DUMPSBOSS.

EC-Council Certified Security Specialist (ECSS) v10

ECCouncil ECSS

Version Demo

Total Demo Questions: 15

Total Premium Questions: 337

Buy Premium PDF

https://dumpsboss.co

support@dumpsboss.co

support@dumpsboss.co
dumpsboss.co

Topic Break Down

Topic	No. of Questions
Topic 1, Volume A	93
Topic 2, Volume B	94
Topic 3, Volume C	150
Total	337

QUESTION NO: 1

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 organize addresses into classes, which are used to determine how to move packets from one network to another.

C. Routers do not limit physical broadcast traffic.

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

ANSWER: A B D

QUESTION NO: 2

You are a professional Computer Hacking forensic investigator. You have been called to collect the evidences of Buffer Overflows or Cookie snooping attack. Which of the following logs will you review to accomplish the task?

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

A. Web server logs

B. Event logs

C. Program logs

D. System logs

ANSWER: B C D

QUESTION NO: 3

Which of the following software can be used to protect a computer system from external threats (viruses, worms, malware, or Trojans) and malicious attacks?

Each correct answer represents a part of the solution. Choose all that apply.

A. Employee monitoring software

B. Burp Suite

C. Antivirus

D. Firewall

ANSWER: C D

QUESTION NO: 4

John works as a Security Administrator for NetPerfect Inc. The company uses Windowsbased 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. Bastion host

B. Honeypot

C. Honeytokens

D. Intrusion Detection System (IDS)

ANSWER: B

QUESTION NO: 5

You work as a Network Administrator for DataSoft Inc. The company needs a secure network. You have been assigned the task to track the network attacks that have occurred within the last one month. To accomplish the task, you need to scan the log files for suspicious events and patterns.

Which of the following will you use to scan the log files?

A. PsTools suite

B. System Integrity Verifiers (SIV)

C. Log File Monitor (LFM)

D. Specter

ANSWER: C

QUESTION NO: 6

Andrew works as a Forensic Investigator for Passguide Inc. The company has a Windowsbased environment. The company's employees use Microsoft Outlook Express as their email client program. E-mails of some employees have been deleted due to a virus attack on the network.

Andrew is therefore assigned the task to recover the deleted mails. Which of the following tools can Andrew use to accomplish the task?

Each correct answer represents a complete solution. Choose two.

A. FINALeMAIL

B. eMailTrackerPro

C. EventCombMT

D. R-mail

ANSWER: A D

QUESTION NO: 7

Which of the following law does not protect intellectual property?

A. Patent law

B. Copyright

C. Murphy's law

D. Trademark

ANSWER: C

QUESTION NO: 8

Which of the following two cryptography methods are used by NTFS Encrypting File System (EFS) to encrypt the data stored on a disk on a file-by-file basis?

A. Digital certificates

B. Twofish

C. Public key

D. RSA

ANSWER: A C

QUESTION NO: 9

What does CSIRT stand for?

A. Computer Security Incident Response Team

B. Chief Security Incident Response Team

C. Computer Security Information Response Team

D. Chief Security Information Response Team

ANSWER: A

QUESTION NO: 10

Which of the following functions does the RSA Digital Signature combine with public key algorithm to create a more secure signature?

A. %

B. $

C. #

D. *

ANSWER: C

QUESTION NO: 11

Fill in the blank with the appropriate layer name of the OSI model.

Secure Socket Layer (SSL) operates at the_____ layer of the OSI model.

A. transport

ANSWER: A

QUESTION NO: 12

John works as a professional Ethical Hacker. He has been assigned a project to test the security of www.we-are-secure.com. He performs Web vulnerability scanning on the Weare-secure server.

The output of the scanning test is as follows:

C.\whisker.pl -h target_IP_address

-- whisker / v1.4.0 / rain forest puppy / www.wiretrip.net -- = - = - = - = - =

= Host: target_IP_address

= Server: Apache/1.3.12 (Win32) ApacheJServ/1.1

mod_ssl/2.6.4 OpenSSL/0.9.5a mod_perl/1.22

+ 200 OK: HEAD /cgi-bin/printenv

John recognizes /cgi-bin/printenv vulnerability ('Printenv' vulnerability) in the

We_are_secure server. Which of the following statements about 'Printenv' vulnerability are true?

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

A. This vulnerability helps in a cross site scripting attack.

B. 'Printenv' vulnerability maintains a log file of user activities on the Website, which may be useful for the attacker.

C. With the help of 'printenv' vulnerability, an attacker can input specially crafted links and/or other malicious scripts.

D. The countermeasure to 'printenv' vulnerability is to remove the CGI script.

ANSWER: A C D

QUESTION NO: 13

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.

ANSWER: B C D

QUESTION NO: 14

Rick, the Network Administrator of the Fimbry Hardware Inc., wants to design the initial test model for Internet Access. He wants to fulfill the following goals:

·No external traffic should be allowed into the network.

·Administrators should be able to restrict the websites which can be accessed by the internal users.

Which of the following technologies should he use to accomplish the above goals?

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

A. Firewall

B. Network Address Translator (NAT)

C. Proxy Server

D. Internet Connection Sharing (ICS)

E. Routing and Remote Access Service (RRAS)

ANSWER: C

QUESTION NO: 15

You work as a Network Administrator for Infonet Inc. The company's network is connected to the Internet. The network has a Web server that is accessible to Internet users. For security, you want to keep the Web server separate from other servers on the network.

Where will you place the Web server?

A. With the authentication server

B. In a demilitarized zone (DMZ)

C. With the database server

D. In a virtual private network (VPN)

ANSWER: B