



**Vendor:** CompTIA

**Exam Code:** JK0-018

**Exam Name:** CompTIA Security+ Certification Exam

**Version:** DEMO

**QUESTION 1**

Which of the following devices is BEST suited for servers that need to store private keys?

- A. Hardware security module
- B. Hardened network firewall
- C. Solid state disk drive
- D. Hardened host firewall

**Answer: A**

**QUESTION 2**

All of the following are valid cryptographic hash functions EXCEPT:

- A. RIPEMD
- B. RC4.
- C. SHA-512.
- D. MD4.

**Answer: B**

**QUESTION 3**

In regards to secure coding practices, why is input validation important?

- A. It mitigates buffer overflow attacks.
- B. It makes the code more readable.
- C. It provides an application configuration baseline.
- D. It meets gray box testing standards.

**Answer: A**

**QUESTION 4**

Which of the following would be used when a higher level of security is desired for encryption key storage?

- A. TACACS+
- B. L2TP
- C. LDAP
- D. TPM

**Answer: D**

**QUESTION 5**

A security administrator needs to determine which system a particular user is trying to login to at various times of the day. Which of the following log types would the administrator check?

- A. Firewall
- B. Application
- C. IDS
- D. Security

**Answer: D**

**QUESTION 6**

Which of the following **MUST** be updated immediately when an employee is terminated to prevent unauthorized access?

- A. Registration
- B. CA
- C. CRL
- D. Recovery agent

**Answer: C**

**QUESTION 7**

Employee badges are encoded with a private encryption key and specific personal information. The encoding is then used to provide access to the network. Which of the following describes this access control type?

- A. Smartcard
- B. Token
- C. Discretionary access control
- D. Mandatory access control

**Answer: A**

**QUESTION 8**

Which of the following devices would **MOST** likely have a DMZ interface?

- A. Firewall
- B. Switch
- C. Load balancer
- D. Proxy

**Answer: A**

**QUESTION 9**

Which of the following application security testing techniques is implemented when an automated system generates random input data?

- A. Fuzzing
- B. XSRF
- C. Hardening
- D. Input validation

**Answer: A**

**QUESTION 10**

Which of the following can be used by a security administrator to successfully recover a user's forgotten password on a password protected file?

- A. Cognitive password
- B. Password sniffing
- C. Brute force
- D. Social engineering

**Answer: C**

**QUESTION 11**

A security administrator wants to check user password complexity. Which of the following is the BEST tool to use?

- A. Password history
- B. Password logging
- C. Password cracker
- D. Password hashing

**Answer: C**

**QUESTION 12**

Certificates are used for: (Select TWO).

- A. Client authentication.
- B. WEP encryption.
- C. Access control lists.
- D. Code signing.
- E. Password hashing.

**Answer: AD**

**QUESTION 13**

Which of the following is a hardware based encryption device?

- A. EFS
- B. TrueCrypt
- C. TPM
- D. SLE

**Answer: C**

**QUESTION 14**

Which of the following BEST describes a protective countermeasure for SQL injection?

- A. Eliminating cross-site scripting vulnerabilities
- B. Installing an IDS to monitor network traffic
- C. Validating user input in web applications

D. Placing a firewall between the Internet and database servers

**Answer: C**

**QUESTION 15**

Which of the following MOST interferes with network-based detection techniques?

- A. Mime-encoding
- B. SSL
- C. FTP
- D. Anonymous email accounts

**Answer: B**

**QUESTION 16**

A certificate authority takes which of the following actions in PKI?

- A. Signs and verifies all infrastructure messages
- B. Issues and signs all private keys
- C. Publishes key escrow lists to CRLs
- D. Issues and signs all root certificates

**Answer: D**

**QUESTION 17**

Use of a smart card to authenticate remote servers remains MOST susceptible to which of the following attacks?

- A. Malicious code on the local system
- B. Shoulder surfing
- C. Brute force certificate cracking
- D. Distributed dictionary attacks

**Answer: A**

**QUESTION 18**

Separation of duties is often implemented between developers and administrators in order to separate which of the following?

- A. More experienced employees from less experienced employees
- B. Changes to program code and the ability to deploy to production
- C. Upper level management users from standard development employees
- D. The network access layer from the application access layer

**Answer: B**

**QUESTION 19**

A security administrator needs to update the OS on all the switches in the company. Which of the

following MUST be done before any actual switch configuration is performed?

- A. The request needs to be sent to the incident management team.
- B. The request needs to be approved through the incident management process.
- C. The request needs to be approved through the change management process.
- D. The request needs to be sent to the change management team.

**Answer: C**

**QUESTION 20**

Jane, an individual, has recently been calling various financial offices pretending to be another person to gain financial information. Which of the following attacks is being described?

- A. Phishing
- B. Tailgating
- C. Pharming
- D. Vishing

**Answer: D**

## 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<sup>®</sup>

**10% Discount Coupon Code: ASTR14**