- **Vendor: CompTIA**
- **Exam Code: CS0-002**
- **Exam Name: CompTIA CSA+ Certification Exam**
- **New Updated Questions from Braindump2go (Updated in March/2021)**

QUESTION 585
An incident response team is responding to a breach of multiple systems that contain PII and PHI. Disclosing the incident to external entities should be based on:

A. the responder's discretion
B. the public relations policy
C. the communication plan
D. senior management's guidance

Answer: A

QUESTION 586
Which of the following assessment methods should be used to analyze how specialized software performs during heavy loads?

A. Stress test
B. API compatibility lest
C. Code review
D. User acceptance test
E. Input validation

Answer: A

QUESTION 587
A user reports the system is behaving oddly following the installation of an approved third-party software application. The application executable was sourced from an internal repository.
Which of the following will ensure the application is valid?

A. Ask the user to refresh the existing definition file for the antivirus software
B. Perform a malware scan on the file in the internal repository
C. Hash the application's installation file and compare it to the hash provided by the vendor
D. Remove the user's system from the network to avoid collateral contamination

Answer: C

QUESTION 588
A security analyst is reviewing vulnerability scan results and notices new workstations are being flagged as having outdated antivirus signatures. The analyst observes the following plugin output:

```
Antivirus is installed on the remote host:
Installation path: C:\Program Files\AVProduct\Win32\
Product Engine: 14.12.101
Engine Version: 3.5.71
Scanner does not currently have information about AVProduct version 3.5.71. It may no
longer be supported.
The engine version is out of date. The oldest supported version from the vendor is 4.2.11.
```

The analyst uses the vendor's website to confirm the oldest supported version is correct.
Which of the following BEST describes the situation?

A. This is a false positive and the scanning plugin needs to be updated by the vendor
B. This is a true negative and the new computers have the correct version of the software
C. This is a true positive and the new computers were imaged with an old version of the software
D. This is a false negative and the new computers need to be updated by the desktop team

Answer: C

QUESTION 589
A contained section of a building is unable to connect to the Internet A security analyst.
A security analyst investigates me issue but does not see any connections to the corporate web proxy However the analyst does notice a small spike in traffic to the Internet.
The help desk technician verifies all users are connected to the connect SSID. But there are two of the same SSIDs listed in the network connections.
Which of the following BEST describes wha is occurring?

A. Bandwidth consumption
B. Denial of service
C. Beaconing
D. Rogue device on the network

Answer: A

QUESTION 590
A Chief Information Security Officer (CISO) is concerned developers have too much visibility into customer data.
Which of the following controls should be implemented to BEST address these concerns?

A. Data masking
B. Data loss prevention
C. Data minimization
D. Data sovereignty

Answer: A

QUESTION 591
An analyst is searching a log for potential credit card leaks. The log stores all data encoded in hexadecimal.
Which of the following commands will allow the security analyst to confirm the incident?

A. cat log xxd -r -p | egrep ' [0-9] {16}
B. egrep '(3(0-9)) (16) ' log
C. cat log | xxd -r -p egrep '(0-9) (16)'
D. egrep ' (0-9) (16) ' log | xxdc

Answer: C

QUESTION 592
During a review of vulnerability scan results an analyst determines the results may be flawed because a control-

baseline system which is used to evaluate a scanning tools effectiveness was reported as not vulnerable. Consequently, the analyst verifies the scope of the scan included the control-baseline host which was available on the network during the scan.
The use of a control-baseline endpoint in this scenario assists the analyst in confirming.

A. verification of mitigation
B. false positives
C. false negatives
D. the critically index
E. hardening validation.

Answer: B

QUESTION 593
An organization is assessing risks so it can prioritize its mitigation actions. Following are the risks and their probability and impact:

Risk	Probability of occurrence	Cost of occurrence
A	50%	$120,000
B	10%	$300,000
C	20%	$100,000
D	80%	$50,000

Which of the following is the order of priority for risk mitigation from highest to lowest?

A. A, B, C, D
B. A, D, B, C
C. B, C, A, D
D. C, B, D, A
E. D, A, C, B

Answer: A

QUESTION 594
As part of a review of incident response plans, which of the following is MOST important for an organization to understand when establishing the breach notification period?

A. Organizational policies
B. Vendor requirements and contracts
C. Service-level agreements
D. Legal requirements

Answer: D

QUESTION 595
A security analyst is reviewing the following requirements (or new time clocks that will be installed in a shipping warehouse:

```
- The clocks must be configured so they do not respond to ARP broadcasts
- The server must be configured with static ARP entries for each clock.
```

Which of the following types of attacks will this configuration mitigate?

A. Spoofing
B. Overflows
C. Rootkits
D. Sniffing

Answer: A

QUESTION 596
Which of the following BEST describes the primary role of 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 he basis for control selection.
C. It prescribes technical control requirements.
D. It is an input to the business impact assessment.

Answer: A

QUESTION 597
A bad actor bypasses authentication and reveals all records in a database through an SQL injection. Implementation of which of the following would work BEST to prevent similar attacks in

A. Strict input validation
B. Blacklisting
C. SQL patching
D. Content filtering
E. Output encoding

Answer: A

QUESTION 598
An analyst is reviewing the following output:

```
if (searchname != null)
 {
  %>
     employee <%searchname%> not found
  <%
 }
```

Which of the following was MOST likely used to discover this?

A. Reverse engineering using a debugger
B. A static analysis vulnerability scan
C. A passive vulnerability scan
D. A web application vulnerability scan

Answer: C

QUESTION 599
A security analyst is investigating an incident that appears to have started with SOL injection against a publicly available web application.
Which of the following is the FIRST step the analyst should take to prevent future attacks?

A. Modify the IDS rules to have a signature for SQL injection.
B. Take the server offline to prevent continued SQL injection attacks.
C. Create a WAF rule In block mode for SQL injection
D. Ask the developers to implement parameterized SQL queries.

Answer: A

QUESTION 600

A Chief Security Officer (CSO) is working on the communication requirements (or an organization's incident response plan.
In addition to technical response activities, which of the following is the main reason why communication must be addressed in an effective incident response program?

A. Public relations must receive information promptly in order to notify the community.
B. Improper communications can create unnecessary complexity and delay response actions.
C. Organizational personnel must only interact with trusted members of the law enforcement community.
D. Senior leadership should act as the only voice for the incident response team when working with forensics teams.

Answer: B

QUESTION 601
The Cruel Executive Officer (CEO) of a large insurance company has reported phishing emails that contain malicious links are targeting the entire organza lion.
Which of the following actions would work BEST to prevent against this type of attack?

A. Turn on full behavioral analysis to avert an infection
B. Implement an EOR mail module that will rewrite and analyze email links.
C. Reconfigure the EDR solution to perform real-time scanning of all files
D. Ensure EDR signatures are updated every day to avert infection.
E. Modify the EDR solution to use heuristic analysis techniques for malware

Answer: D

QUESTION 602
In system hardening, which of the following types of vulnerability scans would work BEST to verify the scanned device meets security policies?

A. SCAP
B. Burp Suite
C. OWASP ZAP
D. Unauthenticated

Answer: D

QUESTION 603
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.

Answer: C

QUESTION 604
A cybersecurity analyst is dissecting an intrusion down to the specific techniques and wants to organize them in a logical manner.
Which of the following frameworks would BEST apply in this situation?

A. Pyramid of Pain

B. MITRE ATT&CK
C. Diamond Model of Intrusion Analysts
D. CVSS v3.0

Answer: B

QUESTION 605
A security analyst is reviewing a suspected phishing campaign that has targeted an organisation. The organization has enabled a few email security technologies in the last year: however, the analyst believes the security features are not working. The analyst runs the following command:
```
> dig domain._domainkey.comptia.orq TXT
```
Which of the following email protection technologies is the analyst MOST likely validating?

A. SPF
B. DNSSEC
C. DMARC
D. DKIM

Answer: A

QUESTION 606
Employees of a large financial company are continuously being Infected by strands of malware that are not detected by EDR tools.
When of the following Is the BEST security control to implement to reduce corporate risk while allowing employees to exchange files at client sites?

A. MFA on the workstations
B. Additional host firewall rules
C. VDI environment
D. Hard drive encryption
E. Network access control
F. Network segmentation

Answer: B

QUESTION 607
An information security analyst on a threat-hunting team is working with administrators to create a hypothesis related to an internally developed web application.
The working hypothesis is as follows:
```
- Due to the nature of the industry, the application hosts sensitive data associated with many clients and Is a significant target
- The platform Is most likely vulnerable to poor patching and Inadequate server hardening, which expose vulnerable services.
- The application is likely to be targeted with SQL injection attacks due to the large number of reporting capabilities within the application.
```
As a result, the systems administrator upgrades outdated service applications and validates the endpoint configuration against an industry benchmark.
The analyst suggests developers receive additional training on implementing identity and access management, and also implements a WAF to protect against SOL injection attacks.
Which of the following BEST represents the technique in use?

A. Improving detection capabilities
B. Bundling critical assets
C. Profiling threat actors and activities
D. Reducing the attack surface area

Answer: D

QUESTION 608
When reviewing a compromised authentication server, a security analyst discovers the following hidden file:

```
root@ldap1:~# cat .pass.txt
jsmith:Welcome123:18073:0:99999:7:::
mjones4:Welcome123:18073:0:99999:7:::
mgreen1:Welcome123:18073:0:99999:7:::
rbarger:Welcome123:18073:0:99999:7:::
mhemme14:Welcome123:18073:0:99999:7:::
mgill:Welcome123:18073:0:99999:7:::
cyoung1:Welcome123:18073:0:99999:7:::
gkiepper3:Welcome123:18073:0:99999:7:::
```

Further analysis shows these use s never logged in to the server.
Which of the following types of attacks was used to obtain the file and what should the analyst recommend to prevent this type of attack from reoccurring?

A. A rogue LDAP server is installed on the system and is connecting passwords. The analyst should recommend wiping and reinstalling the server.
B. A password spraying attack was used to compromise the passwords. The analyst should recommend that all users receive a unique password.
C. A rainbow tables attack was used to compromise the accounts. The analyst should recommend that future password hashes contains a salt.
D. A phishing attack was used to compromise the account. The analyst should recommend users install endpoint protection to disable phishing links.

Answer: B

QUESTION 609
A forensic analyst took an image of a workstation that was involved in an incident.
To BEST ensure the image is not tampered with me analyst should use:

A. hashing
B. backup tapes
C. a legal hold
D. chain of custody.

Answer: D