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.leads4pass.com/ecss.html

100% Passing Guarantee
100% Money Back Assurance

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

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

Which of the following commands is most useful for viewing large files in Linux?

A. less

B. cp

C. touch

D. cat

Correct Answer: A

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

Adam works as a Computer Hacking Forensic Investigator for a garment company in the United States. A project has been assigned to him to investigate a case of a disloyal employee who is suspected of stealing design of the garments, which belongs to the company and selling those garments of the same design under different brand name. Adam investigated that the company does not have any policy related to the copy of design of the garments. He also investigated that the trademark under which the employee is selling the garments is almost identical to the original trademark of the company. On the grounds of which of the following laws can the employee be prosecuted?

A. Copyright law

B. Cyber law

C. Espionage law

D. Trademark law

Correct Answer: D

QUESTION 4

Which of the following organizations is dedicated to computer security research and information sharing?

A. NIPC

B. FBI

C. Honeynet Project

D. IEEE

Correct Answer: C

QUESTION 5

Which of the following is a form of cheating or copying someone else\\'s work or idea without acknowledging the source?

A. Plagiarism

B. Turnitin

C. Copyright

D. Patent

Correct Answer: A

QUESTION 6

John, a malicious hacker, forces a router to stop forwarding packets by flooding it with many open connections simultaneously so that all hosts behind it are effectively disabled. Which of the following attacks is John performing?

A. DoS attack

B. Rainbow attack

C. ARP spoofing

D. Replay attack

Correct Answer: A

QUESTION 7

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 (orInternet)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 fromone network to another.

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

Correct Answer: ACD

QUESTION 8

Which of the following tools is used to clear the event log?

A. Elsave

B. Auditpol

C. John the Ripper

D. AirSnort

Correct Answer: A

QUESTION 9

Which two security components should you implement on the sales personnel portable computers to increase security?

(Click the Exhibit button on the toolbar to see the case study.)

Each correct answer represents a complete solution. Choose two.

A. Remote access policy

B. L2TP over IPSec

C. Encrypting File System (EFS)

D. Remote Authentication Dial-In User Service (RADIUS)

E. PPTP

Correct Answer: BC

QUESTION 10

John works as a professional Ethical Hacker. He has been assigned the project of testing the security of www.we-are-secure.com. He has successfully completed the following steps of the preattack phase:

·Information gathering ·Determining network range ·Identifying active machines ·Finding open ports and applications ·OS fingerprinting ·Fingerprinting services

Now John wants to perform network mapping of the We-are-secure network. Which of the following tools can he use to accomplish his task?

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

A. Traceroute

B. NeoTrace

C. Cheops

D. Ettercap

Correct Answer: ABC

QUESTION 11

John works as a Professional Ethical Hacker for NetPerfect Inc. The company has a Linux-based network. All client computers are running on Red Hat 7.0 Linux. The Sales Manager of the company complains to John that his system contains an unknown package named as tar.gz and his documents are exploited. To resolve the problem, John uses a Port scanner to enquire about the open ports and finds out that the HTTP server service port on 27374 is open. He suspects that the other computers on the network are also facing the same problem. John discovers that a malicious application is using the synscan tool to randomly generate IP addresses.

Which of the following worms has attacked the computer?

A. Code red

B. Ramen

C. LoveLetter

D. Nimda

Correct Answer: B

QUESTION 12

Adam works as a Computer Hacking Forensic Investigator for a garment company in the United States. A project has been assigned to him to investigate a case of a disloyal employee who is suspected of stealing design of the garments, which belongs to the company and selling those garments of the same design under different brand name. Adam investigated that the company does not have any policy related to the copy of design of the garments. He also investigated that the trademark under which the employee is selling the garments is almost identical to the original trademark of the company. On the grounds of which of the following laws can the employee be prosecuted?

A. Copyright law

B. Cyber law

C. Espionage law

D. Trademark law

Correct Answer: D

QUESTION 13

John works as a Security Administrator for NetPerfect Inc. The company uses Windows-based

systems. A project has been assigned to John to track malicious hackers and to strengthen the company\\'s security system. John configures a computer system to trick malicious hackers into thinking that it is the company\\'s main server, which in fact is a decoy system to track hackers.

Which system is John using to track the malicious hackers?

A. Honeypot

B. Intrusion Detection System (IDS)

C. Bastion host

D. Honeytokens

Correct Answer: A

QUESTION 14

In which of the following access control models can a user not grant permissions to other users to see a copy of an object marked as secret that he has received, unless they have the appropriate permissions?

A. Role Based Access Control (RBAC)

B. Mandatory Access Control (MAC)

C. Access Control List (ACL)

D. Discretionary Access Control (DAC)

Correct Answer: B

QUESTION 15

Which of the following tools is used to catch someone installing a rootkit or running a packet sniffer?

A. chkrootkit

B. rkhunter

C. Blue Pill

D. OSSEC

Correct Answer: A