1D0-571 Q&As

CIW V5 Security Essentials

Pass CIW 1D0-571 Exam with 100% Guarantee

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

https://www.pass4itsure.com/1d0-571.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by CIW 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 is a primary weakness of asymmetric-key encryption?

A. It is slow because it requires extensive calculations by the computer. B. It can lead to the corruption of encrypted data during network transfer.

B. It is reliant on the Secure Sockets Layer (SSL) standard, which has been compromised.

C. It is difficult to transfer any portion of an asymmetric key securely.

Correct Answer: A

QUESTION 2

A security breach has occurred in which a third party was able to obtain and misuse legitimate authentication information. After investigation, you determined that the specific cause for the breach was that end users have been placing their passwords underneath their keyboards. Which step will best help you resolve this problem?

A. Discipline specific end users as object lessons to the rest of the staff and reset passwords on all systems immediately.

B. Change all passwords on the company servers immediately and inform end users that their passwords will be changing on a regular basis.

C. Set passwords to expire at specific intervals and establish mandatory continual training sessions.

D. Inform end users that their passwords will be changing on a regular basis and require more complex passwords.

Correct Answer: C

QUESTION 3

Which of the following is a primary auditing activity?

A. Encrypting data files

B. Changing login accounts

C. Checking log files

D. Configuring the firewall

Correct Answer: C

QUESTION 4

You have been assigned to configure a DMZ that uses multiple firewall components. Specifically, you must configure a router that will authoritatively monitor and, if necessary, block traffic. This device will be the last one that inspects traffic

before it passes to the internal network. Which term best describes this device?

A. Screening router

B. Bastion host

C. Proxy server

D. Choke router

Correct Answer: D

QUESTION 5

You have just deployed an application that uses hash-based checksums to monitor changes in the configuration scripts of a database server that is accessible via the Internet. Which of the following is a primary concern for this solution?

A. The extra hard disk space required to store the database of checksums

B. The amount of memory remaining now that the checksum-based application is running

C. The possibility of a bufferoverflow attack leading to a security breach

D. The security of the checksum database on a read-only media format

Correct Answer: D

QUESTION 6

Which of the following standards is used for digital certificates?

A. DES

B. Diffie-Hellman

C. X.509

D. RC5

Correct Answer: C

QUESTION 7

You want to create a quick solution that allows you to obtain real-time login information for the administrative account on an LDAP server that you feel may become a target. Which of the following will accomplish this goal?

A. Reinstall the LDAP service on the server so that it is updated and more secure.

B. Install an application that creates checksums of the contents on the hard disk.

C. Create a login script for the administrative account that records logins to a separate server.

D. Create a dummy administrator account on the system so that a potential hacker is distracted from the

real login account.

Correct Answer: C

QUESTION 8

Which of the following will best help you ensure a database server can withstand a recently discovered vulnerability?

A. Updating the company vulnerability scanner and conducting a new scan

B. Adding a buffer overflow rule to the intrusion detection system

C. Reconfiguring the firewall

D. Installing a system update

Correct Answer: D

QUESTION 9

Which of the following errors most commonly occurs when responding to a security breach?

A. Shutting down network access using the firewall, rather than the network router

B. Adhering to the company policy rather than determining actions based on the IT manager\\'s input

C. Making snap judgments based on emotions, as opposed to company policy

D. Taking too much time to document the attack

Correct Answer: C

QUESTION 10

You have discovered that the ls, su and ps commands no longer function as expected. They do not return information in a manner similar to any other Linux system. Also, the implementation of Tripwire you have installed on this server is returning new hash values. Which of the following has most likely occurred?

A. Atrojan has attacked the system.

B. A SQL injection attack has occurred.

C. A spyware application has been installed. D. A root kit has been installed on the system.

Correct Answer:

QUESTION 11

Which of the following applications can help determine whether a denial-of-service attack is occurring against a network host?

A. Thenetstat command and a packet sniffer

B. Theps command and a network scanner

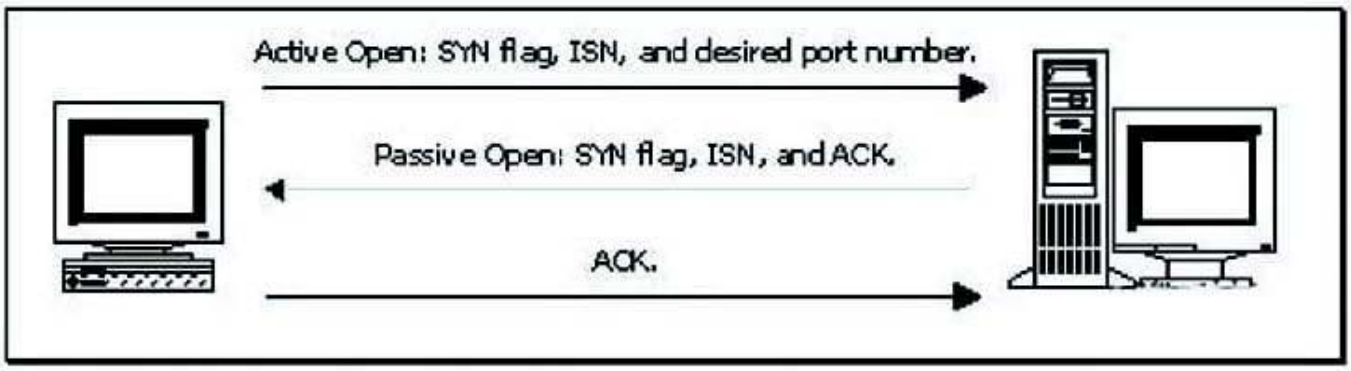
C. The ping command and User Manager

D. Theiptables command and Windows desktop firewall

Correct Answer: A

QUESTION 12

Consider the following diagram:



Which of the following best describes the protocol activity shown in the diagram, along with the most likely potential threat that accompanies this protocol?

A. The ICMP Time Exceeded message, with the threat of a denial-of-service attack

B. The SIP three-way handshake, with the threat of a buffer overflow

C. The TCP three-way handshake, with the threat of a man-in-the-middle attack

D. The DNS name query, with the threat of cache poisoning

Correct Answer: C

QUESTION 13

You have determined that the company Web server has several vulnerabilities, including a buffer overflow that has resulted in an attack. The Web server uses PHP and has direct connections to an Oracle database server. It also uses many CGI scripts. Which of the following is the most effective way to respond to this attack?

A. Installing software updates for the Web server daemon

B. Using the POST method instead of the GET method for a Web form

C. Installing an intrusion detection service to monitor logins

D. Using the GET method instead of the POST method for a Web form

Correct Answer: A

QUESTION 14

You have implemented a version of the Kerberos protocol for your network. What service does Kerberos primarily offer?

A. Authentication

B. Encryption

C. Non-repudiation

D. Data integrity

Correct Answer: A

QUESTION 15

Jason is attempting to gain unauthorized access to a corporate server by running a program that enters passwords from a long list of possible passwords. Which type of attack is this?

A. Brute force

B. Denial of service

C. Botnet

D. Buffer overflow

Correct Answer: A