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.geekcert.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

An organization requires a contractual document that includes

1.

An overview of what is covered

2.

Goals and objectives

3.

Performance metrics for each party

4.

A review of how the agreement is managed by all parties

Which of the following BEST describes this type of contractual document?

A. SLA

B. BAA

C. NDA

D. ISA

Correct Answer: A

QUESTION 2

Which of the following is a risk associated with SDN?

A. Expanded attack surface

B. Increased hardware management costs

C. Reduced visibility of scaling capabilities

D. New firmware vulnerabilities

Correct Answer: A

A risk associated with SDN is the expanded attack surface that it introduces. SDN is a network architecture that decouples the control plane from the data plane, allowing centralized and programmable management of network devices and traffic. However, this also exposes new attack vectors and vulnerabilities that can compromise the security and performance of the network. For example, an attacker can target the SDN controller, which is the core component that communicates with and controls the network devices. A successful attack on the SDN controller can result in denial of service, unauthorized access, data leakage, or network hijacking. An attacker can also exploit the communication channels between the SDN controller and the network devices, such as the OpenFlow protocol, to intercept, modify, or

inject malicious messages or commands. Additionally, an attacker can leverage malicious or compromised applications that run on top of the SDN controller to manipulate or disrupt the network behavior. Verified References: https://www.isaca.org/resources/isaca-journal/issues/2016/volume-4/benefits-and- the-security-risk-of-software-defined-networking https://link.springer.com/article/10.1007/s40860-022-00171-8

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

An analyst determined that the current process for manually handling phishing attacks within the company is ineffective.

The analyst is developing a new process to ensure phishing attempts are handled internally in an appropriate and timely manner. One of the analyst\\'s requirements is that a blocklist be updated automatically when phishing attempts are identified. Which of the following would help satisfy this requirement?

A. SOAR

B. MSSP

C. Containerization

D. Virtualization

E. MDR deployment

Correct Answer: A

QUESTION 5

A Chief Security Officer (CSO) is concerned about the number of successful ransomware attacks that have hit the company. The data indicates most of the attacks came through a fake email. The company has added training, and the CSO now wants to evaluate whether the training has been successful. Which of the following should the CSO implement?

A. Simulating a spam campaign

B. Conducting a sanctioned vishing attack

C. Performing a risk assessment

D. Executing a penetration test

Correct Answer: A