Vendor: CompTIA

Exam Code:CAS-004

Exam Name: CompTIA Advanced Security Practitioner (CASP+)

Version: Demo

QUESTION 1

Company A acquired Company . During an audit, a security engineer found Company B\\'s environment was inadequately patched. In response, Company A placed a firewall between the two environments until Company B\\'s infrastructure could be integrated into Company A\\'s security program.

Which of the following risk-handling techniques was used?

A. Accept

B. Avoid

C. Transfer

D. Mitigate

Correct Answer: D

Reference: https://www.pivotpointsecurity.com/blog/risk-tolerance-in-business/

QUESTION 2

A security engineer has been asked to close all non-secure connections from the corporate network. The engineer is attempting to understand why the corporate UTM will not allow users to download email via IMAPS. The engineer formulates a theory and begins testing by creating the firewall ID 58, and users are able to download emails correctly by using IMAP instead. The network comprises three VLANs:

- VLAN 30	Guest networks	192.168.20.0/25
- VLAN 20	Corporate user network	192.168.0.0/28
- VLAN 110	Corporate server network	192.168.0.16/29

The security engineer looks at the UTM firewall rules and finds the following:

Rule active	Firewall ID	Source	Destination	Ports	Action	TLS decryption
Yes	58	VLAN 20	15.22.33.45	143	Allow and log	Enabled
Yes	33	VLAN 30	Any	80, 443,	Allow and log	Disabled
Yes	22	VLAN 110	VLAN 20	Any	Allow and log	Disabled
No	21	VLAN 20	15.22.33.45	990	Allow and log	Disabled
Yes	20	VLAN 20	VLAN 110	Any	Allow and log	Enabled
Yes	19	VLAN 20	Any	993, 587	Allow and log	Enabled

Which of the following should the security engineer do to ensure IMAPS functions properly on the corporate user network?

A. Contact the email service provider and ask if the company IP is blocked.

B. Confirm the email server certificate is installed on the corporate computers.

C. Make sure the UTM certificate is imported on the corporate computers.

D. Create an IMAPS firewall rule to ensure email is allowed.

Correct Answer: B

QUESTION 3

Immediately following the report of a potential breach, a security engineer creates a forensic image of the server in question as part of the organization incident response procedure. Which of the must occur to ensure the integrity of the image?

A. The image must be password protected against changes.

B. A hash value of the image must be computed.

C. The disk containing the image must be placed in a seated container.

D. A duplicate copy of the image must be maintained

Correct Answer: B

QUESTION 4

In order to save money, a company has moved its data to the cloud with a low-cost provider. The company did not perform a security review prior to the move; however, the company requires all of its data to be stored within the country where the headquarters is located. A new employee on the security team has been asked to evaluate the current provider against the most important requirements. The current cloud provider that the company is using offers:

1.

Only multitenant cloud hosting

2.

Minimal physical security

3.

Few access controls

4.

No access to the data center

The following information has been uncovered:

1.

The company is located in a known floodplain. which flooded last year.

2.

Government regulations require data to be stored within the country.

Which of the following should be addressed FIRST?

A. Update the disaster recovery plan to account for natural disasters.

B. Establish a new memorandum of understanding with the cloud provider.

C. Establish a new service-level agreement with the cloud provider.

D. Provision services according to the appropriate legal requirements.

Correct Answer: D

QUESTION 5

A shipping company that is trying to eliminate entire classes of threats is developing an SELinux policy to ensure its custom Android devices are used exclusively for package tracking. After compiling and implementing the policy, in which of the following modes must the company ensure the devices are configured to run?

A. Protecting

B. Permissive

C. Enforcing

D. Mandatory

Correct Answer: C

Reference: https://source.android.com/security/selinux/customize

---

QUESTION 6

A hospitality company experienced a data breach that included customer PII. The hacker used social engineering to convince an employee to grant a third-party application access to some company documents within a cloud file storage service Which of the following is the BEST solution to help prevent this type of attack in the future?

A. NGFW for web traffic inspection and activity monitoring

B. CSPM for application configuration control

C. Targeted employee training and awareness exercises

D. CASB for OAuth application permission control

Correct Answer: C

QUESTION 7

A security engineer is troubleshooting an issue in which an employee is getting an IP address in the range on the wired network. The engineer plus another PC into the same port, and that PC gets an IP address in the correct range. The engineer then puts the employee\\' PC on the wireless network and finds the PC still not get an IP address in the proper range. The PC is up to date on all software and antivirus definitions, and the IP address is not an APIPA address.

Which of the following is MOST likely the problem?

A. The company is using 802.1x for VLAN assignment, and the user or computer is in the wrong group.

B. The DHCP server has a reservation for the PC\\'s MAC address for the wired interface.

C. The WiFi network is using WPA2 Enterprise, and the computer certificate has the wrong IP address in the SAN field.

D. The DHCP server is unavailable, so no IP address is being sent back to the PC.

Correct Answer: A

QUESTION 8

A threat analyst notices the following URL while going through the HTTP logs.

Which of the following attack types is the threat analyst seeing?

A. SQL injection

B. CSRF

C. Session hijacking

D. XSS

Correct Answer: D

QUESTION 9

A security analyst observes the following while looking through network traffic in a company\\'s cloud log:

```
Nov 02 23:19:42 vpcvirtualhost VPCLogs 224289449368 eni-379ec4f1 10.0.5.52 10.0.50.6 241 79 6 1 40 1604359182 1604359242 ACCEPT OK
Nov 02 23:19:42 vpcvirtualhost VPCLogs 224289449368 eni-379ec4f1 10.0.5.52 172.32.6.66 443 63768 6 1 40 1604359182 1604359242 REJECT OK
Nov 02 23:19:44 vpcvirtualhost VPCLogs 224289449368 eni-379ec4f1 10.0.5.52 172.32.6.66 443 58664 6 1 40 1604359182 1604359242 ACCEPT OK
Nov 02 23:19:46 vpcvirtualhost VPCLogs 224289449368 eni-379ec4f1 10.0.5.52 10.0.50.6 242 80 6 1 40 1604359182 1604359242 ACCEPT OK
Nov 02 23:19:47 vpcvirtualhost VPCLogs 224289449368 eni-379ec4f1 10.0.5.52 10.0.50.6 243 81 6 1 40 1604359182 1604359242 REJECT OK
Nov 02 23:20:01 vpcvirtualhost VPCLogs 224289449368 eni-379ec4f1 10.0.5.52 172.32.6.66 443 61593 6 1 40 1604359182 1604359242 ACCEPT OK
Nov 02 23:20:03 vpcvirtualhost VPCLogs 224289449368 eni-379ec4f1 10.0.5.52 172.32.6.66 443 64279 6 1 40 1604359182 1604359242 ACCEPT OK
Nov 02 23:20:05 vpcvirtualhost VPCLogs 224289449368 eni-379ec4f1 10.0.5.52 10.0.50.6 244 82 1 40 1604359182 1604359242 REJECT OK
Nov 02 23:20:19 vpcvirtualhost VPCLogs 224289449368 eni-379ec4f1 10.0.5.52 172.32.6.66 443 58783 6 1 40 1604359182 1604359242 ACCEPT OK
```

Which of the following steps should the security analyst take FIRST?

A. Quarantine 10.0.5.52 and run a malware scan against the host.

B. Access 10.0.5.52 via EDR and identify processes that have network connections.

C. Isolate 10.0.50.6 via security groups.

D. Investigate web logs on 10.0.50.6 to determine if this is normal traffic.

Correct Answer: B

QUESTION 10

A health company has reached the physical and computing capabilities in its datacenter, but the computing demand continues to increase. The infrastructure is fully virtualized and runs custom and commercial healthcare application that process sensitive health and payment information. Which of the following should the company implement to ensure it can meet the computing demand while complying with healthcare standard for virtualization and cloud computing?

A. Hybrid IaaS solution in a single-tenancy cloud

B. Pass solution in a multinency cloud

C. SaaS solution in a community cloud

D. Private SaaS solution in a single tenancy cloud.

Correct Answer: D

QUESTION 11

A systems engineer is reviewing output from a web application vulnerability scan. The engineer has determined data is entenng the application from an untrusted source and is being used to construct a query dynamically. Which of the following code snippets would BEST protect the application against an SQL injection attack?

A. String input = request.getParameter ("SeqNo"); String characterPattern = "[0-9a0zA-Z] If (! input. Matches (characterPattern)) { out.println ("Invalid Input"); }

B. Cinput type= "text" maxlength= "30" name= "ecsChangePwdForm" size= "40" readonly= "true" value= \\'\\'/>

C. catch (Exception e) { if (log.isDebugEnabled()) log.debug (context, EVENTS.ADHOC, "Caught InvalidGSMException Exception —andquot;

+ e.toString());

}

D.

Correct Answer: B

QUESTION 12

A security officer is requiring all personnel working on a special project to obtain a security clearance requisite with the level of all information being accessed. Data on this network must be protected at the same level of each clearance holder. The need to know must be verified by the data owner. Which of the following should the security officer do to meet these requirements?

A. Create a rule to authorize personnel only from certain IPs to access the files.

B. Assign labels to the files and require formal access authorization.

C. Assign attributes to each file and allow authorized users to share the files.

D. Assign roles to users and authorize access to files based on the roles.

Correct Answer: B

This option aligns with the principle of using security clearances and a "need to know" basis to control access to sensitive information. By labeling files and requiring formal access authorization, the security officer can ensure that only personnel with the appropriate clearance level and a legitimate need to access the data are granted permission. This approach helps maintain the confidentiality and security of the information.