DUMPSARENA

GIAC Security Leadership

GIAC GSLC

Version Demo

Total Demo Questions: 20

Total Premium Questions: 566

Buy Premium PDF

https://dumpsarena.com

sales@dumpsarena.com

dumpsarena.com

Topic Break Down

Topic	No. of Questions
Topic 1, Volume A	139
Topic 2, Volume B	149
Topic 3, Volume C	143
Topic 4, Volume D	135
Total	566

QUESTION NO: 1

John works as a professional Ethical Hacker. He has been assigned the project of testing the security of www.we-are-secure.com. He receives the following e-mail:

> Hello Disney fans,
>
> And thank you for signing up for Bill Gates' Beta Email Tracking. My name is Walt Disney Jr. Here at Disney we are working with Microsoft which has just compiled an email tracing program that tracks everyone to whom this message is forwarded to. It does this through a unique IP (Internet Protocol) address log book database. We are experimenting with this and need your help. Forward this to everyone you know and if it reaches 13,000 people, 1,300 of the people on the list will receive $5,000, and the rest will receive a free trip for two to Disney World for one week during the summer of 1999 at our expense. Enjoy.
>
> Note: Duplicate entries will not be counted. You will be notified by email with further instructions once this email has reached 13,000 people.
>
> Your friends,
> Walt Disney Jr., Disney, Bill Gates
> & The Microsoft Development Team.

The e-mail that John has received is an example of _____.

A. Social engineering attacks

B. Virus hoaxes

C. Spambots

D. Chain letters

ANSWER: D

QUESTION NO: 2

Which of the following attacks allows an attacker to recover the key in an RC4 encrypted stream from a large number of messages in that stream?

A. Rainbow attack

B. SYN flood attack

C. Zero Day attack

D. FMS attack

ANSWER: D

QUESTION NO: 3

Which of the following can be used as a countermeasure against the SQL injection attack? Each correct answer represents a complete solution. Choose two.

A. mysql_escape_string()

B. session_regenerate_id()

C. mysql_real_escape_string()

D. Prepared statement

ANSWER: C D

QUESTION NO: 4

A project team member has just identified a new project risk. The risk event is determined to have significant impact but a low probability in the project. Should the risk event happen it'll cause the project to be delayed by three weeks, which will cause new risk in the project. What should the project manager do with the risk event?

A. Add the identified risk to the issues log.

B. Add the identified risk to a quality control management control chart.

C. Add the identified risk to the low-level risk watchlist.

D. Add the identified risk to the risk register.

ANSWER: D

QUESTION NO: 5 - (SIMULATION)

SIMULATION

Fill in the blank with the appropriate term.

_____is a configuration of a network card that makes the card pass all traffic it receives to the central processing unit rather than just packets addressed to it.

ANSWER: Promiscuous mode

QUESTION NO: 6

John works as a professional Ethical Hacker. He has been assigned the project of testing the security of www.we-are-secure.com. He wants to use Kismet as a wireless sniffer to sniff the Weare-secure network. Which of the following IEEE-based traffic can be sniffed with Kismet? Each correct answer represents a complete solution. Choose all that apply.

A. 802.11g

B. 802.11a

C. 802.11b

D. 802.11n

ANSWER: A B C D

QUESTION NO: 7

Which of the following provides security by implementing authentication and encryption on Wireless LAN (WLAN)?

A. WEP

B. WAP

C. L2TP

D. IPSec

ANSWER: A

QUESTION NO: 8

PassGuide Research and Training Center is developing its new network model. Which of the following protocols should be implemented in the new network? (Click the Exhibit button on the toolbar to see the case study.) Each correct answer represents a complete solution. Choose two.

A. IPX/SPX

B. NetBEUI

C. TCP/IP

D. AppleTalk

ANSWER: C D

QUESTION NO: 9

You work as the Network Administrator for a company that does a large amount of defense contract business. A high level of security, particularly regarding sensitive documents, is required.

Which of the following are the steps you should take to secure network printers? Each correct answer represents a complete solution. Choose two.

A. Remove the printers from the network and do not allow remote printing.

B. Ensure that the printers hard drive is scanned for spyware.

C. Secure all remote administrative protocols such as telnet.

D. Do not allow duplicate print jobs.

E. Limit the size of print jobs on the printer.

ANSWER: B C

QUESTION NO: 10

Victor works as a professional Ethical Hacker for SecureEnet Inc. He has been assigned a job to test an image, in which some secret information is hidden, using Steganography. Victor performs the following techniques to accomplish the task:

1. Smoothening and decreasing contrast by averaging the pixels of the area where significantcolor transitions occurs.

2. Reducing noise by adjusting color and averaging pixel value.

3. Sharpening, Rotating, Resampling, and Softening the image.

Which of the following Steganography attacks is Victor using?

A. Steg-Only Attack

B. Stegdetect Attack

C. Active Attacks

D. Chosen-Stego Attack
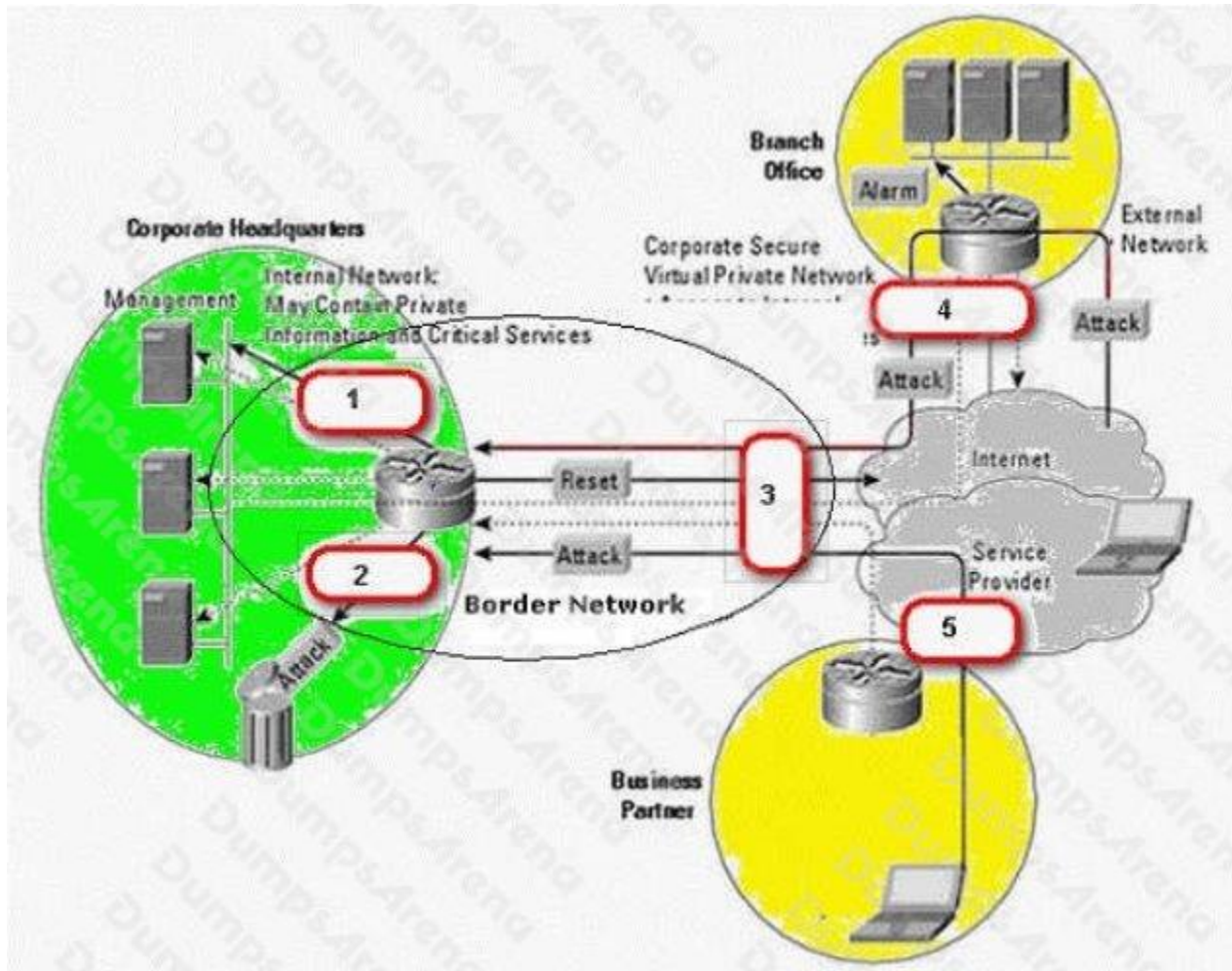
ANSWER: C

QUESTION NO: 11 - (HOTSPOT)

HOTSPOT

You work as a Security manager for Caterxiss Inc. The headquarters of your company is connected to the branch office in another state and a service partner in the same state. The network of the company is being attacked from the connected
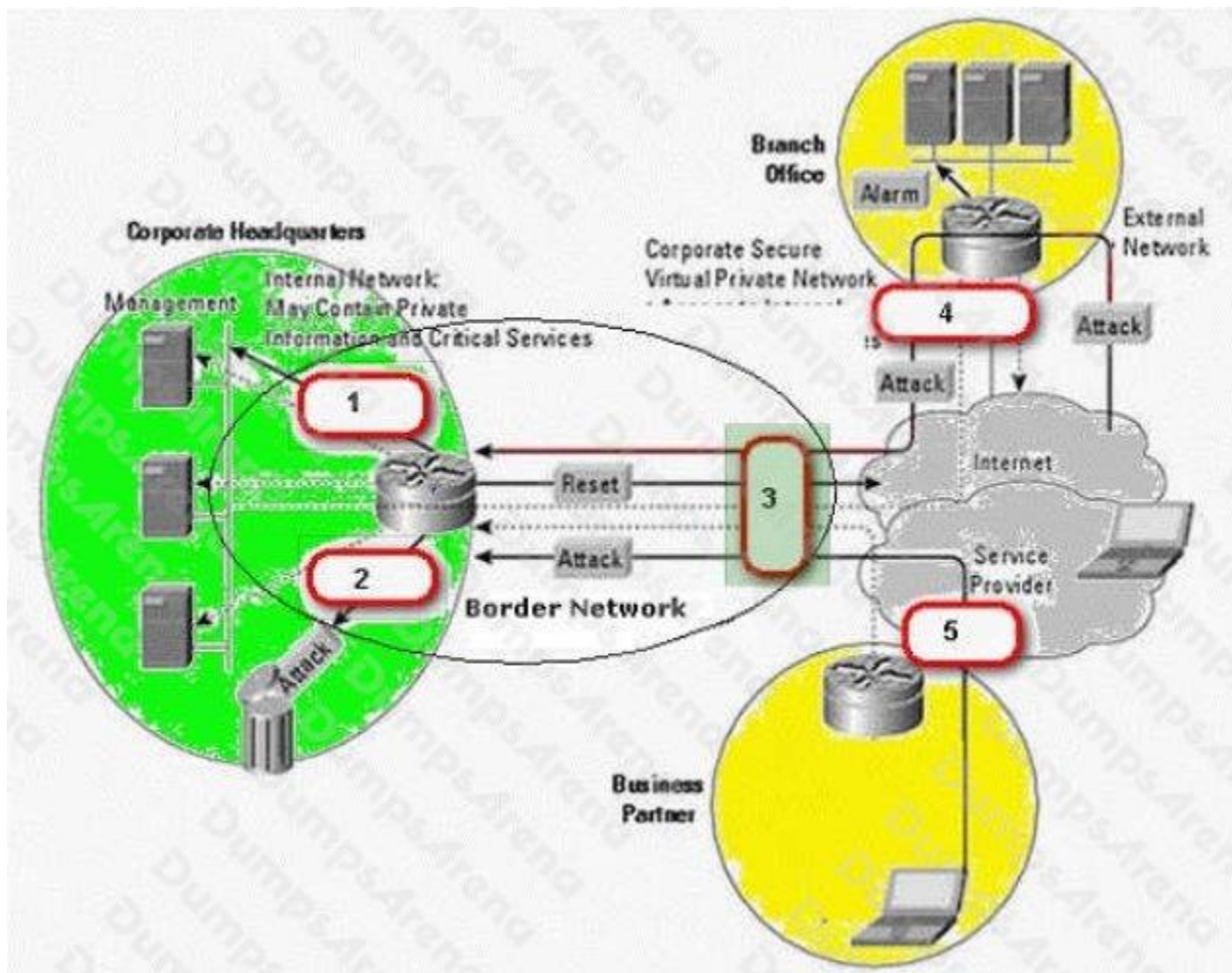
networks. You decide to analyze and then prevent the corporate headquarters network from these attacks using a Snort IDS. What is the most appropriate spot on the network where you should set up an Intrusion detection system (IDS)?

Click on the correct spot in the image. Doing so will place the target icon at the clicked spot.

Hot Area:

ANSWER:

Explanation:

Victor wants to use Wireless Zero Configuration (WZC) to establish a wireless network connection using his computer running on Windows XP operating system. Which of the following are the most likely threats to his computer?

Each correct answer represents a complete solution. Choose two.

A. Attacker can use the Ping Flood DoS attack if WZC is used.

B. Information of probing for networks can be viewed using a wireless analyzer and may be used to gain access.

C. Attacker by creating a fake wireless network with high power antenna cause Victor's computer to associate with his network to gain access.

D. It will not allow the configuration of encryption and MAC filtering. Sending information is not secure on wireless network.

ANSWER: B C

QUESTION NO: 13

Which of the following statements about Secure Shell (SSH) are true?

Each correct answer represents a complete solution. Choose three.

A. It is the core routing protocol of the Internet.

B. It was designed as a replacement for TELNET and other insecure shells.

C. It is a network protocol used primarily on Linux and Unix based systems.

D. It allows data to be exchanged using a secure channel between two networked devices.

ANSWER: B C D

QUESTION NO: 14 - (DRAG DROP)

DRAG DROP

You work as a Network Administrator for Infonet Inc. The company has a Windows Server 2008

Active Directory-based single domain single forest network. The functional level of the forest is Windows Server 2003. All client computers on the network run Windows XP Professional. You configure a public key infrastructure (PKI) on the network. You configure a root CA and a subordinate CA on the network. For security reasons, you want to take the root CA offline. You are required to configure the CA servers to support for certificate revocation. Choose the steps you will require to accomplish the task.
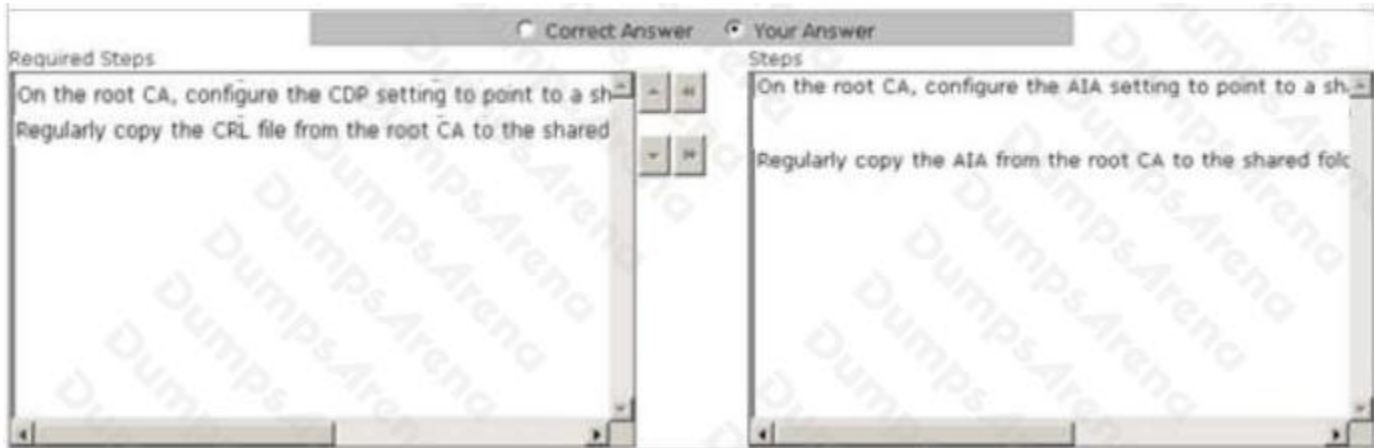
Select and Place:

Correct Answer	Your Answer
Required Steps	Steps
	On the root CA, configure the AIA setting to point to a sh
	On the root CA, configure the CDP setting to point to a sh
	Regularly copy the CRL file from the root CA to the shared
	Regularly copy the AIA from the root CA to the shared fold

ANSWER:

Explanation:

Tomas is the project manager of the QWS Project and is worried that the project stakeholders will want to change the project scope frequently. His fear is based on the many open issues in the project and how the resolution of the issues may lead to additional project changes. On what document are Tomas and the stakeholders working in this scenario?

A. Change management plan

B. Communications management plan

C. Issue log

D. Risk management plan

ANSWER: A

Which of the following is an input of the close procurements process?

A. Organizational process asset updates

B. Procurement credentials

C. Project management plan

D. Closed procurements

ANSWER: C

QUESTION NO: 17

Which of the following tools can be used to automate the MITM attack?

A. Airjack

B. Kismet

C. IKECrack

D. Hotspotter

ANSWER: A

QUESTION NO: 18

Which of the following uses a variable-length Initialization Vector (IV), where the encrypted data begins?

A. DES-OFB

B. DES-ECB

C. DES-CBC

D. DES-CFB

ANSWER: C

QUESTION NO: 19

You have just set up a wireless network for customers at a coffee shop. Which of the following are good security measures to implement?

Each correct answer represents a complete solution. Choose two.

A. Using WPA encryption

B. MAC filtering the router

C. Using WEP encryption

D. Not broadcasting SSID

ANSWER: A C

QUESTION NO: 20

Adrian knows the host names of all the computers on his network. He wants to find the IP addresses of these computers. Which of the following TCP/IP utilities can he use to find the IP addresses of these computers?

Each correct answer represents a complete solution. Choose two.

A. IPCONFIG

B. PING

C. NETSTAT

D. TRACERT

ANSWER: B D