GSLC^{Q&As}

GIAC Security Leadership Certification (GSLC)

Pass GIAC GSLC Exam with 100% Guarantee

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

https://www.pass4itsure.com/gslc.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 of the following tools hides information about IIS Webservers so that they can be prevented from various attacks performed by an attacker?

A. WinSSLMiM

B. httprint

C. ServerMask

D. Whisker

Correct Answer: C

QUESTION 2

The Project Scope Management knowledge area focuses on which of the following processes? Each correct answer represents a complete solution. Choose all that apply.

A. Create Work Breakdown Structure (WBS)

B. Verify Scope

C. Select Sellers

D. Control Scope

Correct Answer: ABD

QUESTION 3

Which model is a software development process combining elements of both design and prototyping-in-stages, in an effort to combine advantages of top-down and bottom-up concepts?

A. Spiral

B. Prototyping

C. View

D. Waterfall

Correct Answer: A

QUESTION 4

You and your project team have identified the project risks and now are analyzing the probability and impact of the risks. What type of analysis of the risks provides a quick and high-level review of each identified risk event?

A. Quantitative risk analysis

B. Seven risk responses

C. Qualitative risk analysis

D. A risk probability-impact matrix

Correct Answer: C

QUESTION 5

When no anomaly is present in an Intrusion Detection, but an alarm is generated, the response is known as
_____.

A. True positive

B. True negative

C. False negative

D. False positive

Correct Answer: D

QUESTION 6

Which networking protocol is used to authenticate users or devices before granting them access to a network?

A. IPSec

B. PAgP

C. RADIUS

D. SRP

Correct Answer: C

QUESTION 7

You are an Incident manager in Orangesect.Inc. You have been tasked to set up a new extension of your enterprise.
The networking, to be done in the new extension, requires different types of cables and an appropriate policy that will be
decided by you. Which of the following stages in the Incident handling process involves your decision making?

A. Containment

B. Eradication

C. Identification

D. Preparation

Correct Answer: D

QUESTION 8

Which of the following relies on a physical characteristic of the user to verify his identity?

A. Kerberos v5

B. Social Engineering

C. CHAP

D. Biometrics

Correct Answer: D

QUESTION 9

A SIEM collects specific log events extracted from network activity.

Which strategy has been implemented?

A. Input-driven using agents on specific devices

B. Input-driven using a single collection point

C. Output-driven using agents on specific devices

D. Output-driven using a single collection point

Correct Answer: A

QUESTION 10

John works as a professional Ethical Hacker. He has been assigned a project to test the security of www.we-are-secure.com. He successfully performs a brute force attack on the We-are-secure server. Now, he suggests some countermeasures to avoid such brute force attacks on the We-are-secure server. Which of the following are countermeasures against a brute force attack? Each correct answer represents a complete solution. Choose all that apply.

A. The site should restrict the number of login attempts to only three times.

B. The site should increase the encryption key length of the password.

C. The site should use CAPTCHA after a specific number of failed login attempts.

D. The site should force its users to change their passwords from time to time.

Correct Answer: AC

QUESTION 11

What is a recommended approach for building a security program that benefits the business?

A. Lower the business\\' risk appetite

B. Focus security initiatives on outcomes

C. Focus security initiatives on results

D. Lower the business\\' risk capacity

Correct Answer: C

QUESTION 12

An analyst is tasked with configuring Windows to log "account logon events".

What should the analyst use to control what Windows will log?

A. Registry keys

B. Audit policies

C. Windows Defender

D. Event Log Viewer

Correct Answer: B

QUESTION 13

When mutual TLS authentication is in use, which of the following would an attacker need to steal in order to access the user\\'s data?

A. One-time token

B. User pin code

C. Cryptographic salt

D. Client certificate

Correct Answer: D

QUESTION 14

Which NIST CSF functions shown below maps to the CIS Boundary Defense critical security control?

Function	Category	CIS Control
Identify	Asset Management (AM) Risk Assessment (RA)	1,2 4
Protect	Access Control (AC) Awareness&Training (AT) Data Security (DS) Information Protection,Process&Procedures (IP) Protective Technology (PT)	5,14,15,16 17 13 3,9,11,18 7,8
Detect	Anomalies&Events (AE) Continuous Monitoring (CM) Detection Process (DP)	6,19 4,8,16 12
Respond	Asset Management (AM) Improvements (IM) Mitigation (MI)	6 20 4
Recover	Response Planning (RP) Improvements (IM) Response Planning (RP)	19 20 10

A. Identify

B. Recover

C. Respond

D. Detect

Correct Answer: D

QUESTION 15

Victor wants to send an encrypted message to his friend. He is using certain steganography technique to accomplish this task. He takes a cover object and changes it accordingly to hide information. This secret information is recovered only when the algorithm compares the changed cover with the original cover. Which of the following Steganography methods is Victor using to accomplish the task?

A. The distortion technique

B. The substitution technique

C. The cover generation technique

D. The spread spectrum technique

Correct Answer: A