VCE4Plus

Choose the version that fits your needs	PDF Version	Desktop Test Engine	Online Test Engine
Latest and Up-to-Date exam dumps with real exam questions answers.	✓	✓	✓
Get 12-Months free updates without any extra charges.	✓	✓	✓
Experience same exam environment before appearing in the certification exam.	✗	✓	✓
100% exam passing guarante in the first attempt.	✓	✓	✓
20% discount on more than one license and 30% discount on 5+ license purchases.	✗	✓	✓
100% secure purchase on SSL.	✓	✓	✓
Completely private purchase without sharing your personal info with anyone.	✓	✓	✓

Exam : **EC0-349**

Title : Computer Hacking Forensic Investigator

Vendor : EC-COUNCIL

Version : DEMO

NO.1 When the operating system marks cluster as used, but does not allocate them to any file, such clusters are known as _____.
A. Lost clusters
B. Bad clusters
C. Empty clusters
D. Unused clusters
Answer: A

NO.2 What happens when a file is deleted by a Microsoft operating system using the FAT file system?
A. The file is erased and cannot be recovered
B. The file is erased but can be recovered partially
C. A copy of the file is stored and the original file is erased
D. Only the reference to the file is removed from the FAT and can be recovered
Answer: D

NO.3 Volatile Memory is one of the leading problems for forensics. Worms such as code Red are memory resident and do not write themselves to the hard drive, if you turn the system off they disappear. In a lab environment, which of the following options would you suggest as the most appropriate to overcome the problem of capturing volatile memory?
A. Use Vmware to be able to capture the data in memory and examine it
B. Give the Operating System a minimal amount of memory, forcing it to use a swap file
C. Create a Separate partition of several hundred megabytes and place the swap file there
D. Use intrusion forensic techniques to study memory resident infections
Answer: AC

NO.4 From the following spam mail header, identify the host IP that sent this spam?
From jie02@netvigator.com jie02@netvigator.com Tue Nov 27 17:27:11 2001 Received: from viruswall.ie.cuhk.edu.hk (viruswall [137.189.96.52]) by eng.ie.cuhk.edu.hk (8.11.6/8.11.6) with ESMTP id fAR9RAP23061 for ; Tue, 27 Nov 2001 17:27:10 +0800 (HKT) Received: from mydomain.com (pcd249020.netvigator.com [203.218.39.20]) by viruswall.ie.cuhk.edu.hk (8.12.1/8.12.1) with SMTP id fAR9QXwZ018431 for ; Tue, 27 Nov 2001 17:26:36 +0800 (HKT) Message-Id: >200111270926.fAR9QXwZ018431@viruswall.ie.cuhk.edu.hk From: "china hotel web" To: "Shlam" Subject: SHANGHAI (HILTON HOTEL) PACKAGE Date: Tue, 27 Nov 2001 17:25:58 +0800 MIME-Version: 1.0 X-Priority: 3 X-MSMail- Priority: Normal Reply-To: "china hotel web"
A. 137.189.96.52
B. 8.12.1.0
C. 203.218.39.20
D. 203.218.39.50
Answer: C

NO.5 What hashing method is used to password protect Blackberry devices?
A. AES
B. RC5

C. MD5
D. SHA-1
Answer: D

NO.6 Which of the following statements does not support the case assessment?
A. Review the case investigator's request for service
B. Identify the legal authority for the forensic examination request
C. Do not document the chain of custody
D. Discuss whether other forensic processes need to be performed on the evidence
Answer: C

NO.7 Before you are called to testify as an expert, what must an attorney do first?
A. engage in damage control
B. prove that the tools you used to conduct your examination are perfect
C. read your curriculum vitae to the jury
D. qualify you as an expert witness
Answer: D

NO.8 Where are files temporarily written in Unix when printing?
A. /usr/spool
B. /var/print
C. /spool
D. /var/spool
Answer: D

NO.9 Which federal computer crime law specifically refers to fraud and related activity in connection with access devices like routers?
A. 18 U.S.C. 1029
B. 18 U.S.C. 1362
C. 18 U.S.C. 2511
D. 18 U.S.C. 2703
Answer: A

NO.10 What is the name of the standard Linux command that can be used to create bit-stream images?
A. mcopy
B. image
C. MD5
D. dd
Answer: D

NO.11 The rule of thumb when shutting down a system is to pull the power plug. However, it has certain drawbacks. Which of the following would that be?

A. Any data not yet flushed to the system will be lost
B. All running processes will be lost
C. The /tmp directory will be flushed
D. Power interruption will corrupt the pagefile
Answer: AB
Explanation:
Volitile memory will be lost.
Data is not flushed to the system, it is flushed to the disk.

NO.12 You have compromised a lower-level administrator account on an Active Directory network of a small company in Dallas, Texas. You discover Domain Controllers through enumeration. You connect to one of the Domain Controllers on port 389 using ldp.exe.
What are you trying to accomplish here?
A. Enumerate domain user accounts and built-in groups
B. Enumerate MX and A records from DNS
C. Establish a remote connection to the Domain Controller
D. Poison the DNS records with false records
Answer: A

NO.13 You have been asked to investigate after a user has reported a threatening e-mail they have received from an external source. Which of the following are you most interested in when trying to trace the source of the message?
A. The X509 Address
B. The SMTP reply Address
C. The E-mail Header
D. The Host Domain Name
Answer: C

NO.14 While working for a prosecutor, What do you think you should do if the evidence you found appears to be exculpatory and is not being released to the defense ?
A. Keep the information of file for later review
B. Destroy the evidence
C. Bring the information to the attention of the prosecutor, his or her supervisor or finally to the judge
D. Present the evidence to the defense attorney
Answer: C

NO.15 Jason is the security administrator of ACMA metal Corporation. One day he notices the company's Oracle database server has been compromised and the customer information along with financial data has been stolen. The financial loss will be in millions of dollars if the database gets into the hands of the competitors. Jason wants to report this crime to the law enforcement agencies immediately. Which organization coordinates computer crimes investigations throughout the United States?
A. Internet Fraud Complaint Center

B. Local or national office of the U.S. Secret Service
C. National Infrastructure Protection Center
D. CERT Coordination Center
Answer: B

NO.16 What is the first step that needs to be carried out to investigate wireless attacks?
A. Obtain a search warrant
B. Identify wireless devices at crime scene
C. Document the scene and maintain a chain of custody
D. Detect the wireless connections
Answer: A

NO.17 You are called in to assist the police in an investigation involving a suspected drug dealer. The police searched the suspect house after aYou are called in to assist the police in an investigation involving a suspected drug dealer. The police searched the suspect? house after a warrant was obtained and they located a floppy disk in the suspect bedroom. The disk contains several files, but they appear to be passwordwarrant was obtained and they located a floppy disk in the suspect? bedroom. The disk contains several files, but they appear to be password protected.
What are two common methods used by password cracking software that you could use to obtain the password?
A. Limited force and library attack
B. Brute force and dictionary attack
C. Maximum force and thesaurus attack
D. Minimum force and appendix attack
Answer: B

NO.18 If you see the files Zer0.tar.gz and copy.tar.gz on a Linux system while doing an investigation, what can you conclude?
A. The system files have been copied by a remote attacker
B. The system administrator has created an incremental backup
C. The system has been compromised using a t0rn rootkit
D. Nothing in particular as these can be operational files
Answer: D

NO.19 What is the smallest allocation unit of a hard disk?
A. Cluster
B. Spinning tracks
C. Disk platters
D. Slack space
Answer: A

NO.20 When collecting electronic evidence at the crime scene, the collection should proceed from the most volatile to the least volatile

A. True
B. False
Answer: A

NO.21 In Linux, what is the smallest possible shellcode?
A. 8 bytes
B. 24 bytes
C. 800 bytes
D. 80 bytes
Answer: B

NO.22 A packet is sent to a router that does not have the packet destination address in its route table, how will the packet get to its properA packet is sent to a router that does not have the packet? destination address in its route table, how will the packet get to its proper destination?
A. Border Gateway Protocol
B. Root Internet servers
C. Gateway of last resort
D. Reverse DNS
Answer: C

NO.23 File deletion is a way of removing a file from a computer's file system. What happens when a file is deleted in windows7?
A. The last letter of a file name is replaced by a hex byte code E5h
B. The operating system marks the file's name in the MFT with a special character that indicates that the file has been deleted
C. Corresponding clusters in FAT are marked as used
D. The computer looks at the clusters occupied by that file and does not avails space to store a new file
Answer: B

NO.24 If you plan to startup a suspect's computer, you must modify the _____ to ensure that you do not contaminate or alter data on the suspect's hard drive by booting to the hard drive.
A. deltree command
B. CMOS
C. Boot.sys
D. Scandisk utility
E. boot.ini
Answer: E
Explanation:
The OS isn't specified, but if this was a Windows OS, then this would be boot.ini The answer is CMOS. The startup of a computer is the boot sequence, and the boot sequence is defined in the CMOS. The common occurrence is to boot off a floppy, and you need to see that the floppy (usually the A drive) is first in the sequence. If you don't, and the hard drive is first, then booting the system wil boot the

hard drive and alter the evidence.

NO.25 A system with a simple logging mechanism has not been given much attention during development, this system is now being targeted by attackers, if the attacker wants to perform a new line injection attack, what will he/she inject into the log file?
A. Plaintext
B. Single pipe character
C. Multiple pipe characters
D. HTML tags
Answer: A

NO.26 Which of the following is not an example of a cyber-crime?
A. Fraud achieved by the manipulation of the computer records
B. Firing an employee for misconduct
C. Deliberate circumvention of the computer security systems
D. Intellectual property theft, including software piracy
Answer: B

NO.27 A forensics investigator is searching the hard drive of a computer for files that were recently moved to the Recycle Bin. He searches for files in C:\RECYCLED using a command line tool but does not find anything. What is the reason for this?
A. He should search in C:\Windows\System32\RECYCLED folder
B. The Recycle Bin does not exist on the hard drive
C. The files are hidden and he must use switch to view themThe files are hidden and he must use ? switch to view them
D. Only FAT system contains RECYCLED folder and not NTFS
Answer: C

NO.28 You are trying to locate Microsoft Outlook Web Access Default Portal using Google search on the Internet. What search string will you use to locate them?
A. allinurl:"exchange/logon.asp"
B. intitle:"exchange server"
C. outlook:"search"
D. locate:"logon page"
Answer: A

NO.29 Which of the following is not a part of disk imaging tool requirements?
A. The tool should not change the original content
B. The tool should log I/O errors in an accessible and readable form, including the type and location of the error
C. The tool must have the ability to be held up to scientific and peer review
D. The tool should not compute a hash value for the complete bit stream copy generated from an image file of the source

Answer: D

NO.30 Which of the following statements is incorrect when preserving digital evidence?
A. Document the actions and changes that you observe in the monitor, computer, printer, or in other peripherals
B. Verily if the monitor is in on, off, or in sleep mode
C. Remove the power cable depending on the power state of the computer i.e., in on. off, or in sleep mode
D. Turn on the computer and extract Windows event viewer log files
Answer: D

NO.31 A steganographic file system is a method to store the files in a way that encrypts and hides the data without the knowledge of others
A. True
B. False
Answer: A

NO.32 Buffer Overflow occurs when an application writes more data to a block of memory, or buffer, than the buffer is allocated to hold. Buffer overflow attacks allow an attacker to modify the _____in order to control the process execution, crash the process and modify internal variables.
A. Target process's address space
B. Target remote access
C. Target rainbow table
D. Target SAM file
Answer: A

NO.33 Web applications provide an Interface between end users and web servers through a set of web pages that are generated at the server-end or contain script code to be executed dynamically within the client Web browser.
A. True
B. False
Answer: A

NO.34 Corporate investigations are typically easier than public investigations because:
A. the users have standard corporate equipment and software
B. the investigator does not have to get a warrant
C. the investigator has to get a warrant
D. the users can load whatever they want on their machines
Answer: B

NO.35 Harold is finishing up a report on a case of network intrusion, corporate spying, and embezzlement that he has been working on for over six months. He is trying to find the right term to use in his report to describe network-enabled spying. What term should Harold use?

A. Spycrack
B. Spynet
C. Netspionage
D. Hackspionage
Answer: C