

ISLEVER

EC-SS

EC-Council Certified Security Specialist
Practice Test(ECSS)

DEMO

<https://www.islever.com/ec-ss.html>

<https://www.islever.com/eccouncil.html>

For the most up-to-date exam questions and materials, we recommend visiting our website, where you can access the latest content and resources.

QUESTION NO: 1

Firewalking is a technique that can be used to gather information about a remote network protected by a firewall. This technique can be used effectively to perform information gathering attacks. In this technique, an attacker sends a crafted packet with a TTL value that is set to expire one hop past the firewall. Which of the following are pre-requisites for an attacker to conduct firewalking?

Each correct answer represents a complete solution. Choose all that apply.

- A. ICMP packets leaving the network should be allowed.
- B. An attacker should know the IP address of the last known gateway before the firewall.
- C. There should be a backdoor installed on the network.
- D. An attacker should know the IP address of a host located behind the firewall.

Answer: A,B,D

Explanation:

QUESTION NO: 2

Which of the following security protocols are based on the *802.11i standard*?

Each correct answer represents a complete solution. Choose all that apply.

- A. WEP
- B. WPA2
- C. WPA
- D. WEP2

Answer: B,C

Explanation:

QUESTION NO: 3

Which of the following OSI layers is responsible for protocol conversion, data encryption/decryption, and data compression?

- A. Transport layer
- B. Presentation layer
- C. Data-link layer

D. Network layer

Answer: B

Explanation:

QUESTION NO: 4

You are responsible for security at a company that uses a lot of Web applications. You are most concerned about flaws in those applications allowing some attacker to get into your network. What method would be best for finding such flaws?

- A. Vulnerability scanning**
- B. Manual penetration testing**
- C. Automated penetration testing**
- D. Code review**

Answer: A

Explanation:

QUESTION NO: 5

Which of the following representatives of incident response team takes forensic backups of the systems that are the focus of the incident?

- A. Lead investigator**
- B. Information security representative**
- C. Technical representative**
- D. Legal representative**

Answer: C

Explanation:

QUESTION NO: 6

Which of the following statements are true about routers?

Each correct answer represents a complete solution. Choose all that apply.

- A. Routers are responsible for making decisions about which of several paths network (or Internet) traffic will follow.**
- B. Routers do not limit physical broadcast traffic.**
- C. Routers organize addresses into classes, which are used to determine how to move packets**

from one network to another.

D. Routers act as protocol translators and bind dissimilar networks.

Answer: A,C,D

Explanation:

QUESTION NO: 7

Which of the following types of attacks cannot be prevented by technical measures only?

- A.** Brute force
- B.** Ping flood attack
- C.** Smurf DoS
- D.** Social engineering

Answer: D

Explanation:

QUESTION NO: 8

You work as a Network Administrator for Tech Perfect Inc. The company requires a secure wireless

network. To provide security, you are configuring ISA Server 2006 as a firewall. While configuring ISA Server 2006, which of the following is NOT necessary?

- A.** Defining how ISA Server would cache Web contents
- B.** Defining ISA Server network configuration
- C.** Setting up of monitoring on ISA Server
- D.** Configuration of VPN access

Answer: D

Explanation:

QUESTION NO: 9

Which of the following attacks CANNOT be detected by an Intrusion Detection System (IDS)?

Each correct answer represents a complete solution. Choose all that apply.