DUMPSARENA

GIAC Security Leadership Certification (GSLC)

GIAC GSLC

Version Demo

Total Demo Questions: 20

Total Premium Questions: 566

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

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

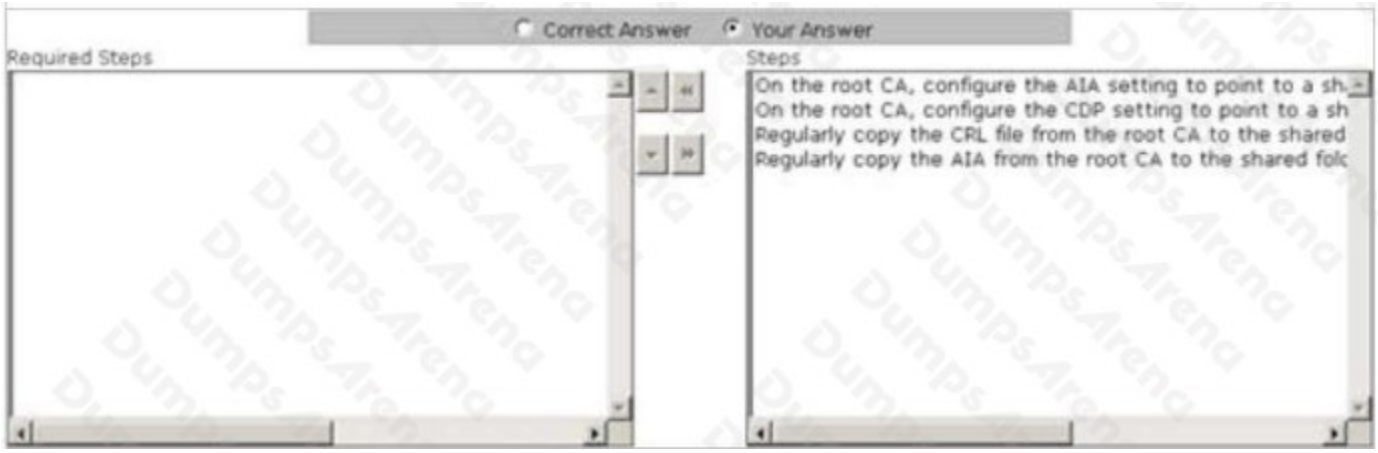
QUESTION NO: 1 - (DRAG DROP)

DRAG DROP

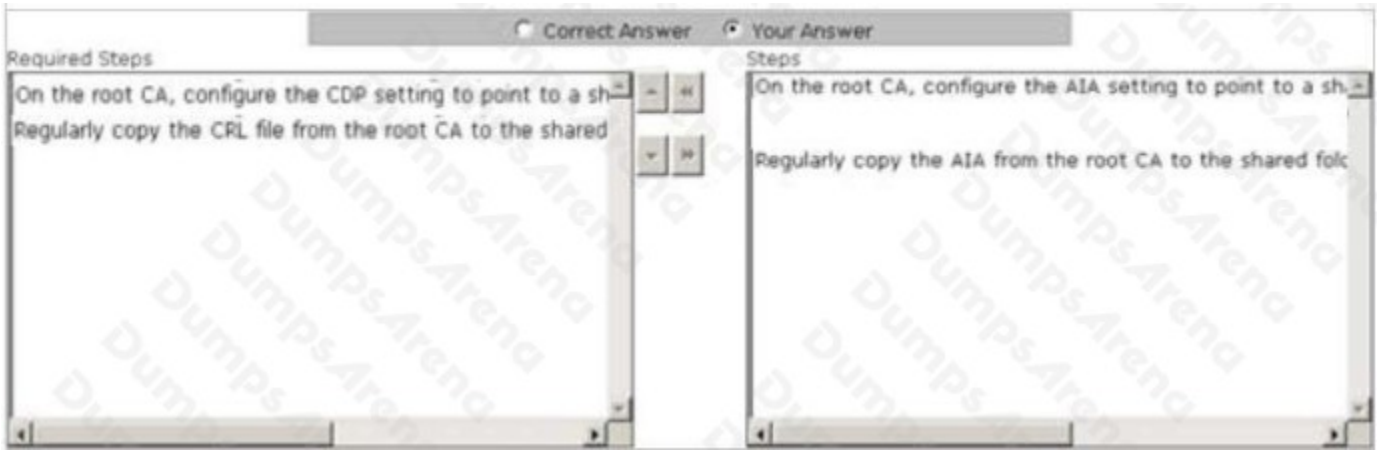
You work as a Network Administrator for Infonet Inc. The company has a Windows Server 2008

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:



ANSWER:



Explanation:

QUESTION NO: 2

You check the logs on several clients and find that there is traffic coming in on an odd port (port 1872). All clients have the Windows XP firewall turned on. What should you do to block this unwanted traffic?

A. Trace back that traffic and find its origin.

B. Check the exceptions in the firewall and unselect that port exception.

C. Perform a virus scan to find the virus responsible for this traffic.

D. Shut down the service that connects to that port.

ANSWER: B

QUESTION NO: 3

Which of the following are types of access control attacks?

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

A. Brute force attack

B. Mail bombing

C. Dictionary attack

D. Spoofing

ANSWER: A C D

QUESTION NO: 4

You are the project manager of the GYG Project. A new scope change is being considered for your project. You are concerned, however, that the scope change may add costs, risks, and adversely affect the project schedule. What project management process is responsible for evaluating the full effect of a proposed scope change on your project?

A. Schedule change control

B. Scope change control

C. Integrated change control

D. Change Control Board approval process

ANSWER: C

QUESTION NO: 5

You work as an Exchange Administrator for McRobert Inc. You are configuring a new Exchange 2000 Server computer and two storage groups, group A and group B, on your network. You have to configure the physical disks on the Exchange 2000 Server computer to provide better performance and availability. Which configuration will you use to achieve this?

A. Mirrored ---- Transaction Log Files (group A)
Mirrored ---- Transaction Log Files (group B)
RAID5 ------ Information store (groups A and B)

B. Single drive ---- Transaction Log Files (group A)
Single drive ---- Transaction Log Files (group B)
RAID5 --------- Information Store (groups A and B)

C. Mirrored ---- Transaction Log Files (groups A and B) RAID5 ------ Information Store (groups A and B)

D. Single drive ----- Transaction Log Files (group A)
Single drive ----- Transaction Log Files (group B)
RAID5 ---------- Information Store (group A)
RAID5 ---------- Information Store (group B)

ANSWER: D

QUESTION NO: 6

John works as a professional Ethical Hacker. He has been assigned the task of testing the security of www.we-are-secure.com. He installs a sniffer on the We-are-secure server thinking that the following protocols of the We-are-secure server are being used in the network:

- HTTP
- SSL
- SSH
- IPSec

Considering the above factors, which of the following types of packets can he expect to see captured in encrypted form when he checks the sniffer's log file?

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

A. SSH

B. SSL

C. HTTP

D. IPSec

ANSWER: A B D

QUESTION NO: 7

You are the Network Administrator for a large corporate network. You want to monitor all network traffic on your local network for suspicious activities and receive a notification when a possible attack is in process. Which of the following actions will you take for this?

A. Install a host-based IDS

B. Enable verbose logging on the firewall

C. Install a DMZ firewall

D. Install a network-based IDS

ANSWER: D

QUESTION NO: 8

Which of the following items are generally analyzed by Internet filters? Each correct answer represents a complete solution. Choose three.

A. Content

B. Certificates

C. Uniform Resource Locators (URLs)

D. Network Topology

ANSWER: A B C

QUESTION NO: 9

Which of the following are symptoms of a virus attack on your computer? Each correct answer represents a complete solution. Choose two.

A. Corrupted or missing files.

B. Sudden reduction in system resources.

C. Faster read/write access of the CD-ROM drive.

D. Unclear monitor display.

ANSWER: A B

QUESTION NO: 10 - (SIMULATION)

SIMULATION

Fill in the blank with the appropriate tool name.

_____ is a wireless network cracking tool that exploits the vulnerabilities in the RC4 Algorithm, which comprises the WEP security parameters.

ANSWER: WEPcrack

QUESTION NO: 11

Which of the following is a software testing method that uses an internal perspective of the system to design test cases based on the internal structure?

A. Water Fall

B. Black box

C. White box

D. Gray box

ANSWER: C

QUESTION NO: 12

You configure a wireless router at your home. To secure your home Wireless LAN (WLAN), you implement WEP. Now you want to connect your client computer to the WLAN. Which of the following is the required information that you will need to configure the client computer? Each correct answer represents a part of the solution. Choose two.

A. WEP key

B. IP address of the router

C. MAC address of the router

D. SSID of the WLAN

ANSWER: A D

QUESTION NO: 13

Which of the following malware spread through the Internet and caused a large DoS attack in 1988?

A. Morris worm

B. LoveLetter worm

C. SQL slammer worm

D. Klez worm

ANSWER: A

QUESTION NO: 14

What does noise in a power line indicate?

A. Power degradation that is low and less than normal

B. Interference superimposed onto the power line

C. Momentary high voltage

D. Prolonged loss of power

ANSWER: B

QUESTION NO: 15

John works as a professional Ethical Hacker. He has been assigned the project of testing the security of www.we-are-secure.com. John notices that the We-are-secure network is vulnerable to a man-inthe-middle attack since the key exchange process of the cryptographic algorithm it is using does not authenticate participants. Which of the following cryptographic algorithms is being used by the Weare-secure server?

A. RSA

B. Diffie-Hellman

C. Twofish

D. Blowfish

ANSWER: B

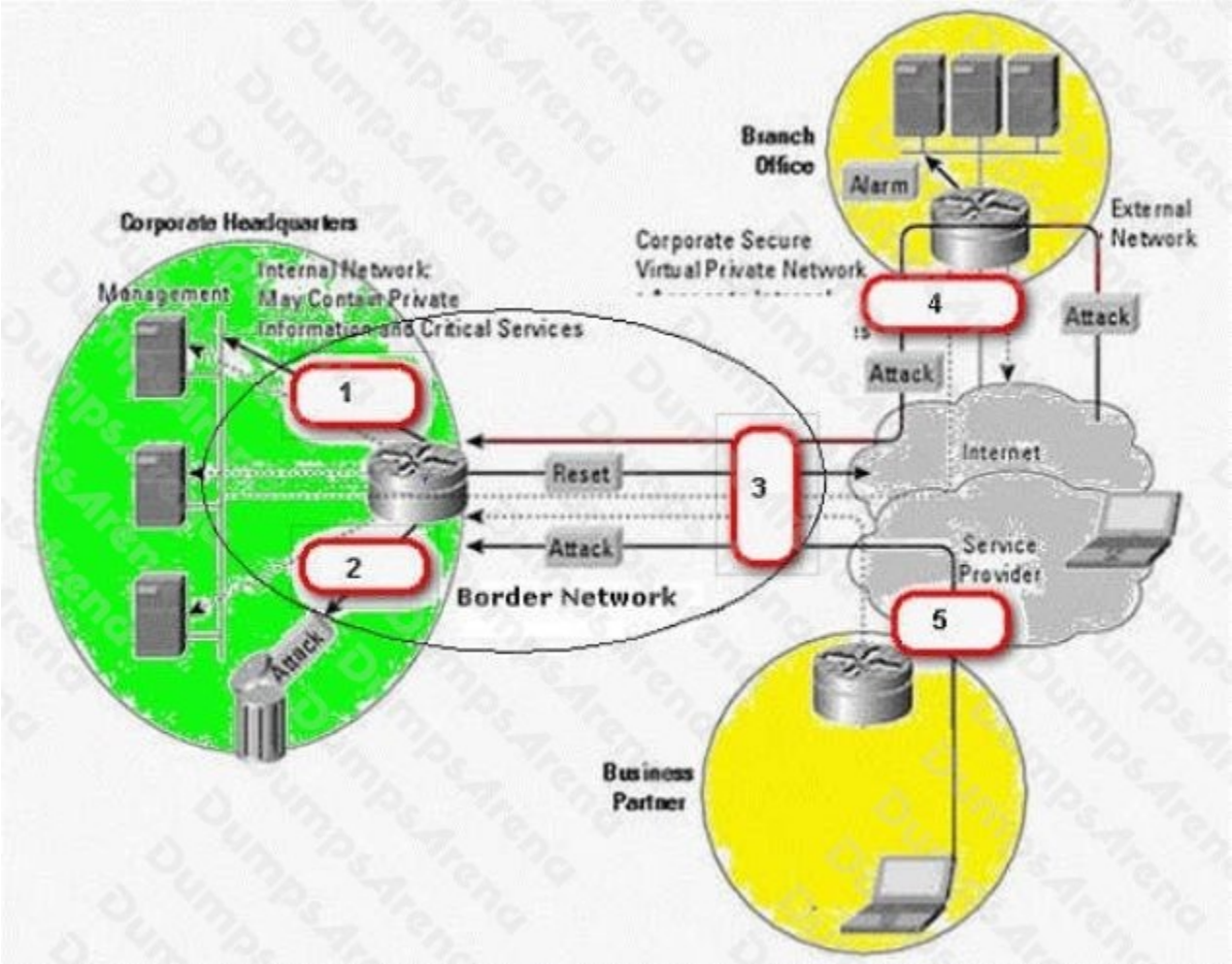
QUESTION NO: 16 - (HOTSPOT)

HOTSPOT

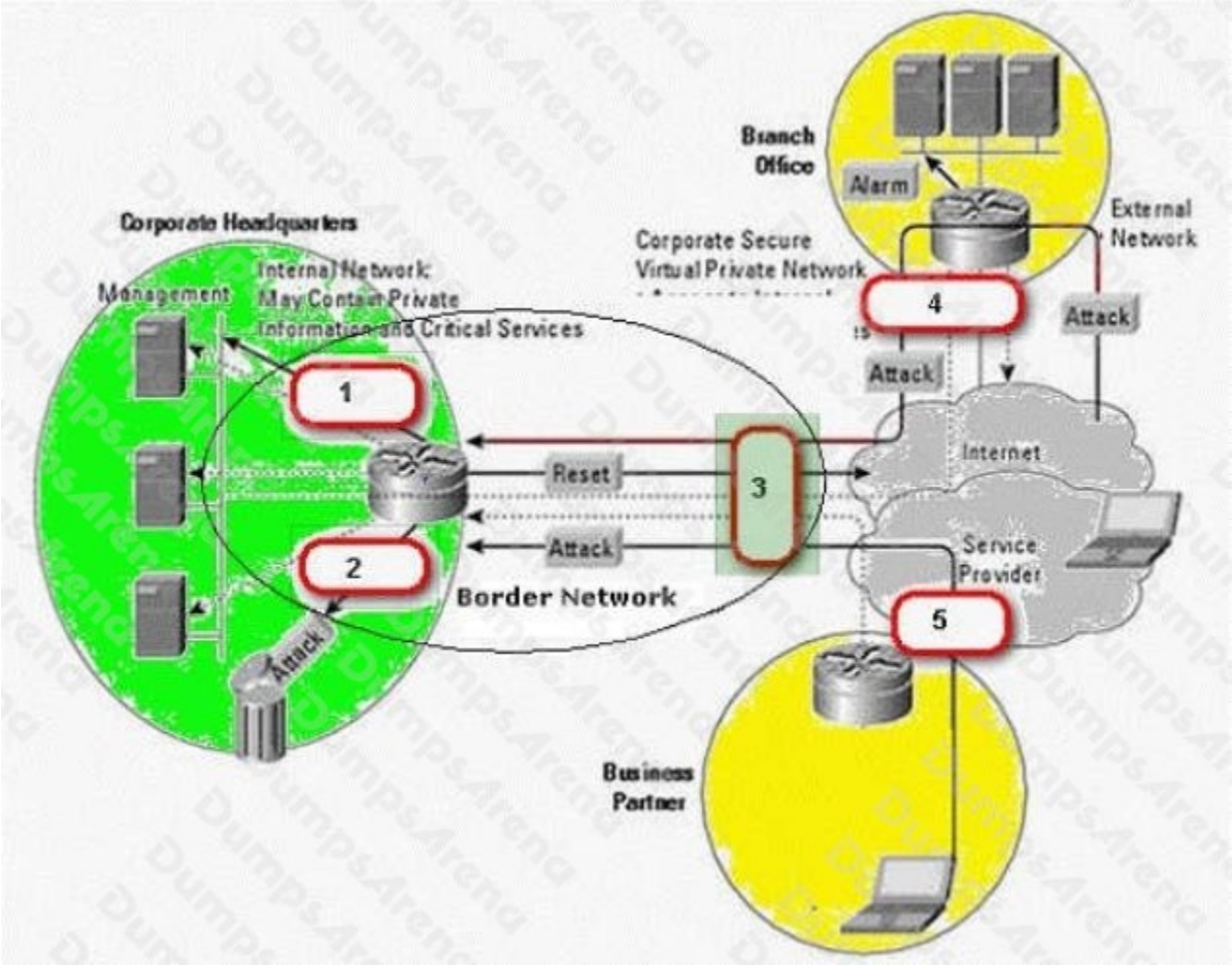
You work as a Security manager for Caterxiss Inc. The headquarters of your company is connected to the branch office in another state and a service partner in the same state. The network of the company is being attacked from the connected networks. You decide to analyze and then prevent the corporate 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:

QUESTION NO: 17

Which of the following work as traffic monitoring tools in the Linux operating system?

Each correct answer represents a complete solution. Choose two.

A. IPTraf

B. Hotspotter

C. Ntop

D. John the Ripper

ANSWER: A C

QUESTION NO: 18

Wired Equivalent Privacy (WEP) is a security protocol for wireless local area networks (WLANs). It has two components, authentication and encryption. It provides security equivalent to wired networks for wireless networks. WEP encrypts data on a wireless network by using a fixed secret key. Which of the following statements are true about WEP?

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

A. WEP uses the RC4 encryption algorithm.

B. Automated tools such as AirSnort are available for discovering WEP keys.

C. It provides better security than the Wi-Fi Protected Access protocol.

D. The Initialization Vector (IV) field of WEP is only 24 bits long.

ANSWER: A B D

QUESTION NO: 19

How can you calculate the Annualized Loss Expectancy (ALE) that may occur due to a threat?

A. Single Loss Expectancy (SLE) X Annualized Rate of Occurrence (ARO)

B. Single Loss Expectancy (SLE)/ Exposure Factor (EF)

C. Asset Value X Exposure Factor (EF)

D. Exposure Factor (EF)/Single Loss Expectancy (SLE)

ANSWER: A

QUESTION NO: 20

Which of the following tools can be used to perform ICMP tunneling? Each correct answer represents a complete solution. Choose two.

A. WinTunnel

B. Ethereal

C. Itunnel

D. Ptunnel

ANSWER: C D