1D0-571

CIW v5 Security Essentials

Version 4.5

1D0-571

QUESTION NO: 1

An application is creating hashes of each file on an attached storage device. Which of the following will typically occur during this process?

A. An increase in the amount of time it takes for the system to respond to requests

B. Reduced risk of an attack

C. Increased risk of an attack

D. A reduction in the amount of time it takes for the system to respond to requests

Answer: A

QUESTION NO: 2

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

Answer: D

QUESTION NO: 3

A distributed denial-of-service (DDOS) attack has occurred where both ICMP and TCP packets have crashed the company's Web server. Which of the following techniques will best help reduce the severity of this attack?

A. Filtering traffic at the firewall

B. Changing your ISP

C. Installing Apache Server rather than Microsoft IIS

D. Placing the database and the Web server on separate systems

Answer: A

QUESTION NO: 4

Which of the following is considered to be the most secure default firewall policy, yet usually causes the most work from an administrative perspective?

A. Configuring the firewall to respond automatically to threats

B. Blocking all access by default, then allowing only necessary connections

C. Configuring the firewall to coordinate with the intrusion-detection system

D. Allowing all access by default, then blocking only suspect network connections

Answer: B

QUESTION NO: 5

Which of the following is most likely to pose a security threat to a Web server?

A. CGI scripts

B. Database connections

C. Flash or Silverlight animation files

D. LDAP servers

Answer: A

QUESTION NO: 6

What is the first tool needed to create a secure networking environment?

A. User authentication

B. Confidentiality

C. Security policy

D. Auditing

Answer: C

QUESTION NO: 7

Irina has contracted with a company to provide Web design consulting services. The company has asked her to use several large files available via an HTTP server. The IT department has provided Irina with user name and password, as well as the DNS name of the HTTP server. She then used this information to obtain the files she needs to complete her task using Mozilla Firefox. Which of the following is a primary risk factor when authenticating with a standard HTTP server?

A. HTTP uses cleartext transmission during authentication, which can lead to a man-in-the-middle attack.

B. Irina has used the wrong application for this protocol, thus increasing the likelihood of a man-in-the-middle attack.

C. A standard HTTP connection uses public-key encryption that is not sufficiently strong, inviting the possibility of a man-in-the-middle attack.

D. Irina has accessed the Web server using a non-standard Web browser.

Answer: A

QUESTION NO: 8

Requests for Web-based resources have become unacceptably slow. You have been assigned to implement a solution that helps solve this problem. Which of the following would you recommend?

A. Enable stateful multi-layer inspection on the packet filter

B. Implement caching on the network proxy server

C. Enable authentication on the network proxy server

D. Implement a screening router on the network DMZ

Answer: B

QUESTION NO: 9

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. A trojan 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.

Answer: D

QUESTION NO: 10

Which of the following organizations provides regular updates concerning security breaches and issues?

A. IETF

B. ISO

C. ICANN

D. CERT

Answer: D

QUESTION NO: 11

You have been asked to encrypt a large file using a secure encryption algorithm so you can send it via e-mail to your supervisor. Encryption speed is important. The key will not be transmitted across a network. Which form of encryption should you use?

A. Asymmetric

B. PGP

C. Hash

D. Symmetric

Answer: D