

Which mode of IPSec should you use to assure security and confidentiality of data within the same LAN?

- A. AH promiscuous
- B. ESP confidential
- C. AH Tunnel mode
- D. ESP transport mode

Answer: D

A tester has been hired to do a web application security test. The tester notices that the site is dynamic and must make use of a back end database. In order for the tester to see if SQL injection is possible, what is the first character that the tester should use to attempt breaking a valid SQL request?

- A. Semicolon
- B. Single quote
- C. Exclamation mark
- D. Double quote

Answer: B

The "Gray-box testing" methodology enforces what kind of restriction?

- A. Only the internal operation of a system is known to the tester.
- B. The internal operation of a system is completely known to the tester.
- C. The internal operation of a system is only partly accessible to the tester.
- D. Only the external operation of a system is accessible to the tester.

Answer: C

Which of the following steps for risk assessment methodology refers to vulnerability identification?

- A. Assigns values to risk probabilities; Impact values
- B. Determines risk probability that vulnerability will be exploited (High, Medium, Low)
- C. Identifies sources of harm to an IT system (Natural, Human, Environmental)
- D. Determines if any flaws exist in systems, policies, or procedures

Answer: D

Tremp is an IT Security Manager, and he is planning to deploy an IDS in his small company. He is looking for an IDS with the following characteristics: -Verifies success or failure of an attack – Monitors system activities – Detects attacks that a network-based IDS fails to detect. – Near real-time detection and response – Does not require additional hardware – Lower entry cost. Which type of IDS is best suited for Tremp's requirements?

- A. Network-based IDS
- B. Open source-based IDS
- C. Host-based IDS
- D. Gateway-based IDS

Answer: C