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

You work as a Network Administrator for Tech Perfect Inc. The company has a Windows Server 2008 network environment. The network is configured as a Windows Active Directory-based single forest domain-based network. The company has recently provided fifty laptops to its sales team members. You are required to configure an 802.11 wireless network for the laptops. The sales team members must be able to use their data placed at a server in a cabled network. The planned network should be able to handle the threat of unauthorized access and data interception by an unauthorized user. You are also required to prevent the sales team members from communicating directly to one another. Which of the following actions will you perform to accomplish the task?

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

A. Implement the open system authentication for the wireless network.

B. Implement the IEEE 802.1X authentication for the wireless network.

C. Configure the wireless network to use WEP encryption for the data transmitted over a wireless network.

D. Using group policies, configure the network to allow the wireless computers to connect to the infrastructure networks only.

E. Using group policies, configure the network to allow the wireless computers to connect to the ad hoc networks only.

Correct Answer: BCD

QUESTION 2

Which of the following Linux rootkits is installed via stolen SSH keys?

A. Phalanx2

B. Beastkit

C. Adore

D. Linux.Ramen

Correct Answer: A

QUESTION 3

A firewall is a combination of hardware and software, used to provide security to a network. It is used to protect an internal network or intranet against unauthorized access from the Internet or other outside networks. It restricts inbound and outbound access and can analyze all traffic between an internal network and the Internet. Users can configure a firewall to pass or block packets from specific IP addresses and ports. Which of the following tools works as a firewall for the Linux 2.4 kernel?

A. Stunnel

B. IPChains

C. IPTables

D. OpenSSH

Correct Answer: C

QUESTION 4

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 5

Which of the following softwares is used to perform constant monitoring of the network infrastructure?

A. Logdog

B. THCHydra

C. IPSentry

D. Cain

Correct Answer: C

QUESTION 6

What does EFI stand for?

A. Extensible Firmware Interface

B. Extended Firewall Interface

C. Extensible Firewall Interface

D. Extended Firmware Interface

Correct Answer: A

QUESTION 7

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 8

Which of the following are the two types of reconnaissance?

A. Direct and Indirect

B. Active and passive

C. Active and Invasive

D. Preliminary and active

Correct Answer: B

QUESTION 9

Which of the following agencies is responsible for handling computer crimes in the United States?

A. The FBI only

B. The Federal Bureau of Investigation (FBI) and the Secret Service

C. The Central Intelligence Agency (CIA)

D. The National Security Agency (NSA)

Correct Answer: B

QUESTION 10

Which of the following is a valid IP address for class B Networks?

A. 212.136.45.8

B. 172.157.88.3

C. 80.33.5.7

D. 225.128.98.7

Correct Answer: B

QUESTION 11

Which of the following protocols is used the most by web servers?

A. COM

B. FTP

C. HTTP

D. ORG

Correct Answer: C

QUESTION 12

According to the Sophos Security Threat Report 2009, which amongst the following countries is on the top, in hosting malware on the web?

A. United States

B. Russia

C. China

D. Germany

Correct Answer: A

QUESTION 13

Adam works as a Security Analyst for Umbrella Inc. He is retrieving large amount of log data from syslog servers and network devices such as Router and switches. He is facing difficulty in analyzing the logs that he has retrieved. To solve

this problem, Adam decides to use software called Sawmill. Which of the following statements are true about Sawmill?

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

A. It is used to analyze any device or software package, which produces a log file such as Web servers, network devices (switches and routers etc.), syslog servers etc.

B. It incorporates real-time reporting and real-time alerting.

C. It comes only as a software package for user deployment.

D. It is a software package for the statistical analysis and reporting of log files.

Correct Answer: ABD

QUESTION 14

Cola Co. manufactures, markets, sells, and distributes non-alcoholic potables such as Lemcaa and Thunder Up under its brand name Cola and uses green and red logo. Mola Co., a new company, starts manufacturing, marketing, selling, and distributing non-alcoholic potables like Lumca and Cloud Up under its brand name Mola and uses green and red logo. Which of the following violations has been committed by Mola Co.?

A. Copyright infringement

B. Trademark infringement

C. Patent law

D. Plagiarism

Correct Answer: B

QUESTION 15

Which of the following is true for XSS, SQL injection, and RFI?

A. These are Trojans.

B. These are hacking tools.

C. These are viruses.

D. These are types of Web application vulnerabilities.

Correct Answer: D