DUMPSARENA

GIAC Certified Forensic Analyst

GIAC GCFA

Version Demo

Total Demo Questions: 15

Total Premium Questions: 318

Buy Premium PDF

https://dumpsarena.com

sales@dumpsarena.com

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

On which of the following locations does the Windows NT/2000 operating system contain the SAM, SAM.LOG, SECURITY.LOG, APPLICATION.LOG, and EVENT.LOG files?

A. \%Systemroot%system32

B. \%Systemroot%profiles

C. \%Systemroot%system32config

D. \%Systemroot%help

ANSWER: C

QUESTION NO: 2

Which of the following type of file systems is not supported by Linux kernel?

A. vFAT

B. NTFS

C. HFS

D. FAT32

ANSWER: D

QUESTION NO: 3

Which of the following is used for remote file access by UNIX/Linux systems?

A. NetWare Core Protocol (NCP)

B. Common Internet File System (CIFS)

C. Server Message Block (SMB)

D. Network File System (NFS)

ANSWER: D

QUESTION NO: 4

Which of the following tools are used for footprinting?

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

A. Sam spade

B. Traceroute

C. Whois

D. Brutus

ANSWER: A B C

QUESTION NO: 5

You work as a Network Administrator for NetTech Inc. To ensure the security of files, you encrypt data files using Encrypting File System (EFS). You want to make a backup copy of the files and maintain security settings. You can backup the files either to a network share or a floppy disk. What will you do to accomplish this?

A. Place the files in an encrypted folder. Then, copy the folder to a floppy disk.

B. Copy the files to a network share on a FAT32 volume.

C. Copy the files to a network share on an NTFS volume.

D. Copy the files to a floppy disk that has been formatted using Windows 2000 Professional.

ANSWER: C

QUESTION NO: 6

The promiscuous mode 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. Which of the following tools works by placing the host system network card into the promiscuous mode?

A. Snort

B. THC-Scan

C. Sniffer

D. NetStumbler

ANSWER: C

QUESTION NO: 7

John works as a professional Ethical Hacker. He has been assigned a project to test the security of www.we-are-secure.com. He wants to test the effect of a virus on the We-are-secure server. He injects the virus on the server and, as a result, the server becomes infected with the virus even though an established antivirus program is installed on the server. Which of the following do you think are the reasons why the antivirus installed on the server did not detect the virus injected by John?

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

A. The mutation engine of the virus is generating a new encrypted code.

B. The virus, used by John, is not in the database of the antivirus program installed on the server.

C. John has created a new virus.

D. John has changed the signature of the virus.

ANSWER: A B C D

QUESTION NO: 8

Which of the following IP addresses are private addresses?

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

A. 19.3.22.17

B. 192.168.15.2

C. 192.166.54.32

D. 10.0.0.3

ANSWER: B D

QUESTION NO: 9 - (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

QUESTION NO: 10

Which of the following statements about registry is true?

Each correct answer represents a complete solution. Choose three.

A. It is divided in many areas known as hives.

B. It was first introduced with Windows 95 operating system.

C. It is a centralized configuration database that stores information related to a Windows computer.

D. It can be edited using SCANREG utility.

ANSWER: A B C

QUESTION NO: 11

Which of the following is a name, symbol, or slogan with which a product is identified?

A. Trade secret

B. Patent

C. Copyright

D. Trademark

ANSWER: D

QUESTION NO: 12

Which of the following file systems are supported by Windows 2000 operating systems? Each correct answer represents a complete solution. Choose all that apply.

A. NTFS4

B. CDFS

C. FAT32

D. HPFS

E. NTFS5

ANSWER: A B C E

QUESTION NO: 13

Which of the following components are usually found in an Intrusion detection system (IDS)? Each correct answer represents a complete solution. Choose two.

A. Sensor

B. Firewall

C. Modem

D. Gateway

E. Console

ANSWER: A E

QUESTION NO: 14

Which of the following statements is NOT true about FAT16 file system?

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

A. FAT16 file system supports Linux operating system.

B. FAT16 file system supports file-level compression.

C. FAT16 file system works well with large disks because the cluster size increases as the disk partition size increases.

D. FAT16 does not support file-level security.

ANSWER: B C

QUESTION NO: 15

Which utility enables you to access files from a Windows .CAB file?

A. ACCESS.EXE

B. WINZIP.EXE

C. XCOPY.EXE

D. EXTRACT.EXE

ANSWER: D