{ISC}2 CISSP Certification - Sample Exam Questions

1

Which of the following is not a result of a penetration test?

- ○ Identify network vulnerabilities
- ○ Evaluate IDS effectiveness
- ○ Evaluate incident response procedures
- ○ Modify access control permissions

2

Jean is an internal auditor who consistently uses the audit logs of various network systems to produce reports. In an e-mail to the VP of IT, she stresses how important it is that proper protection controls are put in place to protect the audit logs. Of the justifications listed below, which is the weakest?

- ○ Audit logs often contain sensitive information and must be protected.
- ○ Unapproved changes to audit logs hurts the consistency and efficiency of automating reporting.
- ○ In the event of an investigation, an unprotected audit log may be deemed inadmissible in court.
- ○ Unprotected audit logs can be easy altered by an intruder after committing a crime.

3

Julie has been tasked with installing “clipping levels” on her segment of the network. This tactic is designed to prevent which act?

- ○ User “fat finger” threats
- ○ Julie from carrying out unnecessary investigations
- ○ DoS attacks
- ○ Password guessing attacks

4

Most operating systems and applications allow for administrators to configure the data that will be captured in audit logs for security purposes. Which of the following is the least important item to be captured in audit logs?

- Last user who accessed the device
- Number of unsuccessful access attempts
- System performance output data
- Number of successful access attempts

5

Host-based intrusion detection systems (IDS) utilize which of the following to perform their analysis?

- Downtime of connected devices
- Audit logs and system files
- Network packets
- Network throughput data

6

Tom is setting up computers at a trade show for his company's booth. The computers will give customers the opportunity to access a new product but will also take them onto a live network. Which control would be the best fit to offer the necessary protection from public users gaining privileged access?

- Discretionary-based
- Constrained user interface
- Network segregation
- Role-based

7

What would be a good reason for the use of thin clients for a company that wants to implement stronger access control?

- Programs become more readily available to users
- Limits user to the functions and capabilities of a secured operating system
- User training reduced
- Fewer desktops to purchase

8

When determining what biometric access control system to buy, which factor should be given the least amount of weight?

- Processing speed of the control
- User acceptance
- Accuracy of the control
- Reporting capabilities

9

Monica is the IT director of a large printing press. She has been made aware of several attempts of brute force password attacks within the past weeks. Which of the following reactions would suit Monica best?

- Implement spyware protection that is integrated into the current antivirus product
- Reduce the clipping level
- Find a more effective encryption mechanism
- Increase employee awareness through warning banners and training

10

Which of the following is not a characteristic of a synchronous token device?

- Counter-based
- Uses secret key
- Random-number based
- Time-based

11

Microprobing is an attack that would most likely be targeted towards which of the following?

- RAS algorithm
- Cipher lock
- Password-protected laptop
- Smart card

12

When a system officially permits access to a file or a program, what is it doing?

- Authenticating
- Authorizing
- Identifying
- Validating