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.certbus.com/1d0-571.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by CIW Official Exam Center

QUESTION 1

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 2

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

Correct Answer: A

QUESTION 3

At what layer of the OSI/RM does a packet filter operate?

A. Layer 1

B. Layer 3

C. Layer 5

D. Layer 7

Correct Answer: B

QUESTION 4

What is the primary drawback of using symmetric-key encryption?

A. Key transport across a network

B. Speed of encryption

C. Denial-of-service attacks

D. Inability to support convergence traffic

Correct Answer: A

QUESTION 5

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 6

Which tool is best suited for identifying applications and code on a Web server that can lead to a SQL injection attack?

A. A vulnerability scanner

B. A packet sniffer

C. An intrusion-detection system

D. A network switch

Correct Answer: A

QUESTION 7

Which of the following is the primary weakness of symmetric-key encryption?

A. Data encrypted using symmetric-key encryption is subject to corruption during transport.

B. Symmetric-key encryption operates slower than asymmetric-key encryption.

C. Symmetric-key encryption does not provide the service of data confidentiality.

D. Keys created using symmetric-key encryption are difficult to distribute securely.

Correct Answer: D

QUESTION 8

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 9

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

A. IETF

B. ISO

C. ICANN

D. CERT

Correct Answer: D

QUESTION 10

You have been assigned to provide security measures for your office\\'s reception area. Although the company needs to provide security measures, costs must be kept to a minimum. Which of the following tools is the most appropriate choice?

A. Firewall

B. Intrusion-detection system

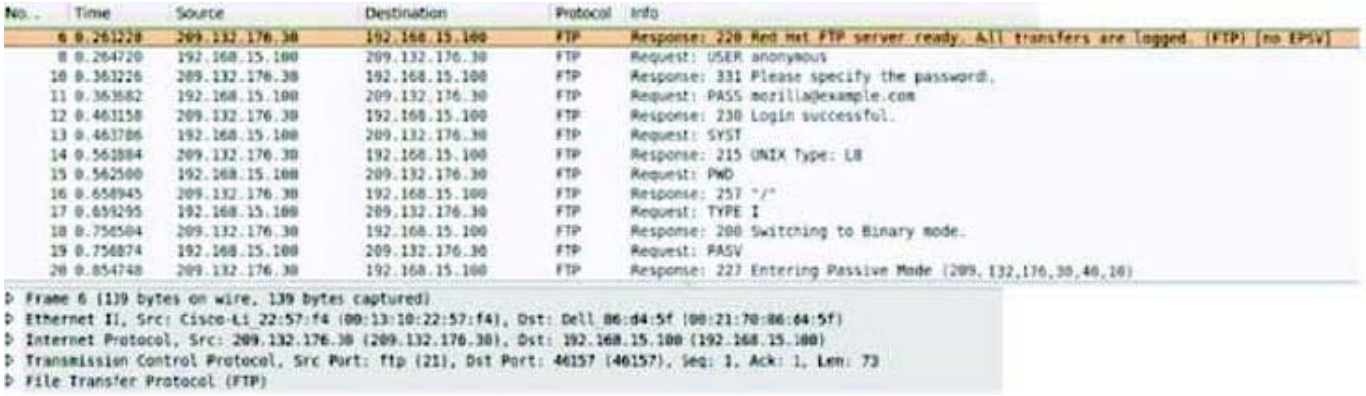
C. Camera

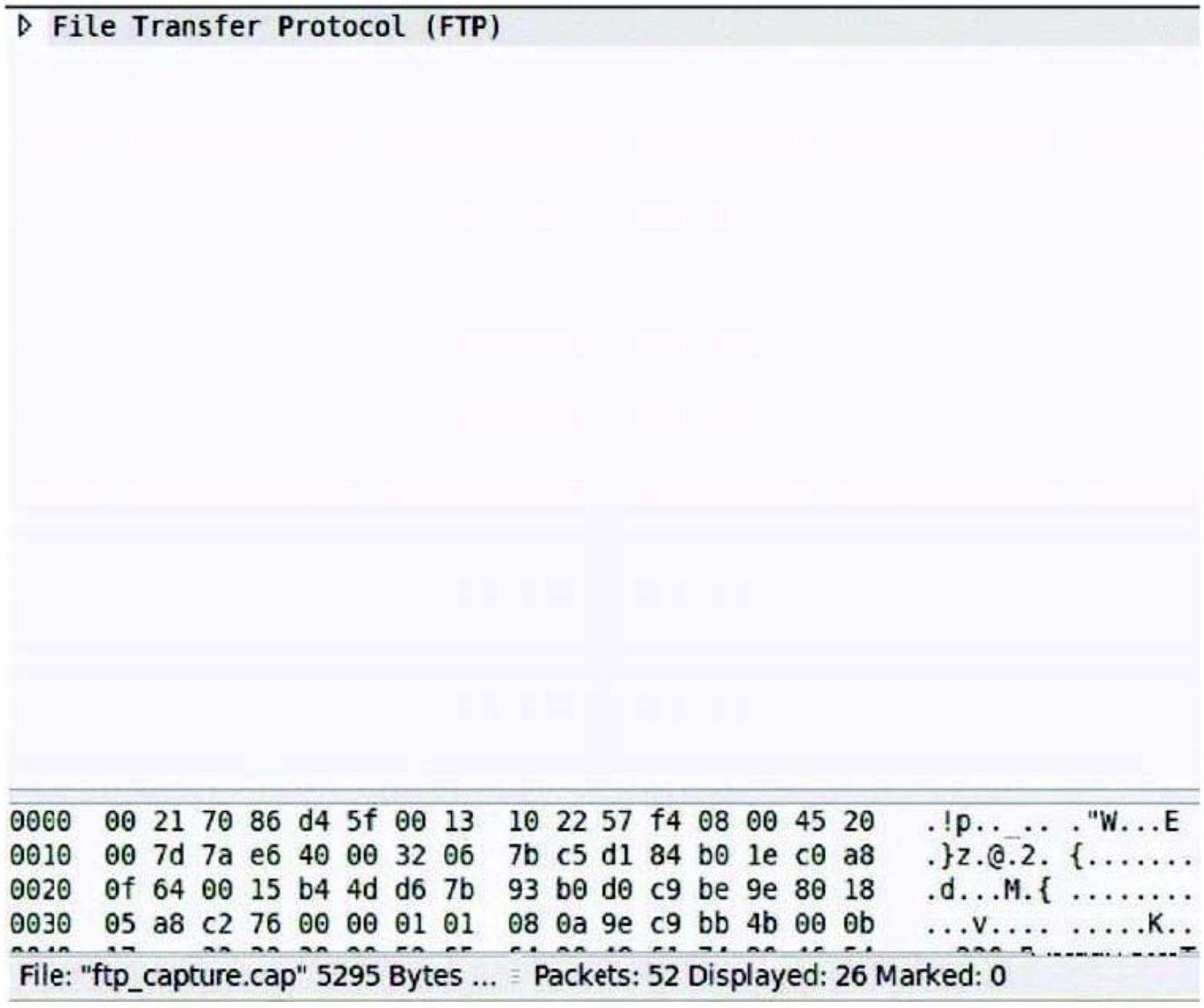
D. Security guard

Correct Answer: C

QUESTION 11

Consider the following image of a packet capture:





Which of the following best describes the protocol used, along with its primary benefit?

A. It is a passive FTP session, which is easier for firewalls to process.

B. It is an active FTP session, which is necessary in order to support IPv6.

C. It is an extended passive FTP session, which is necessary to support IPv6.

D. It is an active FTP session, which is supported by all FTP clients.

Correct Answer: A

QUESTION 12

Which of the following is a common problem, yet commonly overlooked, in regards to physical security in server rooms?

A. Firewalls that do not have a dedicated backup

B. False ceilings

C. Logic bombs

D. Biometric malfunctions

Correct Answer: B

QUESTION 13

Which of the following describes the practice of stateful multi-layer inspection?

A. Using a VLAN on a firewall to enable masquerading of private IP addresses

B. Prioritizing voice and video data to reduce congestion

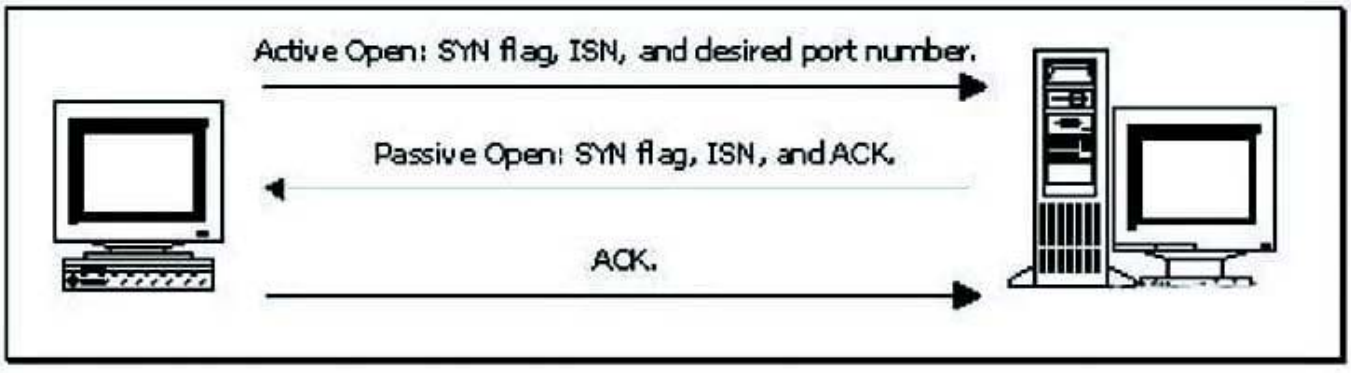
C. Inspecting packets in all layers of the OSI/RM with a packet filter

D. Using Quality of Service (QoS) on a proxy-oriented firewall

Correct Answer: C

QUESTION 14

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 15

What is the primary strength of symmetric-key encryption?

A. It allows easy and secure exchange of the secret key.

B. It creates aash?of a text, enabling data integrity.It creates a ?ash?of a text, enabling data integrity.

C. It can encrypt large amounts of data very quickly.

D. It provides non-repudiation services more efficiently than asymmetric-key encryption.

Correct Answer: C