CAS-003$^{Q\&As}$

CompTIA Advanced Security Practitioner (CASP+)

Pass CompTIA CAS-003 Exam with 100% Guarantee

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

https://www.certbus.com/cas-003.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by CompTIA Official Exam Center

QUESTION 1

To meet a SLA, which of the following documents should be drafted, defining the company\\'s internal interdependent unit responsibilities and delivery timelines.

A. BPA

B. OLA

C. MSA

D. MOU

Correct Answer: B

OLA is an agreement between the internal support groups of an institution that supports SLA. According to the Operational Level Agreement, each internal support group has certain responsibilities to the other group. The OLA clearly depicts the performance and relationship of the internal service groups. The main objective of OLA is to ensure that all the support groups provide the intended ServiceLevelAgreement.

QUESTION 2

The security administrator finds unauthorized tables and records, which were not present before, on a Linux database server. The database server communicates only with one web server, which connects to the database server via an account with SELECT only privileges. Web server logs show the following:

```
90.76.165.40 -- [08/Mar/2014:10:54:04] "GET calendar.php?create%20table%20hidden HTTP/1.1" 200 5724

90.76.165.40 -- [08/Mar/2014:10:54:05] "GET ../../../root/.bash_history HTTP/1.1" 200 5724
```

90.76.165.40 -- [08/Mar/2014:10:54:04] "GET index.php?user;Creat; HTTP/1.1" 200 5724 The security administrator also inspects the following file system locations on the database server using the command `ls -al /root\\' drwxrwxrwx 11 root root 4096 Sep 28 22:45 . drwxr-xr-x 25 root root 4096 Mar 8 09:30 .. -rws------ 25 root root 4096 Mar 8 09:30 .bash_history -rw------- 25 root root 4096 Mar 8 09:30 .bash_history -rw------- 25 root root 4096 Mar 8 09:30 .profile -rw------- 25 root root 4096 Mar 8 09:30 .ssh Which of the following attacks was used to compromise the database server and what can the security administrator implement to detect such attacks in the future? (Select TWO).

A. Privilege escalation

B. Brute force attack

C. SQL injection

D. Cross-site scripting

E. Using input validation, ensure the following characters are sanitized:

F. Update crontab with: find / \(-perm -4000 \) -type f -print0 | xargs -0 ls -l | email.sh

G. Implement the following PHP directive: $clean_user_input = addslashes($user_input)

H. Set an account lockout policy

Correct Answer: AF

This is an example of privilege escalation.

Privilege escalation is the act of exploiting a bug, design flaw or configuration oversight in an operating system or software application to gain elevated access to resources that are normally protected from an application or user.

The question states that the web server communicates with the database server via an account with SELECT only privileges. However, the privileges listed include read, write and execute (rwx). This suggests the privileges have been

`escalated\\'.

Now that we know the system has been attacked, we should investigate what was done to the system.

The command "Update crontab with: find / \(-perm -4000 \) -type f -print0 | xargs -0 ls -l | email.sh" is used to find all the files that are setuid enabled. Setuid means set user ID upon execution. If the setuid bit is turned on for a file, the user

executing that executable file gets the permissions of the individual or group that owns the file.

QUESTION 3

The IT Security Analyst for a small organization is working on a customer\\'s system and identifies a possible intrusion in a database that contains PII. Since PII is involved, the analyst wants to get the issue addressed as soon as possible. Which of the following is the FIRST step the analyst should take in mitigating the impact of the potential intrusion?

A. Contact the local authorities so an investigation can be started as quickly as possible.

B. Shut down the production network interfaces on the server and change all of the DBMS account passwords.

C. Disable the front-end web server and notify the customer by email to determine how the customer would like to proceed.

D. Refer the issue to management for handling according to the incident response process.

Correct Answer: D

The database contains PII (personally identifiable information) so the natural response is to want to get the issue addressed as soon as possible. However, in this question we have an IT Security Analyst working on a customer\\'s system. Therefore, this IT Security Analyst does not know what the customer\\'s incident response process is. In this case, the IT Security Analyst should refer the issue to company management so they can handle the issue (with your help if required) according to their incident response procedures.

QUESTION 4

The security engineer receives an incident ticket from the helpdesk stating that DNS lookup requests are no longer working from the office. The network team has ensured that Layer 2 and Layer 3 connectivity are working. Which of the following tools would a security engineer use to make sure the DNS server is listening on port 53?

A. PING

B. NESSUS

C. NSLOOKUP

D. NMAP

Correct Answer: D

NMAP works as a port scanner and is used to check if the DNS server is listening on port 53.

QUESTION 5

An organization is currently performing a market scan for managed security services and EDR capability. Which of the following business documents should be released to the prospective vendors in the first step of the process? (Select TWO).

A. MSA

B. RFP

C. NDA

D. RFI

E. MOU

F. RFQ

Correct Answer: CD

QUESTION 6

Company ABC\\'s SAN is nearing capacity, and will cause costly downtimes if servers run out disk space. Which of the following is a more cost effective alternative to buying a new SAN?

A. Enable multipath to increase availability

B. Enable deduplication on the storage pools

C. Implement snapshots to reduce virtual disk size

D. Implement replication to offsite datacenter

Correct Answer: B

Storage-based data deduplication reduces the amount of storage needed for a given set of files. It is most effective in applications where many copies of very similar or even identical data are stored on a single disk.

It is common for multiple copies of files to exist on a SAN. By eliminating (deduplicating) repeated copies of the files, we can reduce the disk space used on the existing SAN. This solution is a cost effective alternative to buying a new SAN.

QUESTION 7

Which of the following is an external pressure that causes companies to hire security assessors and penetration testers?

A. Lack of adequate in-house testing skills.

B. Requirements for geographically based assessments

C. Cost reduction measures

D. Regulatory insistence on independent reviews.

Correct Answer: D

QUESTION 8

There have been several exploits to critical devices within the network. However, there is currently no process to perform vulnerability analysis. Which the following should the security analyst implement during production hours to identify critical threats and vulnerabilities?

A. asset inventory of all critical devices

B. Vulnerability scanning frequency that does not interrupt workflow

C. Daily automated reports of exploited devices

D. Scanning of all types of data regardless of sensitivity levels

Correct Answer: B

QUESTION 9

The Chief Information Security Officer (CISO) of an established security department, identifies a customer who has been using a fraudulent credit card. The CISO calls the local authorities, and when they arrive on-site, the authorities ask a

security engineer to create a point-in-time copy of the running database in their presence.

This is an example of:

A. creating a forensic image

B. deploying fraud monitoring

C. following a chain of custody

D. analyzing the order of volatility

Correct Answer: C

QUESTION 10

A security engineer at a company is designing a system to mitigate recent setbacks caused competitors that are beating the company to market with the new products. Several of the products incorporate propriety enhancements developed by the engineer\\'s company. The network already includes a SEIM and a NIPS and requires 2FA for all user access.

Which of the following system should the engineer consider NEXT to mitigate the associated risks?

A. DLP

B. Mail gateway

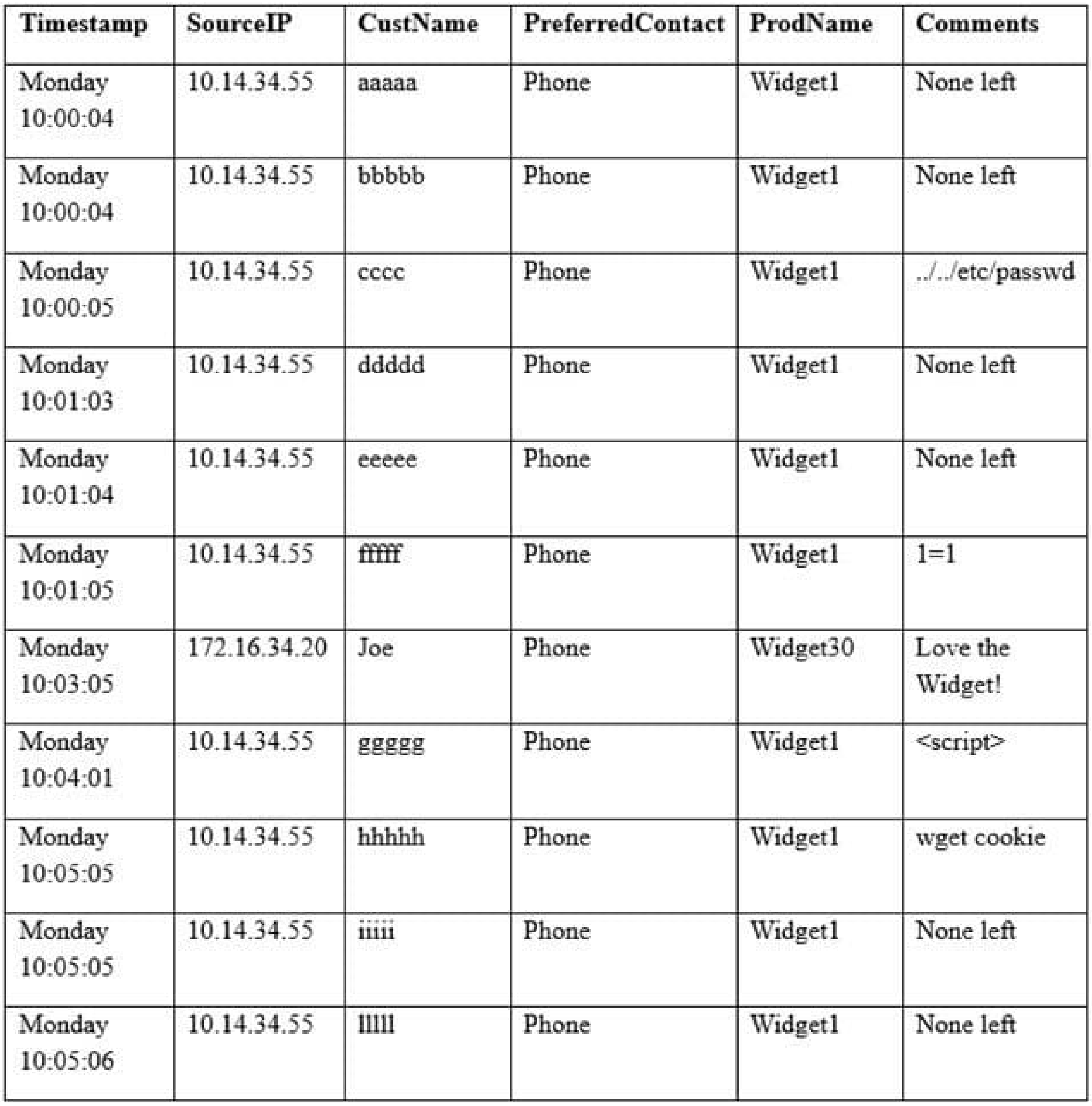
C. Data flow enforcement

D. UTM

Correct Answer: A

QUESTION 11

A security analyst sees some suspicious entries in a log file from a web server website, which has a form that allows customers to leave feedback on the company\\'s products. The analyst believes a malicious actor is scanning the web form. To know which security controls to put in place, the analyst first needs to determine the type of activity occurring to design a control. Given the log below:



Timestamp	SourceIP	CustName	PreferredContact	ProdName	Comments
Monday 10:00:04	10.14.34.55	aaaaa	Phone	Widget1	None left
Monday 10:00:04	10.14.34.55	bbbbb	Phone	Widget1	None left
Monday 10:00:05	10.14.34.55	cccc	Phone	Widget1	../../etc/passwd
Monday 10:01:03	10.14.34.55	ddddd	Phone	Widget1	None left
Monday 10:01:04	10.14.34.55	eeeee	Phone	Widget1	None left
Monday 10:01:05	10.14.34.55	fffff	Phone	Widget1	1=1
Monday 10:03:05	172.16.34.20	Joe	Phone	Widget30	Love the Widget!
Monday 10:04:01	10.14.34.55	ggggg	Phone	Widget1	<script>
Monday 10:05:05	10.14.34.55	hhhhh	Phone	Widget1	wget cookie
Monday 10:05:05	10.14.34.55	iiiii	Phone	Widget1	None left
Monday 10:05:06	10.14.34.55	lllll	Phone	Widget1	None left

Which of the following is the MOST likely type of activity occurring?

A. SQL injection

B. XSS scanning

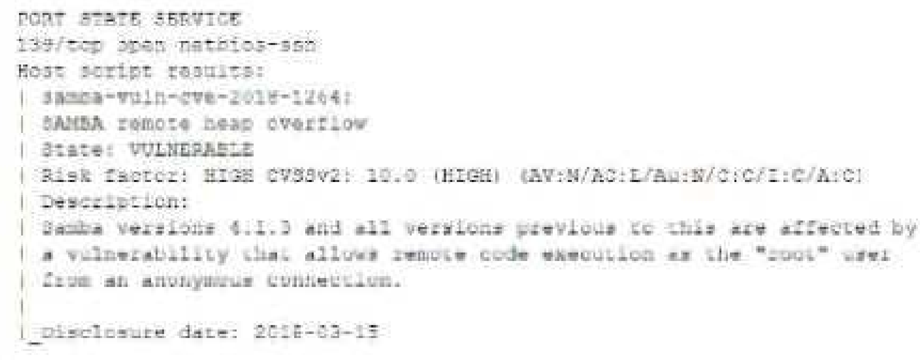
C. Fuzzing

D. Brute forcing

Correct Answer: A

QUESTION 12

A security is testing a server finds the following in the output of a vulnerability scan:



```
PORT STATE SERVICE
139/tcp open netbios-ssn
Host script results:
| samba-vuln-cve-2015-1264:
| SAMBA remote heap overflow
| State: VULNERABLE
| Risk factor: HIGH CVSSv2: 10.0 (HIGH) (AV:N/AC:L/Au:N/C:C/I:C/A:C)
| Description:
| Samba versions 4.1.3 and all versions previous to this are affected by
| a vulnerability that allows remote code execution as the "root" user
| from an anonymous connection.
|
|_Disclosure date: 2015-03-15
```

Which of the following will the security analyst most likely use NEXT to explore this further?

A. Exploitation framework

B. Reverse engineering tools

C. Vulnerability scanner

D. Visualization tool

Correct Answer: A

QUESTION 13

Following a recent outage, a systems administrator is conducting a study to determine a suitable bench stock on server hard drives.

Which of the following metrics is MOST valuable to the administrator in determining how many hard drives to keep-on hand?

A. TTR

B. ALE

C. MTBF

D. SLE

E. RPO

Correct Answer: C

QUESTION 14

An enterprise\\'s Chief Technology Officer (CTO) and Chief Information Security Officer (CISO) are meeting to discuss ongoing capacity and resource planning issues. The enterprise has experienced rapid, massive growth over the last 12 months, and the technology department is stretched thin for resources. A new accounting service is required to support the enterprise\\'s growth, but the only available compute resources that meet the accounting service requirements are on the virtual platform, which is hosting the enterprise\\'s website.

Which of the following should the CISO be MOST concerned about?

A. Poor capacity planning could cause an oversubscribed host, leading to poor performance on the company\\'s website.

B. A security vulnerability that is exploited on the website could expose the accounting service.

C. Transferring as many services as possible to a CSP could free up resources.

D. The CTO does not have the budget available to purchase required resources and manage growth.

Correct Answer: A

QUESTION 15

A company contracts a security consultant to perform a remote white-box penetration test. The company wants the consultant to focus on Internet-facing services without negatively impacting production services Which of the following is the consultant MOST likely to use to identify the company\\'s attack surface? (Select TWO)

A. Web crawler

B. WHOIS registry

C. DNS records

D. Company\\'s firewall ACL

E. Internal routing tables

F. Directory service queries

Correct Answer: BC