



EC-Council

Exam Questions 312-49v10

Computer Hacking Forensic Investigator (CHFI-v10)

About ExamBible

Your Partner of IT Exam

Found in 1998

ExamBible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, ExamBible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

NEW QUESTION 1

- (Exam Topic 3)

What malware analysis operation can the investigator perform using the jv16 tool?

- A. Files and Folder Monitor
- B. Installation Monitor
- C. Network Traffic Monitoring/Analysis
- D. Registry Analysis/Monitoring

Answer: D

NEW QUESTION 2

- (Exam Topic 3)

An 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. Integrated Circuit Code (ICC)
- C. Manufacturer Identification Code (MIC)
- D. Device Origin Code (DOC)

Answer: A

NEW QUESTION 3

- (Exam Topic 3)

Which type of attack is possible when attackers know some credible information about the victim's password, such as the password length, algorithms involved, or the strings and characters used in its creation?

- A. Rule-Based Attack
- B. Brute-Forcing Attack
- C. Dictionary Attack
- D. Hybrid Password Guessing Attack

Answer: A

NEW QUESTION 4

- (Exam Topic 3)

You need to deploy a new web-based software package for your organization. The package requires three separate servers and needs to be available on the Internet. What is the recommended architecture in terms of server placement?

- A. All three servers need to be placed internally
- B. A web server and the database server facing the Internet, an application server on the internal network
- C. A web server facing the Internet, an application server on the internal network, a database server on the internal network
- D. All three servers need to face the Internet so that they can communicate between themselves

Answer: D

NEW QUESTION 5

- (Exam Topic 3)

What does the 56.58.152.114(445) denote in a Cisco router log?

Jun 19 23:25:46.125 EST: %SEC-4-IPACCESSLOGP: list internet-inbound denied udp 67.124.115.35(8084)

-> 56.58.152.114(445), 1 packet

- A. Source IP address
- B. None of the above
- C. Login IP address
- D. Destination IP address

Answer: D

NEW QUESTION 6

- (Exam Topic 3)

Pick the statement which does not belong to the Rule 804. Hearsay Exceptions; Declarant Unavailable.

- A. Statement of personal or family history
- B. Prior statement by witness
- C. Statement against interest
- D. Statement under belief of impending death

Answer: D

NEW QUESTION 7

- (Exam Topic 3)

What value of the "Boot Record Signature" is used to indicate that the boot-loader exists?

- A. AA55
- B. 00AA
- C. AA00
- D. A100

Answer: A

NEW QUESTION 8

- (Exam Topic 3)

Steve, a forensic investigator, was asked to investigate an email incident in his organization. The organization has Microsoft Exchange Server deployed for email communications. Which among the following files will Steve check to analyze message headers, message text, and standard attachments?

- A. PUB.EDB
- B. PRIV.EDB
- C. PUB.STM
- D. PRIV.STM

Answer: B

NEW QUESTION 9

- (Exam Topic 3)

Which of these Windows utility help you to repair logical file system errors?

- A. Resource Monitor
- B. Disk cleanup
- C. Disk defragmenter
- D. CHKDSK

Answer: D

NEW QUESTION 10

- (Exam Topic 3)

Ron, a computer forensics expert, is investigating a case involving corporate espionage. He has recovered several mobile computing devices from the crime scene. One of the evidence that Ron possesses is a mobile phone from Nokia that was left in ON condition. Ron needs to recover the IMEI number of the device to establish the identity of the device owner. Which of the following key combinations can he use to recover the IMEI number?

- A. #*06*#
- B. *#06#
- C. #06#*
- D. *IMEI#

Answer: A

NEW QUESTION 10

- (Exam Topic 3)

Chong-lee, a forensics executive, suspects that a malware is continuously making copies of files and folders on a victim system to consume the available disk space. What type of test would confirm his claim?

- A. File fingerprinting
- B. Identifying file obfuscation
- C. Static analysis
- D. Dynamic analysis

Answer: A

NEW QUESTION 13

- (Exam Topic 3)

In which implementation of RAID will the image of a Hardware RAID volume be different from the image taken separately from the disks?

- A. RAID 1
- B. The images will always be identical because data is mirrored for redundancy
- C. RAID 0
- D. It will always be different

Answer: D

NEW QUESTION 18

- (Exam Topic 3)

Which of the following statements is TRUE about SQL Server error logs?

- A. SQL Server error logs record all the events occurred on the SQL Server and its databases
- B. Forensic investigator uses SQL Server Profiler to view error log files
- C. Error logs contain IP address of SQL Server client connections
- D. Trace files record, user-defined events, and specific system events

Answer: B

NEW QUESTION 23

- (Exam Topic 3)

What do you call the process in which an attacker uses magnetic field over the digital media device to delete any previously stored data?

- A. Disk deletion
- B. Disk cleaning
- C. Disk degaussing
- D. Disk magnetization

Answer: C

NEW QUESTION 27

- (Exam Topic 3)

Which component in the hard disk moves over the platter to read and write information?

- A. Actuator
- B. Spindle
- C. Actuator Axis
- D. Head

Answer: D

NEW QUESTION 32

- (Exam Topic 3)

POP3 is an Internet protocol, which is used to retrieve emails from a mail server. Through which port does an email client connect with a POP3 server?

- A. 110
- B. 143
- C. 25
- D. 993

Answer: A

NEW QUESTION 34

- (Exam Topic 3)

The MAC attributes are timestamps that refer to a time at which the file was last modified or last accessed or originally created. Which of the following file systems store MAC attributes in Coordinated Universal Time (UTC) format?

- A. File Allocation Table (FAT)
- B. New Technology File System (NTFS)
- C. Hierarchical File System (HFS)
- D. Global File System (GFS)

Answer: B

NEW QUESTION 39

- (Exam Topic 3)

Amber, a black hat hacker, has embedded malware into a small enticing advertisement and posted it on a popular ad-network that displays across various websites. What is she doing?

- A. Malvertising
- B. Compromising a legitimate site
- C. Click-jacking
- D. Spearphishing

Answer: A

NEW QUESTION 43

- (Exam Topic 3)

Gary, a computer technician, is facing allegations of abusing children online by befriending them and sending them illicit adult images from his office computer. What type of investigation does this case require?

- A. Administrative Investigation
- B. Criminal Investigation
- C. Both Criminal and Administrative Investigation
- D. Civil Investigation

Answer: B

NEW QUESTION 45

- (Exam Topic 3)

Which of the following Android libraries are used to render 2D (SGL) or 3D (OpenGL/ES) graphics content to the screen?

- A. OpenGL/ES and SGL
- B. Surface Manager
- C. Media framework
- D. WebKit

Answer: A

NEW QUESTION 49

- (Exam Topic 3)

Adam, a forensic analyst, is preparing VMs for analyzing a malware. Which of the following is NOT a best practice?

- A. Isolating the host device
- B. Installing malware analysis tools
- C. Using network simulation tools
- D. Enabling shared folders

Answer: D

NEW QUESTION 54

- (Exam Topic 3)

Which of the following Linux command searches through the current processes and lists the process IDs those match the selection criteria to stdout?

- A. pstree
- B. pgrep
- C. ps
- D. grep

Answer: B

NEW QUESTION 59

- (Exam Topic 3)

Data Files contain Multiple Data Pages, which are further divided into Page Header, Data Rows, and Offset Table. Which of the following is true for Data Rows?

- A. Data Rows store the actual data
- B. Data Rows present Page typ
- C. Page ID, and so on
- D. Data Rows point to the location of actual data
- E. Data Rows spreads data across multiple databases

Answer: B

NEW QUESTION 60

- (Exam Topic 3)

Which of the following statements is TRUE with respect to the Registry settings in the user start-up folder HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce\.

- A. All the values in this subkey run when specific user logs on, as this setting is user-specific
- B. The string specified in the value run executes when user logs on
- C. All the values in this key are executed at system start-up
- D. All values in this subkey run when specific user logs on and then the values are deleted

Answer: D

NEW QUESTION 64

- (Exam Topic 3)

An investigator has found certain details after analysis of a mobile device. What can reveal the manufacturer information?

- A. Equipment Identity Register (EIR)
- B. Electronic Serial Number (ESN)
- C. International mobile subscriber identity (IMSI)
- D. Integrated circuit card identifier (ICCID)

Answer: B

NEW QUESTION 66

- (Exam Topic 3)

James, a hacker, identifies a vulnerability in a website. To exploit the vulnerability, he visits the login page and notes down the session ID that is created. He appends this session ID to the login URL and shares the link with a victim. Once the victim logs into the website using the shared URL, James reloads the webpage (containing the URL with the session ID appended) and now, he can browse the active session of the victim. Which attack did James successfully execute?

- A. Cross Site Request Forgery
- B. Cookie Tampering
- C. Parameter Tampering
- D. Session Fixation Attack

Answer: D

NEW QUESTION 68

- (Exam Topic 3)

Jim's company regularly performs backups of their critical servers. But the company can't afford to send backup tapes to an off-site vendor for long term storage and archiving. Instead Jim's company keeps the backup tapes in a safe in the office. Jim's company is audited each year, and the results from this year's audit show a risk because backup tapes aren't stored off-site. The Manager of Information Technology has a plan to take the backup tapes home with him and wants to know what two things he can do to secure the backup tapes while in transit?

- A. Encrypt the backup tapes and use a courier to transport them.
- B. Encrypt the backup tapes and transport them in a lock box
- C. Degauss the backup tapes and transport them in a lock box.
- D. Hash the backup tapes and transport them in a lock box.

Answer: B

NEW QUESTION 69

- (Exam Topic 3)

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

- A. SmartWhois
- B. Deep Log Analyzer
- C. Towelroot
- D. XRY LOGICAL

Answer: A

NEW QUESTION 72

- (Exam Topic 3)

What is cold boot (hard boot)?

- A. It is the process of restarting a computer that is already in sleep mode
- B. It is the process of shutting down a computer from a powered-on or on state
- C. It is the process of restarting a computer that is already turned on through the operating system
- D. It is the process of starting a computer from a powered-down or off state

Answer: D

NEW QUESTION 77

- (Exam Topic 3)

What is the name of the first reserved sector in File allocation table?

- A. Volume Boot Record
- B. Partition Boot Sector
- C. Master Boot Record
- D. BIOS Parameter Block

Answer: C

NEW QUESTION 78

- (Exam Topic 3)

A Linux system is undergoing investigation. In which directory should the investigators look for its current state data if the system is in powered on state?

- A. /auth
- B. /proc
- C. /var/log/debug
- D. /var/spool/cron/

Answer: B

NEW QUESTION 83

- (Exam Topic 3)

Consider that you are investigating a machine running an Windows OS released prior to Windows Vista. You are trying to gather information about the deleted files by examining the master database file named INFO2 located at C:\Recycler\<USER SID>. You read an entry named "Dd5.exe". What does Dd5.exe mean?

- A. D driv
- B. fifth file deleted, a .exe file
- C. D drive, fourth file restored, a .exe file
- D. D drive, fourth file deleted, a .exe file
- E. D drive, sixth file deleted, a .exe file

Answer: B

NEW QUESTION 88

- (Exam Topic 3)

Which of the following is found within the unique instance ID key and helps investigators to map the entry from USBSTOR key to the MountedDevices key?

- A. ParentIDPrefix
- B. LastWrite
- C. UserAssist key
- D. MRUListEx key

Answer: A

NEW QUESTION 92

- (Exam Topic 3)

Lynne receives the following email:

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

- A. Mail Bombing
- B. Phishing
- C. Email Spamming
- D. Email Spoofing

Answer: B

NEW QUESTION 94

- (Exam Topic 3)

Hard disk data addressing is a method of allotting addresses to each _____ of data on a hard disk.

- A. Physical block
- B. Operating system block
- C. Hard disk block
- D. Logical block

Answer: A

NEW QUESTION 98

- (Exam Topic 3)

Which list contains the most recent actions performed by a Windows User?

- A. MRU
- B. Activity
- C. Recents
- D. Windows Error Log

Answer: A

NEW QUESTION 99

- (Exam Topic 3)

Checkpoint Firewall logs can be viewed through a Check Point Log viewer that uses icons and colors in the log table to represent different security events and their severity. What does the icon in the checkpoint logs represent?

- A. The firewall rejected a connection
- B. A virus was detected in an email
- C. The firewall dropped a connection
- D. An email was marked as potential spam

Answer: C

NEW QUESTION 101

- (Exam Topic 3)

During forensics investigations, investigators tend to collect the system time at first and compare it with UTC. What does the abbreviation UTC stand for?

- A. Coordinated Universal Time
- B. Universal Computer Time
- C. Universal Time for Computers
- D. Correlated Universal Time

Answer: A

NEW QUESTION 105

- (Exam Topic 3)

Jacob is a computer forensics investigator with over 10 years of 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's testimony in this case?

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

Answer: D

NEW QUESTION 106

- (Exam Topic 3)

Robert is a regional manager working in a reputed organization. One day, he suspected malware attack after unwanted programs started to popup after logging into his computer. The network administrator was called upon to trace out any intrusion on the computer and he/she finds that suspicious activity has taken place within Autostart locations. In this situation, which of the following tools is used by the network administrator to detect any intrusion on a system?

- A. Hex Editor
- B. Internet Evidence Finder
- C. Process Monitor
- D. Report Viewer

Answer: C

NEW QUESTION 110

- (Exam Topic 3)

If the partition size is 4 GB, each cluster will be 32 K. Even if a file needs only 10 K, the entire 32 K will be allocated, resulting in 22 K of _____ .

- A. Slack space
- B. Deleted space
- C. Sector space
- D. Cluster space

Answer: A

NEW QUESTION 112

- (Exam Topic 3)

In a computer that has Dropbox client installed, which of the following files related to the Dropbox client store information about local Dropbox installation and the Dropbox user account, along with email IDs linked with the account?

- A. config.db
- B. install.db
- C. sigstore.db
- D. filecache.db

Answer: A

NEW QUESTION 114

- (Exam Topic 3)

During the trial, an investigator observes that one of the principal witnesses is severely ill and cannot be present for the hearing. He decides to record the evidence and present it to the court. Under which rule should he present such evidence?

- A. Rule 1003: Admissibility of Duplicates
- B. Limited admissibility
- C. Locard's Principle
- D. Hearsay

Answer: B

NEW QUESTION 118

- (Exam Topic 3)

Which of the following network attacks refers to sending huge volumes of email to an address in an attempt to overflow the mailbox or overwhelm the server where the email address is hosted so as to cause a denial-of-service attack?

- A. Email spamming
- B. Phishing
- C. Email spoofing
- D. Mail bombing

Answer: D

NEW QUESTION 120

- (Exam Topic 3)

CAN-SPAM act requires that you:

- A. Don't use deceptive subject lines
- B. Don't tell the recipients where you are located
- C. Don't identify the message as an ad
- D. Don't use true header information

Answer: A

NEW QUESTION 122

- (Exam Topic 3)

Which Event Correlation approach assumes and predicts what an attacker can do next after the attack by studying statistics and probability?

- A. Profile/Fingerprint-Based Approach
- B. Bayesian Correlation

- C. Time (Clock Time) or Role-Based Approach
- D. Automated Field Correlation

Answer: B

NEW QUESTION 123

- (Exam Topic 3)

Which among the following U.S. laws requires financial institutions—companies that offer consumers financial products or services such as loans, financial or investment advice, or insurance—to protect their customers' information against security threats?

- A. SOX
- B. HIPAA
- C. GLBA
- D. FISMA

Answer: C

NEW QUESTION 124

- (Exam Topic 3)

Which of the following is a precomputed table containing word lists like dictionary files and brute force lists and their hash values?

- A. Directory Table
- B. Rainbow Table
- C. Master file Table (MFT)
- D. Partition Table

Answer: B

NEW QUESTION 129

- (Exam Topic 3)

In which cloud crime do attackers try to compromise the security of the cloud environment in order to steal data or inject a malware?

- A. Cloud as an Object
- B. Cloud as a Tool
- C. Cloud as an Application
- D. Cloud as a Subject

Answer: D

NEW QUESTION 134

- (Exam Topic 3)

In which registry does the system store the Microsoft security IDs?

- A. HKEY_CLASSES_ROOT (HKCR)
- B. HKEY_CURRENT_CONFIG (HKCC)
- C. HKEY_CURRENT_USER (HKCU)
- D. HKEY_LOCAL_MACHINE (HKLM)

Answer: D

NEW QUESTION 135

- (Exam Topic 3)

Smith is an IT technician that has been appointed to his company's network vulnerability assessment team. He is the only IT employee on the team. The other team members include employees from Accounting, Management, Shipping, and Marketing. Smith and the team members are having their first meeting to discuss how they will proceed. What is the first step they should do to create the network vulnerability assessment plan?

- A. Their first step is to make a hypothesis of what their final findings will be.
- B. Their first step is to create an initial Executive report to show the management team.
- C. Their first step is to analyze the data they have currently gathered from the company or interviews.
- D. Their first step is the acquisition of required documents, reviewing of security policies and compliance.

Answer: D

NEW QUESTION 139

- (Exam Topic 3)

An investigator has extracted the device descriptor for a 1GB thumb drive that looks like: Disk&Ven_Best_Buy&Prod_Geek_Squad_U3&Rev_6.15. What does the "Geek_Squad" part represent?

- A. Product description
- B. Manufacturer Details
- C. Developer description
- D. Software or OS used

Answer: A

NEW QUESTION 141

- (Exam Topic 3)

What does the command "C:\>wevtutil gl <log name>" display?

- A. Configuration information of a specific Event Log
- B. Event logs are saved in .xml format
- C. Event log record structure
- D. List of available Event Logs

Answer: A

NEW QUESTION 146

- (Exam Topic 3)

Which of the following standard represents a legal precedent set in 1993 by the Supreme Court of the United States regarding the admissibility of expert witnesses' testimony during federal legal proceedings?

- A. SWGDE & SWGIT
- B. IOCE
- C. Frye
- D. Daubert

Answer: D

NEW QUESTION 150

- (Exam Topic 3)

Which command line tool is used to determine active network connections?

- A. netsh
- B. nbstat
- C. nslookup
- D. netstat

Answer: D

NEW QUESTION 151

- (Exam Topic 3)

Select the tool appropriate for examining the dynamically linked libraries of an application or malware.

- A. DependencyWalker
- B. SysAnalyzer
- C. PEiD
- D. ResourcesExtract

Answer: A

NEW QUESTION 153

- (Exam Topic 3)

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

- A. Model.log
- B. Model.txt
- C. Model.ldf
- D. Model.lgf

Answer: C

NEW QUESTION 157

- (Exam Topic 3)

Which among the following tools can help a forensic investigator to access the registry files during postmortem analysis?

- A. RegistryChangesView
- B. RegDIIView
- C. RegRipper
- D. ProDiscover

Answer: C

NEW QUESTION 161

- (Exam Topic 3)

Which of the following statements is incorrect when preserving digital evidence?

- A. Verify if the monitor is in on, off, or in sleep mode
- B. Turn on the computer and extract Windows event viewer log files
- C. Remove the plug from the power router or modem
- D. Document the actions and changes that you observe in the monitor, computer, printer, or in other peripherals

Answer:

B

NEW QUESTION 166

- (Exam Topic 3)

Which among the following web application threats is resulted when developers expose various internal implementation objects, such as files, directories, database records, or key-through references?

- A. Remote File Inclusion
- B. Cross Site Scripting
- C. Insecure Direct Object References
- D. Cross Site Request Forgery

Answer: C

NEW QUESTION 169

- (Exam Topic 3)

The Recycle Bin exists as a metaphor for throwing files away, but it also allows a 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
- B. INFO1
- C. LOGINFO1
- D. LOGINFO2

Answer: A

NEW QUESTION 170

- (Exam Topic 3)

When a user deletes a file, the system creates a \$I file to store its details. What detail does the \$I file not contain?

- A. File Size
- B. File origin and modification
- C. Time and date of deletion
- D. File Name

Answer: B

NEW QUESTION 173

- (Exam Topic 3)

Event correlation is the process of finding relevance between the events that produce a final result. What type of correlation will help an organization to correlate events across a set of servers, systems, routers and network?

- A. Same-platform correlation
- B. Network-platform correlation
- C. Cross-platform correlation
- D. Multiple-platform correlation

Answer: C

NEW QUESTION 174

- (Exam Topic 3)

Which of the following registry hive gives the configuration information about which application was used to open various files on the system?

- A. HKEY_CLASSES_ROOT
- B. HKEY_CURRENT_CONFIG
- C. HKEY_LOCAL_MACHINE
- D. HKEY_USERS

Answer: A

NEW QUESTION 177

- (Exam Topic 3)

Robert, a cloud architect, received a huge bill from the cloud service provider, which usually doesn't happen. After analyzing the bill, he found that the cloud resource consumption was very high. He then examined the cloud server and discovered that a malicious code was running on the server, which was generating huge but harmless traffic from the server. This means that the server has been compromised by an attacker with the sole intention to hurt the cloud customer financially. Which attack is described in the above scenario?

- A. XSS Attack
- B. DDoS Attack (Distributed Denial of Service)
- C. Man-in-the-cloud Attack
- D. EDoS Attack (Economic Denial of Service)

Answer: B

NEW QUESTION 182

- (Exam Topic 3)

Which of the following is NOT an anti-forensics technique?

- A. Data Deduplication
- B. Steganography
- C. Encryption
- D. Password Protection

Answer: A

NEW QUESTION 185

- (Exam Topic 3)

Which of the following statements is true regarding SMTP Server?

- A. SMTP Server breaks the recipient's address into Recipient's name and his/her designation before passing it to the DNS Server
- B. SMTP Server breaks the recipient's address into Recipient's name and recipient's address before passing it to the DNS Server
- C. SMTP Server breaks the recipient's address into Recipient's name and domain name before passing it to the DNS Server
- D. SMTP Server breaks the recipient's address into Recipient's name and his/her initial before passing it to the DNS Server

Answer: C

NEW QUESTION 187

- (Exam Topic 3)

MAC filtering is a security access control methodology, where a _____ is assigned to each network card to determine access to the network.

- A. 48-bit address
- B. 24-bit address
- C. 16-bit address
- D. 32-bit address

Answer: A

NEW QUESTION 190

- (Exam Topic 3)

To reach a bank web site, the traffic from workstations must pass through a firewall. You have been asked to review the firewall configuration to ensure that workstations in network 10.10.10.0/24 can only reach the bank web site 10.20.20.1 using https. Which of the following firewall rules meets this requirement?

- A. if (source matches 10.10.10.0/24 and destination matches 10.20.20.1 and port matches 443) then permit
- B. if (source matches 10.10.10.0/24 and destination matches 10.20.20.1 and port matches 80 or 443) then permit
- C. if (source matches 10.10.10.0 and destination matches 10.20.20.1 and port matches 443) then permit

Answer: A

NEW QUESTION 195

- (Exam Topic 3)

Which among the following search warrants allows the first responder to search and seize the victim's computer components such as hardware, software, storage devices, and documentation?

- A. John Doe Search Warrant
- B. Citizen Informant Search Warrant
- C. Electronic Storage Device Search Warrant
- D. Service Provider Search Warrant

Answer: C

NEW QUESTION 197

- (Exam Topic 3)

Which tool allows dumping the contents of process memory without stopping the process?

- A. psdump.exe
- B. pmdump.exe
- C. processdump.exe
- D. pdump.exe

Answer: B

NEW QUESTION 202

- (Exam Topic 3)

Which of the following Windows-based tool displays who is logged onto a computer, either locally or remotely?

- A. Tokenmon
- B. PSLoggedon
- C. TCPView
- D. Process Monitor

Answer: B

NEW QUESTION 206

- (Exam Topic 3)

Which cloud model allows an investigator to acquire the instance of a virtual machine and initiate the forensics examination process?

- A. PaaS model
- B. IaaS model
- C. SaaS model
- D. SecaaS model

Answer: B

NEW QUESTION 211

- (Exam Topic 3)

Gary is checking for the devices connected to USB ports of a suspect system during an investigation. Select the appropriate tool that will help him document all the connected devices.

- A. DevScan
- B. Devcon
- C. fsutil
- D. Reg.exe

Answer: B

NEW QUESTION 216

- (Exam Topic 3)

Which program uses different techniques to conceal a malware's code, thereby making it difficult for security mechanisms to detect or remove it?

- A. Dropper
- B. Packer
- C. Injector
- D. Obfuscator

Answer: D

NEW QUESTION 219

- (Exam Topic 3)

Raw data acquisition format creates _____ of a data set or suspect drive.

- A. Segmented image files
- B. Simple sequential flat files
- C. Compressed image files
- D. Segmented files

Answer: B

NEW QUESTION 222

- (Exam Topic 3)

Which of the following is a tool to reset Windows admin password?

- A. R-Studio
- B. Windows Password Recovery Bootdisk
- C. Windows Data Recovery Software
- D. TestDisk for Windows

Answer: B

NEW QUESTION 226

- (Exam Topic 3)

In a Linux-based system, what does the command "Last -F" display?

- A. Login and logout times and dates of the system
- B. Last run processes
- C. Last functions performed
- D. Recently opened files

Answer: A

NEW QUESTION 229

- (Exam Topic 3)

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

Answer: A

NEW QUESTION 231

- (Exam Topic 3)

Which of the following protocols allows non-ASCII files, such as video, graphics, and audio, to be sent through the email messages?

- A. MIME
- B. BINHEX
- C. UT-16
- D. UUCODE

Answer: A

NEW QUESTION 235

- (Exam Topic 3)

What does Locard's Exchange Principle state?

- A. Any information of probative value that is either stored or transmitted in a digital form
- B. Digital evidence must have some characteristics to be disclosed in the court of law
- C. Anyone or anything, entering a crime scene takes something of the scene with them, and leaves something of themselves behind when they leave
- D. Forensic investigators face many challenges during forensics investigation of a digital crime, such as extracting, preserving, and analyzing the digital evidence

Answer: C

NEW QUESTION 237

- (Exam Topic 3)

Bob has encountered a system crash and has lost vital data stored on the hard drive of his Windows computer. He has no cloud storage or backup hard drives. He wants to recover all the data, which includes his personal photos, music, documents, videos, official emails, etc. Which of the following tools shall resolve Bob's purpose?

- A. Cain & Abel
- B. Recuva
- C. Xplico
- D. Colasoft's Capsa

Answer: B

NEW QUESTION 240

- (Exam Topic 3)

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

- A. Qualify you as an expert witness
- B. Read your curriculum vitae to the jury
- C. Engage in damage control
- D. Prove that the tools you used to conduct your examination are perfect

Answer: A

NEW QUESTION 241

- (Exam Topic 3)

Amelia has got an email from a well-reputed company stating in the subject line that she has won a prize money, whereas the email body says that she has to pay a certain amount for being eligible for the contest.

Which of the following acts does the email breach?

- A. CAN-SPAM Act
- B. HIPAA
- C. GLBA
- D. SOX

Answer: A

NEW QUESTION 243

- (Exam Topic 3)

As a part of the investigation, Caroline, a forensic expert, was assigned the task to examine the transaction logs pertaining to a database named Transfers. She used SQL Server Management Studio to collect the active transaction log files of the database. Caroline wants to extract detailed information on the logs, including AllocUnitId, page id, slot id, etc. Which of the following commands does she need to execute in order to extract the desired information?

- A. DBCC LOG(Transfers, 1)
- B. DBCC LOG(Transfers, 3)
- C. DBCC LOG(Transfers, 0)
- D. DBCC LOG(Transfers, 2)

Answer: D

NEW QUESTION 244

- (Exam Topic 3)

What does the Rule 101 of Federal Rules of Evidence states?

- A. Scope of the Rules, where they can be applied
- B. Purpose of the Rules
- C. Limited Admissibility of the Evidence
- D. Rulings on Evidence

Answer: A

NEW QUESTION 247

- (Exam Topic 3)

Which principle states that “anyone or anything, entering a crime scene takes something of the scene with them, and leaves something of themselves behind when they leave”?

- A. Locard's Exchange Principle
- B. Enterprise Theory of Investigation
- C. Locard's Evidence Principle
- D. Evidence Theory of Investigation

Answer: A

NEW QUESTION 250

- (Exam Topic 3)

Which of the following information is displayed when Netstat is used with -ano switch?

- A. Ethernet statistics
- B. Contents of IP routing table
- C. Details of routing table
- D. Details of TCP and UDP connections

Answer: D

NEW QUESTION 254

- (Exam Topic 3)

An investigator is analyzing a checkpoint firewall log and comes across symbols. What type of log is he looking at?

- A. Security event was monitored but not stopped
- B. Malicious URL detected
- C. An email marked as potential spam
- D. Connection rejected

Answer: C

NEW QUESTION 255

- (Exam Topic 2)

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 257

- (Exam Topic 2)

Which of the following attacks allows an attacker to access restricted directories, including application source code, configuration and critical system files, and to execute commands outside of the web server's root directory?

- A. Parameter/form tampering
- B. Unvalidated input
- C. Directory traversal
- D. Security misconfiguration

Answer: C

NEW QUESTION 259

- (Exam Topic 2)

Which of the following files gives information about the client sync sessions in Google Drive on Windows?

- A. sync_log.log
- B. Sync_log.log
- C. sync.log
- D. Sync.log

Answer: B

NEW QUESTION 262

- (Exam Topic 2)

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.

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 264

- (Exam Topic 2)

Which of the following tool creates a bit-by-bit image of an evidence media?

- A. Recuva
- B. FileMerlin
- C. AccessData FTK Imager
- D. Xplico

Answer: C

NEW QUESTION 266

- (Exam Topic 2)

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 271

- (Exam Topic 2)

What feature of Decryption Collection allows an investigator to crack a password as quickly as possible?

- A. Cracks every password in 10 minutes
- B. Distribute processing over 16 or fewer computers
- C. Support for Encrypted File System
- D. Support for MD5 hash verification

Answer: B

NEW QUESTION 276

- (Exam Topic 2)

What type of flash memory card comes in either Type I or Type II and consumes only five percent of the power required by small hard drives?

- A. SD memory
- B. CF memory
- C. MMC memory
- D. SM memory

Answer: B

NEW QUESTION 278

- (Exam Topic 2)

Which of the following are small pieces of data sent from a website and stored on the user's computer by the user's web browser to track, validate, and maintain specific user information?

- A. Temporary Files
- B. Open files
- C. Cookies
- D. Web Browser Cache

Answer: C

NEW QUESTION 279

- (Exam Topic 2)

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 280

- (Exam Topic 2)

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 284

- (Exam Topic 2)

Bob works as information security analyst for a big finance company. One day, the anomaly-based intrusion detection system alerted that a volumetric DDOS targeting the main IP of the main web server was occurring. What kind of attack is it?

- A. IDS attack
- B. APT
- C. Web application attack
- D. Network attack

Answer: D

NEW QUESTION 289

- (Exam Topic 2)

What file is processed at the end of a Windows XP boot to initialize the logon dialog box?

- A. NTOSKRNL.EXE
- B. NTLDR
- C. LSASS.EXE
- D. NTDETECT.COM

Answer: A

NEW QUESTION 290

- (Exam Topic 2)

What encryption technology is used on Blackberry devices Password Keeper?

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

Answer: B

NEW QUESTION 292

- (Exam Topic 2)

Which of the following commands shows you all of the network services running on Windows-based servers?

- A. Netstart
- B. Net Session
- C. Net use
- D. Net config

Answer: A

NEW QUESTION 295

- (Exam Topic 2)

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 all internal MAC address from using SNMP
- B. Block access to UDP port 171
- C. Block access to TCP port 171
- D. Change the default community string names

Answer: D

NEW QUESTION 298

- (Exam Topic 2)

What will the following Linux command accomplish? `dd if=/dev/mem of=/home/sam/mem.bin bs=1024`

- A. Copy the master boot record to a file
- B. Copy the contents of the system folder to a file
- C. Copy the running memory to a file
- D. Copy the memory dump file to an image file

Answer: C

NEW QUESTION 299

- (Exam Topic 2)

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 303

- (Exam Topic 2)

Julie is a college student majoring in Information Systems and Computer Science. She is currently writing an essay for her computer crimes class. Julie paper focuses on white-collar crimes in America and how forensics investigators investigate the cases. Julie would like to focus the subject. Julie would like to focus the

subject of the essay on the most common type of crime found in corporate America. What crime should Julie focus on?

- A. Physical theft
- B. Copyright infringement
- C. Industrial espionage
- D. Denial of Service attacks

Answer: C

NEW QUESTION 307

- (Exam Topic 2)

Which of the following commands shows you the names of all open shared files on a server and the number of file locks on each file?

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

Answer: B

NEW QUESTION 312

- (Exam Topic 2)

Paraben Lockdown device uses which operating system to write hard drive data?

- A. Mac OS
- B. Red Hat
- C. Unix
- D. Windows

Answer: D

NEW QUESTION 314

- (Exam Topic 2)

Which code does the FAT file system use to mark the file as deleted?

- A. ESH
- B. 5EH
- C. H5E
- D. E5H

Answer: D

NEW QUESTION 316

- (Exam Topic 2)

What will the following command accomplish? `dd if=/dev/xxx of=mbr.backup bs=512 count=1`

- A. Back up the master boot record
- B. Restore the master boot record
- C. Mount the master boot record on the first partition of the hard drive
- D. Restore the first 512 bytes of the first partition of the hard drive

Answer: A

NEW QUESTION 317

- (Exam Topic 2)

Which of the following standard represents a legal precedent sent in 1993 by the Supreme Court of the United States regarding the admissibility of expert witnesses' testimony during federal legal proceedings?

- A. IOCE
- B. SWGDE & SWGIT
- C. Frye
- D. Daubert

Answer: D

NEW QUESTION 318

- (Exam Topic 2)

Which of the following files DOES NOT use Object Linking and Embedding (OLE) technology to embed and link to other objects?

- A. Portable Document Format
- B. MS-office Word Document
- C. MS-office Word OneNote
- D. MS-office Word PowerPoint

Answer: A

NEW QUESTION 320

- (Exam Topic 2)

Pagefile.sys is a virtual memory file used to expand the physical memory of a computer. Select the registry path for the page file:

- A. HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management
- B. HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\System Management
- C. HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Device Management
- D. HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management\PrefetchParameters

Answer: A

NEW QUESTION 324

- (Exam Topic 2)

An executive has leaked the company trade secrets through an external drive. What process should the investigation team take if they could retrieve his system?

- A. Postmortem Analysis
- B. Real-Time Analysis
- C. Packet Analysis
- D. Malware Analysis

Answer: A

NEW QUESTION 326

- (Exam Topic 2)

What does the 63.78.199.4(161) denotes in a Cisco router log?

Mar 14 22:57:53.425 EST: %SEC-6-IPACCESSLOGP: list internet-inbound denied udp 66.56.16.77(1029) -> 63.78.199.4(161), 1 packet

- A. Destination IP address
- B. Source IP address
- C. Login IP address
- D. None of the above

Answer: A

NEW QUESTION 330

- (Exam Topic 2)

Which of the following refers to the process of the witness being questioned by the attorney who called the latter to the stand?

- A. Witness Authentication
- B. Direct Examination
- C. Expert Witness
- D. Cross Questioning

Answer: B

NEW QUESTION 334

- (Exam Topic 2)

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

- A. Domain Controller
- B. Firewall
- C. SIEM
- D. IDS

Answer: C

NEW QUESTION 339

- (Exam Topic 2)

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 341

- (Exam Topic 2)

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 342

- (Exam Topic 2)

What must be obtained before an investigation is carried out at a location?

- A. Search warrant
- B. Subpoena
- C. Habeas corpus
- D. Modus operandi

Answer: A

NEW QUESTION 343

- (Exam Topic 2)

Who is responsible for the following tasks?

- A. Non-forensics staff
- B. Lawyers
- C. System administrators
- D. Local managers or other non-forensic staff

Answer: A

NEW QUESTION 346

- (Exam Topic 2)

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 350

- (Exam Topic 2)

Which of the following files stores information about local Dropbox installation and account, email IDs linked with the account, current version/build for the local application, the host_id, and local path information?

- A. host.db
- B. sigstore.db
- C. config.db
- D. filecache.db

Answer: C

NEW QUESTION 355

- (Exam Topic 2)

What is the location of the binary files required for the functioning of the OS in a Linux system?

- A. /run
- B. /bin
- C. /root
- D. /sbin

Answer: B

NEW QUESTION 358

- (Exam Topic 2)

Which rule requires an original recording to be provided to prove the content of a recording?

- A. 1004
- B. 1002
- C. 1003
- D. 1005

Answer: B

NEW QUESTION 362

- (Exam Topic 2)

What does the part of the log, "% SEC-6-IPACCESSLOGP", extracted from a Cisco router represent?

- A. The system was not able to process the packet because there was not enough room for all of the desired IP header options
- B. Immediate action required messages
- C. Some packet-matching logs were missed because the access list log messages were rate limited, or no access list log buffers were available
- D. A packet matching the log criteria for the given access list has been detected (TCP or UDP)

Answer: D

NEW QUESTION 367

- (Exam Topic 2)

In the following directory listing,

Which file should be used to restore archived email messages for someone using Microsoft Outlook?

- A. Outlook bak
- B. Outlook ost
- C. Outlook NK2
- D. Outlook pst

Answer: D

NEW QUESTION 371

- (Exam Topic 2)

Which of the following options will help users to enable or disable the last access time on a system running Windows 10 OS?

- A. wmic service
- B. Reg.exe
- C. fsutil
- D. Devcon

Answer: C

NEW QUESTION 374

- (Exam Topic 2)

When carrying out a forensics investigation, why should you never delete a partition on a dynamic disk?

- A. All virtual memory will be deleted
- B. The wrong partition may be set to active
- C. This action can corrupt the disk
- D. The computer will be set in a constant reboot state

Answer: C

NEW QUESTION 377

- (Exam Topic 2)

What feature of Windows is the following command trying to utilize?

- A. White space
- B. AFS
- C. ADS
- D. Slack file

Answer: C

NEW QUESTION 379

- (Exam Topic 2)

Which among the following files provides email header information in the Microsoft Exchange server?

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

Answer: B

NEW QUESTION 382

- (Exam Topic 2)

Adam, a forensic investigator, is investigating an attack on Microsoft Exchange Server of a large organization. As the first step of the investigation, he examined the PRIV.EDB file and found the source from where the mail originated and the name of the file that disappeared upon execution. Now, he wants to examine the MIME stream content. Which of the following files is he going to examine?

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

Answer: A

NEW QUESTION 387

- (Exam Topic 2)

Which network attack is described by the following statement?

“At least five Russian major banks came under a continuous hacker attack, although online client services were not disrupted. The attack came from a wide-scale botnet involving at least 24,000 computers, located in 30 countries.”

- A. DDoS
- B. Sniffer Attack
- C. Buffer Overflow
- D. Man-in-the-Middle Attack

Answer: A

NEW QUESTION 389

- (Exam Topic 2)

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 391

- (Exam Topic 2)

Smith, a forensic examiner, was analyzing a hard disk image to find and acquire deleted sensitive files. He stumbled upon a \$Recycle.Bin folder in the root directory of the disk. Identify the operating system in use.

- A. Windows 98
- B. Linux
- C. Windows 8.1
- D. Windows XP

Answer: D

NEW QUESTION 396

- (Exam Topic 2)

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

- A. 202
- B. 404
- C. 606
- D. 999

Answer: B

NEW QUESTION 398

- (Exam Topic 2)

What is one method of bypassing a system BIOS password?

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

Answer: B

NEW QUESTION 400

- (Exam Topic 2)

When a user deletes a file or folder, the system stores complete path including the original filename in a special hidden file called "INFO2" in the Recycled folder. If the INFO2 file is deleted, it is recovered when you _____.

- A. Undo the last action performed on the system
- B. Reboot Windows
- C. Use a recovery tool to undelete the file
- D. Download the file from Microsoft website

Answer: A

NEW QUESTION 404

- (Exam Topic 2)

What is considered a grant of a property right given to an individual who discovers or invents a new machine, process, useful composition of matter or manufacture?

- A. Copyright
- B. Design patent
- C. Trademark
- D. Utility patent

Answer: D

NEW QUESTION 406

- (Exam Topic 2)

Which of the following tasks DOES NOT come under the investigation phase of a cybercrime forensics investigation case?

- A. Data collection
- B. Secure the evidence
- C. First response
- D. Data analysis

Answer: C

NEW QUESTION 407

- (Exam Topic 2)

In Steganalysis, which of the following describes a Known-stego attack?

- A. The hidden message and the corresponding stego-image are known
- B. During the communication process, active attackers can change cover
- C. Original and stego-object are available and the steganography algorithm is known
- D. Only the steganography medium is available for analysis

Answer: C

NEW QUESTION 412

- (Exam Topic 2)

Which network attack is described by the following statement? "At least five Russian major banks came under a continuous hacker attack, although online client services were not disrupted. The attack came from a wide-scale botnet involving at least 24,000 computers, located in 30 countries."

- A. Man-in-the-Middle Attack
- B. Sniffer Attack
- C. Buffer Overflow
- D. DDoS

Answer: D

NEW QUESTION 414

- (Exam Topic 2)

What is the primary function of the tool CHKDSK in Windows that authenticates the file system reliability of a volume?

- A. Repairs logical file system errors
- B. Check the disk for hardware errors
- C. Check the disk for connectivity errors
- D. Check the disk for Slack Space

Answer: A

NEW QUESTION 415

- (Exam Topic 2)

Which of the following acts as a network intrusion detection system as well as network intrusion prevention system?

- A. Accunetix
- B. Nikto
- C. Snort
- D. Kismet

Answer: C

NEW QUESTION 419

- (Exam Topic 2)

When is it appropriate to use computer forensics?

- A. If copyright and intellectual property theft/misuse has occurred
- B. If employees do not care for their boss management techniques
- C. If sales drop off for no apparent reason for an extended period of time
- D. If a financial institution is burglarized by robbers

Answer: A

NEW QUESTION 422

- (Exam Topic 2)

Which of the following data structures stores attributes of a process, as well as pointers to other attributes and data structures?

- A. Lsproc
- B. DumpChk
- C. RegEdit
- D. EProcess

Answer: D

NEW QUESTION 425

- (Exam Topic 2)

A small law firm located in the Midwest has possibly been breached by a computer hacker looking to obtain information on their clientele. The law firm does not have any on-site IT employees, but wants to search for evidence of the breach themselves to prevent any possible media attention. Why would this not be recommended?

- A. Searching for evidence themselves would not have any ill effects
- B. Searching could possibly crash the machine or device
- C. Searching creates cache files, which would hinder the investigation
- D. Searching can change date/time stamps

Answer: D

NEW QUESTION 427

- (Exam Topic 2)

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 430

- (Exam Topic 2)

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

- A. Net sessions
- B. Net config
- C. Net share
- D. Net use

Answer: D

NEW QUESTION 432

- (Exam Topic 2)

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?

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

Answer: D

NEW QUESTION 434

- (Exam Topic 2)

What does 254 represent in ICCID 89254021520014515744?

- A. Industry Identifier Prefix
- B. Country Code
- C. Individual Account Identification Number
- D. Issuer Identifier Number

Answer: B

NEW QUESTION 436

- (Exam Topic 2)

To which phase of the Computer Forensics Investigation Process does the Planning and Budgeting of a Forensics Lab belong?

- A. Post-investigation Phase
- B. Reporting Phase
- C. Pre-investigation Phase
- D. Investigation Phase

Answer: C

NEW QUESTION 438

- (Exam Topic 2)

The investigator wants to examine changes made to the system's registry by the suspect program. Which of the following tool can help the investigator?

- A. TRIPWIRE
- B. RAM Capturer
- C. Regshot
- D. What's Running

Answer: C

NEW QUESTION 443

- (Exam Topic 2)

Annie is searching for certain deleted files on a system running Windows XP OS. Where will she find the files if they were not completely deleted from the system?

- A. C: \$Recycled.Bin
- B. C: \Recycle.Bin
- C. C:\RECYCLER
- D. C:\\$RECYCLER

Answer: B

NEW QUESTION 448

- (Exam Topic 2)

John is working on his company policies and guidelines. The section he is currently working on covers company documents; how they should be handled, stored, and eventually destroyed. John is concerned about the process whereby outdated documents are destroyed. What type of shredder should John write in the guidelines to be used when destroying documents?

- A. Strip-cut shredder
- B. Cross-cut shredder
- C. Cross-hatch shredder
- D. Cris-cross shredder

Answer: B

NEW QUESTION 453

- (Exam Topic 2)

What is the smallest physical storage unit on a hard drive?

- A. Track
- B. Cluster
- C. Sector

D. Platter

Answer: C

NEW QUESTION 458

- (Exam Topic 2)

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 them
- D. Only FAT system contains RECYCLED folder and not NTFS

Answer: C

NEW QUESTION 461

- (Exam Topic 2)

What is the default IIS log location?

- A. SystemDrive\inetpub\LogFiles
- B. %SystemDrive%\inetpub\logs\LogFiles
- C. %SystemDrive%\logs\LogFiles
- D. SystemDrive\logs\LogFiles

Answer: B

NEW QUESTION 463

- (Exam Topic 2)

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 464

- (Exam Topic 2)

How often must a company keep log files for them to be admissible in a court of law?

- A. All log files are admissible in court no matter their frequency
- B. Weekly
- C. Monthly
- D. Continuously

Answer: D

NEW QUESTION 468

- (Exam Topic 2)

When searching through file headers for picture file formats, what should be searched to find a JPEG file in hexadecimal format?

- A. FF D8 FF E0 00 10
- B. FF FF FF FF FF FF
- C. FF 00 FF 00 FF 00
- D. EF 00 EF 00 EF 00

Answer: A

NEW QUESTION 472

- (Exam Topic 2)

Which of the following tool enables a user to reset his/her lost admin password in a Windows system?

- A. Advanced Office Password Recovery
- B. Active@ Password Changer
- C. Smartkey Password Recovery Bundle Standard
- D. Passware Kit Forensic

Answer: B

NEW QUESTION 473

- (Exam Topic 2)

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: D

NEW QUESTION 475

- (Exam Topic 2)

Jacky encrypts her documents using a password. It is known that she uses her daughter's year of birth as part of the password. Which password cracking technique would be optimal to crack her password?

- A. Rule-based attack
- B. Brute force attack
- C. Syllable attack
- D. Hybrid attack

Answer: A

NEW QUESTION 478

- (Exam Topic 2)

What layer of the OSI model do TCP and UDP utilize?

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

Answer: C

NEW QUESTION 482

- (Exam Topic 2)

Which of the following is a list of recently used programs or opened files?

- A. Most Recently Used (MRU)
- B. Recently Used Programs (RUP)
- C. Master File Table (MFT)
- D. GUID Partition Table (GPT)

Answer: A

NEW QUESTION 486

- (Exam Topic 2)

Which among the following search warrants allows the first responder to get the victim's computer information such as service records, billing records, and subscriber information from the service provider?

- A. Citizen Informant Search Warrant
- B. Electronic Storage Device Search Warrant
- C. John Doe Search Warrant
- D. Service Provider Search Warrant

Answer: B

NEW QUESTION 489

- (Exam Topic 2)

Which of the following techniques can be used to beat steganography?

- A. Encryption
- B. Steganalysis
- C. Decryption
- D. Cryptanalysis

Answer: B

NEW QUESTION 492

- (Exam Topic 2)

Jack Smith is a forensics investigator who works for Mason Computer Investigation Services. He is investigating a computer that was infected by Ramen Virus.

He runs the netstat command on the machine to see its current connections. In the following screenshot, what do the 0.0.0.0 IP addresses signify?

- A. Those connections are established
- B. Those connections are in listening mode
- C. Those connections are in closed/waiting mode
- D. Those connections are in timed out/waiting mode

Answer: B

NEW QUESTION 493

- (Exam Topic 2)

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 496

- (Exam Topic 2)

Smith, as a part his forensic investigation assignment, seized a mobile device. He was asked to recover the Subscriber Identity Module (SIM card) data in 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 made three unsuccessful attempts, which blocked the SIM card. What can Jason do in this scenario to reset the PIN and access SIM data?

- A. He should contact the network operator for a Temporary Unlock Code (TUK)
- B. Use system and hardware tools to gain access
- C. He can attempt PIN guesses after 24 hours
- D. He should contact the network operator for Personal Unlock Number (PUK)

Answer: D

NEW QUESTION 500

- (Exam Topic 2)

Which of the following files stores information about a local Google Drive installation such as User email ID, Local Sync Root Path, and Client version installed?

- A. filecache.db
- B. config.db
- C. sigstore.db
- D. Sync_config.db

Answer: D

NEW QUESTION 501

- (Exam Topic 2)

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 502

- (Exam Topic 2)

When a router receives an update for its routing table, what is the metric value change to that path?

- A. Increased by 2
- B. Decreased by 1
- C. Increased by 1
- D. Decreased by 2

Answer: C

NEW QUESTION 504

- (Exam Topic 2)

If you are concerned about a high level of compression but not concerned about any possible data loss, what type of compression would you use?

- A. Lossful compression
- B. Lossy compression
- C. Lossless compression
- D. Time-loss compression

Answer: B

NEW QUESTION 508

- (Exam Topic 2)

Which of the following is an iOS Jailbreaking tool?

- A. Kingo Android ROOT
- B. Towelroot
- C. One Click Root

D. Redsn0w

Answer: D

NEW QUESTION 509

- (Exam Topic 2)

Paul is a computer forensics investigator working for Tyler & Company Consultants. Paul has been called upon to help investigate a computer hacking ring broken up by the local police. Paul begins to inventory the PCs found in the hackers hideout. Paul then comes across a PDA left by them that is attached to a number of different peripheral devices. What is the first step that Paul must take with the PDA to ensure the integrity of the investigation?

- A. Place PDA, including all devices, in an antistatic bag
- B. Unplug all connected devices
- C. Power off all devices if currently on
- D. Photograph and document the peripheral devices

Answer: D

NEW QUESTION 512

- (Exam Topic 2)

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 515

- (Exam Topic 2)

What type of equipment would a forensics investigator store in a StrongHold bag?

- A. PDAPDA?
- B. Backup tapes
- C. Hard drives
- D. Wireless cards

Answer: D

NEW QUESTION 516

- (Exam Topic 2)

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 the company 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 521

- (Exam Topic 2)

Bob has encountered a system crash and has lost vital data stored on the hard drive of his Windows computer. He has no cloud storage or backup hard drives. he wants to recover all those data, which includes his personal photos, music, documents, videos, official email, etc. Which of the following tools shall resolve Bob's purpose?

- A. Colasoft's Capsa
- B. Recuva
- C. Cain & Abel
- D. Xplico

Answer: D

NEW QUESTION 522

- (Exam Topic 2)

What hashing method is used to password protect Blackberry devices?

- A. AES
- B. RC5
- C. MD5
- D. SHA-1

Answer: D

NEW QUESTION 525

- (Exam Topic 2)

Watson, a forensic investigator, is examining a copy of an ISO file stored in CDFS format. What type of evidence is this?

- A. Data from a CD copied using Windows
- B. Data from a CD copied using Mac-based system
- C. Data from a DVD copied using Windows system
- D. Data from a CD copied using Linux system

Answer: A

NEW QUESTION 530

- (Exam Topic 2)

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 535

- (Exam Topic 2)

Which password cracking technique uses details such as length of password, character sets used to construct the password, etc.?

- A. Dictionary attack
- B. Brute force attack
- C. Rule-based attack
- D. Man in the middle attack

Answer: A

NEW QUESTION 537

- (Exam Topic 1)

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. Because 70% of attacks are from inside the organization
- C. To attack a network from a hacker's perspective
- D. It is easier to hack from the inside

Answer: B

NEW QUESTION 540

- (Exam Topic 1)

Why are Linux/Unix based computers better to use than Windows computers for idle scanning?

- A. Linux/Unix computers are easier to compromise
- B. Linux/Unix computers are constantly talking
- C. Windows computers are constantly talking
- D. Windows computers will not respond to idle scans

Answer: C

NEW QUESTION 541

- (Exam Topic 1)

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 respond 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. A switched network will not respond to packets sent to the broadcast address
- D. Only Unix and Unix-like systems will reply to this scan

Answer: D

NEW QUESTION 544

- (Exam Topic 1)

You are a security analyst performing a penetration tests for a company in the Midwest. After some initial reconnaissance, you discover the IP addresses of some Cisco routers used by the company. You type in the following URL that includes the IP address of one of the routers:

`http://172.168.4.131/level/99/exec/show/config`

After typing in this URL, you are presented with the entire configuration file for that router. What have you discovered?

- A. HTTP Configuration Arbitrary Administrative Access Vulnerability
- B. HTML Configuration Arbitrary Administrative Access Vulnerability

- C. Cisco IOS Arbitrary Administrative Access Online Vulnerability
- D. URL Obfuscation Arbitrary Administrative Access Vulnerability

Answer: A

NEW QUESTION 548

- (Exam Topic 1)

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: A

NEW QUESTION 553

- (Exam Topic 1)

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 554

- (Exam Topic 1)

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

- A. Clusters
- B. Drives
- C. Bitstreams
- D. Partitions

Answer: A

NEW QUESTION 559

- (Exam Topic 1)

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

Answer: C

NEW QUESTION 561

- (Exam Topic 1)

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

Answer: D

NEW QUESTION 564

- (Exam Topic 1)

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

Answer: D

NEW QUESTION 567

- (Exam Topic 1)

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 571

- (Exam Topic 1)

Which of the following is NOT a graphics file?

- A. Picture1.tga
- B. Picture2.bmp
- C. Picture3.nfo
- D. Picture4.psd

Answer: C

NEW QUESTION 575

- (Exam Topic 1)

Windows identifies which application to open a file with by examining which of the following?

- A. The File extension
- B. The file attributes
- C. The file Signature at the end of the file
- D. The file signature at the beginning of the file

Answer: A

NEW QUESTION 578

- (Exam Topic 1)

The objective of this act was to protect consumers' personal financial information held by financial institutions and their service providers.

- A. Gramm-Leach-Bliley Act
- B. Sarbanes-Oxley 2002
- C. California SB 1386
- D. HIPAA

Answer: A

NEW QUESTION 582

- (Exam Topic 1)

If an attacker's computer sends an IPID of 31400 to a zombie computer on an open port in IDLE scanning, what will be the response?

- A. The zombie will not send a response
- B. 31402
- C. 31399
- D. 31401

Answer: D

NEW QUESTION 587

- (Exam Topic 1)

You are assisting a Department of Defense contract company to become compliant with the stringent security policies set by the DoD. One such strict rule is that firewalls must only allow incoming connections that were first initiated by internal computers. What type of firewall must you implement to abide by this policy?

- A. Packet filtering firewall
- B. Circuit-level proxy firewall
- C. Application-level proxy firewall
- D. Stateful firewall

Answer: D

NEW QUESTION 592

- (Exam Topic 1)

Office documents (Word, Excel, PowerPoint) contain a code that allows tracking the MAC, or unique identifier, of the machine that created the document. What is that code called?

- A. the Microsoft Virtual Machine Identifier
- B. the Personal Application Protocol
- C. the Globally Unique ID
- D. the Individual ASCII String

Answer: C

NEW QUESTION 597

- (Exam Topic 1)

Printing under a Windows Computer normally requires which one of the following files types to be created?

- A. EME
- B. MEM
- C. EMF
- D. CME

Answer: C

NEW QUESTION 598

- (Exam Topic 1)

You are working for a large clothing manufacturer as a computer forensics investigator and are called in to investigate an unusual case of an employee possibly stealing clothing designs from the company and selling them under a different brand name for a different company. What you discover during the course of the investigation is that the clothing designs are actually original products of the employee and the company has no policy against an employee selling his own designs on his own time. The only thing that you can find that the employee is doing wrong is that his clothing design incorporates the same graphic symbol as that of the company with only the wording in the graphic being different. What area of the law is the employee violating?

- A. trademark law
- B. copyright law
- C. printright law
- D. landmark law

Answer: A

NEW QUESTION 599

- (Exam Topic 1)

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

NEW QUESTION 601

- (Exam Topic 1)

What is kept in the following directory? HKLM\SECURITY\Policy\Secrets

- A. Cached password hashes for the past 20 users
- B. Service account passwords in plain text
- C. IAS account names and passwords
- D. Local store PKI Kerberos certificates

Answer: B

NEW QUESTION 602

- (Exam Topic 1)

Item 2If you come across a sheepdip machine at your client site, what would you infer?

- A. A sheepdip coordinates several honeypots
- B. A sheepdip computer is another name for a honeypot
- C. A sheepdip computer is used only for virus-checking.
- D. A sheepdip computer defers a denial of service attack

Answer: C

NEW QUESTION 605

- (Exam Topic 1)

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 606

- (Exam Topic 1)

Paul's company is in the process of undergoing a complete security audit including logical and physical security testing. After all logical tests were performed; it is now time for the physical round to begin. None of the employees are made aware of this round of testing. The security-auditing firm sends in a technician dressed as an electrician. He waits outside in the lobby for some employees to get to work and follows behind them when they access the restricted areas. After entering the main office, he is able to get into the server room telling the IT manager that there is a problem with the outlets in that room. What type of attack has the technician performed?

- A. Tailgating
- B. Backtrapping
- C. Man trap attack
- D. Fuzzing

Answer: A

NEW QUESTION 610

- (Exam Topic 1)

Harold wants to set up a firewall on his network but is not sure which one would be the most appropriate. He knows he needs to allow FTP traffic to one of the servers on his network, but he wants to only allow FTP-PUT. Which firewall would be most appropriate for Harold? needs?

- A. Circuit-level proxy firewall
- B. Packet filtering firewall
- C. Application-level proxy firewall
- D. Data link layer firewall

Answer: C

NEW QUESTION 612

- (Exam Topic 1)

What does ICMP Type 3/Code 13 mean?

- A. Host Unreachable
- B. Administratively Blocked
- C. Port Unreachable
- D. Protocol Unreachable

Answer: B

NEW QUESTION 616

- (Exam Topic 1)

When investigating a Windows System, it is important to view the contents of the page or swap file because:

- A. Windows stores all of the systems configuration information in this file
- B. This is file that windows use to communicate directly with Registry
- C. A Large volume of data can exist within the swap file of which the computer user has no knowledge
- D. This is the file that windows use to store the history of the last 100 commands that were run from the command line

Answer: C

NEW QUESTION 617

- (Exam Topic 1)

The efforts to obtain information before a trial by demanding documents, depositions, questioned 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 622

- (Exam Topic 1)

What operating system would respond to the following command?

- A. Windows 95
- B. FreeBSD
- C. Windows XP
- D. Mac OS X

Answer: B

NEW QUESTION 624

- (Exam Topic 1)

Office Documents (Word, Excel and PowerPoint) contain a code that allows tracking the MAC or unique identifier of the machine that created the document. What

is that code called?

- A. Globally unique ID
- B. Microsoft Virtual Machine Identifier
- C. Personal Application Protocol
- D. Individual ASCII string

Answer: A

NEW QUESTION 626

- (Exam Topic 1)

What will the following command accomplish?

- A. Test ability of a router to handle over-sized packets
- B. Test the ability of a router to handle under-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: A

NEW QUESTION 627

- (Exam Topic 1)

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. udp port 22 and host 172.16.28.1/24
- C. net port 22
- D. src port 22 and dst port 22

Answer: D

NEW QUESTION 629

- (Exam Topic 1)

Sectors in hard disks typically contain how many bytes?

- A. 256
- B. 512
- C. 1024
- D. 2048

Answer: B

NEW QUESTION 633

- (Exam Topic 1)

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

Answer: B

NEW QUESTION 634

- (Exam Topic 1)

You are working in the security Department of law firm. One of the attorneys asks you about the topic of sending fake email because he has a client who has been charged with doing just that. His client alleges that he is innocent and that there is no way for a fake email to actually be sent. You inform the attorney that his client is mistaken and that fake email is possibility and that you can prove it. You return to your desk and craft a fake email to the attorney that appears to come from his boss. What port do you send the email to on the company SMTP server?

- A. 10
- B. 25
- C. 110
- D. 135

Answer: B

NEW QUESTION 639

- (Exam Topic 1)

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 printer 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 640

- (Exam Topic 1)

Which of the following file system is used by Mac OS X?

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

Answer: B

NEW QUESTION 645

- (Exam Topic 1)

The police believe that Melvin 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 suspects door and searching his home and seizing all of his computer equipment if they have not yet obtained a warrant?

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

Answer: A

NEW QUESTION 648

- (Exam Topic 1)

To make sure the evidence you recover and analyze with computer forensics software can be admitted in court, you must test and validate the software. What group is actively providing tools and creating procedures for testing and validating computer forensics software?

- A. Computer Forensics Tools and Validation Committee (CFTVC)
- B. Association of Computer Forensics Software Manufactures (ACFSM)
- C. National Institute of Standards and Technology (NIST)
- D. Society for Valid Forensics Tools and Testing (SVFTT)

Answer: C

NEW QUESTION 650

- (Exam Topic 1)

You are working as a Computer forensics investigator for a corporation on a computer abuse case. You discover evidence that shows the subject of your investigation is also embezzling money from the company. The company CEO and the corporate legal counsel advise you to contact law enforcement and provide them with the evidence that you have found. The law enforcement officer that responds requests that you put a network sniffer on your network and monitor all traffic to the subject's computer. You inform the officer that you will not be able to comply with that request because doing so would:

- A. Violate your contract
- B. Cause network congestion
- C. Make you an agent of law enforcement
- D. Write information to the subject's hard drive

Answer: C

NEW QUESTION 654

- (Exam Topic 1)

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

NEW QUESTION 658

- (Exam Topic 1)

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, "no comment"
- C. Answer all the reporter's questions as completely as possible

D. Answer only the questions that help your case

Answer: A

NEW QUESTION 659

- (Exam Topic 1)

Larry is an IT consultant who works for corporations and government agencies. Larry plans on shutting down the city's network using BGP devices and zombies? What type of Penetration Testing is Larry planning to carry out?

- A. Router Penetration Testing
- B. DoS Penetration Testing
- C. Firewall Penetration Testing
- D. Internal Penetration Testing

Answer: B

NEW QUESTION 662

- (Exam Topic 1)

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

Answer: A

NEW QUESTION 664

- (Exam Topic 1)

You have been asked to investigate after a user has reported a threatening e-mail they have received from an external source. Which of the following are you most interested in when trying to trace the source of the message?

- A. The X509 Address
- B. The SMTP reply Address
- C. The E-mail Header
- D. The Host Domain Name

Answer: C

NEW QUESTION 668

- (Exam Topic 1)

What does mactime, an essential part of the coroner's toolkit do?

- A. It traverses the file system and produces a listing of all files based on the modification, access and change timestamps
- B. It can recover deleted file space and search it for dat
- C. However, it does not allow the investigator to preview them
- D. The tools scans for i-node information, which is used by other tools in the tool kit
- E. It is too specific to the MAC OS and forms a core component of the toolkit

Answer: A

NEW QUESTION 669

- (Exam Topic 1)

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

- A. 128
- B. 64
- C. 32
- D. 16

Answer: C

NEW QUESTION 671

- (Exam Topic 1)

After passing her CEH exam, Carol wants to ensure that her network is completely secure. She implements a DMZ, stateful firewall, NAT, IPSEC, and a packet filtering firewall. Since all security measures were taken, none of the hosts on her network can reach the Internet. Why is that?

- A. Stateful firewalls do not work with packet filtering firewalls
- B. NAT does not work with stateful firewalls
- C. IPSEC does not work with packet filtering firewalls
- D. NAT does not work with IPSEC

Answer: D

NEW QUESTION 673

- (Exam Topic 1)

You have used a newly released forensic investigation tool, which doesn't meet the Daubert Test, during a case. The case has ended-up in court. What argument could the defense make to weaken your case?

- A. The tool hasn't been tested by the International Standards Organization (ISO)
- B. Only the local law enforcement should use the tool
- C. The total has not been reviewed and accepted by your peers
- D. You are not certified for using the tool

Answer: C

NEW QUESTION 678

- (Exam Topic 1)

If you plan to startup a suspect's computer, you must modify the _____ to ensure that you do not contaminate or alter data on the suspect's hard drive by booting to the hard drive.

- A. deltree command
- B. CMOS
- C. Boot.sys
- D. Scandisk utility

Answer: C

NEW QUESTION 681

- (Exam Topic 1)

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

Answer: C

NEW QUESTION 682

- (Exam Topic 1)

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 686

- (Exam Topic 1)

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

Answer: C

NEW QUESTION 688

- (Exam Topic 1)

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

Answer: D

NEW QUESTION 693

- (Exam Topic 1)

- A. Right to work
- B. Right of free speech
- C. Right to Internet Access
- D. Right of Privacy

Answer: D

NEW QUESTION 710

- (Exam Topic 1)

As a CHFI professional, which of the following is the most important to your professional reputation?

- A. Your Certifications
- B. The correct, successful management of each and every case
- C. The free that you charge
- D. The friendship of local law enforcement officers

Answer: B

NEW QUESTION 715

- (Exam Topic 1)

Jonathan is a network administrator who is currently testing the internal security of his network. He is attempting to hijack a session, using Ettercap, of a user connected to his Web server. Why will Jonathan not succeed?

- A. Only an HTTPS session can be hijacked
- B. HTTP protocol does not maintain session
- C. Only FTP traffic can be hijacked
- D. Only DNS traffic can be hijacked

Answer: B

NEW QUESTION 717

- (Exam Topic 1)

When using Windows acquisitions tools to acquire digital evidence, it is important to use a well-tested hardware write-blocking device to:

- A. Automate Collection from image files
- B. Avoiding copying data from the boot partition
- C. Acquire data from host-protected area on a disk
- D. Prevent Contamination to the evidence drive

Answer: D

NEW QUESTION 718

- (Exam Topic 1)

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

- A. Multiple access points can be set up on the same channel without any issues
- B. Avoid over-saturation of wireless signals
- C. So that the access points will work on different frequencies
- D. Avoid cross talk

Answer: D

NEW QUESTION 721

- (Exam Topic 1)

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?

- 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 722

- (Exam Topic 1)

You are carrying out the last round of testing for your new website before it goes live. The website has many dynamic pages and connects to a SQL backend that accesses your product inventory in a database. You come across a web security site that recommends inputting the following code into a search field on web pages to check for vulnerabilities: When you type this and click on search, you receive a pop-up window that says: "This is a test."
What is the result of this test?

- A. Your website is vulnerable to CSS
- B. Your website is not vulnerable
- C. Your website is vulnerable to SQL injection
- D. Your website is vulnerable to web bugs

Answer: A

NEW QUESTION 726

- (Exam Topic 1)

One technique for hiding information is to change the file extension from the correct one to one that might not be noticed by an investigator. For example, changing a .jpg extension to a .doc extension so that a picture file appears to be a document. What can an investigator examine to verify that a file has the correct extension?

- A. the File Allocation Table
- B. the file header
- C. the file footer
- D. the sector map

Answer: B

NEW QUESTION 727

- (Exam Topic 1)

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 t0rnrootkit
- D. Nothing in particular as these can be operational files

Answer: D

NEW QUESTION 730

- (Exam Topic 1)

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

- A. rules of evidence
- B. law of probability
- C. chain of custody
- D. policy of separation

Answer: C

NEW QUESTION 733

- (Exam Topic 1)

Lance wants to place a honeypot on his network. Which of the following would be your recommendations?

- A. Use a system that has a dynamic addressing on the network
- B. Use a system that is not directly interacting with the router
- C. Use it on a system in an external DMZ in front of the firewall
- D. It doesn't matter as all replies are faked

Answer: D

NEW QUESTION 734

- (Exam Topic 1)

You are working on a thesis for your doctorate degree in Computer Science. Your thesis is based on HTML, DHTML, and other web-based languages and how they have evolved over the years.

You navigate to archive.org and view the HTML code of news.com. You then navigate to the current news.com website and copy over the source code. While searching through the code, you come across something abnormal: What have you found?

- A. Web bug
- B. CGI code
- C. Trojan.downloader
- D. Blind bug

Answer: A

NEW QUESTION 737

- (Exam Topic 1)

Chris has been called upon to investigate a hacking incident reported by one of his clients. The company suspects the involvement of an insider accomplice in the attack. Upon reaching the incident scene, Chris secures the physical area, records the scene using visual media. He shuts the system down by pulling the power plug so that he does not disturb the system in any way. He labels all cables and connectors prior to disconnecting any. What do you think would be the next sequence of events?

- A. Connect the target media; prepare the system for acquisition; Secure the evidence; Copy the media
- B. Prepare the system for acquisition; Connect the target media; copy the media; Secure the evidence
- C. Connect the target media; Prepare the system for acquisition; Secure the evidence; Copy the media
- D. Secure the evidence; prepare the system for acquisition; Connect the target media; copy the media

Answer: B

NEW QUESTION 742

- (Exam Topic 1)

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 745

- (Exam Topic 1)

Your company uses Cisco routers exclusively throughout the network. After securing the routers to the best of your knowledge, an outside security firm is brought in to assess the network security.

Although they found very few issues, they were able to enumerate the model, OS version, and capabilities for all your Cisco routers with very little effort. Which feature will you disable to eliminate the ability to enumerate this information on your Cisco routers?

- A. Border Gateway Protocol
- B. Cisco Discovery Protocol
- C. Broadcast System Protocol
- D. Simple Network Management Protocol

Answer: B

NEW QUESTION 747

- (Exam Topic 1)

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.ghitech.net What will this search produce?

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

Answer: B

NEW QUESTION 749

- (Exam Topic 1)

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 750

- (Exam Topic 1)

_____ is simply the application of Computer Investigation and analysis techniques in the interests of determining potential legal evidence.

- A. Network Forensics
- B. Computer Forensics
- C. Incident Response
- D. Event Reaction

Answer: B

NEW QUESTION 753

- (Exam Topic 1)

You are the security analyst working for a private company out of France. Your current assignment is to obtain credit card information from a Swiss bank owned by that company. After initial reconnaissance, you discover that the bank security defenses are very strong and would take too long to penetrate. You decide to get the information by monitoring the traffic between the bank and one of its subsidiaries in London. After monitoring some of the traffic, you see a lot of FTP packets traveling back and forth. You want to sniff the traffic and extract usernames and passwords. What tool could you use to get this information?

- A. Airsnort
- B. Snort
- C. Ettercap
- D. RaidSniff

Answer: C

NEW QUESTION 757

- (Exam Topic 1)

Kyle is performing the final testing of an application he developed for the accounting department. His last round of testing is to ensure that the program is as

secure as possible. Kyle runs the following command. What is he testing at this point?

```
#include <string.h>
int main(int argc, char
*argv[]) { char buffer[10]; if (argc < 2) { printf (stderr, "USAGE: %s string\n", argv[0]); return 1; } strcpy(buffer, argv[1]); return 0; }
```

- A. Buffer overflow
- B. SQL injection
- C. Format string bug
- D. Kernel injection

Answer: A

NEW QUESTION 761

- (Exam Topic 1)

What is the target host IP in the following command?

- A. 172.16.28.95
- B. 10.10.150.1
- C. Firewall does not scan target hosts
- D. This command is using FIN packets, which cannot scan target hosts

Answer: A

NEW QUESTION 762

- (Exam Topic 1)

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

Answer: A

NEW QUESTION 766

- (Exam Topic 1)

An Expert witness give 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 769

- (Exam Topic 1)

Simon is a former employee of Trinitron XML Inc. He feels he was wrongly terminated and wants to hack into his former company's network. Since Simon remembers some of the server names, he attempts to run the axfr and ixfr commands using DIG. What is Simon trying to accomplish here?

- A. Send DOS commands to crash the DNS servers
- B. Perform DNS poisoning
- C. Perform a zone transfer
- D. Enumerate all the users in the domain

Answer: C

NEW QUESTION 773

- (Exam Topic 1)

When examining the log files from a Windows IIS Web Server, how often is a new log file created?

- A. the same log is used at all times
- B. a new log file is created everyday
- C. a new log file is created each week
- D. a new log is created each time the Web Server is started

Answer: A

NEW QUESTION 775

- (Exam Topic 1)

What does the acronym POST mean as it relates to a PC?

- A. Primary Operations Short Test
- B. PowerOn Self Test
- C. Pre Operational Situation Test

D. Primary Operating System Test

Answer: B

NEW QUESTION 778

- (Exam Topic 1)

An "idle" system is also referred to as what?

- A. PC not connected to the Internet
- B. Zombie
- C. PC not being used
- D. Bot

Answer: B

NEW QUESTION 783

- (Exam Topic 1)

In conducting a computer abuse investigation you become aware that the suspect of the investigation is using ABC Company as his Internet Service Provider (ISP). You contact ISP and request that they provide you assistance with your investigation. What assistance can the ISP provide?

- A. The ISP can investigate anyone using their service and can provide you with assistance
- B. The ISP can investigate computer abuse committed by their employees, but must preserve the privacy of their customers and therefore cannot assist you without a warrant
- C. The ISP can't conduct any type of investigations on anyone and therefore can't assist you
- D. ISP's never maintain log files so they would be of no use to your investigation

Answer: B

NEW QUESTION 787

- (Exam Topic 1)

With the standard Linux second extended file system (Ext2fs), a file is deleted when the inode internal link count reaches _____.

- A. 10
- B. 100
- C. 1

Answer: A

NEW QUESTION 788

- (Exam Topic 1)

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

Answer: A

NEW QUESTION 793

- (Exam Topic 1)

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 794

- (Exam Topic 1)

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 798

- (Exam Topic 1)

With Regard to using an Antivirus scanner during a computer forensics investigation, You should:

- A. Scan the suspect hard drive before beginning an investigation
- B. Never run a scan on your forensics workstation because it could change your systems configuration
- C. Scan your forensics workstation at intervals of no more than once every five minutes during an investigation
- D. Scan your Forensics workstation before beginning an investigation

Answer: D

NEW QUESTION 799

- (Exam Topic 1)

If you discover a criminal act while investigating a corporate policy abuse, it becomes a publicsector investigation and should be referred to law enforcement?

- A. true
- B. false

Answer: A

NEW QUESTION 802

- (Exam Topic 1)

You are assisting in the investigation of a possible Web Server Hack. The company who called you stated that customers reported to them that whenever they entered the web address of the company in their browser, what they received was a porno graphic web site. The company checked the web server and nothing appears wrong. When you type in the IP address of the web site in your browser everything appears normal. What is the name of the attack that affects the DNS cache of the name resolution servers, resulting in those servers directing users to the wrong web site?

- A. ARP Poisoning
- B. DNS Poisoning
- C. HTTP redirect attack
- D. IP Spoofing

Answer: B

NEW QUESTION 803

.....

Relate Links

100% Pass Your 312-49v10 Exam with ExamBible Prep Materials

<https://www.exambible.com/312-49v10-exam/>

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - <https://www.exambible.com/>