Exam Dumps GCFA Practice Free Latest GIAC Practice Tests [Q71-Q85

Exam Dumps GCFA Practice Free Latest GIAC Practice Tests
GCFA Exam Questions | Real GCFA Practice Dumps

Difficulty in writing the GCFA Exam

As all people know about this fact that GCFAexam is not easy to pass because it requires a lot of efforts and a dependable and latest study material to efficiently pass the exam.
Many Candidates have doubts in their mind before writing the Cisco Understanding Cisco Cybersecurity Fundamentals (210-250) certification exam that is a pattern of the test, the types of questions asked in it and the difficulty level of the questions and time required to complete the questions. The best way to pass GCFAexam is to challenge and improve knowledge. Candidates test their learning and identify improvement areas with actual exam format. The best solution is to practice with GCFACertification Practice Exam because the practice test is one of the most important elements of CCNA Cyber Ops exam study strategy in which Candidates can discover their strengths and weaknesses to improve time management skills and to get an idea of the score that they can expect. VCEPrep offers the latest exam questions for the GCFA Exam which can be understood by the candidates deprived of any difficulty. Our 210-250 exam dumps study material is best-suited to busy professionals who don't have much to spend on preparation and want to pass it in a week. Our CCNA Cyber Ops practice exam has been duly prepared by the team of experts after an in-depth analysis of Cisco recommended syllabus. We update our material regularly. So, it is intended to keep candidates updated because as and when Cisco will announce any changes in the material; we will update the material right away. After practicing with our GCFA exam dumps Candidate can pass GCFAexam with good grades.

QUESTION 71

Normally, RAM is used for temporary storage of data. But sometimes RAM data is stored in the hard disk, what is this method called?
* Cache memory
* Static memory
* Virtual memory
* Volatile memory
Section: Volume A

QUESTION 72

Which of the following statements best describes the consequences of the disaster recovery plan test?
* If no deficiencies were found during the test, then the plan is probably perfect.
* The results of the test should be kept secret.
* The plan should not be changed no matter what the results of the test would be.
* If no deficiencies were found during the test, then the test was probably flawed.

QUESTION 73

Which of the following types of evidence proves or disproves a specific act through oral testimony based on information gathered through the witness’s five senses?
* Conclusive evidence
* Best evidence
* Hearsay evidence
* Direct evidence

QUESTION 74

Which of the following methods can be used to start the Disk Defragmenter utility in Windows 9x?

Each correct answer represents a complete solution. Choose two.
* From Start menu > Programs > Accessories > System Tools, click Disk Defragmenter.
* From Start menu > Programs > Windows Explorer, right-click on the drive to be defragmented > click Properties in the popup menu > Tools tab, then click the Defragment Now button.
* From Start menu > Programs > Windows Explorer, right-click on the drive to be defragmented, then click the Disk Defragmenter in the popup window.
* From Start menu > Programs, click Disk Defragmenter.
Section: Volume C

QUESTION 75

John works as a professional Ethical Hacker. He has been assigned a project to test the security of www.we- are-secure.com. He copies the whole structure of the We-are-secure Web site to the local disk and obtains all the files on the Web site. Which of the following techniques is he using to accomplish his task?
* Web ripping
* TCP FTP proxy scanning
* Fingerprinting

* Eavesdropping

Section: Volume C

QUESTION 76

Which of the following involves changing data prior to or during input to a computer in an effort to commit fraud?

* Data diddling
* Spoofing
* Eavesdropping
* Wiretapping

QUESTION 77

Which of the following tools can be used to perform a whois query?

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

* Sam Spade
* SuperScan
* Traceroute
* WsPingPro

QUESTION 78

Sandra wants to create a full system state backup of her computer, which is running on Microsoft Windows XP operating system. Which of the following is saved in full state system backup?

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

* file system information
* Registry
* Windows boot files
* Active Directory (NTDS)

Section: Volume B

QUESTION 79

Adam works as a Computer Hacking Forensic Investigator. He has been assigned a project to investigate child pornography. As the first step, Adam found that the accused is using a Peer-to-peer application to network different computers together over the internet and sharing pornographic materials of children with others. Which of the following are Peer-to-Peer applications?

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

* Gnutella
* Kismet
* Hamachi
* Freenet

Section: Volume B

QUESTION 80

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

* NetWare Core Protocol (NCP)

* Common Internet File System (CIFS)
* Server Message Block (SMB)
* Network File System (NFS)

QUESTION 81

Which of the following U.S. Federal laws addresses computer crime activities in communication lines, stations, or systems?
* 18 U.S.C. 1030
* 18 U.S.C. 1362
* 18 U.S.C. 2701
* 18 U.S.C. 2510
* 18 U.S.C. 1029

QUESTION 82

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?
* ping
* Psloggedon
* Pslist
* fport

Section: Volume A

QUESTION 83

Every network device contains a unique built in Media Access Control (MAC) address, which is used to identify the authentic device to limit the network access. Which of the following addresses is a valid MAC address?
* 132.298.1.23
* A3-07-B9-E3-BC-F9
* F936.28A1.5BCD.DEFA
* 1011-0011-1010-1110-1100-0001

QUESTION 84

TCP FIN scanning is a type of stealth scanning through which the attacker sends a FIN packet to the target port. If the port is closed, the victim assumes that this packet was sent mistakenly by the attacker and sends the RST packet to the attacker. If the port is open, the FIN packet will be ignored and the port will drop the packet. Which of the following operating systems can be easily identified with the help of TCP FIN scanning?
* Solaris
* Red Hat
* Knoppix
* Windows

QUESTION 85

Which of the following evidences are the collection of facts that, when considered together, can be used to infer a conclusion about the malicious activity/person?
* Corroborating
* Circumstantial

* Incontrovertible
* Direct

Verified GCFA Exam Dumps Q&As - Provide GCFA with Correct Answers:
https://www.vceprep.com/GCFA-latest-vce-prep.html]