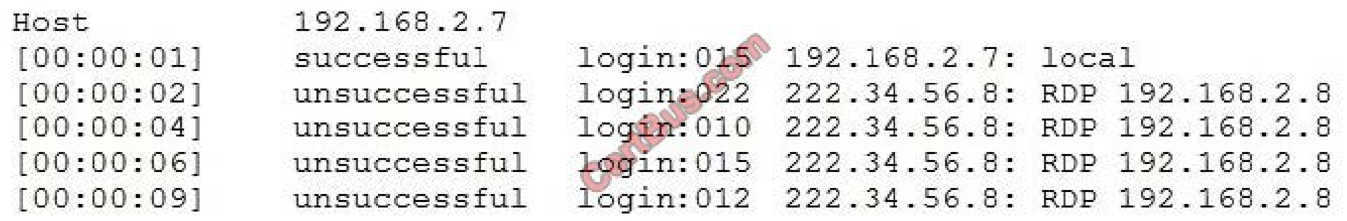
C. Encrypt the file but do not compress it.

D. Compress and then encrypt the file.

Correct Answer: D

QUESTION 9

A security analyst has determined the security team should take action based on the following log:



```
Host          192.168.2.7
[00:00:01]    successful      login:015  192.168.2.7:  local
[00:00:02]    unsuccessful    login:022  222.34.56.8:  RDP 192.168.2.8
[00:00:04]    unsuccessful    login:010  222.34.56.8:  RDP 192.168.2.8
[00:00:06]    unsuccessful    login:015  222.34.56.8:  RDP 192.168.2.8
[00:00:09]    unsuccessful    login:012  222.34.56.8:  RDP 192.168.2.8
```

Which of the following should be used to improve the security posture of the system?

A. Enable login account auditing.

B. Limit the number of unsuccessful login attempts.

C. Upgrade the firewalls.

D. Increase password complexity requirements.

Correct Answer: B

QUESTION 10

A Chief Information Security Officer (CISO) wants to standardize the company\\'s security program so it can be objectively assessed as part of an upcoming audit requested by management.

Which of the following would holistically assist in this effort?

A. ITIL

B. NIST

C. Scrum

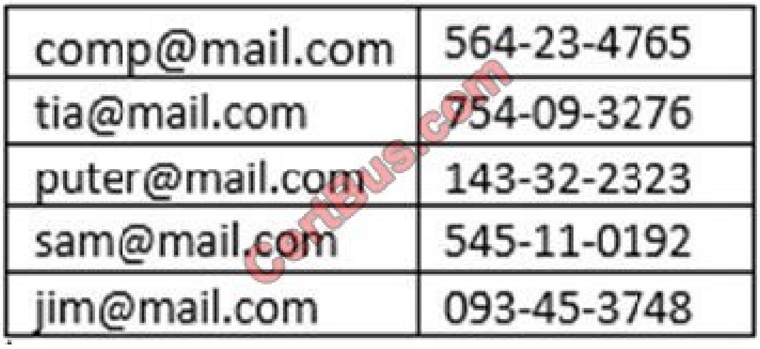
D. AUP

E. Nessus

Correct Answer: B

QUESTION 11

Company A suspects an employee has been exfiltrating PII via a USB thumb drive. An analyst is tasked with attempting to locate the information on the drive. The PII in question includes the following:



comp@mail.com	564-23-4765
tia@mail.com	754-09-3276
puter@mail.com	143-32-2323
sam@mail.com	545-11-0192
jim@mail.com	093-45-3748

Which of the following would BEST accomplish the task assigned to the analyst?

A. 3 [0-9]\d-2[0-9]\d-4[0-9]\d

B. \d(3)-d(2)-\d(4)

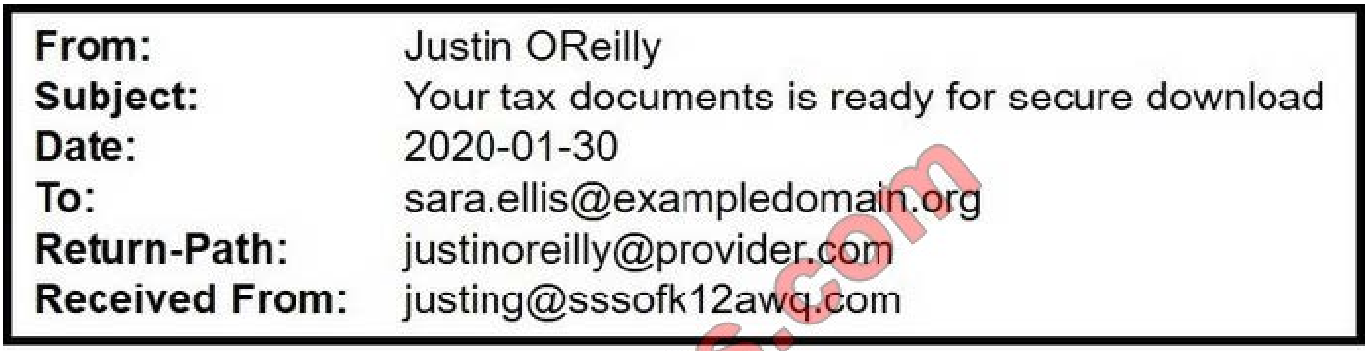
C. ?[3]-?[2]-?[3]

D. \d[9] `XXX-XX-XX\\'

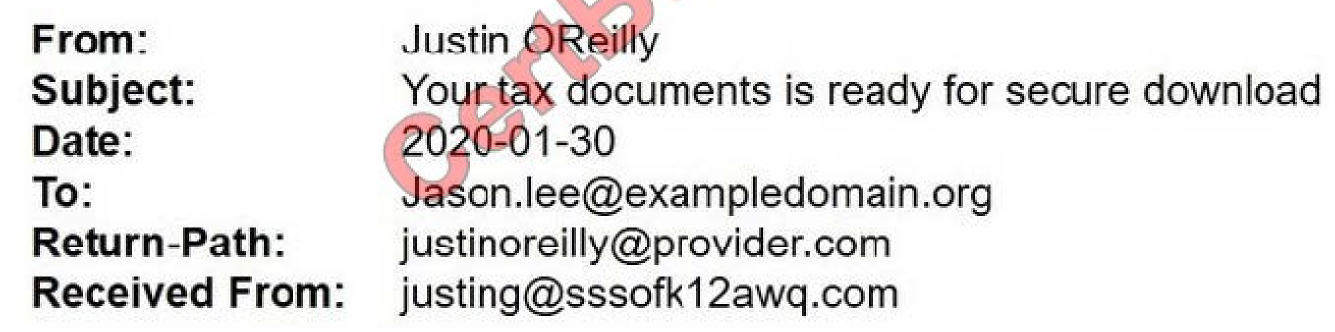
Correct Answer: B

QUESTION 12

A security analyst is looking at the headers of a few emails that appear to be targeting all users at an organization:



From:	Justin OReilly
Subject:	Your tax documents is ready for secure download
Date:	2020-01-30
To:	sara.ellis@exampledomain.org
Return-Path:	justinoreilly@provider.com
Received From:	justing@sssofk12awq.com



From:	Justin OReilly
Subject:	Your tax documents is ready for secure download
Date:	2020-01-30
To:	Jason.lee@exampledomain.org
Return-Path:	justinoreilly@provider.com
Received From:	justing@sssofk12awq.com

Which of the following technologies would MOST likely be used to prevent this phishing attempt?

A. DNSSEC

B. DMARC

C. STP

D. S/IMAP

Correct Answer: B

Reference: https://dmarc.org/

QUESTION 13

A logistics company\\'s vulnerability scan identifies the following vulnerabilities on Internet-facing devices in the DMZ: SQL injection on an infrequently used web server that provides files to vendors SSL/TLS not used for a website that contains promotional information

The scan also shows the following vulnerabilities on internal resources: Microsoft Office Remote Code Execution on test server for a human resources system TLS downgrade vulnerability on a server in a development network

In order of risk, which of the following should be patched FIRST?

A. Microsoft Office Remote Code Execution

B. SQL injection

C. SSL/TLS not used

D. TLS downgrade

Correct Answer: A

QUESTION 14

While planning segmentation for an ICS environment, a security engineer determines IT resources will need access to devices within the ICS environment without compromising security. To provide the MOST secure access model in this scenario, the jumpbox should be ___________.

A. placed in an isolated network segment, authenticated on the IT side, and forwarded into the ICS network.

B. placed on the ICS network with a static firewall rule that allows IT network resources to authenticate.

C. bridged between the IT and operational technology networks to allow authenticated access.

D. placed on the IT side of the network, authenticated, and tunneled into the ICS environment.

Correct Answer: A

QUESTION 15

Which of the following BEST describes the primary role ol a risk assessment as it relates to compliance with risk-based frameworks?

A. It demonstrates the organization\\'s mitigation of risks associated with internal threats.

B. It serves as the basis for control selection.

C. It prescribes technical control requirements.

D. It is an input to the business impact assessment.

Correct Answer: A

To Read the Whole Q&As, please purchase the Complete Version from Our website.

Try our product !

100% Guaranteed Success
100% Money Back Guarantee
365 Days Free Update
Instant Download After Purchase
24x7 Customer Support
Average 99.9% Success Rate
More than 800,000 Satisfied Customers Worldwide
Multi-Platform capabilities - Windows, Mac, Android, iPhone, iPod, iPad, Kindle

We provide exam PDF and VCE of Cisco, Microsoft, IBM, CompTIA, Oracle and other IT Certifications.
You can view Vendor list of All Certification Exams offered:

https://www.certbus.com/allproducts

Need Help

Please provide as much detail as possible so we can best assist you.
To update a previously submitted ticket:

One Year Free Update

Free update is available within One Year after your purchase. After One Year, you will get 50% discounts for updating. And we are proud to boast a 24/7 efficient Customer Support system via Email.

Money Back Guarantee

To ensure that you are spending on quality products, we provide 100% money back guarantee for 30 days from the date of purchase.

Security & Privacy

We respect customer privacy. We use McAfee's security service to provide you with utmost security for your personal information & peace of mind.