

DUMPS ARENA

CIW v5 Security Essentials

CIW 1D0-571

Version Demo

Total Demo Questions: 10

Total Premium Questions: 62

Buy Premium PDF

<https://dumpsarena.co>

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

QUESTION NO: 1

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.

ANSWER: D**QUESTION NO: 2**

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

ANSWER: A**QUESTION NO: 3**

Which of the following standards is used for digital certificates?

- A. DES
- B. Diffie-Hellman
- C. X.509
- D. RC5

ANSWER: C

QUESTION NO: 4

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

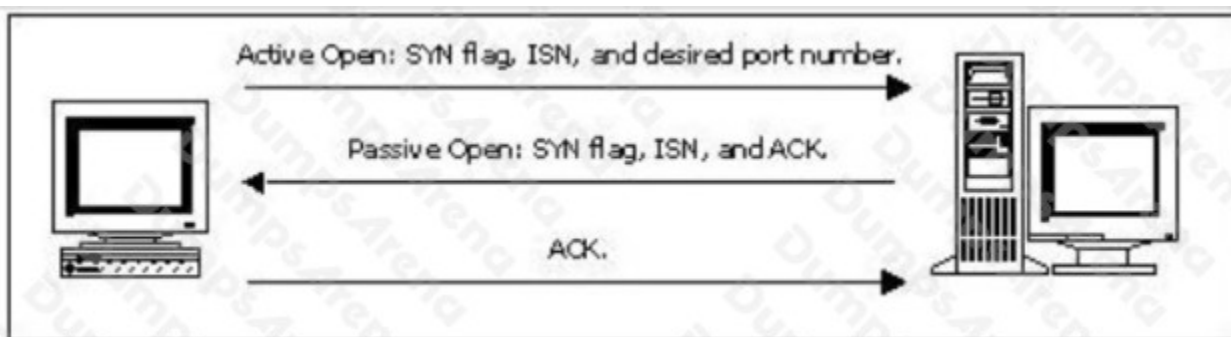
ANSWER: B**QUESTION NO: 5**

A new video conferencing device has been installed on the network. You have been assigned to troubleshoot a connectivity problem between remote workers and the central company. Specifically, remote workers are having problems making any connection at all. Which technique will most likely help you solve this problem while retaining the existing level of security at the firewall?

- A. Deny all use of UDP above Port 1024.
- B. Configure the firewall to provide VPN access.
- C. Configure a second network connection directly to the video conferencing device.
- D. Allow all use of UDP below Port 1024.

ANSWER: B**QUESTION NO: 6**

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

ANSWER: C

QUESTION NO: 7

Consider the following image of a packet capture:

No.	Time	Source	Destination	Protocol	Info
6	0.261228	209.132.176.30	192.168.15.100	FTP	Response: 220 Red Hat FTP server ready. All transfers are logged. (FTP) [no EPSV]
8	0.264720	192.168.15.100	209.132.176.30	FTP	Request: USER anonymous
10	0.363226	209.132.176.30	192.168.15.100	FTP	Response: 331 Please specify the password.
11	0.363682	192.168.15.100	209.132.176.30	FTP	Request: PASS mozilla@example.com
12	0.463158	209.132.176.30	192.168.15.100	FTP	Response: 230 Login successful.
13	0.463786	192.168.15.100	209.132.176.30	FTP	Request: SYST
14	0.561884	209.132.176.30	192.168.15.100	FTP	Response: 215 UNIX Type: L8
15	0.562500	192.168.15.100	209.132.176.30	FTP	Request: PWD
16	0.658945	209.132.176.30	192.168.15.100	FTP	Response: 257 "/"
17	0.659295	192.168.15.100	209.132.176.30	FTP	Request: TYPE I
18	0.756504	209.132.176.30	192.168.15.100	FTP	Response: 200 Switching to Binary mode.
19	0.756874	192.168.15.100	209.132.176.30	FTP	Request: PASV
20	0.854748	209.132.176.30	192.168.15.100	FTP	Response: 227 Entering Passive Mode (209,132,176,30,40,16)

▶ Frame 6 (139 bytes on wire, 139 bytes captured)
▶ Ethernet II, Src: Cisco-L1 22:57:f4 (00:13:10:22:57:f4), Dst: Dell 86:d4:5f (00:21:70:86:d4:5f)
▶ Internet Protocol, Src: 209.132.176.30 (209.132.176.30), Dst: 192.168.15.100 (192.168.15.100)
▶ Transmission Control Protocol, Src Port: ftp (21), Dst Port: 46157 (46157), Seq: 1, Ack: 1, Len: 73
▶ File Transfer Protocol (FTP)

```
File Transfer Protocol (FTP)

0000  00 21 70 86 d4 5f 00 13 10 22 57 f4 08 00 45 20  .!p... .."W...E
0010  00 7d 7a e6 40 00 32 06 7b c5 d1 84 b0 1e c0 a8  .}z.@.2. {.....
0020  0f 64 00 15 b4 4d d6 7b 93 b0 d0 c9 be 9e 80 18  .d...M.{ .....
0030  05 a8 c2 76 00 00 01 01 08 0a 9e c9 bb 4b 00 0b  ...v.... ....K..
0040  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
```

File: "ftp_capture.cap" 5295 Bytes ... Packets: 52 Displayed: 26 Marked: 0

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.

ANSWER: A

QUESTION NO: 8

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

ANSWER: C

QUESTION NO: 9

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

ANSWER: C

QUESTION NO: 10

What is the primary use of hash (one-way) encryption in networking?

- A. Signing files, for data integrity
- B. Encrypting files, for data confidentiality
- C. Key exchange, for user authentication
- D. User authentication, for non-repudiation

ANSWER: A