ECSS Q&As

EC-Council Certified Security Specialist Practice Test

Pass EC-COUNCIL ECSS Exam with 100% Guarantee

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

https://www.pass2lead.com/ecss.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by EC-COUNCIL Official Exam Center

QUESTION 1

What does CSIRT stand for?

A. Computer Security Information Response Team

B. Chief Security Incident Response Team

C. Computer Security Incident Response Team

D. Chief Security Information Response Team

Correct Answer: C

QUESTION 2

Mark works as a Network Security Administrator for Umbrella Inc. The company has a Windows domain-based network. To provide security to the network, Mark plans to configure IDS. He wants to ensure that attackers are not able to modify or delete the system files. To determine such attacks, the IDS must be able to monitor the file structure of the system. Which of the following intrusion detection technologies can be used to accomplish the task?

A. Network IDS

B. Log File Monitor (LFM)

C. Host-based IDS

D. Systems Integrity Verifier (SIV)

Correct Answer: D

QUESTION 3

Kerberos is a computer network authentication protocol that allows individuals communicating over a non-secure network to prove their identity to one another in a secure manner. Which of the following statements are true about the Kerberos authentication scheme?

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

A. Kerberos requires continuous availability of a central server.

B. Kerberos builds on Asymmetric key cryptography and requires a trusted third party.

C. Dictionary and brute force attacks on the initial TGS response to a client may reveal the subject\\'spasswords.

D. Kerberos requires the clocks of the involved hosts to be synchronized.

Correct Answer: ACD

QUESTION 4

Which of the following techniques is used to log network traffic?

A. IP address spoofing

B. Tunneling

C. Sniffing

D. Cracking

Correct Answer: C

QUESTION 5

Which of the following commands is used in Mac OS X to exit Open Firmware and to continue the booting process?

A. mac-load

B. boot

C. load

D. mac-boot

Correct Answer: D