DUMPSARENA

GIACCertified Forensics Analyst

GIAC GCFA

Version Demo

Total Demo Questions: 15

Total Premium Questions: 318

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	98
Topic 2, Volume B	97
Topic 3, Volume C	123
Total	318

QUESTION NO: 1

John works as a Network Administrator for Perfect Solutions Inc. The company has a Linux-based network. John is working as a root user on the Linux operating system. He wants to forward all the kernel messages to the remote host having IP address 192.168.0.1. Which of the following changes will he perform in the syslog.conf file to accomplish the task?

A. kern.* @192.168.0.1

B. !*.* @192.168.0.1

C. *.* @192.168.0.1

D. !kern.* @192.168.0.1

ANSWER: A

QUESTION NO: 2

Which of the following encryption methods use the RC4 technology?

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

A. Dynamic WEP

B. TKIP

C. Static WEP

D. CCMP

ANSWER: A B C

QUESTION NO: 3

Which of the following tools is used to block email, Instant Message, Web site, or other media if inappropriate words such as pornography, violence etc. is used?

A. iProtect

B. Reveal

C. iProtectYou

D. Child Exploitation Tracking System

ANSWER: C

QUESTION NO: 4

Nathan works as a professional Ethical Hacker. He wants to see all open TCP/IP and UDP ports of his computer. Nathan uses the netstat command for this purpose but he is still unable to map open ports to the running process with PID, process name, and path. Which of the following commands will Nathan use to accomplish the task?

A. ping

B. Psloggedon

C. Pslist

D. fport

ANSWER: D

QUESTION NO: 5

You work as a Network Administrator for Blue Well Inc. Your company's network has a Windows 2000 server with the FAT file system. This server stores sensitive data. You want to encrypt this data to protect it from unauthorized access. You also have to accomplish the following goals:

- Data should be encrypted and secure.
- Administrative effort should be minimum.
- You should have the ability to recover encrypted files in case the file owner leaves the company.
- Other permissions on encrypted files should be unaffected.
- File-level security is required on the disk where data is stored.
- Encryption or decryption of files should not be the responsibility of the file owner.

You take the following steps to accomplish these goals:

- Convert the FAT file system to NTFS file system.
- Use third-party data encryption software.

What will happen after taking these steps?

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

A. File-level security will be available on the disk where data is stored.

B. Data will be encrypted and secure.

C. Encryption or decryption of files will no longer be the responsibility of the file owner.

D. Other permissions on encrypted files will remain unaffected.

E. Administrative effort will be minimum.

ANSWER: A B D

QUESTION NO: 6

Joseph works as a Web Designer for WebTech Inc. He creates a Web site and wants to protect it from lawsuits. Which of the following steps will he take to accomplish the task?

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

A. Restrict the access to the site.

B. Restrict shipping in certain areas.

C. Restrict the transfer of information.

D. Restrict customers according to their locations.

ANSWER: A B D

QUESTION NO: 7

An organization wants to mitigate the risks associated with the lost or stolen laptops and the associated disclosure laws, while reporting data breaches. Which of the following solutions will be best for the organization?

A. Hashing function

B. Digital signature

C. Trusted Platform Module

D. Whole disk encryption

ANSWER: D

QUESTION NO: 8

Mark works as a Network Administrator for Net Perfect Inc. The company has a Linux-based network. Mark installs a Checkpoint Firewall NGX on a SecurePlatform device. He performs a scheduled backup of his system settings and products configuration. Where are these backup files stored?

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

A. SCP

B. TFTP

C. Locally on the SecurePlatform machine hard drive

D. On a PC in a file named userC

ANSWER: A B C

QUESTION NO: 9

Which of the following command line tools are available in Helix Live acquisition tool on Windows? Each correct answer represents a complete solution. Choose all that apply.

A. .cab extractors

B. ipconfig

C. netstat

D. whois

ANSWER: A B C

QUESTION NO: 10

Which of the following are the primary goals of the incident handling team?

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

A. Prevent any further damage.

B. Freeze the scene.

C. Repair any damage caused by an incident.

D. Inform higher authorities.

ANSWER: A B C

QUESTION NO: 11

The incident response team has turned the evidence over to the forensic team. Now, it is the time to begin looking for the ways to improve the incident response process for next time. What are the typical areas for improvement? Each correct answer represents a complete solution. Choose all that apply.

A. Information dissemination policy

B. Additional personnel security controls

C. Incident response plan

D. Electronic monitoring statement

ANSWER: A B C D

QUESTION NO: 12

Peter, an expert computer user, attached a new sound card to his computer. He then restarts the computer, so that the BIOS can scan the hardware changes. What will be the memory range of ROM that the BIOS scan for additional code to be executed for proper working of soundcard?

A. hC800 to hDF80

B. hCA79 to hAC20

C. hAA43 to hF345

D. hDF80 to hFF80

ANSWER: A

QUESTION NO: 13

Which of the following registry hives contains information about all users who have logged on to the system?

A. HKEY_CLASSES_ROOT

B. HKEY_CURRENT_USERS

C. HKEY_USERS

D. HKEY_CURRENT_CONFIG

ANSWER: C

QUESTION NO: 14

An organization monitors the hard disks of its employees' computers from time to time. Which policy does this pertain to?

A. Network security policy

B. User password policy

C. Privacy policy

D. Backup policy

ANSWER: C

QUESTION NO: 15 - (SIMULATION)

SIMULATION

Fill in the blank with the appropriate file system.

Alternate Data Streams (ADS) is a feature of the_____ file system, which allows more than one data stream to be associated with a filename.

ANSWER: NTFS