



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.passapply.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

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.

Correct Answer: A

QUESTION 2

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 3

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	0.363862	192.168.15.100	209.132.176.30	FTP	Request: PASS morilla@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	0.562884	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: 40157 (40157), 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  17 22 22 22 22 22 22 22 22 22 22 22 22 22 22  22 22 22 22 22 22
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.

Correct Answer: A

QUESTION 4

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.



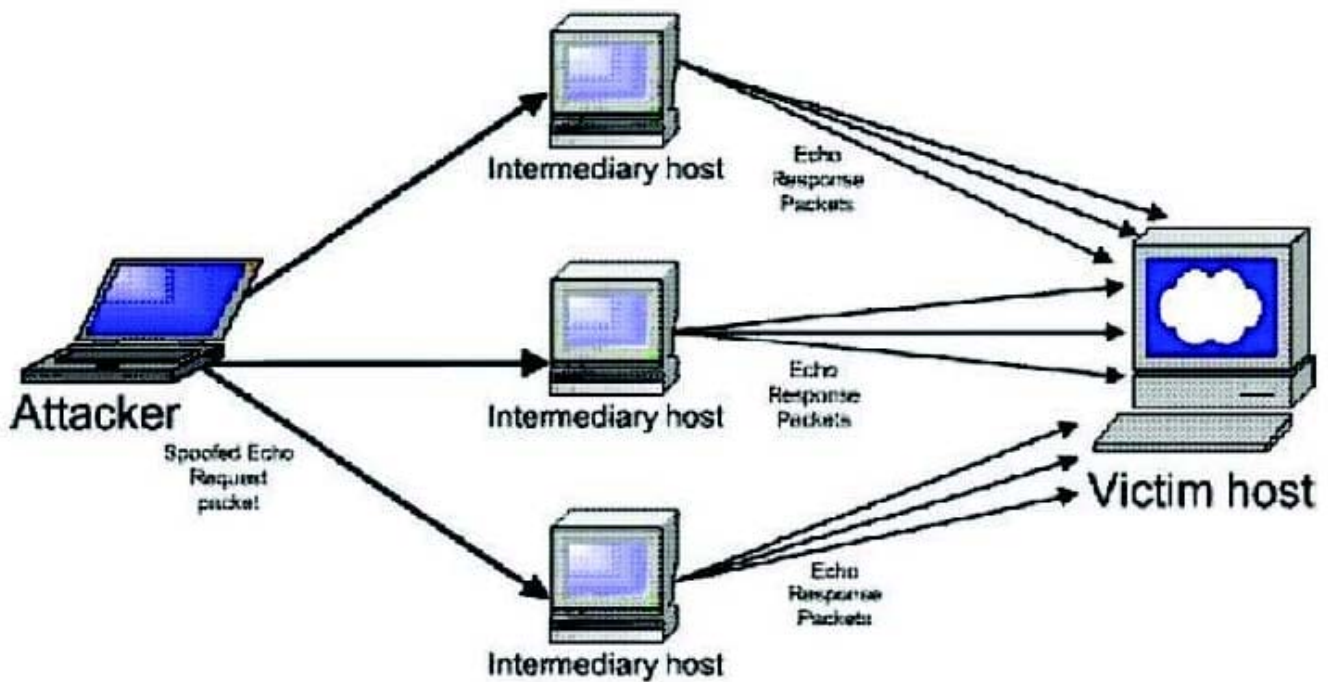
B. It is reliant on the Secure Sockets Layer (SSL) standard, which has been compromised.

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

Correct Answer: A

QUESTION 5

Consider the following diagram:



Which type of attack is occurring?

A. Polymorphic virus-based attack

B. Denial-of-service attack

C. Distributed denial-of-service attack

D. Man-in-the-middle attack using a packet sniffer

Correct Answer: C

[Latest 1D0-571 Dumps](#)

[1D0-571 Study Guide](#)

[1D0-571 Exam Questions](#)