

312-49v9 Dumps

ECCouncil Computer Hacking Forensic Investigator (V9)

<https://www.certleader.com/312-49v9-dumps.html>



NEW QUESTION 1

The Electronic Serial Number (ESN) is a unique _ recorded on a secure chip in a mobile phone by the manufacturer.

- A. 16-bit identifier
- B. 24-bit identifier
- C. 32-bit identifier
- D. 64-bit identifier

Answer: C

NEW QUESTION 2

The Recycle Bin is located on the Windows desktop. When you delete an item from the hard disk, Windows sends that deleted item to the Recycle Bin and the icon changes to full from empty, but items deleted from removable media, such as a floppy disk or network drive, are not stored in the Recycle Bin. What is the size limit for Recycle Bin in Vista and later versions of the Windows?

- A. No size limit
- B. Maximum of 3.99 GB
- C. Maximum of 4.99 GB
- D. Maximum of 5.99 GB

Answer: A

NEW QUESTION 3

The need for computer forensics is highlighted by an exponential increase in the number of cybercrimes and litigations where large organizations were involved. Computer forensics plays an important role in tracking the cyber criminals. The main role of computer forensics is to:

- A. Maximize the investigative potential by maximizing the costs
- B. Harden organization perimeter security
- C. Document monitoring processes of employees of the organization
- D. Extract, process, and interpret the factual evidence so that it proves the attacker's actions in the court

Answer: D

NEW QUESTION 4

What document does the screenshot represent?

CERTIFIED INVENTORY OF EVIDENCE

CASE NAME: _____

Inventoried By: _____

Date: _____

ID	Date Received	Quantity	Description of Evidence

CHAIN OF CUSTODY

Date	Action	Released By <i>Sign and print name</i>	Received By <i>Sign and print name</i>

- A. Chain of custody form
- B. Search warrant form
- C. Evidence collection form
- D. Expert witness form

Answer: A

NEW QUESTION 5

Data compression involves encoding the data to take up less storage space and less bandwidth for transmission. It helps in saving cost and high data manipulation in many business applications. Which data compression technique maintains data integrity?

- A. Lossless compression
- B. Lossy compression
- C. Speech encoding compression
- D. Lossy video compression

Answer: A

NEW QUESTION 6

Which of the following statements is incorrect related to acquiring electronic evidence at crime scene?

- A. Sample banners are used to record the system activities when used by the unauthorized user
- B. In warning banners, organizations give clear and unequivocal notice to intruders that by signing onto the system they are expressly consenting to such monitoring
- C. The equipment is seized which is connected to the case, knowing the role of the computer which will indicate what should be taken
- D. At the time of seizing process, you need to shut down the computer immediately

Answer: D

NEW QUESTION 7

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: A

NEW QUESTION 8

Which wireless standard has bandwidth up to 54 Mbps and signals in a regulated frequency spectrum around 5 GHz?

- A. 802.11a
- B. 802.11b
- C. 802.11g
- D. 802.11i

Answer: A

NEW QUESTION 9

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. SQL Injection
- B. Password brute force
- C. Nmap Scanning
- D. Footprinting

Answer: A

NEW QUESTION 10

Which of the following approaches checks and compares all the fields systematically and intentionally for positive and negative correlation with each other to determine the correlation across one or multiple fields?

- A. Graph-based approach
- B. Neural network-based approach
- C. Rule-based approach
- D. Automated field correlation approach

Answer: D

NEW QUESTION 10

Tracks numbering on a hard disk begins at 0 from the outer edge and moves towards the center, typically reaching a value of ____.

- A. 1023
- B. 1020
- C. 1024
- D. 2023

Answer: A

NEW QUESTION 12

What is the goal of forensic science?

- A. To determine the evidential value of the crime scene and related evidence
- B. Mitigate the effects of the information security breach
- C. Save the good will of the investigating organization
- D. It is a discipline to deal with the legal processes

Answer: A

NEW QUESTION 16

Attackers can manipulate variables that reference files with "dot-dot-slash (./)" sequences and their variations such as `http://www.juggyDoy.corn/GET/process.php../../../../etc/passwd`. Identify the attack referred.

- A. Directory traversal
- B. SQL Injection
- C. XSS attack
- D. File injection

Answer: A

NEW QUESTION 20

Which Is a Linux journaling file system?

- A. Ext3
- B. HFS
- C. FAT
- D. BFS

Answer: A

NEW QUESTION 25

Which of the following statements is not a part of securing and evaluating electronic crime scene checklist?

- A. Locate and help the victim
- B. Transmit additional flash messages to other responding units
- C. Request additional help at the scene if needed
- D. Blog about the incident on the internet

Answer: D

NEW QUESTION 29

Which of the following log injection attacks uses white space padding to create unusual log entries?

- A. Word wrap abuse attack
- B. HTML injection attack
- C. Terminal injection attack
- D. Timestamp injection attack

Answer: A

NEW QUESTION 34

Subscriber Identity Module (SIM) is a removable component that contains essential information about the subscriber. Its main function entails authenticating the user of the cell phone to the network to gain access to subscribed services. SIM contains a 20-digit long Integrated Circuit Card identification (ICCID) number, identify the issuer identifier Number from the ICCID below.



- A. 89
- B. 44
- C. 245252
- D. 001451548

Answer: C

NEW QUESTION 36

If a file (readme.txt) on a hard disk has a size of 2600 bytes, how many sectors are normally allocated to this file?

- A. 4 Sectors
- B. 5 Sectors
- C. 6 Sectors
- D. 7 Sectors

Answer: C

NEW QUESTION 40

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. MD5
- C. SHA-1
- D. SHA-512

Answer: B

NEW QUESTION 42

LBA (Logical Block Address) addresses data by allotting a to each sector of the hard disk.

- A. Sequential number
- B. Index number
- C. Operating system number
- D. Sector number

Answer: A

NEW QUESTION 45

Which of the following attacks allows attacker to acquire access to the communication channels between the victim and server to extract the information?

- A. Man-in-the-middle (MITM) attack
- B. Replay attack
- C. Rainbow attack
- D. Distributed network attack

Answer: A

NEW QUESTION 46

SMTP (Simple Mail Transfer protocol) receives outgoing mail from clients and validates source and destination addresses, and also sends and receives emails to and from other SMTP servers.

- A. True
- B. False

Answer: A

NEW QUESTION 51

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. Suspend automated document destruction and recycling policies that may pertain to any relevant media or users at Issue
- D. Identify the type of data you are seeking, the Information you are looking for, and the urgency level of the examination

Answer: A

NEW QUESTION 53

An Internet standard protocol (built on top of TCP/IP) that assures accurate synchronization to the millisecond of computer clock times in a network of computers. Which of the following statement is true for NTP Stratum Levels?

- A. Stratum-0 servers are used on the network; they are not directly connected to computers which then operate as stratum-1 servers
- B. Stratum-1 time server is linked over a network path to a reliable source of UTC time such as GPS, WWV, or CDMA transmissions
- C. A stratum-2 server is directly linked (not over a network path) to a reliable source of UTC time such as GPS, WWV, or CDMA transmissions
- D. A stratum-3 server gets its time over a network link, via NTP, from a stratum-2 server, and so on

Answer: D

NEW QUESTION 58

Physical security recommendations: There should be only one entrance to a forensics lab

- A. True
- B. False

Answer: A

NEW QUESTION 62

A forensic investigator is a person who handles the complete Investigation process, that is, the preservation, identification, extraction, and documentation of the evidence. The investigator has many roles and responsibilities relating to the cybercrime analysis. The role of the forensic investigator is to:

- A. Take permission from all employees of the organization for investigation
- B. Harden organization network security
- C. Create an image backup of the original evidence without tampering with potential evidence
- D. Keep the evidence a highly confidential and hide the evidence from law enforcement agencies

Answer: C

NEW QUESTION 66

Which one of the following is not a consideration in a forensic readiness planning checklist?

- A. Define the business states that need digital evidence
- B. Identify the potential evidence available
- C. Decide the procedure for securely collecting the evidence that meets the requirement fn a forensically sound manner
- D. Take permission from all employees of the organization

Answer: D

NEW QUESTION 67

Shortcuts are the files with the extension .lnk that are created and are accessed by the users. These files provide you with information about:

- A. Files or network shares
- B. Running application
- C. Application logs
- D. System logs

Answer: A

NEW QUESTION 71

A computer forensic report is a report which provides detailed information on the complete forensics investigation process.

- A. True
- B. False

Answer: A

NEW QUESTION 75

Computer security logs contain information about the events occurring within an organization's systems and networks. Application and Web server log files are useful in detecting web attacks. The source, nature, and time of the attack can be determined by ____ of the compromised system.

- A. Analyzing log files
- B. Analyzing SAM file
- C. Analyzing rainbow tables
- D. Analyzing hard disk boot records

Answer: A

NEW QUESTION 80

An intrusion detection system (IDS) gathers and analyzes information from within a computer or a network to identify any possible violations of security policy, including unauthorized access, as well as misuse.

Which of the following intrusion detection systems audit events that occur on a specific host?

- A. Network-based intrusion detection
- B. Host-based intrusion detection
- C. Log file monitoring
- D. File integrity checking

Answer: B

NEW QUESTION 84

When a system is compromised, attackers often try to disable auditing, in Windows 7; modifications to the audit policy are recorded as entries of Event ID ____ .

- A. 4902
- B. 3902
- C. 4904
- D. 3904

Answer: A

NEW QUESTION 85

International Mobile Equipment Identifier (IMEI) is a 15-digit number that indicates the manufacturer, model type, and country of approval for GSM devices. The first eight digits of an IMEI number that provide information about the model and origin of the mobile device is also known as:

- A. Type Allocation Code (TAC)
- B. Device Origin Code (DOC)
- C. Manufacturer identification Code (MIC)
- D. Integrated Circuit Code (ICC)

Answer: A

NEW QUESTION 90

You should always work with original evidence

- A. True
- B. False

Answer: B

NEW QUESTION 91

How do you define forensic computing?

- A. It is the science of capturing, processing, and investigating data security incidents and making it acceptable to a court of law.
- B. It is a methodology of guidelines that deals with the process of cyber investigation
- C. It is a preliminary and mandatory course necessary to pursue and understand fundamental principles of ethical hacking
- D. It is the administrative and legal proceeding in the process of forensic investigation

Answer: A

NEW QUESTION 94

What is the first step that needs to be carried out to crack the password?

- A. A word list is created using a dictionary generator program or dictionaries
- B. The list of dictionary words is hashed or encrypted
- C. The hashed wordlist is compared against the target hashed password, generally one word at a time
- D. If it matches, that password has been cracked and the password cracker displays the unencrypted version of the password

Answer: A

NEW QUESTION 95

Damaged portions of a disk on which no read/write operation can be performed is known as ____ .

- A. Lost sector
- B. Bad sector
- C. Empty sector
- D. Unused sector

Answer: B

NEW QUESTION 99

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

NEW QUESTION 103

Under no circumstances should anyone, with the exception of qualified computer forensics personnel, make any attempts to restore or recover information from a computer system or device that holds electronic information.

- A. True
- B. False

Answer: A

NEW QUESTION 105

In which step of the computer forensics investigation methodology would you run MD5 checksum on the evidence?

- A. Obtain search warrant
- B. Evaluate and secure the scene
- C. Collect the evidence
- D. Acquire the data

Answer: D

B

NEW QUESTION 129

Jason, a renowned forensic investigator, is investigating a network attack that resulted in the compromise of several systems in a reputed multinational's network. He started Wireshark to capture the network traffic. Upon investigation, he found that the DNS packets travelling across the network belonged to a non-company configured IP. Which of the following attack Jason can infer from his findings?

- A. DNS Poisoning
- B. Cookie Poisoning Attack
- C. DNS Redirection
- D. Session poisoning

Answer: A

NEW QUESTION 130

In what circumstances would you conduct searches without a warrant?

- A. When destruction of evidence is imminent, a warrantless seizure of that evidence is justified if there is probable cause to believe that the item seized constitutes evidence of criminal activity
- B. Agents may search a place or object without a warrant if he suspect the crime was committed
- C. A search warrant is not required if the crime involves Denial-Of-Service attack over the Internet
- D. Law enforcement agencies located in California under section SB 567 are authorized to seize computers without warrant under all circumstances

Answer: A

NEW QUESTION 131

What is a chain of custody?

- A. A legal document that demonstrates the progression of evidence as it travels from the original evidence location to the forensic laboratory
- B. It is a search warrant that is required for seizing evidence at a crime scene
- C. It is a document that lists chain of windows process events
- D. Chain of custody refers to obtaining preemptive court order to restrict further damage of evidence in electronic seizures

Answer: A

NEW QUESTION 133

Wi-Fi Protected Access (WPA) is a data encryption method for WLANs based on 802.11 standards. Temporal Key Integrity Protocol (TKIP) enhances WEP by adding a rekeying mechanism to provide fresh encryption and integrity keys. Temporal keys are changed for every ____ .

- A. 5,000 packets
- B. 10,000 packets
- C. 15,000 packets
- D. 20,000 packets

Answer: B

NEW QUESTION 138

File signature analysis involves collecting information from the ____ of a file to determine the type and function of the file

- A. First 10 bytes
- B. First 20 bytes
- C. First 30 bytes
- D. First 40 bytes

Answer: B

NEW QUESTION 141

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

- A. True
- B. False

Answer: A

NEW QUESTION 143

A system with a simple logging mechanism has not been given much attention during development, this system is now being targeted by attackers, if the attacker wants to perform a new line injection attack, what will he/she inject into the log file?

- A. Plaintext
- B. Single pipe character
- C. Multiple pipe characters
- D. HTML tags

Answer: A

NEW QUESTION 146

When a file or folder is deleted, the complete path, including the original file name, is stored in a special hidden file called "INF02" in the Recycled folder. If the INF02 file is deleted, it is re-created when you ____ .

- A. Restart Windows
- B. Kill the running processes in Windows task manager
- C. Run the antivirus tool on the system
- D. Run the anti-spyware tool on the system

Answer: A

NEW QUESTION 151

Windows Security Accounts Manager (SAM) is a registry file which stores passwords in a hashed format. SAM file in Windows is located at:

- A. C:\windows\system32\config\SAM
- B. C:\windows\system32\con\SAM
- C. C:\windows\system32\Boot\SAM
- D. C:\windows\system32\drivers\SAM

Answer: A

NEW QUESTION 152

During the seizure of digital evidence, the suspect can be allowed touch the computer system.

- A. True
- B. False

Answer: B

NEW QUESTION 157

Which is not a part of environmental conditions of a forensics lab?

- A. Large dimensions of the room
- B. Good cooling system to overcome excess heat generated by the work station
- C. Allocation of workstations as per the room dimensions
- D. Open windows facing the public road

Answer: D

NEW QUESTION 161

Why is it Important to consider health and safety factors in the work carried out at all stages of the forensic process conducted by the forensic analysts?

- A. This is to protect the staff and preserve any fingerprints that may need to be recovered at a later date
- B. All forensic teams should wear protective latex gloves which makes them look professional and cool
- C. Local law enforcement agencies compel them to wear latest gloves
- D. It is a part of ANSI 346 forensics standard

Answer: A

NEW QUESTION 165

The Recycle Bin exists as a metaphor for throwing files away, but it also allows user to retrieve and restore files. Once the file is moved to the recycle bin, a record is added to the log file that exists in the Recycle Bin.

Which of the following files contains records that correspond to each deleted file in the Recycle Bin?

- A. INFO2 file
- B. INFO1 file
- C. LOGINFO2 file
- D. LOGINFO1 file

Answer: A

NEW QUESTION 170

Determine the message length from following hex viewer record:



- A. 6E2F
- B. 13
- C. 27
- D. 810D

Answer: D

NEW QUESTION 172

You can interact with the Registry through intermediate programs. Graphical user interface (GUI) Registry editors such as Regedit.exe or Regedt32.exe are commonly used as intermediate programs in Windows 7. Which of the following is a root folder of the registry editor?

- A. HKEY_USERS
- B. HKEY_LOCAL_ADMIN
- C. HKEY_CLASSES_ADMIN
- D. HKEY_CLASSES_SYSTEM

Answer: A

NEW QUESTION 175

Computer security logs contain information about the events occurring within an organization's systems and networks. Which of the following security logs contains Logs of network and host-based security software?

- A. Operating System (OS) logs
- B. Application logs
- C. Security software logs
- D. Audit logs

Answer: C

NEW QUESTION 177

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 sessions
- B. Net file
- C. Net config
- D. Net share

Answer: A

NEW QUESTION 178

Which of the following file in Novel GroupWise stores information about user accounts?

- A. ngwguard.db
- B. gwcheck.db
- C. PRIV.EDB
- D. PRIV.STM

Answer: A

NEW QUESTION 181

Billy, a computer forensics expert, has recovered a large number of DBX files during forensic investigation of a laptop. Which of the following email clients he can use to analyze the DBX files?

- A. Microsoft Outlook
- B. Microsoft Outlook Express
- C. Mozilla Thunderbird
- D. Eudora

Answer: B

NEW QUESTION 186

File deletion is a way of removing a file from a computer's file system. What happens when a file is deleted in windows7?

- A. The last letter of a file name is replaced by a hex byte code E5h
- B. The operating system marks the file's name in the MFT with a special character that indicates that the file has been deleted
- C. Corresponding clusters in FAT are marked as used
- D. The computer looks at the clusters occupied by that file and does not avails space to store a new file

Answer: B

NEW QUESTION 189

A rogue/unauthorized access point is one that is not authorized for operation by a particular firm or network

- A. True
- B. False

Answer: A

NEW QUESTION 190

Which of the following passwords are sent over the wire (and wireless) network, or stored on some media as it is typed without any alteration?

- A. Clear text passwords
- B. Obfuscated passwords
- C. Hashed passwords
- D. Hex passwords

Answer: A

NEW QUESTION 194

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. Broadcasting a probe request frame
- B. Sniffing the packets from the airwave
- C. Scanning the network
- D. Inspecting WLAN and surrounding networks

Answer: A

NEW QUESTION 199

Graphics Interchange Format (GIF) is a ____ RGB bitmap Image format for Images with up to 256 distinct colors per frame.

- A. 8-bit
- B. 16-bit
- C. 24-bit
- D. 32-bit

Answer: A

NEW QUESTION 201

Which of the following is not a part of data acquisition forensics Investigation?

- A. Permit only authorized personnel to access
- B. Protect the evidence from extremes in temperature
- C. Work on the original storage medium not on the duplicated copy
- D. Disable all remote access to the system

Answer: C

NEW QUESTION 205

Router log files provide detailed Information about the network traffic on the Internet. It gives information about the attacks to and from the networks. The router stores log files in the ____ .

- A. Router cache
- B. Application logs

- C. IDS logs
- D. Audit logs

Answer: A

NEW QUESTION 209

At the time of evidence transfer, both sender and receiver need to give the information about date and time of transfer in the chain of custody record.

- A. True
- B. False

Answer: A

NEW QUESTION 210

The disk in the disk drive rotates at high speed, and heads in the disk drive are used only to read data.

- A. True
- B. False

Answer: B

NEW QUESTION 212

Which root folder (hive) of registry editor contains a vast array of configuration information for the system, including hardware settings and software settings?

- A. HKEY_USERS
- B. HKEY_CURRENT_USER
- C. HKEY_LOCAL_MACHINE
- D. HKEY-CURRENT_CONFIG

Answer: C

NEW QUESTION 214

WPA2 provides enterprise and Wi-Fi users with stronger data protection and network access control which of the following encryption algorithm is used DVWPA2?

- A. RC4-CCMP
- B. RC4-TKIP
- C. AES-CCMP
- D. AES-TKIP

Answer: C

NEW QUESTION 219

Smith, as a part his forensic investigation assignment, has seized a mobile device. He was asked to recover the Subscriber Identity Module (SIM card) data the mobile device. Smith found that the SIM was protected by a Personal identification Number (PIN) code but he was also aware that people generally leave the PIN numbers to the defaults or use easily guessable numbers such as 1234. He unsuccessfully tried three PIN numbers that blocked the SIM card. What Jason can do in this scenario to reset the PIN and access SIM data?

- A. He should contact the device manufacturer for a Temporary Unlock Code (TUK) to gain access to the SIM
- B. He cannot access the SIM data in this scenario as the network operators or device manufacturers have no idea about a device PIN
- C. He should again attempt PIN guesses after a time of 24 hours
- D. He should ask the network operator for Personal Unlock Number (PUK) to gain access to the SIM

Answer: D

NEW QUESTION 224

Attacker uses vulnerabilities in the authentication or session management functions such as exposed accounts, session IDs, logout, password management, timeouts, remember me. secret question, account update etc. to impersonate users, if a user simply closes the browser without logging out from sites accessed through a public computer, attacker can use the same browser later and exploit the user's privileges. Which of the following vulnerability/exploitation is referred above?

- A. Session ID in URLs
- B. Timeout Exploitation
- C. I/O exploitation
- D. Password Exploitation

Answer: B

NEW QUESTION 225

A swap file is a space on a hard disk used as the virtual memory extension of a computer's RAM. Where is the hidden swap file in Windows located?

- A. C:\pagefile.sys
- B. C:\hiberfil.sys
- C. C:\config.sys
- D. C:\ALCSetup.log

Answer: A

NEW QUESTION 228

In an echo data hiding technique, the secret message is embedded into a _____ as an echo.

- A. Cover audio signal
- B. Phase spectrum of a digital signal
- C. Pseudo-random signal
- D. Pseudo- spectrum signal

Answer: A

NEW QUESTION 229

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. True
- B. False

Answer: A

NEW QUESTION 232

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. IP address spoofing
- B. Man-in-the-middle attack
- C. Denial of Service attack
- D. Session sniffing

Answer: A

NEW QUESTION 235

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. Errors-To header
- B. Content-Transfer-Encoding header
- C. Mime-Version header
- D. Content-Type header

Answer: A

NEW QUESTION 237

An image is an artifact that reproduces the likeness of some subject. These are produced by optical devices (i.e. cameras, mirrors, lenses, telescopes, and microscopes).

Which property of the image shows you the number of colors available for each pixel in an image?

- A. Pixel
- B. Bit Depth
- C. File Formats
- D. Image File Size

Answer: B

NEW QUESTION 241

The IIS log file format is a fixed (cannot be customized) ASCII text-based format. The IIS format includes basic items, such as client IP address, user name, date and time, service and instance, server name and IP address, request type, target of operation, etc. Identify the service status code from the following IIS log.

192.168.100.150, -, 03/6/11, 8:45:30, W3SVC2, SERVER, 172.15.10.30, 4210, 125, 3524, 100, 0, GET, /dollerlogo.gif,

- A. W3SVC2
- B. 4210
- C. 3524
- D. 100

Answer: D

NEW QUESTION 245

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. RS422
- B. RS423
- C. RS232

D. RS231

Answer: C

NEW QUESTION 248

Network forensics allows Investigators to inspect network traffic and logs to identify and locate the attack system Network forensics can reveal: (Select three answers)

- A. Source of security incidents' and network attacks
- B. Path of the attack
- C. Intrusion techniques used by attackers
- D. Hardware configuration of the attacker's system

Answer: ABC

NEW QUESTION 250

Which of the following Wi-Fi chalking methods refers to drawing symbols in public places to advertise open Wi-Fi networks?

- A. WarWalking
- B. WarFlying
- C. WarChalking
- D. WarDhving

Answer: C

NEW QUESTION 253

BMP (Bitmap) is a standard file format for computers running the Windows operating system. BMP images can range from black and white (1 bit per pixel) up to 24 bit color (16.7 million colors). Each bitmap file contains header, the RGBQUAD array, information header, and image data. Which of the following element specifies the dimensions, compression type, and color format for the bitmap?

- A. Header
- B. The RGBQUAD array
- C. Information header
- D. Image data

Answer: B

NEW QUESTION 256

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 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
- C. If a monitor is powered on and the display is blank, move the mouse slowly without depressing any mouse button and take a photograph
- D. If the computer is switched of
- E. power on the computer to take screenshot of the desktop

Answer: D

NEW QUESTION 261

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. Symbian OS Architecture
- C. Android OS Architecture
- D. Windows Phone 7 Architecture

Answer: C

NEW QUESTION 264

Preparing an image drive to copy files to is the first step in Linux forensics. For this purpose, what would the following command accomplish? `dcfldd if=/dev/zero of=/dev/hda bs=4096 conv=noerror, sync`

- A. Fill the disk with zeros
- B. Low-level format
- C. Fill the disk with 4096 zeros
- D. Copy files from the master disk to the slave disk on the secondary IDE controller

Answer: A

NEW QUESTION 268

When examining a file with a Hex Editor, what space does the file header occupy?

- A. The first several bytes of the file
- B. One byte at the beginning of the file
- C. None, file headers are contained in the FAT
- D. The last several bytes of the file

Answer: A

NEW QUESTION 273

What type of file is represented by a colon (:) with a name following it in the Master File Table (MFT) of an NTFS disk?

- A. Compressed file
- B. Data stream file
- C. Encrypted file
- D. Reserved file

Answer: B

NEW QUESTION 276

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. The life of the author
- C. The life of the author plus 70 years
- D. Copyrights last forever

Answer: C

NEW QUESTION 280

What is one method of bypassing a system BIOS password?

- A. Removing the processor
- B. Removing the CMOS battery
- C. Remove all the system memoryRemove all the system? memory
- D. Login to Windows and disable the BIOS password

Answer: B

NEW QUESTION 281

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. On the individual computer ARP cacheOn the individual computer? ARP cache
- B. In the Web Server log files
- C. In the DHCP Server log files
- D. There is no way to determine the specific IP address

Answer: C

NEW QUESTION 285

What hashing method is used to password protect Blackberry devices?

- A. AES
- B. RC5
- C. MD5

D. SHA-1

Answer: D

NEW QUESTION 288

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. Steganography
- C. Rootkit
- D. Offset

Answer: B

NEW QUESTION 292

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?its contents. The picture? quality is not degraded at all from this process. What kind of picture is this file?

- A. Raster image
- B. Vector image
- C. Metafile image
- D. Catalog image

Answer: B

NEW QUESTION 296

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 year the evidence was taken
- B. The sequence number for the parts of the same exhibit
- C. The initials of the forensics analyst
- D. The sequential number of the exhibits seized

Answer: D

NEW QUESTION 299

Where does Encase search to recover NTFS files and folders?

- A. MBR
- B. MFT
- C. Slack space
- D. HAL

Answer: B

NEW QUESTION 301

To preserve digital evidence, an investigator should _____

- A. Make two copies of each evidence item using a single imaging tool
- B. Make a single copy of each evidence item using an approved imaging tool
- C. Make two copies of each evidence item using different imaging tools
- D. Only store the original evidence item

Answer: C

NEW QUESTION 303

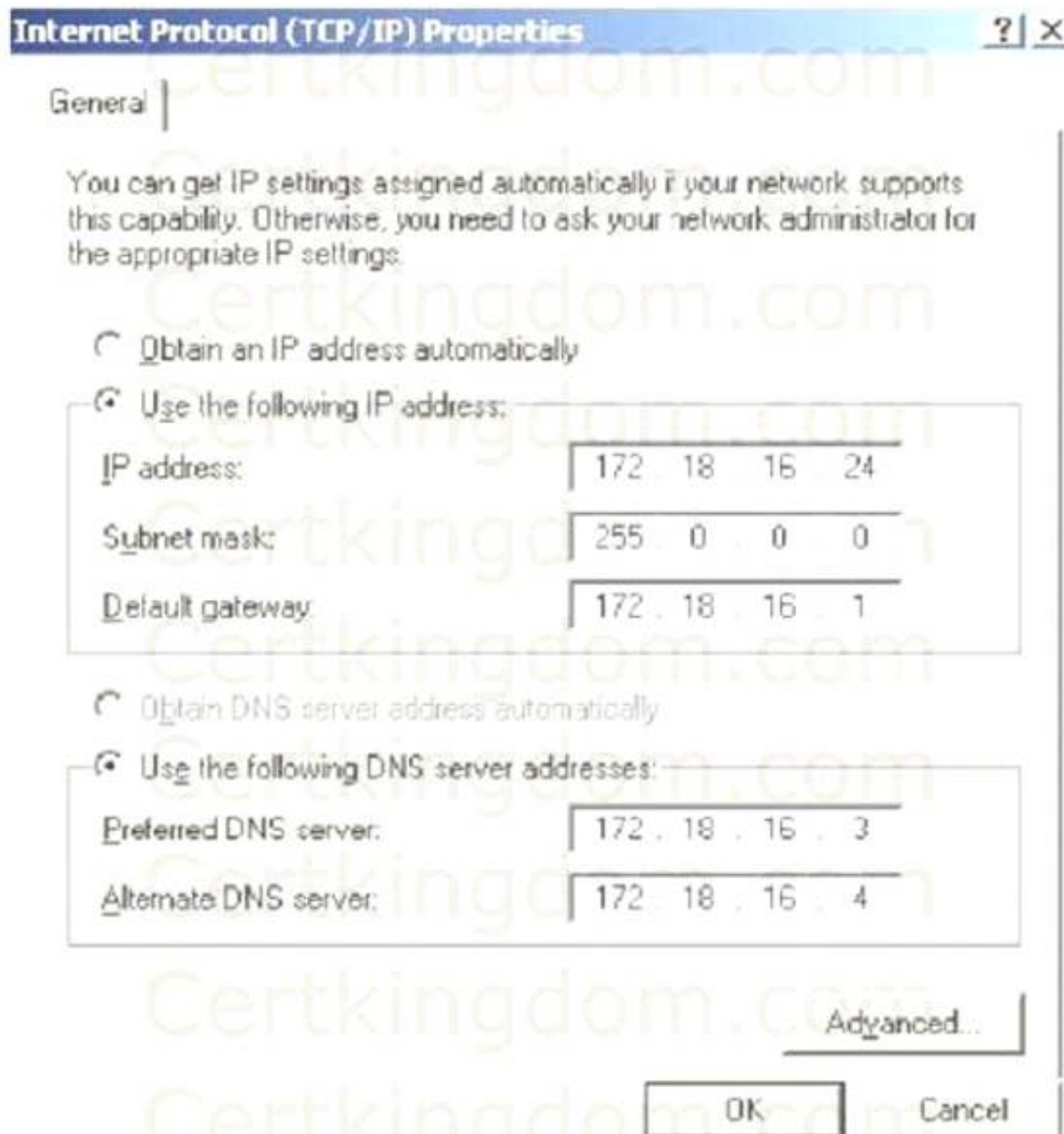
Where is the default location for Apache access logs on a Linux computer?

- A. usr/local/apache/logs/access_log
- B. bin/local/home/apache/logs/access_log
- C. usr/logs/access_log
- D. logs/usr/apache/access_log

Answer: A

NEW QUESTION 305

What is the CIDR from the following screenshot?



- A. /24A./24A./24
- B. /32 B./32 B./32
- C. /16 C./16 C./16
- D. /8D./8D./8

Answer: D

NEW QUESTION 307

When needing to search for a website that is no longer present on the Internet today but was online few years back, what site can be used to view the website collection of pages?view the website? collection of pages?

- A. Proxify.net
- B. Dnsstuff.com
- C. Samspace.org
- D. Archive.org

Answer: D

NEW QUESTION 308

When using an iPod and the host computer is running Windows, what file system will be used?

- A. iPod+
- B. HFS
- C. FAT16
- D. FAT32

Answer: D

NEW QUESTION 309

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 were 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. Visual semagram
- C. Grill cipher
- D. Visual cipher

Answer: B

NEW QUESTION 313

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. TIFF-8
- B. DOC
- C. WPD
- D. PDF

Answer: D

NEW QUESTION 318

You 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 password protected. What are two common methods used by password cracking software that you could use to obtain the password?

- A. Limited force and library attack
- B. Brute force and dictionary attack
- C. Maximum force and thesaurus attack
- D. Minimum force and appendix attack

Answer: B

NEW QUESTION 319

What is the slave device connected to the secondary IDE controller on a Linux OS referred to?

- A. hda
- B. hdd
- C. hdb
- D. hdc

Answer: B

NEW QUESTION 321

Under confession, an accused criminal admitted to encrypting child pornography pictures and then hiding them within other pictures. What technique did the accused criminal employ?

- A. Typography
- B. Steganalysis
- C. Picture encoding
- D. Steganography

Answer: D

NEW QUESTION 325

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

- A. One
- B. Two
- C. Three
- D. Four

Answer: B

NEW QUESTION 330

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 clean?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. 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
- D. Powering on a computer has no affect when needing to acquire digital evidence from it

Answer: A

NEW QUESTION 334

What type of attack sends SYN requests to a target system with spoofed IP addresses?

- A. SYN flood
- B. Ping of death
- C. Cross site scripting
- D. Land

Answer: A

NEW QUESTION 338

What must an investigator do before disconnecting an iPod from any type of computer?

- A. Unmount the iPod
- B. Mount the iPod
- C. Disjoin the iPod
- D. Join the iPod

Answer: A

NEW QUESTION 339

Which is a standard procedure to perform during all computer forensics investigations?

- A. With the hard drive in the suspect PC, check the date and time in the system CMOSWith the hard drive in the suspect PC, check the date and time in the system? CMOS
- B. With the hard drive removed from the suspect PC, check the date and time in the system CMOSWith the hard drive removed from the suspect PC, check the date and time in the system? CMOS
- C. With the hard drive in the suspect PC, check the date and time in the File Allocation Table
- D. With the hard drive removed from the suspect PC, check the date and time in the system RAMWith the hard drive removed from the suspect PC, check the date and time in the system? RAM

Answer: B

NEW QUESTION 343

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. Detection
- B. Hearsay
- C. Spoliation
- D. Discovery

Answer: D

NEW QUESTION 348

John is working as a computer forensics investigator for a consulting firm in Canada. He is called to seize a computer at a local web caf?John is working as a computer forensics investigator for a consulting firm in Canada. He is called to seize a computer at a local web caf purportedly used as a botnet server. John thoroughly scans the computer and finds nothing that would lead him to think the computer was a botnet server. John decides to scan the virtual memory of the computer to possibly find something he had missed. What information will the virtual memory scan produce?

- A. It contains the times and dates of when the system was last patched
- B. It is not necessary to scan the virtual memory of a computer
- C. It contains the times and dates of all the system files
- D. Hidden running processes

Answer: D

NEW QUESTION 352

Given the drive dimensions as follows and assuming a sector has 512 bytes, what is the capacity of the described hard drive?

22,164 cylinders/disk
80 heads/cylinder
63 sectors/track

- A. 53.26 GB
- B. 57.19 GB
- C. 11.17 GB
- D. 10 GB

Answer: A

NEW QUESTION 356

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. Two
- B. One
- C. Three
- D. Four

Answer: A

NEW QUESTION 361

A forensics investigator is searching the hard drive of a computer for files that were recently moved to the Recycle Bin. He searches for files in C:\RECYCLED using a command line tool but does not find anything. What is the reason for this?

- A. He should search in C:\Windows\System32\RECYCLED folder
- B. The Recycle Bin does not exist on the hard drive
- C. The files are hidden and he must use switch to view themThe files are hidden and he must use ? switch to view them
- D. Only FAT system contains RECYCLED folder and not NTFS

Answer: C

NEW QUESTION 363

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. Justification
- B. Authentication
- C. Reiteration
- D. Certification

Answer: B

NEW QUESTION 364

At what layer does a cross site scripting attack occur on?

- A. Presentation
- B. Application
- C. Session
- D. Data Link

Answer: B

NEW QUESTION 369

When should an MD5 hash check be performed when processing evidence?

- A. After the evidence examination has been completed
- B. On an hourly basis during the evidence examination
- C. Before and after evidence examination
- D. Before the evidence examination has been completed

Answer: C

NEW QUESTION 374

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 ow level? How long will the team have to respond to the incident?the investigation, the CEO informs them that the incident will be classified as ?ow level? How long will the team have to respond to the incident?

- A. One working day
- B. Two working days
- C. Immediately
- D. Four hours

Answer: A

NEW QUESTION 376

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. Ping of death
- C. Fraggles
- D. Nmap scan

Answer: B

NEW QUESTION 380

In the context of file deletion process, which of the following statement holds true?

- A. When files are deleted, the data is overwritten and the cluster marked as available
- B. The longer a disk is in use, the less likely it is that deleted files will be overwritten
- C. While booting, the machine may create temporary files that can delete evidence
- D. Secure delete programs work by completely overwriting the file in one go

Answer: C

NEW QUESTION 384

What advantage does the tool Evidor have over the built-in Windows search?

- A. It can find deleted files even after they have been physically removed
- B. It can find bad sectors on the hard drive
- C. It can search slack space
- D. It can find files hidden within ADS

Answer: C

NEW QUESTION 387

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. True
- B. False

Answer: A

NEW QUESTION 391

You are using DriveSpy, a forensic tool and want to copy 150 sectors where the starting sector is 1709 on the primary hard drive. Which of the following formats correctly specifies these sectors?

- A. 0:1000, 150
- B. 0:1709, 150
- C. 1:1709, 150
- D. 0:1709-1858

Answer: B

Explanation: DriveSpy can except two different formats: Drive #:Start Sector, # Sectors Drive#:Start Sector-Absolute End Sector. Drive # is zero based Both Answer B and D would appear correct, and both formats are valid.

NEW QUESTION 396

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. Phreaking
- B. Squatting
- C. Crunching
- D. Pretexting

Answer: A

NEW QUESTION 397

John and Hillary works at the same department in the company. John wants to find out Hillary's network password so he can take a look at her documents on the file server. He enables Lophtcrack program to sniffing mode. John sends Hillary an email with a link to Error! Reference source not found. What information will he be able to gather from this?

- A. The SID of Hillary network account
- B. The SAM file from Hillary computer
- C. The network shares that Hillary has permissions
- D. Hillary network username and password hash

Answer: D

Explanation: Note: From the question, we would have to assume that John is not the Administrator, since he needs to run L0phtcrack in sniffing mode. But what if the company is using switches instead of Hubs? John would either try to degarde the switch or perform a man in the middle attack.

NEW QUESTION 398

Microsoft Outlook maintains email messages in a proprietary format in what type of file?

- A. .email
- B. .mail
- C. .pst
- D. .doc

Answer: C

NEW QUESTION 402

Where are files temporarily written in Unix when printing?

- A. /usr/spool
- B. /var/print
- C. /spool
- D. /var/spool

Answer: D

NEW QUESTION 405

Area density refers to:

- A. the amount of data per disk
- B. the amount of data per partition
- C. the amount of data per square inch
- D. the amount of data per platter

Answer: AC

NEW QUESTION 409

A(n) _____ is one that's performed by a computer program rather than the attacker manually performing the steps in the attack sequence.

- A. blackout attack
- B. automated attack
- C. distributed attack
- D. central processing attack

Answer: B

NEW QUESTION 413

Steven has been given the task of designing a computer forensics lab for the company he works for. He has found documentation on all aspects of how to design a lab except the number of exits needed. How many exits should Steven include in his design for the computer forensics lab?

- A. Three
- B. One
- C. Two
- D. Four

Answer: B

NEW QUESTION 417

On an Active Directory network using NTLM authentication, where on the domain controllers are the passwords stored?

- A. SAM
- B. AMS
- C. Shadow file
- D. Password.conf

Answer: A

NEW QUESTION 418

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. Directory listing of C: drive on the web server
- B. Execute a buffer flow in the C: drive of the web server
- C. Directory listing of the C:\windows\system32 folder on the web server
- D. Insert a Trojan horse into the C: drive of the web server

Answer: A

NEW QUESTION 422

Why is it still possible to recover files that have been emptied from the Recycle Bin on a Windows computer?

- A. The data is still present until the original location of the file is used
- B. The data is moved to the Restore directory and is kept there indefinitely
- C. The data will reside in the L2 cache on a Windows computer until it is manually deleted
- D. It is not possible to recover data that has been emptied from the Recycle Bin

Answer: A

NEW QUESTION 425

What binary coding is used most often for e-mail purposes?

- A. SMTP
- B. Uuencode
- C. IMAP

D. MIME

Answer: D

NEW QUESTION 428

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: AD

Explanation:

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 433

You are a computer forensics investigator working with local police department and you are called to assist in an investigation of threatening emails. The complainant has printed out 27 email messages from the suspect and gives the printouts to you. You inform her that you will need to examine her computer because you need access to the ____ in order to track the emails back to the suspect.

- A. Routing Table
- B. Firewall log
- C. Configuration files
- D. Email Header

Answer: D

NEW QUESTION 438

During the course of an investigation, you locate evidence that may prove the innocence of the suspect of the investigation. You must maintain an unbiased opinion and be objective in your entire fact finding process. Therefore you report this evidence. This type of evidence is known as:

- A. Inculpatory evidence
- B. mandatory evidence
- C. exculpatory evidence
- D. Terrible evidence

Answer: C

NEW QUESTION 440

While working for a prosecutor, What do you think you should do if the evidence you found appears to be exculpatory and is not being released to the defense ?

- A. Keep the information of file for later review
- B. Destroy the evidence
- C. Bring the information to the attention of the prosecutor, his or her supervisor or finally to the judge
- D. Present the evidence to the defense attorney

Answer: C

NEW QUESTION 444

When conducting computer forensic analysis, you must guard against

____ So that you remain focused on the primary job and insure that the level of work does not increase beyond what was originally expected.

- A. Hard Drive Failure
- B. Scope Creep
- C. Unauthorized expenses
- D. Overzealous marketing

Answer: B

NEW QUESTION 445

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. Blu-Ray dual-layer
- D. DVD-18

Answer: C

NEW QUESTION 448

In Linux, what is the smallest possible shellcode?

- A. 8 bytes
- B. 24 bytes
- C. 800 bytes
- D. 80 bytes

Answer: B

NEW QUESTION 452

After passively scanning the network of Department of Defense (DoD), you switch over to active scanning to identify live hosts on their network. DoD is a large organization and should respond to any number of scans. You start an ICMP ping sweep by sending an IP packet to the broadcast address. Only five hosts responds to your ICMP pings; definitely not the number of hosts you were expecting. Why did this ping sweep only produce a few responses?

- A. Only IBM AS/400 will reply to this scan
- B. Only Windows systems will reply to this scan
- C. Only Unix and Unix-like systems will reply to this scan
- D. A switched network will not respond to packets sent to the broadcast address

Answer: C

NEW QUESTION 457

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

- A. Something other than root
- B. Root
- C. Guest
- D. You cannot determine what privilege runs the daemon service

Answer: A

NEW QUESTION 462

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. Check the Windows registry for connection data (You may or may not recover)
- D. Approach the websites for evidence

Answer: A

NEW QUESTION 466

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. MSDOS.sys
- C. BIOS
- D. Case files

Answer: A

NEW QUESTION 469

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: BC

Explanation: 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 470

George is the network administrator of a large Internet company on the west coast. Per corporate policy, none of the employees in the company are allowed to use FTP or SFTP programs without obtaining approval from the IT department. Few managers are using SFTP program on their computers. Before talking to his boss, George wants to have some proof of their activity. George wants to use Ethereal to monitor network traffic, but only SFTP traffic to and from his network. What filter should George use in Ethereal?

- A. src port 23 and dst port 23
- B. src port 22 and dst port 22
- C. udp port 22 and host 172.16.28.1/24

D. net port 22

Answer: B

NEW QUESTION 474

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. The zombie will not send a response
- C. 31401
- D. 31399

Answer: C

NEW QUESTION 479

In what way do the procedures for dealing with evidence in a criminal case differ from the procedures for dealing with evidence in a civil case?

- A. evidence must be handled in the same way regardless of the type of case
- B. evidence procedures are not important unless you work for a law enforcement agency
- C. evidence in a criminal case must be secured more tightly than in a civil case
- D. evidence in a civil case must be secured more tightly than in a criminal case

Answer: C

NEW QUESTION 483

What stage of the incident handling process involves reporting events?

- A. Containment
- B. Follow-up
- C. Identification
- D. Recovery

Answer: C

NEW QUESTION 487

Which forensic investigating concept trails the whole incident from how the attack began to how the victim was affected?

- A. Point-to-point
- B. End-to-end
- C. Thorough
- D. Complete event analysis

Answer: B

NEW QUESTION 489

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. Pattern matching
- B. Statistical-based anomaly detection
- C. Real-time anomaly detection
- D. Signature-based anomaly detection

Answer: C

NEW QUESTION 494

James is testing the ability of his routers to withstand DoS attacks. James sends ICMP ECHO requests to the broadcast address of his network. What type of DoS attack is James testing against his network?

- A. Fraggle
- B. Smurf
- C. SYN flood
- D. Trinoo

Answer: B

Explanation: The Fraggle attack is like a smurf attack, but uses UDP packets and not ICMP.

NEW QUESTION 498

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

Answer:

NEW QUESTION 502

Which response organization tracks hoaxes as well as viruses?

- A. NIPC
- B. FEDCIRC
- C. CERT
- D. CIAC

Answer: D

Explanation: Note: CIAC (Computer Incident Advisory Capability) Was run by the US Department of energy

NEW QUESTION 504

How many bits is Source Port Number in TCP Header packet?

- A. 16
- B. 48
- C. 32
- D. 64

Answer: A

NEW QUESTION 509

When a file is deleted by Windows Explorer or through the MS-DOS delete command, the operating system inserts ____ in the first letter position of the filename in the FAT database.

- A. A Capital X
- B. A Blank Space
- C. The Underscore Symbol
- D. The lowercase Greek Letter Sigma (s)

Answer: D

Explanation: When a file is deleted, the first byte is replaced with 0xE5 to marked the file as deleted or erased, and is the same for FAT12/16/32. An 0xE5 translates also to a ASCII 229, a “O” with a tilde.

However, using the greek alphabet (see: <http://www.ascii.ca/iso8859.7.htm>) the ASCII code 229 is “the lowercase Greek Letter Epsilon, and Ascii code 243 is Lower case Greek Letter Sigma.

<http://chexed.com/ComputerTips/asciicodes.php> says that Ascii 229 is Lowercase Greek Letter Sigma

So, although D looks like the correct answer here, it may require more understanding of the underlying intent of the question.

NEW QUESTION 511

This type of testimony is presented by someone who does the actual fieldwork and does not offer a view in court.

- A. Civil litigation testimony
- B. Expert testimony
- C. Victim advocate testimony
- D. Technical testimony

Answer: A

NEW QUESTION 514

What type of attack sends spoofed UDP packets (instead of ping packets) with a fake source address to the IP broadcast address of a large network?

- A. Fraggles
- B. Smurf scan
- C. SYN flood
- D. Teardrop

Answer: A

NEW QUESTION 517

You have compromised a lower-level administrator account on an Active Directory network of a small company in Dallas, Texas. You discover Domain Controllers through enumeration. You connect to one of the Domain Controllers on port 389 using ldp.exe. What are you trying to accomplish here?

- A. Enumerate domain user accounts and built-in groups
- B. Enumerate MX and A records from DNS
- C. Establish a remote connection to the Domain Controller
- D. Poison the DNS records with false records

Answer: A

NEW QUESTION 522

In a forensic examination of hard drives for digital evidence, what type of user is most likely to have the most file slack to analyze?

- A. one who has NTFS 4 or 5 partitions
- B. one who uses dynamic swap file capability
- C. one who uses hard disk writes on IRQ 13 and 21
- D. one who has lots of allocation units per block or cluster

Answer: D

NEW QUESTION 524

In the following email header, where did the email first originate from?

```
Microsoft Mail Internet Headers version 2.0
Received: from smtp1.somedomain.com ([199.190.129.133]) by somedomain.com
with Microsoft SMTPSVC(6.0.3790.1830);
    Fri, 1 Jun 2007 09:43:08 -0500
Received: from david1.state.us.gov.us (david1.state.ok.gov [172.16.28.115])
    by smtp1.somedomain.com (8.13.1/8.12.11) with ESMTP id 151efceh032241
    for <someone@somedomain.com>; Fri, 1 Jun 2007 09:41:13 -0500
Received: from simon1.state.ok.gov.us ([172.18.0.199]) by
david1.state.ok.gov.us with Microsoft SMTPSVC(6.0.3790.1830);
    Fri, 1 Jun 2007 09:41:13 -0500
X-Ninja-PIM: Scanned by Ninja
X-Ninja-AttachmentFiltering: (no action)
X-MimeOLE: Produced By Microsoft Exchange V6.5.7235.2
Content-class: urn:content-classes:message
Return-Receipt-To: "Johnson, Jimmy" <jimmy@somewhereelse.com>
MIME-version: 1.0
```

- A. Somedomain.com
- B. Smtp1.somedomain.com
- C. Simon1.state.ok.gov.us
- D. David1.state.ok.gov.us

Answer: C

NEW QUESTION 529

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. ARP redirect
- B. Physical attack
- C. Digital attack
- D. Denial of service

Answer: D

NEW QUESTION 530

What will the following command accomplish in Linux? `fdisk /dev/hda`

- A. Partition the hard drive
- B. Format the hard drive
- C. Delete all files under the `/dev/hda` folder
- D. Fill the disk with zeros

Answer: A

NEW QUESTION 534

Why should you note all cable connections for a computer you want to seize as evidence?

- A. to know what outside connections existed
- B. in case other devices were connected
- C. to know what peripheral devices exist
- D. to know what hardware existed

Answer: A

NEW QUESTION 537

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. Add up the total size of all known partitions and compare it to the total size of the hard drive
- B. 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
- C. 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

Answer: A

NEW QUESTION 541

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. Passive IDS

- B. Active IDS
- C. NIPS
- D. Progressive IDS

Answer: B

NEW QUESTION 546

In General, _____ Involves the investigation of data that can be retrieved from the hard disk or other disks of a computer by applying scientific methods to retrieve the data.

- A. Network Forensics
- B. Data Recovery
- C. Disaster Recovery
- D. Computer Forensics

Answer: D

NEW QUESTION 547

Law enforcement officers are conducting a legal search for which a valid warrant was obtained. While conducting the search, officers observe an item of evidence for an unrelated crime that was not included in the warrant. The item was clearly visible to the officers and immediately identified as evidence. What is the term used to describe how this evidence is admissible?

- A. Plain view doctrine
- B. Corpus delicti
- C. Locard Exchange Principle
- D. Ex Parte Order

Answer: A

NEW QUESTION 549

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 retrieve company? 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 to work
- B. Right of free speech
- C. Right to Internet access
- D. Right of privacy

Answer: D

NEW QUESTION 554

How many possible sequence number combinations are there in TCP/IP protocol?

- A. 320 billion
- B. 1 billion
- C. 4 billion
- D. 32 million

Answer: C

NEW QUESTION 559

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. RIM Messaging center
- B. Blackberry Enterprise server
- C. Microsoft Exchange server
- D. Blackberry desktop redirector

Answer: C

NEW QUESTION 563

After undergoing an external IT audit, George realizes his network is vulnerable to DDoS attacks. What countermeasures could he take to prevent DDoS attacks?

- A. Enable BGP
- B. Enable direct broadcasts
- C. Disable BGP
- D. Disable direct broadcasts

Answer: D

NEW QUESTION 564

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. Bit-stream copy
- B. Robust copy
- C. Full backup copy
- D. Incremental backup copy

Answer: A

NEW QUESTION 568

Harold is a web designer who has completed a website for ghttech.net. As part of the maintenance agreement he signed with the client, Harold is performing research online and seeing how much exposure the site has received so far. Harold navigates to google.com and types in the following search. link:www.ghttech.net What will this search produce?

- A. All search engines that link to .net domains
- B. All sites that link to ghttech.net
- C. Sites that contain the code: link:www.ghttech.net
- D. All sites that ghttech.net links to

Answer: B

NEW QUESTION 569

What information do you need to recover when searching a victim computer for a crime committed with specific e-mail message?What information do you need to recover when searching a victim? computer for a crime committed with specific e-mail message?

- A. Internet service provider information
- B. E-mail header
- C. Username and password
- D. Firewall log

Answer: B

NEW QUESTION 573

In a FAT32 system, a 123 KB file will use how many sectors?

- A. 34
- B. 25
- C. 11
- D. 56
- E. 246

Answer: E

Explanation: If you assume that we are using 512 bytes sectors, then $123 \times 1024 / 512 = 246$ sectors would be needed.

NEW QUESTION 577

A law enforcement officer may only search for and seize criminal evidence with ____ , which are facts or circumstances that would lead a reasonable person to believe a crime has been committed or is about to be committed, evidence of the specific crime exists and the evidence of the specific crime exists at the place to be searched.

- A. Mere Suspicion
- B. A preponderance of the evidence
- C. Probable cause
- D. Beyond a reasonable doubt

Answer: C

Explanation: A preponderance of the evidence is the proof requirement in a civil case Beyond a reasonable doubt is the proof requirement in a criminal case

NEW QUESTION 579

What does the superbblock in Linux define?

- A. file synames
- B. disk geometr
- C. location of the first inode
- D. available space

Answer: C

NEW QUESTION 583

Kimberly is studying to be an IT security analyst at a vocational school in her town. The school offers many different programming as well as networking languages. What networking protocol language should she learn that routers utilize?

- A. BPG
- B. ATM
- C. OSPF
- D. UDP

Answer: C

NEW QUESTION 588

From the following spam mail header, identify the host IP that sent this spam? From jie02@netvigator.com jie02@netvigator.com Tue Nov 27 17:27:11 2001
Received: from viruswall.ie.cuhk.edu.hk (viruswall [137.189.96.52]) by eng.ie.cuhk.edu.hk (8.11.6/8.11.6) with ESMTP id fAR9RAP23061 for ; Tue, 27 Nov 2001 17:27:10 +0800 (HKT)
Received: from mydomain.com (pcd249020.netvigator.com [203.218.39.20]) by viruswall.ie.cuhk.edu.hk (8.12.1/8.12.1) with SMTP id fAR9QXwZ018431 for ; Tue, 27 Nov 2001 17:26:36 +0800 (HKT)
Message-Id: >200111270926.fAR9QXwZ018431@viruswall.ie.cuhk.edu.hk From: "china hotel web"
To: "Shlam"
Subject: SHANGHAI (HILTON HOTEL) PACKAGE Date: Tue, 27 Nov 2001 17:25:58 +0800 MIME-Version: 1.0
X-Priority: 3 X-MSMail- Priority: Normal
Reply-To: "china hotel web"

- A. 137.189.96.52
- B. 8.12.1.0
- C. 203.218.39.20
- D. 203.218.39.50

Answer: C

NEW QUESTION 591

While presenting his case to the court, Simon calls many witnesses to the stand to testify. Simon decides to call Hillary Taft, a lay witness, to the stand. Since Hillary is a lay witness, what field would she be considered an expert in?

- A. Technical material related to forensics
- B. No particular field
- C. Judging the character of defendants/victims
- D. Legal issues

Answer: B

NEW QUESTION 593

Under which Federal Statutes does FBI investigate for computer crimes involving e-mail scams and mail fraud?

- A. 18 U.S.
- B. 1029 Possession of Access Devices
- C. 18 U.S.
- D. 1030 Fraud and related activity in connection with computers
- E. 18 U.S.
- F. 1343 Fraud by wire, radio or television
- G. 18 U.S.
- H. 1361 Injury to Government Property
- I. 18 U.S.
- J. 1362 Government communication systems
- K. 18 U.S.
- L. 1831 Economic Espionage Act
- M. 18 U.S.
- N. 1832 Trade Secrets Act

Answer: B

NEW QUESTION 594

Click on the Exhibit Button To test your website for vulnerabilities, you type in a Quotation mark (?) for the username field. After you click Ok, you receive the following error message window: What can you infer from this error window?

- A. SQL injection is not possible
- B. SQL injection is possible
- C. The user for line 3306 in the SQL database has a weak password
- D. The Quotation mark (?) is a valid username

Answer: B

NEW QUESTION 599

This organization maintains a database of hash signatures for known software

- A. International Standards Organization
- B. Institute of Electrical and Electronics Engineers
- C. National Software Reference Library
- D. American National standards Institute

Answer: C

NEW QUESTION 603

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 against DoS attacks
- B. List weak points on their network
- C. Show outdated equipment so it can be replaced
- D. Use attack as a launching point to penetrate deeper into the network

Answer: B

NEW QUESTION 607

You have completed a forensic investigation case. You would like to destroy the data contained in various disks at the forensics lab due to sensitivity of the case. How would you permanently erase the data on the hard disk?

- A. Throw the hard disk into the fire
- B. Run the powerful magnets over the hard disk
- C. Format the hard disk multiple times using a low level disk utility
- D. Overwrite the contents of the hard disk with Junk data

Answer: AC

Explanation: To be effective with throwing the hard drive into the fire, the fire would have to be hot enough to melt the platters into molten metal, which requires an industrial furnace. This requires special facilities.

Running powerful magnets over the disk, such as degaussing the disk, may destroy the data, but may also be ineffective. In some cases, the degaussing process for tape and disk may render the disk unusable for use again. (Of course throwing the drives into a furnace also guarantees that as well).

Formatting the disk multiple times with a low level disk utility is the best way to go, and still be able to re-use the disk for later projects. The keys are “multiple” and “low level”. A low level format is typically a slow, thorough, format that is a wipe. Multiple – as opposed to once – is recommended. There is a theory on “how many times”, some schools say at least three times. The problem with this answer is that with newer drives, such as ATA and SCSI, low level formats can destroy the volumes as well, and some BIOS may actually ignore the LLF directives.

Overwriting the disk with junk data would perform some form of wipe because the old data is wiped out, but still may be recovered.

Note:

According to some websites:

Physical Methods that will not work to destroy data on a hard drive include: Throwing it in the water (this does not do much) Setting it on fire (the temperature is not going to be high enough at home) Throwing it out of the window. Hard drives can take quite a bit of G force. They are not heavy so the impact of the hard drive on the ground is not likely to destroy the platters. Drive over the hard drive. A car, or even a tank, driving over a hard drive will do nothing, any more than they would driving over a book. Unless the drive is actually flattened, the platters are not going to be destroyed

NEW QUESTION 612

Before performing a logical or physical search of a drive in Encase, what must be added to the program?

- A. File signatures
- B. Keywords
- C. Hash sets
- D. Bookmarks

Answer: B

NEW QUESTION 617

You are working as Computer Forensics investigator and are called by the owner of an accounting firm to investigate possible computer abuse by one of the firm's employees. You meet with the owner of the firm and discover that the company has never published a policy stating that they reserve the right to inspect their computing assets at will. What do you do?

- A. Inform the owner that conducting an investigation without a policy is not a problem because the company is privately owned
- B. Inform the owner that conducting an investigation without a policy is a violation of the 4th amendment
- C. Inform the owner that conducting an investigation without a policy is a violation of the employees' expectation of privacy
- D. Inform the owner that conducting an investigation without a policy is not a problem because a policy is only necessary for government agencies

Answer: C

NEW QUESTION 622

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. Search for disk errors within an image file
- B. Backup a disk to an image file
- C. Copy a partition to an image file
- D. Restore a disk from an image file

Answer: D

NEW QUESTION 623

While looking through the IIS log file of a web server, you find the following entries:


```
2007-01-23 14:18:39 W3SVC1 172.16.28.102 GET /Development/index.asp
2007-01-23 14:18:39 W3SVC1 172.16.28.102 GET /login.asp?username=if'(({select user}='sa' OR {select user}='dbo'})
select 1 else select 1/0
2007-01-23 14:18:39 W3SVC1 172.16.28.102 GET /Developments/index_02.jpg
2007-01-23 14:18:39 W3SVC1 172.16.28.102 GET /Development/index 04.jpg
```

What is evident from this log file?

- A. Web bugs
- B. Cross site scripting
- C. Hidden fields
- D. SQL injection is possible

Answer: D

NEW QUESTION 624

You are assigned to work in the computer forensics lab of a state police agency. While working on a high profile criminal case, you have followed every applicable procedure, however your boss is still concerned that the defense attorney might question wheather evidence has been changed while at the lab. What can you do to prove that the evidence is the same as it was when it first entered the lab?

- A. Sign a statement attesting that the evidence is the same as it was when it entered the lab
- B. There is no reason to worry about this possible claim because state labs are certified
- C. Make MD5 hashes of the evidence and compare it to the standard database developed by NIST
- D. Make MD5 hashes of the evidence and compare it with the original MD5 hash that was taken when the evidence first entered the lab

Answer: D

NEW QUESTION 625

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. Enticement
- B. Entrapment
- C. Intruding into ahoneypot is not illegal
- D. Intruding into a DMZ is not illegal

Answer: B

NEW QUESTION 627

Why is it a good idea to perform a penetration test from the inside?

- A. It is never a good idea to perform a penetration test from the inside
- B. It is easier to hack from the inside
- C. Because 70% of attacks are from inside the organization
- D. To attack a network from a hacker's perspective

Answer: C

NEW QUESTION 631

What are the security risks of running a "repair" installation for Windows XP?

- A. Pressing Shift+F1 gives the user administrative rights
- B. Pressing Ctrl+F10 gives the user administrative rights
- C. There are no security risks when running the "repair" installation for Windows XP
- D. Pressing Shift+F10 gives the user administrative rights

Answer: D

NEW QUESTION 633

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-open
- B. The firewall failed-closed
- C. The firewall ACL has been purged
- D. The firewall failed-bypass

Answer: A

NEW QUESTION 637

Which of the following filesystem is used by Mac OS X?

- A. EFS
- B. HFS+
- C. EXT2

D. NFS

Answer: B

Explanation: EFS (Encrypting File System) is part of NTFS and used on Windows EXT2 is used on Linux NFS (Network File System) is for access to a network file system over TCP/IP

NEW QUESTION 638

What will the following command accomplish? C:\> nmap -v -sS -Po 172.16.28.251 - data_length 66000 - packet_trace

- A. Test the ability of a router to handle under-sized packets
- B. Test ability of a router to handle over-sized packets
- C. Test the ability of a WLAN to handle fragmented packets
- D. Test the ability of a router to handle fragmented packets

Answer: B

NEW QUESTION 642

When reviewing web logs, you see an entry for resource not found in the HTTP status code filed. What is the actual error code that you would see in the log for resource not found?

- A. 202
- B. 404
- C. 505
- D. 909

Answer: B

NEW QUESTION 643

Diskcopy is:

- A. a utility by AccessData
- B. a standard MS-DOS command
- C. Digital Intelligence utility
- D. dd copying tool

Answer: B

Explanation: diskcopy is a STANDARD DOS utility. C:\WINDOWS>diskcopy /? Copies the contents of one floppy disk to another.

NEW QUESTION 644

Jessica works as systems administrator for a large electronics firm. She wants to scan her network quickly to detect live hosts by using ICMP ECHO Requests. What type of scan is Jessica going to perform?

- A. ICMP ping sweep
- B. Ping trace
- C. Tracert
- D. Smurf scan

Answer: A

NEW QUESTION 645

A packet is sent to a router that does not have the packet destination address in its route table, how will the packet get to its properA packet is sent to a router that does not have the packet? destination address in its route table, how will the packet get to its proper destination?

- A. Border Gateway Protocol
- B. Root Internet servers
- C. Gateway of last resort
- D. Reverse DNS

Answer: C

NEW QUESTION 648

An employee is suspected of stealing proprietary information belonging to your company that he had no rights to possess. The information was stored on the employee computer that was protected with the NTFS Encrypted File System (EFS) and you had observed him copy the files to a stored on the employee? computer that was protected with the NTFS Encrypted File System (EFS) and you had observed him copy the files to a floppy disk just before leaving work for the weekend. You detain the employee before he leaves the building and recover the floppy disk and secure his computer. Will you be able to break the encryption so that you can verify that the employee was in possession of the proprietary information?

- A. EFS uses a 128-bit key that cannot be cracked, so you will not be able to recover the information
- B. The EFS Revoked Key Agent can be used on the computer to recover the information
- C. When the encrypted file was copied to the floppy disk, it was automatically unencrypted, so you can recover the information
- D. When the encrypted file was copied to the floppy disk, the EFS private key was also copied to the floppy disk, so you can recover the information

Answer: C

NEW QUESTION 650

What TCP/UDP port does the toolkit program netstat use?

- A. Port 7
- B. Port 15
- C. Port 23
- D. Port 69

Answer: B

NEW QUESTION 655

When cataloging digital evidence, the primary goal is to

- A. Make bit-stream images of all hard drives
- B. Preserve evidence integrity
- C. Not remove the evidence from the scene
- D. Not allow the computer to be turned off

Answer: B

NEW QUESTION 657

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

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

Answer: B

NEW QUESTION 659

What is the name of the standard Linux command that can be used to create bit-stream images?

- A. mcopy
- B. image
- C. MD5
- D. dd

Answer: D

NEW QUESTION 661

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. True negatives
- C. True positives
- D. False positives

Answer: A

NEW QUESTION 666

It takes ____ mismanaged case/s to ruin your professional reputation as a computer forensics examiner?

- A. by law, three
- B. quite a few
- C. only one
- D. at least two

Answer: C

NEW QUESTION 668

If a suspect computer is located in an area that may have toxic chemicals, you must:

- A. coordinate with the HAZMAT team
- B. determine a way to obtain the suspect computer
- C. assume the suspect machine is contaminated
- D. do not enter alone

Answer: A

NEW QUESTION 678

Melanie was newly assigned to an investigation and asked to make a copy of all the evidence from the compromised system. Melanie did a DOS copy of all the files on the system. What would be the primary reason for you to recommend a disk imaging tool?

- A. A disk imaging tool would check for CRC32s for internal self checking and validation and have MD5 checksum
- B. Evidence file format will contain case data entered by the examiner and encrypted at the beginning of the evidence file
- C. A simple DOS copy will not include deleted files, file slack and other information
- D. There is no case for an imaging tool as it will use a closed, proprietary format that if compared to the original will not match up sector for sector

Answer: C

NEW QUESTION 682

Harold is finishing up a report on a case of network intrusion, corporate spying, and embezzlement that he has been working on for over six months. He is trying to find the right term to use in his report to describe network-enabled spying. What term should Harold use?

- A. Spycrack
- B. Spynet
- C. Netspionage
- D. Hackspionage

Answer: C

NEW QUESTION 685

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. CB radio
- B. 2.4Ghz Cordless phones
- C. Satellite television
- D. Computers on his wired network

Answer: B

NEW QUESTION 688

An Expert witness gives an opinion if:

- A. The Opinion, inferences or conclusions depend on special knowledge, skill or training not within the ordinary experience of lay jurors
- B. To define the issues of the case for determination by the finder of fact
- C. To stimulate discussion between the consulting expert and the expert witness
- D. To deter the witness from expanding the scope of his or her investigation beyond the requirements of the case

Answer: A

NEW QUESTION 693

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
- E. email address into the members table

Answer: C

Explanation: The third line deletes the table named members.

NEW QUESTION 694

All Blackberry email is eventually sent and received through what proprietary RIM-operated mechanism?

- A. Blackberry Message Center
- B. Microsoft Exchange
- C. Blackberry WAP gateway
- D. Blackberry WEP gateway

Answer: A

NEW QUESTION 699

At what layer of the OSI model do routers function on?

- A. 4
- B. 3

- C. 1
- D. 5

Answer: B

NEW QUESTION 702

If you see the files Zer0.tar.gz and copy.tar.gz on a Linux system while doing an investigation, what can you conclude?

- A. The system files have been copied by a remote attacker
- B. The system administrator has created an incremental backup
- C. The system has been compromised using a t0rn rootkit
- D. Nothing in particular as these can be operational files

Answer: C

NEW QUESTION 704

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 cannot perform wireless testing
- B. Nessus is too loud
- C. There are no ways of performing a "stealthy" wireless scan
- D. Nessus is not a network scanner

Answer: B

NEW QUESTION 707

Which of the following should a computer forensics lab used for investigations have?

- A. isolation
- B. restricted access
- C. open access
- D. an entry log

Answer: B

NEW QUESTION 709

What encryption technology is used on Blackberry devices?Password Keeper?

- A. 3DES
- B. AES
- C. Blowfish
- D. RC5

Answer: B

NEW QUESTION 714

The rule of thumb when shutting down a system is to pull the power plug. However, it has certain drawbacks. Which of the following would that be?

- A. Any data not yet flushed to the system will be lost
- B. All running processes will be lost
- C. The /tmp directory will be flushed
- D. Power interruption will corrupt the pagefile

Answer: AB

Explanation: Volatile memory will be lost.

Data is not flushed to the system, it is flushed to the disk.

NEW QUESTION 715

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. Network
- B. Transport
- C. Data Link
- D. Session

Answer: A

NEW QUESTION 716

A computer forensics investigator is inspecting the firewall logs for a large financial institution that has employees working 24 hours a day, 7 days a week.

```
2007-06-14 13:59:05 192.168.254.1 action=Permit sent=16369 rcvd=180962 src=24.119.229.125 dst=10.120.10.122 src_port=38
2007-06-14 13:59:06 192.168.254.1 action=Deny sent=0 rcvd=12288 src=10.130.9.3 dst=224.0.0.2 src_port=49415 dst_port=49
2007-06-14 13:59:07 192.168.254.1 action=Permit sent=844 rcvd=486 src=24.119.229.125 dst=10.120.10.123 src_port=38660 d
2007-06-14 13:59:07 192.168.254.1 action=Permit sent=545 rcvd=404 src=192.168.254.80 dst=208.188.166.68 src_port=15113
2007-06-14 13:59:07 192.168.254.1 action=Permit sent=545 rcvd=404 src=192.168.254.80 dst=208.188.166.68 src_port=14857
2007-06-14 13:59:07 192.168.254.1 action=Deny sent=0 rcvd=12288 src=10.130.9.3 dst=224.0.0.2 src_port=49415 dst_port=49
2007-06-14 13:59:09 192.168.254.1 action=Permit sent=13795 rcvd=149962 src=70.185.206.122 dst=10.120.10.122 src_port=61
2007-06-14 13:59:09 192.168.254.1 action=Permit sent=696 rcvd=415 src=70.185.198.247 dst=10.120.10.123 src_port=48392 d
2007-06-14 13:59:09 192.168.254.1 action=Permit sent=17219 rcvd=140495 src=70.185.206.122 dst=10.120.10.122 src_port=61
2007-06-14 13:59:09 192.168.254.1 action=Deny sent=0 rcvd=12288 src=10.130.9.3 dst=224.0.0.2 src_port=49415 dst_port=49
2007-06-14 13:59:10 192.168.254.1 action=Deny sent=0 rcvd=12288 src=10.130.9.3 dst=224.0.0.2 src_port=49415 dst_port=49
2007-06-14 18:34:04 192.168.254.1 action=Permit sent=3038 rcvd=34134 src=70.185.198.247 dst=10.120.10.122 src_port=4480
2007-06-14 18:34:05 192.168.254.1 action=Permit sent=795 rcvd=6686 src=70.185.198.247 dst=10.120.10.122 src_port=46344
2007-06-14 18:34:07 192.168.254.1 action=Permit sent=2780 rcvd=18874 src=70.185.198.247 dst=10.120.10.122 src_port=4532
2007-06-14 18:34:07 192.168.254.1 action=Permit sent=2737 rcvd=8922 src=24.119.169.162 dst=10.120.10.122 src_port=2689
2007-06-14 18:34:09 192.168.254.1 action=Permit sent=2054 rcvd=23180 src=70.185.198.247 dst=10.120.10.122 src_port=4685
2007-06-14 18:34:11 192.168.254.1 action=Permit sent=2632 rcvd=68608 src=70.185.198.247 dst=10.120.10.122 src_port=4711
2007-06-14 18:34:12 192.168.254.1 action=Permit sent=4131 rcvd=72135 src=24.119.169.162 dst=10.120.10.122 src_port=1665
2007-06-14 18:34:13 192.168.254.1 action=Permit sent=646 rcvd=1803 src=70.185.198.247 dst=10.120.10.122 src_port=47368
2007-06-14 11:47:29 192.168.254.1 action=Permit sent=725 rcvd=1115 src=70.185.198.247 dst=10.120.10.122 src_port=48136
2007-06-14 11:47:30 192.168.254.1 action=Permit sent=766 rcvd=415 src=70.185.206.122 dst=10.120.10.123 src_port=62212 d
2007-06-14 11:47:35 192.168.254.1 action=Permit sent=5054 rcvd=81725 src=24.119.169.162 dst=10.120.10.122 src_port=7809
2007-06-14 11:47:37 192.168.254.1 action=Permit sent=26396 rcvd=233409 src=24.119.229.125 dst=10.120.10.122 src_port=38
2007-06-14 11:47:40 192.168.254.1 action=Deny sent=0 rcvd=12288 src=10.130.9.3 dst=224.0.0.2 src_port=49415 dst_port=49
2007-06-14 11:47:41 192.168.254.1 action=Permit sent=18221 rcvd=210841 src=216.97.160.253 dst=10.120.10.122 src_port=94
2007-06-14 11:47:42 192.168.254.1 action=Permit sent=5741 rcvd=102596 src=24.119.169.162 dst=10.120.10.122 src_port=579
2007-06-14 11:47:42 192.168.254.1 action=Permit sent=2552 rcvd=24075 src=24.119.169.162 dst=10.120.10.122 src_port=661
2007-06-14 11:47:43 192.168.254.1 action=Permit sent=2557 rcvd=28655 src=24.119.169.162 dst=10.120.10.122 src_port=1600
2007-06-14 11:47:46 192.168.254.1 action=Permit sent=844 rcvd=491 src=24.119.169.162 dst=10.120.10.123 src_port=13185 d
2007-06-14 11:47:49 192.168.254.1 action=Permit sent=3348 rcvd=18192 src=24.119.169.162 dst=10.120.10.122 src_port=4737
2007-06-14 11:47:53 192.168.254.1 action=Permit sent=3760 rcvd=34120 src=24.119.169.162 dst=10.120.10.122 src_port=3713
2007-06-14 11:47:57 192.168.254.1 action=Permit sent=3646 rcvd=30265 src=24.119.169.162 dst=10.120.10.122 src_port=6785
2007-06-14 11:47:58 192.168.254.1 action=Permit sent=3446 rcvd=39223 src=24.119.169.162 dst=10.120.10.122 src_port=5761
2007-06-14 11:47:59 192.168.254.1 action=Deny sent=0 rcvd=12288 src=10.130.9.3 dst=224.0.0.2 src_port=49415 dst_port=49
2007-06-14 11:48:04 192.168.254.1 action=Permit sent=545 rcvd=404 src=192.168.254.42 dst=208.188.166.68 src_port=7696 d
2007-06-14 11:48:05 192.168.254.1 action=Deny sent=0 rcvd=12288 src=10.130.9.3 dst=224.0.0.2 src_port=49415 dst_port=49
2007-06-14 11:48:09 192.168.254.1 action=Deny sent=0 rcvd=12288 src=10.130.9.3 dst=224.0.0.2 src_port=49415 dst_port=49
2007-06-14 11:48:09 192.168.254.1 action=Deny sent=0 rcvd=12288 src=10.130.9.3 dst=224.0.0.2 src_port=49415 dst_port=49
2007-06-14 11:48:10 192.168.254.1 action=Permit sent=407 rcvd=0 src=192.168.254.14 dst=204.61.5.130 src_port=200 dst_gw
2007-06-14 11:48:13 192.168.254.1 action=Permit sent=1640 rcvd=0 src=192.168.254.14 dst=204.61.5.130 src_port=41216 dst
2007-06-14 11:48:15 192.168.254.1 action=Deny sent=0 rcvd=12288 src=10.130.9.3 dst=224.0.0.2 src_port=49415 dst_port=49
2007-06-14 11:48:16 192.168.254.1 action=Deny sent=0 rcvd=11264 src=10.130.9.3 dst=224.0.0.2 src_port=49415 dst_port=49
```

What can the investigator infer from the screenshot seen below?

- A. A smurf attack has been attempted
- B. A denial of service has been attempted
- C. Network intrusion has occurred
- D. Buffer overflow attempt on the firewall

Answer: C

NEW QUESTION 719

The police believe that Mevin Matthew has been obtaining unauthorized access to computers belonging to numerous computer software and computer operating systems manufacturers, cellular telephone manufacturers, Internet Service Providers, and educational institutions. They also suspect that he has been stealing, copying, and misappropriating proprietary computer software belonging to the several victim companies. What is preventing the police from breaking down the suspect door and searching his home and seizing all of his computer equipment if they have is preventing the police from breaking down the suspect? door and searching his home and seizing all of his computer equipment if they have not yet obtained a warrant?

- A. The USA Patriot Act
- B. The Good Samaritan Laws
- C. The Federal Rules of Evidence
- D. The Fourth Amendment

Answer: D

NEW QUESTION 720

This is the original file structure database that Microsoft originally designed for floppy disks. It is written to the outermost track of a disk and contains information about each file stored on the drive.

- A. Master Boot Record (MBR)
- B. Master File Table (MFT)
- C. File Allocation Table (FAT)
- D. Disk Operating System (DOS)

Answer: C

Explanation: A MBR is usually found on fixed disks, not floppy. A MFT is part of NTFS, and NTFS is not used on floppy DOS is an operating system, not a file structure database

NEW QUESTION 723

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

- A. 32
- B. 16
- C. 250
- D. 25

Answer: C

Explanation: If you assume that we are using 512 bytes sectors, then $125 \times 1024 / 512 = 250$ sectors would be needed. Actually, this is the same for a FAT16 file system as well.

NEW QUESTION 727

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

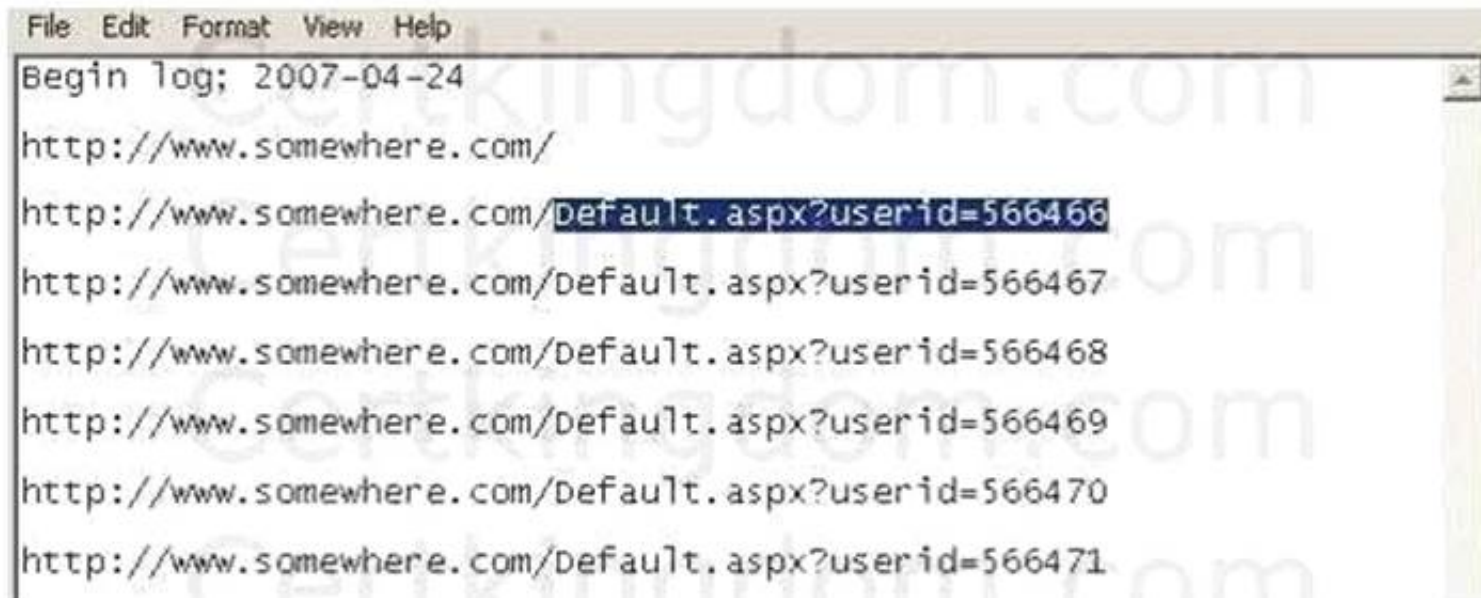
preferred No Unix/Linux Experience needed What is this information posted on the job website considered?

- A. Trade secret
- B. Social engineering exploit
- C. Competitive exploit
- D. Information vulnerability

Answer: D

NEW QUESTION 729

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. Cross site scripting
- C. SQL injection
- D. Cookie Poisoning

Answer: A

NEW QUESTION 731

Frank is working on a vulnerability assessment for a company on the West coast. The company hired Frank to assess its network security through scanning, pen tests, and vulnerability assessments. After discovering numerous known vulnerabilities detected by a temporary IDS he set up, he notices a number of items that show up as unknown but Questionable in the logs. He looks up the behavior on the Internet, but cannot find anything related. What organization should Frank submit the log to find out if it is a new vulnerability or not?

- A. CVE
- B. IANA
- C. RIPE
- D. APIPA

Answer: A

NEW QUESTION 736

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. Linux/Unix computers are easier to compromise
- C. Windows computers are constantly talking
- D. Linux/Unix computers are constantly talking

Answer: C

NEW QUESTION 741

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 all internal MAC address from using SNMP
- D. Block access to UDP port 171

Answer: B

NEW QUESTION 744

When monitoring for both intrusion and security events between multiple computers, it is essential that the computers' clocks are synchronized. Synchronized time allows an administrator to reconstruct what took place during an attack against multiple computers. Without synchronized time, it is very difficult to determine exactly when specific events took place, and how events interlace. What is the name of the service used to synchronize time

among multiple computers?

- A. Time-Sync Protocol
- B. SyncTime Service
- C. Network Time Protocol
- D. Universal Time Set

Answer: C

NEW QUESTION 747

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. Passwords of 14 characters or less are broken up into two 7-character hashes
- B. A password Group Policy change takes at least 3 weeks to completely replicate throughout a network
- C. Networks using Active Directory never use SAM databases so the SAM database pulled was empty
- D. The passwords that were cracked are local accounts on the Domain Controller

Answer: A

NEW QUESTION 752

.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your 312-49v9 Exam with Our Prep Materials Via below:

<https://www.certleader.com/312-49v9-dumps.html>