CAS-004$^{Q\&As}$

CompTIA Advanced Security Practitioner (CASP+)

Pass CompTIA CAS-004 Exam with 100% Guarantee

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

https://www.leads4pass.com/cas-004.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

A security engineer is creating a single CSR for the following web server hostnames:

1.

wwwint.internal

2.

www.company.com

3.

home.internal

4.

www.internal

Which of the following would meet the requirement?

A. SAN

B. CN

C. CA

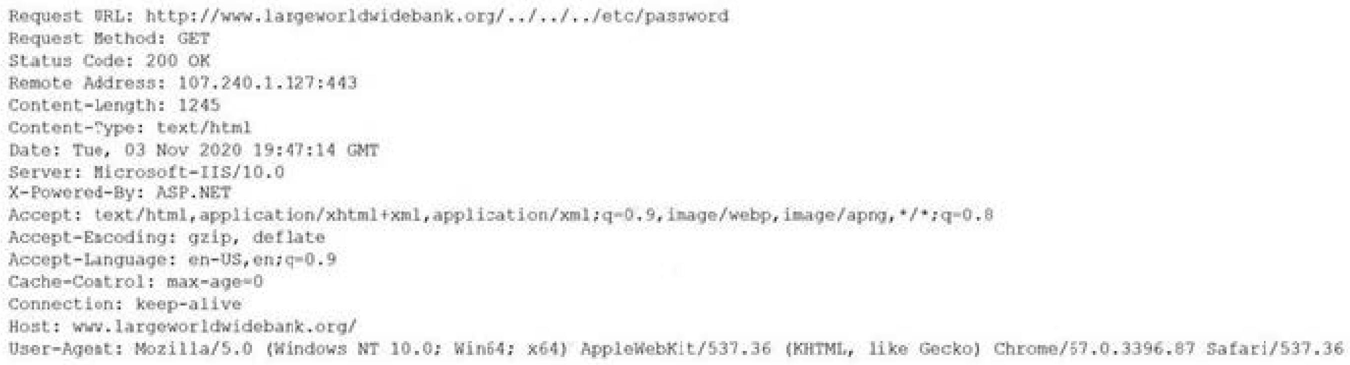
D. CRL

E. Issuer

Correct Answer: A

QUESTION 2

A security analyst is reviewing the following output:



```
Request URL: http://www.largeworldwidebank.org/../../../etc/password
Request Method: GET
Status Code: 200 OK
Remote Address: 107.240.1.127:443
Content-Length: 1245
Content-Type: text/html
Date: Tue, 03 Nov 2020 19:47:14 GMT
Server: Microsoft-IIS/10.0
X-Powered-By: ASP.NET
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cache-Control: max-age=0
Connection: keep-alive
Host: www.largeworldwidebank.org/
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/57.0.3396.87 Safari/537.36
```

Which of the following would BEST mitigate this type of attack?

A. Installing a network firewall

B. Placing a WAF inline

C. Implementing an IDS

D. Deploying a honeypot

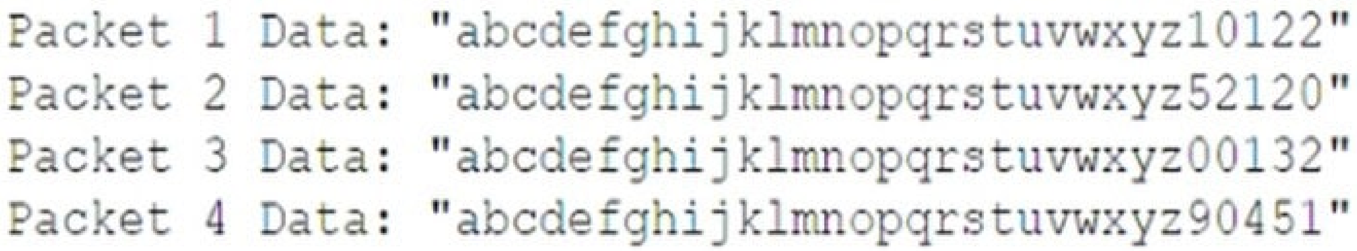
Correct Answer: B

QUESTION 3

A security analyst is reviewing the data portion acquired from the following command:

tcpdump -lnvi icmp and src net 192.168.1.0/24 and dst net 0.0.0.0/0 -w output.pcap

The data portion of the packet capture shows the following:



```
Packet 1 Data: "abcdefghijklmnopqrstuvwxyz10122"
Packet 2 Data: "abcdefghijklmnopqrstuvwxyz52120"
Packet 3 Data: "abcdefghijklmnopqrstuvwxyz00132"
Packet 4 Data: "abcdefghijklmnopqrstuvwxyz90451"
```

The analyst suspects that a data exfiltration attack is occurring using a pattern in which the last five digits are encoding sensitive information. Which of the following technologies and associated rules should the analyst implement to stop this specific attack? (Choose two.)

A. Intrusion prevention system

B. Data loss prevention

C. sed -e \\'s/a-z.*0-9.*//g\\'

D. reject icmp any any any any (msg:"alert"; regex [a-z]{26}[0-9]{5})

E. Second-generation firewall

F. drop icmp from 192.168.1.0/24 to 0.0.0.0/0

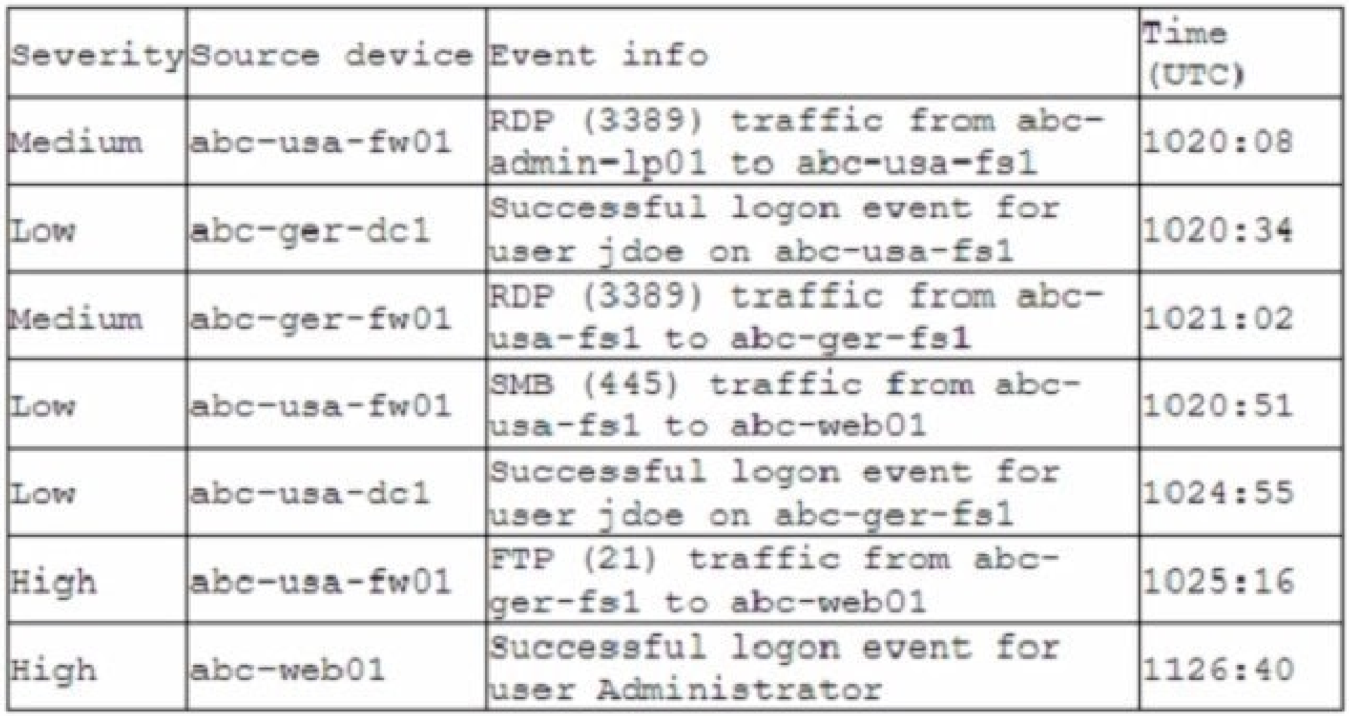
Correct Answer: BD

Data loss prevention (DLP): DLP solutions are designed to identify, monitor, and protect sensitive data to prevent unauthorized access or transmission. By implementing DLP policies that specifically target and inspect traffic for patterns resembling the suspected data exfiltration (e.g., identifying the sensitive information format in the last five digits), the DLP system can block or alert on such transmissions.

Intrusion prevention system (IPS): IPS solutions can be configured with rules and signatures to detect and prevent suspicious or malicious network activity. A custom signature or rule can be created within the IPS that specifically looks for the suspected pattern observed in the data portion of the captured packets. For instance, a signature similar to the provided regex pattern [a-z]{26}[0-9]{5} might be employed within the IPS to detect this specific data exfiltration attempt.

QUESTION 4

A company recently deployed a SIEM and began importing logs from a firewall, a file server, a domain controller a web server, and a laptop. A security analyst receives a series of SIEM alerts and prepares to respond. The following is the alert information:



Severity	Source device	Event info	Time (UTC)
Medium	abc-usa-fw01	RDP (3389) traffic from abc-admin-lp01 to abc-usa-fs1	1020:08
Low	abc-ger-dc1	Successful logon event for user jdoe on abc-usa-fs1	1020:34
Medium	abc-ger-fw01	RDP (3389) traffic from abc-usa-fs1 to abc-ger-fs1	1021:02
Low	abc-usa-fw01	SMB (445) traffic from abc-usa-fs1 to abc-web01	1020:51
Low	abc-usa-dc1	Successful logon event for user jdoe on abc-ger-fs1	1024:55
High	abc-usa-fw01	FTP (21) traffic from abc-ger-fs1 to abc-web01	1025:16
High	abc-web01	Successful logon event for user Administrator	1126:40

Which of the following should the security analyst do FIRST?

A. Disable Administrator on abc-uaa-fsl, the local account is compromised

B. Shut down the abc-usa-fsl server, a plaintext credential is being used

C. Disable the jdoe account, it is likely compromised

D. Shut down abc-usa-fw01; the remote access VPN vulnerability is exploited

Correct Answer: C

Based on the SIEM alerts, the security analyst should first disable the jdoe account, as it is likely compromised by an attacker. The alerts show that the jdoe account successfully logged on to the abc-usa-fsl server, which is a file server, and then initiated SMB (445) traffic to the abc-web01 server, which is a web server. This indicates that the attacker may be trying to exfiltrate data from the file server to the web server. Disabling the jdoe account would help stop this unauthorized activity and prevent further damage. Disabling Administrator on abc-usa-fsl, the local account is compromised, is not the first action to take, as it is not clear from the alerts if the local account is compromised or not. The alert shows that there was a successful logon event for Administrator on abc-usa-fsl, but it does not specify if it was a local or domain account, or if it was authorized or not. Moreover, disabling the local account would not stop the SMB traffic from jdoe to abcweb01. Shutting down the abc-usa-fsl server, a plaintext credential is being used, is not the first action to take, as it is not clear from the alerts if a plaintext credential is being used or not. The alert shows that there was RDP (3389) traffic from abcadmin1-logon to abc-usa-fsl, but it does not specify if the credential was encrypted or not. Moreover, shutting down the file server would disrupt its normal operations and affect other users. Shutting down abc-usa-fw01; the remote access VPN vulnerability is exploited, is not the first action to take, as it is not clear from the alerts if the remote access VPN vulnerability is exploited or not. The alert shows that there was FTP (21) traffic from abc-usa-dcl to abc- web01, but it does not specify if it was related to the VPN or not. Moreover, shutting down the firewall would expose the network to other threats and affect other services. References: What is SIEM? | Microsoft Security, What is a SIEM Alert? | Cofense

QUESTION 5

A security architect is tasked with scoping a penetration test that will start next month. The architect wants to define what security controls will be impacted. Which of the following would be the BEST document to consult?

A. Rules of engagement

B. Master service agreement

C. Statement of work

D. Target audience

Correct Answer: C

QUESTION 6

A company is rewriting a vulnerable application and adding the mprotect() system call in multiple parts of the application\\'s code that was being leveraged by a recent exploitation tool. Which of the following should be enabled to ensure the application can leverage the new system call against similar attacks in the future?

A. TPM

B. Secure boot

C. NX bit

D. HSM

Correct Answer: C

Enabling the NX bit ensures that the rewritten application can effectively use the mprotect() system call to manage memory execution permissions, thereby strengthening its defenses against exploitation tools that attempt to execute code from unauthorized memory regions. This approach aligns with best practices in modern application security to mitigate memory-based vulnerabilities

QUESTION 7

A systems administrator is preparing to run a vulnerability scan on a set of information systems in the organization. The systems administrator wants to ensure that the targeted systems produce accurate information especially regarding configuration settings.

Which of the following scan types will provide the systems administrator with the MOST accurate information?

A. A passive, credentialed scan

B. A passive, non-credentialed scan

C. An active, non-credentialed scan

D. An active, credentialed scan

Correct Answer: D

QUESTION 8

After investigating a recent security incident, a SOC analyst is charged with creating a reference guide for the entire team to use. Which of the following should the analyst create to address future incidents?

A. Root cause analysis

B. Communication plan

C. Runbook D. Lessons learned

Correct Answer: C

QUESTION 9

A software development company makes Its software version available to customers from a web portal. On several occasions, hackers were able to access the software repository to change the package that is automatically published on the website. Which of the following would be the BEST technique to ensure the software the users download is the official software released by the company?

A. Distribute the software via a third-party repository.

B. Close the web repository and deliver the software via email.

C. Email the software link to all customers.

D. Display the SHA checksum on the website.

Correct Answer: D

QUESTION 10

A security architect recommends replacing the company\\'s monolithic software application with a containerized solution. Historically, secrets have been stored in the application\\'s configuration files. Which of the following changes should the security architect make in the new system?

A. Use a secrets management tool.

B. Save secrets in key escrow.

C. Store the secrets inside the Dockerfiles.

D. Run all Dockerfiles in a randomized namespace.

Correct Answer: A

QUESTION 11

A third-party organization has implemented a system that allows it to analyze customers\\' data and deliver analysis results without being able to see the raw data. Which of the following is the organization implementing?

A. Asynchronous keys

B. Homomorphic encryption

C. Data lake

D. Machine learning

Correct Answer: B

QUESTION 12

A small company needs to reduce its operating costs. vendors have proposed solutions, which all focus on management of the company\\'s website and services. The Chief information Security Officer (CISO) insist all available resources in the proposal must be dedicated, but managing a private cloud is not an option. Which of the following is the BEST solution for this company?

A. Community cloud service model

B. Multinency SaaS

C. Single-tenancy SaaS

D. On-premises cloud service model

Correct Answer: A

QUESTION 13

A penetration tester is on an active engagement and has access to a remote system. The penetration tester wants to bypass the DLP, which is blocking emails that are encrypted or contain sensitive company information. Which of the following cryptographic techniques should the penetration tester use?

A. GNU Privacy Guard

B. UUencoding

C. DNSCrypt

D. Steganography

Correct Answer: D

QUESTION 14

Which of the following is the MOST important cloud-specific risk from the CSP\\'s viewpoint?

A. Isolation control failure

B. Management plane breach

C. Insecure data deletion

D. Resource exhaustion

Correct Answer: B

QUESTION 15

A company has a website with a huge database. The company wants to ensure that a DR site could be brought online quickly in the event of a failover, and end users would miss no more than 30 minutes of data. Which of the following should the company do to meet these objectives?

A. Build a content caching system at the DR site.

B. Store the nightly full backups at the DR site.

C. Increase the network bandwidth to the DR site.

D. Implement real-time replication for the DR site.

Correct Answer: D