



# 1D0-571<sup>Q&As</sup>

CIW V5 Security Essentials

## Pass CIW 1D0-571 Exam with 100% Guarantee

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

<https://www.geekcert.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

What is the primary strength of symmetric-key encryption?

- A. It allows easy and secure exchange of the secret key.
- B. It creates a hash of a text, enabling data integrity. It creates a hash 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

---

### QUESTION 2

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

- A. The netstat command and a packet sniffer
- B. The ps command and a network scanner
- C. The ping command and User Manager
- D. The iptables command and Windows desktop firewall

Correct Answer: A

---

### QUESTION 3

Consider the following image of a packet capture: This packet capture has recorded two types of attacks. Which choice lists both attack types?



No.	Time	Source	Destination	Protocol	Info
1	0.000000	168.214.252.91	192.168.2.57	TCP	32283 > 4718 [SYN] Seq=0 Win=1337 [TCP CHECKSUM INCORRECT] Len=9
2	0.019578	253.132.104.32	192.168.2.57	TCP	6186 > 15014 [SYN] Seq=0 Win=1337 [TCP CHECKSUM INCORRECT] Len=9
3	0.053091	12.159.44.247	192.168.2.57	TCP	8576 > 7609 [SYN] Seq=0 Win=1337 [TCP CHECKSUM INCORRECT] Len=9
4	0.072091	49.172.145.4	192.168.2.57	TCP	18581 > 15944 [SYN] Seq=0 Win=1337 [TCP CHECKSUM INCORRECT] Len=9
5	0.097353	140.47.267.160	192.168.2.57	TCP	19957 > 15554 [SYN] Seq=0 Win=1337 [TCP CHECKSUM INCORRECT] Len=9
6	0.115593	229.102.20.153	192.168.2.57	TCP	18454 > 7328 [SYN] Seq=0 Win=1337 [TCP CHECKSUM INCORRECT] Len=9
7	0.136736	198.17.167.98	192.168.2.57	TCP	4883 > 14453 [SYN] Seq=0 Win=1337 [TCP CHECKSUM INCORRECT] Len=9
8	0.165782	38.114.200.48	192.168.2.57	TCP	8068server-2 > 22118 [SYN] Seq=0 Win=1337 [TCP CHECKSUM INCORRECT] Len=9
9	0.187354	11.195.252.8	192.168.2.57	TCP	30548 > 14961 [SYN] Seq=0 Win=1337 [TCP CHECKSUM INCORRECT] Len=9
10	0.207306	9.143.69.172	192.168.2.57	TCP	10600 > 12052 [SYN] Seq=0 Win=1337 [TCP CHECKSUM INCORRECT] Len=9
11	0.232321	94.195.176.171	192.168.2.57	TCP	32262 > 6928 [SYN] Seq=0 Win=1337 [TCP CHECKSUM INCORRECT] Len=9
12	0.266265	180.3.107.179	192.168.2.57	TCP	20247 > 14120 [SYN] Seq=0 Win=1337 [TCP CHECKSUM INCORRECT] Len=9
13	0.289395	235.11.110.132	192.168.2.57	TCP	22345 > 8564 [SYN] Seq=0 Win=1337 [TCP CHECKSUM INCORRECT] Len=9
14	0.312948	145.179.71.242	192.168.2.57	TCP	15918 > 15713 [SYN] Seq=0 Win=1337 [TCP CHECKSUM INCORRECT] Len=9
15	0.337993	117.152.0.148	192.168.2.57	TCP	9388 > 4582 [SYN] Seq=0 Win=1337 [TCP CHECKSUM INCORRECT] Len=9
16	0.359288	142.119.20.187	192.168.2.57	TCP	10504 > 32170 [SYN] Seq=0 Win=1337 [TCP CHECKSUM INCORRECT] Len=9
17	0.383244	127.16.76.127	192.168.2.57	TCP	0MEagress > 9841 [SYN] Seq=0 Win=1337 [TCP CHECKSUM INCORRECT] Len=9
18	0.403091	185.74.145.125	192.168.2.57	TCP	29715 > 9691 [SYN] Seq=0 Win=1337 [TCP CHECKSUM INCORRECT] Len=9
19	0.423809	95.185.139.291	192.168.2.57	TCP	11318 > 19982 [SYN] Seq=0 Win=1337 [TCP CHECKSUM INCORRECT] Len=9
20	0.447850	247.23.235.64	192.168.2.57	TCP	10012 > 30700 [SYN] Seq=0 Win=1337 [TCP CHECKSUM INCORRECT] Len=9
21	0.476013	150.46.88.171	192.168.2.57	TCP	10012 > 30700 [SYN] Seq=0 Win=1337 [TCP CHECKSUM INCORRECT] Len=9
22	0.496126	46.73.65.3	192.168.2.57	TCP	ddi-tcp-7 > 13497 [SYN] Seq=0 Win=1337 [TCP CHECKSUM INCORRECT] Len=9

  

Frame 1 (63 bytes on wire (53 bytes captured))  
 Ethernet II, Src: 3com 24-e2:ac (08:01:03:24-e2:ac), Dst: Linksys6 82:4a:18 (08:06:25:82:4a:18)  
 Internet Protocol, Src: 168.214.252.91 (168.214.252.91), Dst: 192.168.2.57 (192.168.2.57)  
 Transmission Control Protocol, Src Port: 32283 (32283), Dst Port: 4718 (4718), Seq: 0, Len: 9  
 Source port: 32283 (32283)  
 Destination port: 4718 (4718)  
 Sequence number: 0 (relative sequence number)  
 [Next sequence number: 9 (relative sequence number)]  
 Header length: 20 bytes  
 Flags: 0x02 (SYN)  
 Window size: 1337  
 Checksum: 0x3718 [Incorrect, should be 0x3712 (payload padded by "TCP CHECKSUM OFFLOAD")]  
 Data (0 bytes)

0018 00 31 0f 40 00 00 00 45 6b a8 06 fc 50 c8 a8 .L.H...Eh...  
 0020 02 39 7d cb 12 66 00 00 7a 69 00 00 00 50 50 9f...f..Zi...P  
 0030 05 39 37 fb 00 00 00 00 00 60 00 00 00 00 00 92.....

Flags (tcp.flags): 1 byte      Packets: 3343 Displayed: 3343 Marked: 0      Profile: Default

- A. A dictionary attack and a worm-based attack A.A dictionary attack and a worm-based attack
- B. Asyn flood attack and a spoofing attack B.A syn flood attack and a spoofing attack
- C. A worm attack and abotnet attack C.A worm attack and a botnet attack
- D. A SQL injection attack and a virus attack D.A SQL injection attack and a virus attack

Correct Answer: B

#### QUESTION 4

You are using a PKI solution that is based on Secure Sockets Layer (SSL). Which of the following describes the function of the asymmetric-key-encryption algorithm used?

- A. It encrypts the symmetric key.
- B. It encrypts all of the data.
- C. It encrypts the hash code used for data integrity.
- D. It encrypts the X.509 key.

Correct Answer: A



#### QUESTION 5

Which algorithm can use a 128-bit key, and has been adopted as a standard by various governments and corporations?

- A. MARS
- B. RC2
- C. Advanced Encryption Standard (AES)
- D. International Data Encryption Algorithm (IDEA)

Correct Answer: C

[Latest 1D0-571 Dumps](#)

[1D0-571 VCE Dumps](#)

[1D0-571 Practice Test](#)