



**Vendor:** GIAC

**Exam Code:** GISP

**Exam Name:** GIAC Information Security Professional

**Version:** DEMO

**QUESTION 1**

Which of the following is a technique used to attack an Ethernet wired or wireless network?

- A. DNS poisoning
- B. Keystroke logging
- C. Mail bombing
- D. ARP poisoning

**Answer: D**

**QUESTION 2**

Which of the following refers to encrypted text?

- A. Plaintext
- B. Cookies
- C. Hypertext
- D. Ciphertext

**Answer: D**

**QUESTION 3**

Which of the following are the benefits of information classification for an organization?

- A. It helps identify which information is the most sensitive or vital to an organization.
- B. It ensures that modifications are not made to data by unauthorized personnel or processes.
- C. It helps identify which protections apply to which information.
- D. It helps reduce the Total Cost of Ownership (TCO).

**Answer: AC**

**QUESTION 4**

Mark works as a Network Administrator for NetTech Inc. He wants users to access only those resources that are required for them. Which of the following access control models will he use?

- A. Role-Based Access Control
- B. Discretionary Access Control
- C. Mandatory Access Control
- D. Policy Access Control

**Answer: A**

**QUESTION 5**

Which of the following are methods used for authentication?

Each correct answer represents a complete solution. Choose all that apply.

- A. Smart card
- B. Biometrics
- C. Username and password

D. Magnetic stripe card

**Answer:** ABCD

**QUESTION 6**

Which of the following protocols is used to verify the status of a certificate?

- A. CEP
- B. HTTP
- C. OSPF
- D. OCSP

**Answer:** D

**QUESTION 7**

CORRECT TEXT

Fill in the blank with the appropriate value.

Service Set Identifiers (SSIDs) are case sensitive text strings that have a maximum length of \_\_\_\_\_ characters.

- A.
- B.
- C.
- D.

**Answer:**

**QUESTION 8**

You work as a Network Administrator for NetTech Inc. The company has a network that consists of 200 client computers and ten database servers. One morning, you find that a hacker is accessing unauthorized data on a database server on the network. Which of the following actions will you take to preserve the evidences?

Each correct answer represents a complete solution. Choose three.

- A. Prevent a forensics experts team from entering the server room.
- B. Preserve the log files for a forensics expert.
- C. Prevent the company employees from entering the server room.
- D. Detach the network cable from the database server.

**Answer:** BCD

**QUESTION 9**

Which of the following heights of fence deters only casual trespassers?

- A. 3 to 4 feet
- B. 2 to 2.5 feet

- C. 8 feet
- D. 6 to 7 feet

**Answer: A**

#### **QUESTION 10**

Which of the following statements about role-based access control (RBAC) model is true?

- A. In this model, a user can access resources according to his role in the organization.
- B. In this model, the permissions are uniquely assigned to each user account.
- C. In this model, the same permission is assigned to each user account.
- D. In this model, the users can access resources according to their seniority.

**Answer: A**

#### **QUESTION 11**

Which of the following statements about a fiber-optic cable are true?

Each correct answer represents a complete solution. Choose three.

- A. It is immune to electromagnetic interference (EMI).
- B. It can transmit undistorted signals over great distances.
- C. It has eight wires twisted into four pairs.
- D. It uses light pulses for signal transmission.

**Answer: ABD**

#### **QUESTION 12**

Which of the following statements about the bridge are true?

Each correct answer represents a complete solution. Choose two.

- A. It filters traffic based on IP addresses.
- B. It forwards broadcast packets.
- C. It assigns a different network address per port.
- D. It filters traffic based on MAC addresses.

**Answer: BD**

#### **QUESTION 13**

Sam works as a Web Developer for McRobert Inc. He wants to control the way in which a Web browser receives information and downloads content from Web sites. Which of the following browser settings will Sam use to accomplish this?

- A. Proxy server
- B. Security
- C. Cookies
- D. Certificate

**Answer: B**

**QUESTION 14**

Which of the following are used to suppress paper or wood fires?

Each correct answer represents a complete solution. Choose two.

- A. Water
- B. Kerosene
- C. CO2
- D. Soda acid

**Answer: AD**

**QUESTION 15**

Which of the following steps can be taken to protect laptops and data they hold?

Each correct answer represents a complete solution. Choose all that apply.

- A. Use slot locks with cable to connect the laptop to a stationary object.
- B. Keep inventory of all laptops including serial numbers.
- C. Harden the operating system.
- D. Encrypt all sensitive data.

**Answer: ABCD**

**QUESTION 16**

Which of the following attacks involves multiple compromised systems to attack a single target?

- A. Brute force attack
- B. DDoS attack
- C. Dictionary attack
- D. Replay attack

**Answer: B**

**QUESTION 17**

Which of the following statements about DMZ are true?

Each correct answer represents a complete solution. Choose two.

- A. It is an anti-virus software that scans the incoming traffic on an internal network.
- B. It is the boundary between the Internet and a private network.
- C. It contains company resources that are available on the Internet, such as Web servers and FTP servers.
- D. It contains an access control list (ACL).

**Answer: BC**

**QUESTION 18**

Which of the following protocols is used to establish a secure TELNET session over TCP/IP?

- A. SSL
- B. PGP
- C. IPSEC
- D. SSH

**Answer: D**

**QUESTION 19**

Which methods help you to recover your data in the event of a system or hard disk failure?

Each correct answer represents a complete solution. Choose two.

- A. Install a RAID system
- B. Use data encryption
- C. Install and use a tape backup unit
- D. Install UPS systems on all important devices

**Answer: AC**

**QUESTION 20**

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

- A. False positive
- B. False negative
- C. True negative
- D. True positive

**Answer: A**

**QUESTION 21**

Which of the following statements about smurf is true?

- A. It is an ICMP attack that involves spoofing and flooding.
- B. It is a UDP attack that involves spoofing and flooding.
- C. It is a denial of service (DoS) attack that leaves TCP ports open.
- D. It is an attack with IP fragments that cannot be reassembled.

**Answer: A**

## Thank You for Trying Our Product

### Lead2pass Certification Exam Features:

- ★ More than **99,900** Satisfied Customers Worldwide.
- ★ Average **99.9%** Success Rate.
- ★ **Free Update** to match latest and real exam scenarios.
- ★ **Instant Download** Access! No Setup required.
- ★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.
- ★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.
- ★ **100%** Guaranteed Success or **100%** Money Back Guarantee.
- ★ **Fast**, helpful support **24x7**.



View list of all certification exams: <http://www.lead2pass.com/all-products.html>



Microsoft



ORACLE



CITRIX



JUNIPER  
NETWORKS



EMC<sup>2</sup>  
where information lives®

**10% Discount Coupon Code: ASTR14**