GSEC Q&As

GIAC Security Essentials Certification

Pass GIAC GSEC Exam with 100% Guarantee

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

https://www.pass4itsure.com/gsec.html

100% Passing Guarantee
100% Money Back Assurance

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

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

Which class of IDS events occur when the IDS fails to alert on malicious data?

A. True Negative

B. True Positive

C. False Positive

D. False Negative

Correct Answer: D

QUESTION 2

Which of the following logging tasks should be evaluated in real-time?

A. Inside and perimeter log trends review

B. Routine account creation/removal

C. Log management system performance

D. Loss of service on critical assets

Correct Answer: D

QUESTION 3

To be considered a strong algorithm, an encryption algorithm must be which of the following?

A. Secret

B. Well-known

C. Confidential

D. Proprietary

Correct Answer: B

QUESTION 4

Which of the following is used to allow or deny access to network resources?

A. Spoofing

B. ACL

C. System hardening

D. NFS

Correct Answer: B

QUESTION 5

Which of the following authentication methods are used by Wired Equivalent Privacy (WEP)? Each correct answer represents a complete solution. Choose two.

A. Anonymous authentication

B. Mutual authentication

C. Open system authentication

D. Shared key authentication

Correct Answer: CD

QUESTION 6

What does PowerShell remoting use to authenticate to another host in a domain environment?

A. Two factor codes

B. Unique application passwords

C. PreShared keys

D. Kerberos tickets

Correct Answer: D

QUESTION 7

Your organization is developing a network protection plan. No single aspect of your network seems more important than any other. You decide to avoid separating your network into segments or categorizing the systems on the network. Each device on the network is essentially protected in the same manner as all other devices.

This style of defense-in-depth protection is best described as which of the following?

A. Uniform protection

B. Threat-oriented

C. Information-centric

D. Protected enclaves

Correct Answer: A

QUESTION 8

Which of the following is generally practiced by the police or any other recognized governmental authority?

A. Spoofing

B. SMB signing

C. Wiretapping

D. Phishing

Correct Answer: C

QUESTION 9

An organization keeps its intellectual property in a database. Protection of the data is assigned to one system administrator who marks the data, and monitors for this intellectual property leaving the network. Which defense-In-depth principle does this describe?

A. Threat-Vector Analysis

B. Protected Enclave

C. Information Centric

D. Uniform Protection

Correct Answer: C

QUESTION 10

Which of the following statements would be seen in a Disaster Recovery Plan?

A. "Instructions for notification of the media can be found in Appendix A"

B. "The Emergency Response Plan should be executed in the case of any physical disaster listed on page 3."

C. "The target for restoration of business operations is 72 hours from the declaration of disaster."

D. "After arriving at the alternate site, utilize the server build checklist to rebuild all servers on the server rebuild list."

Correct Answer: D

QUESTION 11

You are responsible for a Microsoft based network. Your servers are all clustered. Which of the following are the likely

reasons for the clustering? Each correct answer represents a complete solution. Choose two.

A. Reduce power consumption

B. Ease of maintenance

C. Load balancing

D. Failover

Correct Answer: CD

QUESTION 12

You are an Intrusion Detection Analyst and the system has alerted you to an Event of Interest (EOI) that appears to be activity generated by a worm. You investigate and find that the network traffic was normal. How would this type of alert be categorized?

A. False Positive

B. True Negative

C. True Positive

D. False Negative

Correct Answer: A

QUESTION 13

Which of the following Unix syslog message priorities is the MOST severe?

A. err

B. emerg

C. crit

D. alert

Correct Answer: B

QUESTION 14

A system administrator sees the following URL in the webserver logs:

```
https://www.site.com/content.asp?
user=IASDFJKEWHSIJ&password=DROP+TABLE+members;+--
```

Which action will mitigate against this attack?

A. Force all web applications to use SSL/US

B. Encode web traffic using Base64 before transmission

C. Filter potentially harmful characters from user input

D. Authenticate users before allowing database queries

Correct Answer: C

QUESTION 15

What Amazon Web Services (AWS) term describes a grouping of at least one datacenter with redundant power, high speed connections to other data centres and the Internet?

A. Management subnet

B. Availability zone

C. Region

D. virtual private cloud

Correct Answer: B