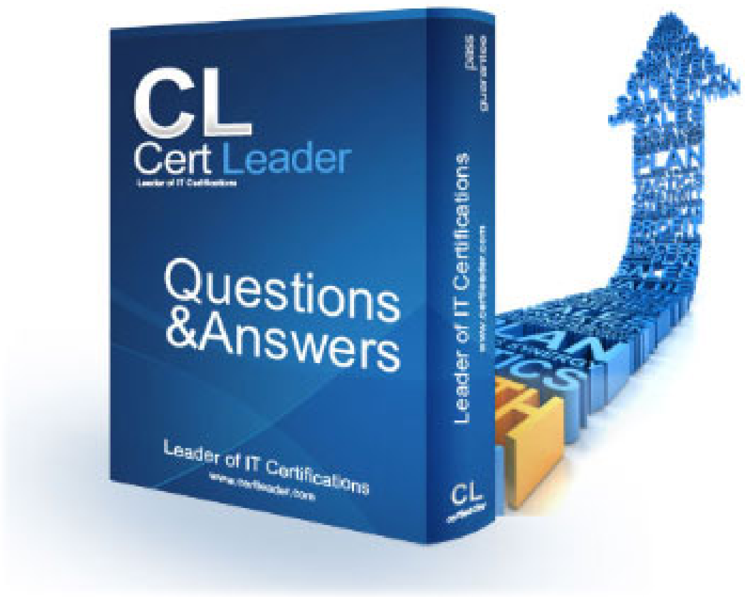
312-49v10 Dumps

Computer Hacking Forensic Investigator (CHFI-v10)

https://www.certleader.com/312-49v10-dumps.html



NEW QUESTION 1
- (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 2
- (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 3
- (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 4
- (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 5
- (Exam Topic 3)
Which of the following is a non-zero data that an application allocates on a hard disk cluster in systems running on Windows OS?

A. Sparse File
B. Master File Table
C. Meta Block Group
D. Slack Space

Answer: B

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)
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 9
- (Exam Topic 3)
Investigators can use the Type Allocation Code (TAC) to find the model and origin of a mobile device. Where is TAC located in mobile devices?

A. International Mobile Equipment Identifier (IMEI)
B. Integrated circuit card identifier (ICCID)
C. International mobile subscriber identity (IMSI)
D. Equipment Identity Register (EIR)

Answer: A

NEW QUESTION 10
- (Exam Topic 3)
When analyzing logs, it is important that the clocks of all the network devices are synchronized. Which protocol will help in synchronizing these clocks?

A. UTC
B. PTP
C. Time Protocol
D. NTP

Answer: D

NEW QUESTION 10
- (Exam Topic 3)
In Windows, prefetching is done to improve system performance. There are two types of prefetching: boot prefetching and application prefetching. During boot prefetching, what does the Cache Manager do?

A. Determines the data associated with value EnablePrefetcher
B. Monitors the first 10 seconds after the process is started
C. Checks whether the data is processed
D. Checks hard page faults and soft page faults

Answer: C

NEW QUESTION 15
- (Exam Topic 3)
Where should the investigator look for the Edge browser’s browsing records, including history, cache, and cookies?

A. ESE Database
B. Virtual Memory
C. Sparse files
D. Slack Space

Answer: A

NEW QUESTION 20
- (Exam Topic 3)
While collecting Active Transaction Logs using SQL Server Management Studio, the query Select * from
::fn_dblog(NULL, NULL) displays the active portion of the transaction log file. Here, assigning NULL values implies?

A. Start and end points for log sequence numbers are specified
B. Start and end points for log files are not specified
C. Start and end points for log files are specified
D. Start and end points for log sequence numbers are not specified

Answer: B

NEW QUESTION 24
- (Exam Topic 3)
Which U.S. law sets the rules for sending emails for commercial purposes, establishes the minimum requirements for commercial messaging, gives the recipients of emails the right to ask the senders to stop emailing them, and spells out the penalties in case the above said rules are violated?

A. NO-SPAM Act
B. American: NAVSO P-5239-26 (RLL)
C. CAN-SPAM Act
D. American: DoD 5220.22-M

Answer: C

NEW QUESTION 26
- (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 30
- (Exam Topic 3)
What document does the screenshot represent?

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

Answer: D

NEW QUESTION 32
- (Exam Topic 3)
Which of the following tools is not a data acquisition hardware tool?

A. UltraKit
B. Atola Insight Forensic
C. F-Response Imager
D. Triage-Responder

Answer: C

NEW QUESTION 37
- (Exam Topic 3)
Which of the following components within the android architecture stack take care of displaying windows owned by different applications?

A. Media Framework
B. Surface Manager
C. Resource Manager
D. Application Framework

Answer: D

NEW QUESTION 42
- (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 44
- (Exam Topic 3)
> NMAP -sn 192.168.11.200-215 The NMAP command above performs which of the following?

A. A trace sweep
B. A port scan
C. A ping scan
D. An operating system detect

Answer: C

NEW QUESTION 48
- (Exam Topic 3)
What do you call the process of studying the changes that have taken place across a system or a machine after a series of actions or incidents?

A. Windows Services Monitoring
B. System Baselining
C. Start-up Programs Monitoring
D. Host integrity Monitoring

Answer: D

NEW QUESTION 50
- (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 53
- (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 58
- (Exam Topic 3)
Which among the following laws emphasizes the need for each Federal agency to develop, document, and implement an organization-wide program to provide information security for the information systems that support its operations and assets?

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

Answer: A

NEW QUESTION 63
- (Exam Topic 3)
Which of these rootkit detection techniques function by comparing a snapshot of the file system, boot records, or memory with a known and trusted baseline?

A. Signature-Based Detection
B. Integrity-Based Detection
C. Cross View-Based Detection
D. Heuristic/Behavior-Based Detection

Answer: B

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 67
- (Exam Topic 3)
A company’s policy requires employees to perform file transfers using protocols which encrypt traffic. You suspect some employees are still performing file transfers using unencrypted protocols because the employees don’t like changes. You have positioned a network sniffer to capture traffic from the laptops used by employees in the data ingest department. Using Wireshark to examine the captured traffic, which command can be used as a display filter to find unencrypted file transfers?

A. tcp.port = 23
B. tcp.port == 21
C. tcp.port == 21 || tcp.port == 22
D. tcp.port != 21

Answer: B

NEW QUESTION 69
- (Exam Topic 3)
During an investigation, Noel found the following SIM card from the suspect's mobile. What does the code 89 44 represent?

A. Issuer Identifier Number and TAC
B. Industry Identifier and Country code
C. Individual Account Identification Number and Country Code
D. TAC and Industry Identifier

Answer: B

NEW QUESTION 70
- (Exam Topic 3)
Andie, a network administrator, suspects unusual network services running on a windows system. Which of the following commands should he use to verify unusual network services started on a Windows system?

A. net serv
B. netmgr
C. lusrmgr
D. net start

Answer: D

NEW QUESTION 71
- (Exam Topic 3)
Which one of the following is not a first response procedure?

A. Preserve volatile data
B. Fill forms
C. Crack passwords
D. Take photos

Answer: C

NEW QUESTION 76
- (Exam Topic 3)
Which of the following files store the MySQL database data permanently, including the data that had been deleted, helping the forensic investigator in examining the case and finding the culprit?

A. mysql-bin
B. mysql-log
C. iblog
D. ibdata1

Answer: D

NEW QUESTION 77
- (Exam Topic 3)
What is the framework used for application development for iOS-based mobile devices?

A. Cocoa Touch
B. Dalvik
C. Zygote
D. AirPlay

Answer: A

NEW QUESTION 78
- (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 81
- (Exam Topic 3)
The Apache server saves diagnostic information and error messages that it encounters while processing requests. The default path of this file is usr/local/apache/logs/error.log in Linux. Identify the Apache error log from the following logs.

A. http://victim.com/scripts/..%c0%af../..%c0%af../..%c0%af../..%c0%af../..%c0%af../..%c0%af../..%c0%af../..%c0%af../winnt/system32/cmd.exe?/c+dir+C:\Winnt\system32\Logfiles\W3SVC1
B. [Wed Oct 11 14:32:52 2000] [error] [client 127.0.0.1] client denied by server configuration:/export/home/live/ap/htdocs/test
C. 127.0.0.1 - frank [10/Oct/2000:13:55:36 -0700]"GET /apache_pb.gif HTTP/1.0" 200 2326
D. 127.0.0.1 - - [10/Apr/2007:10:39:11 +0300]] [error] "GET /apache_pb.gif HTTP/1.0" 200 2326

Answer: B

NEW QUESTION 84
- (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 87
- (Exam Topic 3)
You are a Penetration Tester and are assigned to scan a server. You need to use a scanning technique wherein the TCP Header is split into many packets so that it becomes difficult to detect what the packets are meant for. Which of the below scanning technique will you use?

A. Inverse TCP flag scanning
B. ACK flag scanning
C. TCP Scanning
D. IP Fragment Scanning

Answer: D

NEW QUESTION 89
- (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 92
- (Exam Topic 3)
Which of the following processes is part of the dynamic malware analysis?

A. Process Monitoring
B. Malware disassembly
C. Searching for the strings
D. File fingerprinting

Answer: A

NEW QUESTION 96
- (Exam Topic 3)
What is the location of a Protective MBR in a GPT disk layout?

A. Logical Block Address (LBA) 2
B. Logical Block Address (LBA) 0
C. Logical Block Address (LBA) 1
D. Logical Block Address (LBA) 3

Answer: C

NEW QUESTION 98
- (Exam Topic 3)
Which of the following file system uses Master File Table (MFT) database to store information about every file and directory on a volume?

A. FAT File System
B. ReFS
C. exFAT
D. NTFS File System

Answer: D

NEW QUESTION 99
- (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 100
- (Exam Topic 3)
Identify the term that refers to individuals who, by virtue of their knowledge and expertise, express an independent opinion on a matter related to a case based on the information that is provided.

A. Expert Witness
B. Evidence Examiner
C. Forensic Examiner
D. Defense Witness

Answer: A

NEW QUESTION 104
- (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 106
- (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 110
- (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 115
- (Exam Topic 3)
You are asked to build a forensic lab and your manager has specifically informed you to use copper for lining the walls, ceilings, and floor. What is the main purpose of lining the walls, ceilings, and floor with copper?

A. To control the room temperature
B. To strengthen the walls, ceilings, and floor
C. To avoid electromagnetic emanations
D. To make the lab sound proof

Answer: D

NEW QUESTION 116
- (Exam Topic 3)
In both pharming and phishing attacks an attacker can create websites that look similar to legitimate sites with the intent of collecting personal identifiable information from its victims. What is the difference between pharming and phishing attacks?

A. Both pharming and phishing attacks are purely technical and are not considered forms of social engineering
B. In a pharming attack a victim is redirected to a fake website by modifying their host configuration file or by exploiting vulnerabilities in DN
C. In a phishing attack an attacker provides the victim with a URL that is either misspelled or looks similar to the actual websites domain name
D. In a phishing attack a victim is redirected to a fake website by modifying their host configuration file or by exploiting vulnerabilities in DN
E. In a pharming attack an attacker provides the victim with a URLthat is either misspelled or looks very similar to the actual websites domain name
F. Both pharming and phishing attacks are identical

Answer: B

NEW QUESTION 119
- (Exam Topic 3)
You are assigned a task to examine the log files pertaining to MyISAM storage engine. While examining, you are asked to perform a recovery operation on a MyISAM log file. Which among the following MySQL Utilities allow you to do so?

A. mysqldump
B. myisamaccess
C. myisamlog
D. myisamchk

Answer: C

NEW QUESTION 120
- (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 125

- (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 129
- (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 131
- (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 135
- (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 136
- (Exam Topic 3)
Which of the following application password cracking tool can discover all password-protected items on a computer and decrypts them?

A. TestDisk for Windows
B. R-Studio
C. Windows Password Recovery Bootdisk
D. Passware Kit Forensic

Answer: D

NEW QUESTION 138
- (Exam Topic 3)
Which of the following email headers specifies an address for mailer-generated errors, like "no such user" bounce messages, to go to (instead of the sender's address)?

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

Answer: D

NEW QUESTION 143
- (Exam Topic 3)
Which forensic investigation methodology believes that criminals commit crimes solely to benefit their criminal enterprises?

A. Scientific Working Group on Digital Evidence
B. Daubert Standard

C. Enterprise Theory of Investigation
D. Fyre Standard

Answer: C

NEW QUESTION 147
- (Exam Topic 3)
Which of the following ISO standard defines file systems and protocol for exchanging data between optical disks?

A. ISO 9660
B. ISO/IEC 13940
C. ISO 9060
D. IEC 3490

Answer: A

NEW QUESTION 150
- (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 155
- (Exam Topic 3)
Smith, an employee of a reputed forensic investigation firm, has been hired by a private organization to investigate a laptop that is suspected to be involved in the hacking of the organization’s DC server. Smith wants to find all the values typed into the Run box in the Start menu. Which of the following registry keys will Smith check to find the above information?

A. TypedURLs key
B. MountedDevices key
C. UserAssist Key
D. RunMRU key

Answer: D

NEW QUESTION 157
- (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 161
- (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 164
- (Exam Topic 3)
During an investigation of an XSS attack, the investigator comes across the term “[a-zA-Z0-9\%]+” in analyzed evidence details. What is the expression used for?

A. Checks for upper and lower-case alphanumeric string inside the tag, or its hex representation
B. Checks for forward slash used in HTML closing tags, its hex or double-encoded hex equivalent
C. Checks for opening angle bracket, its hex or double-encoded hex equivalent
D. Checks for closing angle bracket, hex or double-encoded hex equivalent

Answer: B

NEW QUESTION 169

- (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 171
- (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 174
- (Exam Topic 3)
Randy has extracted data from an old version of a Windows-based system and discovered info file Dc5.txt in the system recycle bin. What does the file name denote?

A. A text file deleted from C drive in sixth sequential order
B. A text file deleted from C drive in fifth sequential order
C. A text file copied from D drive to C drive in fifth sequential order
D. A text file copied from C drive to D drive in fifth sequential order

Answer: B

NEW QUESTION 176
- (Exam Topic 3)
companyXYZ has asked you to assess the security of their perimeter email gateway. From your office in New York you craft a specially formatted email message and send it across the Internet to an employee of CompanyXYZ. The employee of CompanyXYZ is aware.

A. Source code review
B. Reviewing the firewalls configuration
C. Data items and vulnerability scanning
D. Interviewing employees and network engineers

Answer: A

NEW QUESTION 178
- (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 180
- (Exam Topic 3)
Which layer of iOS architecture should a forensics investigator evaluate to analyze services such as Threading, File Access, Preferences, Networking and high-level features?

A. Core Services
B. Media services
C. Cocoa Touch
D. Core OS

Answer: D

NEW QUESTION 183
- (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 188
- (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 191
- (Exam Topic 3)
James is dealing with a case regarding a cybercrime that has taken place in Arizona, USA. James needs to lawfully seize the evidence from an electronic device without affecting the user's anonymity. Which of the following law should he comply with, before retrieving the evidence?

A. First Amendment of the U.
B. Constitution
C. Fourth Amendment of the U.
D. Constitution
E. Third Amendment of the U.
F. Constitution
G. Fifth Amendment of the U.
H. Constitution

Answer: D

NEW QUESTION 196
- (Exam Topic 3)
What is the role of Alloc.c in Apache core?

A. It handles allocation of resource pools
B. It is useful for reading and handling of the configuration files
C. It takes care of all the data exchange and socket connections between the client and the server
D. It handles server start-ups and timeouts

Answer: A

NEW QUESTION 199
- (Exam Topic 3)
Identify the file system that uses $BitMap file to keep track of all used and unused clusters on a volume.

A. NTFS
B. FAT
C. EXT
D. FAT32

Answer: A

NEW QUESTION 203
- (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 207
- (Exam Topic 3)
As part of extracting the system data, Jenifer has used the netstat command. What does this tool reveal?

A. Status of users connected to the internet
B. Net status of computer usage
C. Information about network connections
D. Status of network hardware

Answer: C

NEW QUESTION 209
- (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 212
- (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 216
- (Exam Topic 3)
While analyzing a hard disk, the investigator finds that the file system does not use UEFI-based interface. Which of the following operating systems is present on the hard disk?

A. Windows 10
B. Windows 8
C. Windows 7
D. Windows 8.1

Answer: C

NEW QUESTION 218
- (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 221
- (Exam Topic 3)
A section of your forensics lab houses several electrical and electronic equipment. Which type of fire extinguisher you must install in this area to contain any fire incident?

A. Class B
B. Class D
C. Class C
D. Class A

Answer: C

NEW QUESTION 223
- (Exam Topic 3)
Sheila is a forensics trainee and is searching for hidden image files on a hard disk. She used a forensic investigation tool to view the media in hexadecimal code for simplifying the search process. Which of the following hex codes should she look for to identify image files?

A. ff d8 ff
B. 25 50 44 46
C. d0 0f 11 e0
D. 50 41 03 04

Answer: A

NEW QUESTION 225
- (Exam Topic 3)
Which of the following files contains the traces of the applications installed, run, or uninstalled from a system?

A. Virtual Files
B. Image Files
C. Shortcut Files
D. Prefetch Files

Answer: C

NEW QUESTION 227
- (Exam Topic 3)
Which of the following is a federal law enacted in the US to control the ways that financial institutions deal with the private information of individuals?

A. SOX
B. HIPAA 1996
C. GLBA
D. PCI DSS

Answer: C

NEW QUESTION 232
- (Exam Topic 3)
Which of the following is a MAC-based File Recovery Tool?

A. VirtualLab
B. GetDataBack
C. Cisdem DataRecovery 3
D. Smart Undeleter

Answer: C

NEW QUESTION 234
- (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 239
- (Exam Topic 3)
Which of the following Perl scripts will help an investigator to access the executable image of a process?

A. Lspd.pl
B. Lpsi.pl
C. Lspm.pl
D. Lspi.pl

Answer: D

NEW QUESTION 242
- (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 246
- (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 249
- (Exam Topic 3)
Which of the following is a device monitoring tool?

A. Capsa

B. Driver Detective
C. Regshot
D. RAM Capturer

Answer: A

NEW QUESTION 254
- (Exam Topic 3)
One technique for hiding information is to change the file extension from the correct one to the one that might not be noticed by an investigator. For example, changing a .jpg extension to a .doc extension so that a picture file appears to be a document. What can an investigator examine to verify that a file has the correct extension?

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

Answer: A

NEW QUESTION 257
- (Exam Topic 3)
Which of the following tool can reverse machine code to assembly language?

A. PEiD
B. RAM Capturer
C. IDA Pro
D. Deep Log Analyzer

Answer: C

NEW QUESTION 262
- (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 263
- (Exam Topic 3)
Which of the following file formats allows the user to compress the acquired data as well as keep it randomly accessible?

A. Proprietary Format
B. Generic Forensic Zip (gfzip)
C. Advanced Forensic Framework 4
D. Advanced Forensics Format (AFF)

Answer: B

NEW QUESTION 266
- (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 270
- (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 275
- (Exam Topic 3)
Which of the following is a responsibility of the first responder?

A. Determine the severity of the incident
B. Collect as much information about the incident as possible
C. Share the collected information to determine the root cause
D. Document the findings

Answer: B

NEW QUESTION 280
- (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 283
- (Exam Topic 3)
An attacker has compromised a cloud environment of a company and used the employee information to perform an identity theft attack. Which type of attack is this?

A. Cloud as a subject
B. Cloud as a tool
C. Cloud as an object
D. Cloud as a service

Answer: A

NEW QUESTION 287
- (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 290
- (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 293
- (Exam Topic 2)
What technique used by Encase makes it virtually impossible to tamper with evidence once it has been acquired?

A. Every byte of the file(s) is given an MD5 hash to match against a master file
B. Every byte of the file(s) is verified using 32-bit CRC
C. Every byte of the file(s) is copied to three different hard drives
D. Every byte of the file(s) is encrypted using three different methods

Answer: B

NEW QUESTION 295
- (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 297
- (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 301
- (Exam Topic 2)
Sniffers that place NICs in promiscuous mode work at what layer of the OSI model?

A. Network
B. Transport
C. Physical
D. Data Link

Answer: C

NEW QUESTION 302
- (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 306
- (Exam Topic 2)
Amber, a black hat hacker, has embedded a malware into a small enticing advertisement and posted it on a popular ad-network that displays across various websites. What is she doing?

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

Answer: D

NEW QUESTION 311
- (Exam Topic 2)
How many times can data be written to a DVD+R disk?

A. Twice
B. Once
C. Zero
D. Infinite

Answer: B

NEW QUESTION 313
- (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 318
- (Exam Topic 2)
Where are files temporarily written in Unix when printing?

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

Answer: D

NEW QUESTION 323
- (Exam Topic 2)
Preparing an image drive to copy files to is the first step in Linux forensics. For this purpose, what would the following command accomplish?
dcfldd if=/dev/zero of=/dev/hda bs=4096 conv=noerror, sync

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

Answer: A

NEW QUESTION 327
- (Exam Topic 2)
After attending a CEH security seminar, you make a list of changes you would like to perform on your network to increase its security. One of the first things you change is to switch the RestrictAnonymous setting from 0 to 1 on your servers. This, as you were told, would prevent anonymous users from establishing a null session on the server. Using Userinfo tool mentioned at the seminar, you succeed in establishing a null session with one of the servers. Why is that?

A. RestrictAnonymous must be set to "10" for complete security
B. RestrictAnonymous must be set to "3" for complete security
C. RestrictAnonymous must be set to "2" for complete security
D. There is no way to always prevent an anonymous null session from establishing

Answer: C

NEW QUESTION 329
- (Exam Topic 2)
What will the following command accomplish in Linux?
fdisk /dev/hda

A. Partition the hard drive
B. Format the hard drive

C. Delete all files under the /dev/hda folder
D. Fill the disk with zeros

Answer: A

NEW QUESTION 331
- (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 335
- (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 336
- (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 339
- (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 344
- (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 349
- (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 354
- (Exam Topic 2)
Billy, a computer forensics expert, has recovered a large number of DBX files during the forensic investigation of a laptop. Which of the following email clients can he use to analyze the DBX files?

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

Answer: D

NEW QUESTION 355
- (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 356
- (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 361
- (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 363
- (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 367
- (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 372
- (Exam Topic 2)
When operating systems mark a cluster as used but not allocated, the cluster is considered as ________

A. Corrupt
B. Bad
C. Lost
D. Unallocated

Answer: C

NEW QUESTION 377
- (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 379
- (Exam Topic 2)
Casey has acquired data from a hard disk in an open source acquisition format that allows her to generate compressed or uncompressed image files. What format did she use?

A. Portable Document Format
B. Advanced Forensics Format (AFF)
C. Proprietary Format
D. Raw Format

Answer: B

NEW QUESTION 381
- (Exam Topic 2)
While searching through a computer under investigation, you discover numerous files that appear to have had the first letter of the file name replaced by the hex code byte 5h. What does this indicate on the computer?

A. The files have been marked as hidden
B. The files have been marked for deletion
C. The files are corrupt and cannot be recovered
D. The files have been marked as read-only

Answer: B

NEW QUESTION 383
- (Exam Topic 2)
When investigating a wireless attack, what information can be obtained from the DHCP logs?

A. The operating system of the attacker and victim computers
B. IP traffic between the attacker and the victim
C. MAC address of the attacker
D. If any computers on the network are running in promiscuous mode

Answer: C

NEW QUESTION 385
- (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 386
- (Exam Topic 2)
Stephen is checking an image using Compare Files by The Wizard, and he sees the file signature is shown as FF D8 FF E1. What is the file type of the image?

A. gif
B. bmp
C. jpeg
D. png

Answer: C

NEW QUESTION 388
- (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 389
- (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 394
- (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 396
- (Exam Topic 2)
The process of restarting a computer that is already turned on through the operating system is called?

A. Warm boot
B. Ice boot
C. Hot Boot
D. Cold boot

Answer: A

NEW QUESTION 400
- (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 402
- (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 404
- (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 407

- (Exam Topic 2)
How many possible sequence number combinations are there in TCP/IP protocol?

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

Answer: C

NEW QUESTION 411
- (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 413
- (Exam Topic 2)
When a user deletes a file or folder, the system stores complete path including the original filename is 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 416
- (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 421
- (Exam Topic 2)
Davidson Trucking is a small transportation company that has three local offices in Detroit Michigan. Ten
female employees that work for the company have gone to an attorney reporting that male employees repeatedly harassed them and that management did nothing to stop the problem. Davidson has employee policies that outline all company guidelines, including awareness on harassment and how it will not be tolerated. When the case is brought to court, whom should the prosecuting attorney call upon for not upholding company policy?

A. IT personnel
B. Employees themselves
C. Supervisors
D. Administrative assistant in charge of writing policies

Answer: C

NEW QUESTION 423
- (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 426
- (Exam Topic 2)
Which among the following is an act passed by the U.S. Congress in 2002 to protect investors from the possibility of fraudulent accounting activities by corporations?

A. HIPAA
B. GLBA

C. SOX
D. FISMA

Answer: C

NEW QUESTION 431
- (Exam Topic 2)
A master boot record (MBR) is the first sector (“sector zero”) of a data storage device. What is the size of MBR?

A. Depends on the capacity of the storage device
B. 1048 Bytes
C. 4092 Bytes
D. 512 Bytes

Answer: D

NEW QUESTION 434
- (Exam Topic 2)
In the following email header, where did the email first originate from?

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

Answer: C

NEW QUESTION 437
- (Exam Topic 2)
Which of the following stages in a Linux boot process involve initialization of the system’s hardware?

A. BIOS Stage
B. Bootloader Stage
C. BootROM Stage
D. Kernel Stage

Answer: A

NEW QUESTION 442
- (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 445
- (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 450
- (Exam Topic 2)
Smith, a network administrator with a large MNC, was the first to arrive at a suspected crime scene involving criminal use of compromised computers. What should be his first response while maintaining the integrity of evidence?

A. Record the system state by taking photographs of physical system and the display
B. Perform data acquisition without disturbing the state of the systems
C. Open the systems, remove the hard disk and secure it
D. Switch off the systems and carry them to the laboratory

Answer: A

NEW QUESTION 451
- (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 456
- (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. Samspade.org
D. Archive.org

Answer: D

NEW QUESTION 457
- (Exam Topic 2)
Steven has been given the task of designing a computer forensics lab for the company he works for. He has found documentation on all aspects of how to design a lab except the number of exits needed. How many exits should Steven include in his design for the computer forensics lab?

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

Answer: B

NEW QUESTION 461
- (Exam Topic 2)
Which of the following reports are delivered under oath to a board of directors/managers/panel of the jury?

A. Written Formal Report
B. Verbal Formal Report
C. Verbal Informal Report
D. Written Informal Report

Answer: B

NEW QUESTION 463
- (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 464
- (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 467
- (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 470
- (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 474
- (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 479
- (Exam Topic 2)
Travis, a computer forensics investigator, is finishing up a case he has been working on for over a month involving copyright infringement and embezzlement. His last task is to prepare an investigative report for the president of the company he has been working for. Travis must submit a hard copy and an electronic copy to this president. In what electronic format should Travis send this report?

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

Answer: D

NEW QUESTION 482
- (Exam Topic 2)
Why would a company issue a dongle with the software they sell?

A. To provide source code protection
B. To provide wireless functionality with the software
C. To provide copyright protection
D. To ensure that keyloggers cannot be used

Answer: C

NEW QUESTION 483
- (Exam Topic 2)
When marking evidence that has been collected with the “aaa/ddmmyy/nnnn/zz” format, what does the “nnnn” denote?

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

Answer: D

NEW QUESTION 488
- (Exam Topic 2)
Which of the following is a record of the characteristics of a file system, including its size, the block size, the empty and the filled blocks and their respective counts, the size and location of the inode tables, the disk block map and usage information, and the size of the block groups?

A. Inode bitmap block
B. Superblock
C. Block bitmap block
D. Data block

Answer: B

NEW QUESTION 492
- (Exam Topic 2)
An on-site incident response team is called to investigate an alleged case of computer tampering within their company. Before proceeding with the investigation, the CEO informs them that the incident will be classified as low level. How long will the team have to respond to the incident?

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

Answer: A

NEW QUESTION 496
- (Exam Topic 2)
Which forensic investigating concept trails the whole incident from how the attack began to how the victim was affected?

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

Answer: B

NEW QUESTION 499
- (Exam Topic 2)
Which of the following technique creates a replica of an evidence media?

A. Data Extraction
B. Backup
C. Bit Stream Imaging
D. Data Deduplication

Answer: C

NEW QUESTION 503
- (Exam Topic 2)
Which of the following file contains the traces of the applications installed, run, or uninstalled from a system?

A. Shortcut Files
B. Virtual files
C. Prefetch Files
D. Image Files

Answer: A

NEW QUESTION 508
- (Exam Topic 2)
NTFS has reduced slack space than FAT, thus having lesser potential to hide data in the slack space. This is because:

A. FAT does not index files
B. NTFS is a journaling file system
C. NTFS has lower cluster size space
D. FAT is an older and inefficient file system

Answer: C

NEW QUESTION 509
- (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 511
- (Exam Topic 2)
What type of attack sends spoofed UDP packets (instead of ping packets) with a fake source address to the IP broadcast address of a large network?

A. Fraggle
B. Smurf scan
C. SYN flood
D. Teardrop

Answer: A

NEW QUESTION 512
- (Exam Topic 2)
Which of the following Event Correlation Approach is an advanced correlation method that assumes and predicts what an attacker can do next after the attack by studying the statistics and probability and uses only two variables?

A. Bayesian Correlation
B. Vulnerability-Based Approach
C. Rule-Based Approach
D. Route Correlation

Answer: A

NEW QUESTION 517
- (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 522
- (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 526
- (Exam Topic 2)
An investigator is searching through the firewall logs of a company and notices ICMP packets that are larger than 65,536 bytes. What type of activity is the investigator seeing?

A. Smurf
B. Ping of death
C. Fraggle
D. Nmap scan

Answer: B

NEW QUESTION 530
- (Exam Topic 2)
Linux operating system has two types of typical bootloaders namely LILO (Linux Loader) and GRUB (Grand Unified Bootloader). In which stage of the booting process do the bootloaders become active?

A. Bootloader Stage
B. Kernel Stage
C. BootROM Stage
D. BIOS Stage

Answer: A

NEW QUESTION 532
- (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 533
- (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 534
- (Exam Topic 2)
Sectors are pie-shaped regions on a hard disk that store data. Which of the following parts of a hard disk do not contribute in determining the addresses of data?

A. Sectors
B. Interface
C. Cylinder
D. Heads

Answer: B

NEW QUESTION 536
- (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 541
- (Exam Topic 2)
Why should you never power on a computer that you need to acquire digital evidence from?

A. When the computer boots up, files are written to the computer rendering the data nclean
B. When the computer boots up, the system cache is cleared which could destroy evidence
C. When the computer boots up, data in the memory buffer is cleared which could destroy evidence
D. Powering on a computer has no affect when needing to acquire digital evidence from it

Answer: A

NEW QUESTION 542
- (Exam Topic 2)
Which US law does the interstate or international transportation and receiving of child pornography fall under?

A. §18. U.S.
B. 1466A
C. §18. U.S.C 252
D. §18. U.S.C 146A
E. §18. U.S.C 2252

Answer: D

NEW QUESTION 544
- (Exam Topic 2)
Microsoft Security IDs are available in Windows Registry Editor. The path to locate IDs in Windows 7 is:

A. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList
B. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ProfileList
C. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\RegList
D. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Regedit

Answer: A

NEW QUESTION 545
- (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 546
- (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 548
- (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 549
- (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 551
- (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 553
- (Exam Topic 2)
When investigating a computer forensics case where Microsoft Exchange and Blackberry Enterprise server are used, where would investigator need to search to find email sent from a Blackberry device?

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

Answer: C

NEW QUESTION 558
- (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 560
- (Exam Topic 1)
What information do you need to recover when searching a victim’s computer for a crime committed with specific e-mail message?

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

Answer: B

NEW QUESTION 562
- (Exam Topic 1)
What will the following command produce on a website login page? SELECT email, passwd, login_id, full_name FROM members WHERE email = 'someone@somehwere.com'; DROP TABLE members; --'

A. Deletes the entire members table
B. Inserts the Error! Reference source not found.email address into the members table
C. Retrieves the password for the first user in the members table
D. This command will not produce anything since the syntax is incorrect

Answer: A

NEW QUESTION 567
- (Exam Topic 1)
When examining a hard disk without a write-blocker, you should not start windows because Windows will write data to the:

A. Recycle Bin
B. MSDOS.sys
C. BIOS
D. Case files

Answer: A

NEW QUESTION 572
- (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 575
- (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 578
- (Exam Topic 1)
When investigating a network that uses DHCP to assign IP addresses, where would you look to determine which system (MAC address) had a specific IP address at a specific time?

A. on the individual computer's ARP cache
B. in the Web Server log files
C. in the DHCP Server log files
D. there is no way to determine the specific IP address

Answer: C

NEW QUESTION 580
- (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 582
- (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 585
- (Exam Topic 1)
In a FAT32 system, a 123 KB file will use how many sectors?

A. 34
B. 25
C. 11
D. 56

Answer: B

NEW QUESTION 586
- (Exam Topic 1)
When you are running a vulnerability scan on a network and the IDS cuts off your connection, what type of IDS is being used?

A. Passive IDS
B. Active IDS
C. Progressive IDS
D. NIPS

Answer: B

NEW QUESTION 588
- (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 593
- (Exam Topic 1)
Michael works for Kimball Construction Company as senior security analyst. As part of yearly security audit, Michael scans his network for vulnerabilities. Using Nmap, Michael conducts XMAS scan and most of the ports scanned do not give a response. In what state are these ports?

A. Closed
B. Open
C. Stealth

D. Filtered

Answer: B

NEW QUESTION 595
- (Exam Topic 1)
When monitoring for both intrusion and security events between multiple computers, it is essential that the computers' clocks are synchronized. Synchronized time allows an administrator to reconstruct what took place during an attack against multiple computers. Without synchronized time, it is very difficult to determine exactly when specific events took place, and how events interlace. What is the name of the service used to synchronize time among multiple computers?

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

Answer: B

NEW QUESTION 600
- (Exam Topic 1)
What binary coding is used most often for e-mail purposes?

A. MIME
B. Uuencode
C. IMAP
D. SMTP

Answer: A

NEW QUESTION 601
- (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 602
- (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 607
- (Exam Topic 1)
In a forensic examination of hard drives for digital evidence, what type of user is most likely to have the most file slack to analyze?

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

Answer: D

NEW QUESTION 608
- (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 611
- (Exam Topic 1)

Which legal document allows law enforcement to search an office, place of business, or other locale for evidence relating to an alleged crime?

A. bench warrant
B. wire tap
C. subpoena
D. search warrant

Answer: D

NEW QUESTION 615
- (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 620
- (Exam Topic 1)
You just passed your ECSA exam and are about to start your first consulting job running security audits for a financial institution in Los Angeles. The IT manager of the company you will be working for tries to see if you remember your ECSA class. He asks about the methodology you will be using to test the company's network. How would you answer?

A. Microsoft Methodology
B. Google Methodology
C. IBM Methodology
D. LPT Methodology

Answer: D

NEW QUESTION 625
- (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 630
- (Exam Topic 1)
Study the log given below and answer the following question:

```
Apr 24 14:46:46 [4663]: spp_portscan: portscan detected from 194.222.156.169
Apr 24 14:46:46 [4663]: IDS27/FIN Scan: 194.222.156.169:56693 -> 172.16.1.107:482
Apr 24 18:01:05 [4663]: IDS/DNS-version-query: 212.244.97.121:3485 -> 172.16.1.107:53
Apr 24 19:04:01 [4663]: IDS213/ftp-passwd-retrieval: 194.222.156.169:1425 -> 172.16.1.107:21
Apr 25 08:02:41 [5875]: spp_portscan: PORTSCAN DETECTED from 24.9.255.53
Apr 25 02:08:07 [5875]: IDS277/DNS-version-query: 63.226.81.13:4499 -> 172.16.1.107:53
Apr 25 02:08:07 [5875]: IDS277/DNS-version-query: 63.226.81.13:4630 -> 172.16.1.101:53
Apr 25 02:38:17 [5875]: IDS/RPC-rpcinfo-query: 212.251.1.94:642 -> 172.16.1.107:111
Apr 25 19:37:32 [5875]: IDS230/web-cgi-space-wildcard: 198.173.35.164:4221 -> 172.16.1.107:80
Apr 26 05:45:12 [6283]: IDS212/dns-zone-transfer: 38.31.107.87:2291 -> 172.16.1.101:53
Apr 26 06:43:05 [6283]: IDS181/nops-x86: 63.226.81.13:1351 -> 172.16.1.107:53
Apr 26 06:44:25 victim7 PAM_pwdb[12509]: (login) session opened for user simple by (uid=0)
Apr 26 06:44:36 victim7 PAM_pwdb[12521]: (su) session opened for user simon by simple(uid=506) Apr 26 06:45:34 [6283]: IDS175/socks-probe:
24.112.167.35:20 -> 172.16.1.107:1080
Apr 26 06:52:10 [6283]: IDS127/telnet-login-incorrect: 172.16.1.107:23 -> 213.28.22.189:4558
```

Precautionary measures to prevent this attack would include writing firewall rules. Of these firewall rules, which among the following would be appropriate?

A. Disallow UDP53 in from outside to DNS server
B. Allow UDP53 in from DNS server to outside
C. Disallow TCP53 in from secondaries or ISP server to DNS server
D. Block all UDP traffic

Answer: A

NEW QUESTION 634
- (Exam Topic 1)
The efforts to obtain information before a trail 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 639
- (Exam Topic 1)
To preserve digital evidence, an investigator should _______.

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

Answer: C

NEW QUESTION 640
- (Exam Topic 1)
When examining a file with a Hex Editor, what space does the file header occupy?

A. the last several bytes of the file
B. the first several bytes of the file
C. none, file headers are contained in the FAT
D. one byte at the beginning of the file

Answer: D

NEW QUESTION 644
- (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 649
- (Exam Topic 1)
Sectors in hard disks typically contain how many bytes?

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

Answer: B

NEW QUESTION 653
- (Exam Topic 1)
One way to identify the presence of hidden partitions on a suspect's hard drive is to:

A. Add up the total size of all known partitions and compare it to the total size of the hard drive
B. Examine the FAT and identify hidden partitions by noting an H in the partition Type field
C. Examine the LILO and note an H in the partition Type field
D. It is not possible to have hidden partitions on a hard drive

Answer: A

NEW QUESTION 657
- (Exam Topic 1)
What is the name of the Standard Linux Command that is also available as windows application that can be used to create bit-stream images?

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

Answer: D

NEW QUESTION 662
- (Exam Topic 1)
Terri works for a security consulting firm that is currently performing a penetration test on First National Bank in Tokyo. Terri's duties include bypassing firewalls

and switches to gain access to the network. Terri sends an IP packet to one of the company's switches with ACK bit and the source address of her machine set.
What is Terri trying to accomplish by sending this IP packet?

A. Trick the switch into thinking it already has a session with Terri's computer
B. Poison the switch's MAC address table by flooding it with ACK bits
C. Crash the switch with a DoS attack since switches cannot send ACK bits
D. Enable tunneling feature on the switch

Answer: A

NEW QUESTION 667
- (Exam Topic 1)
Under which Federal Statutes does FBI investigate for computer crimes involving e-mail scams and mail fraud?

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

Answer: B

NEW QUESTION 668
- (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 670
- (Exam Topic 1)
During the course of a corporate investigation, you find that an Employee is committing a crime.
Can the Employer file a criminal complaint with Police?

A. Yes, and all evidence can be turned over to the police
B. Yes, but only if you turn the evidence over to a federal law enforcement agency
C. No, because the investigation was conducted without following standard police procedures
D. No, because the investigation was conducted without warrant

Answer: A

NEW QUESTION 674
- (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 676
- (Exam Topic 1)
Software firewalls work at which layer of the OSI model?

A. Application
B. Network
C. Transport
D. Data Link

Answer: D

NEW QUESTION 681
- (Exam Topic 1)
What are the security risks of running a "repair" installation for Windows XP?

A. Pressing Shift+F10gives the user administrative rights
B. Pressing Shift+F1gives the user administrative rights
C. Pressing Ctrl+F10 gives the user administrative rights
D. There are no security risks when running the "repair" installation for Windows XP

Answer: A

NEW QUESTION 683
- (Exam Topic 1)
Microsoft Outlook maintains email messages in a proprietary format in what type of file?

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

Answer: C

NEW QUESTION 685
- (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 686
- (Exam Topic 1)
You are called in to assist the police in an investigation involving a suspected drug dealer. The suspects house was searched by the police after a warrant was obtained and they located a floppy disk in the suspects bedroom. The disk contains several files, but they appear to be password protected. What are two common methods used by password cracking software that you can use to obtain the password?

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

Answer: B

NEW QUESTION 690
- (Exam Topic 1)
When conducting computer forensic analysis, you must guard against _______ So that you remain focused on the primary job and insure that the level of work does not increase beyond what was originally expected.

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

Answer: B

NEW QUESTION 693
- (Exam Topic 1)
You are working for a local police department that services a population of 1,000,000 people and you have been given the task of building a computer forensics lab. How many law-enforcement computer investigators should you request to staff the lab?

A. 8
B. 1
C. 4
D. 2

Answer: C

NEW QUESTION 697
- (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 698
- (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 701
- (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 703
- (Exam Topic 1)
E- mail logs contain which of the following information to help you in your investigation? (Choose four.)

A. user account that was used to send the account
B. attachments sent with the e-mail message
C. unique message identifier
D. contents of the e-mail message
E. date and time the message was sent

Answer: ACDE

NEW QUESTION 704
- (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 707
- (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 708
- (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 709
- (Exam Topic 1)
In General, _______ Involves the investigation of data that can be retrieved from the hard disk or other disks of a computer by applying scientific methods to retrieve the data.

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

Answer: D

NEW QUESTION 710
- (Exam Topic 1)
What term is used to describe a cryptographic technique for embedding information into something else for the sole purpose of hiding that information from the casual observer?

A. rootkit
B. key escrow
C. steganography
D. Offset

Answer: C

NEW QUESTION 714
- (Exam Topic 1)
The rule of thumb when shutting down a system is to pull the power plug. However, it has certain drawbacks. Which of the following would that be?

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

Answer: A

NEW QUESTION 718
- (Exam Topic 1)
The offset in a hexadecimal code is:

A. The last byte after the colon
B. The 0x at the beginning of the code
C. The 0x at the end of the code
D. The first byte after the colon

Answer: B

NEW QUESTION 722
- (Exam Topic 1)
The _______ refers to handing over the results of private investigations to the authorities because of indications of criminal activity.

A. Locard Exchange Principle
B. Clark Standard
C. Kelly Policy
D. Silver-Platter Doctrine

Answer: D

NEW QUESTION 724
- (Exam Topic 1)
Which Intrusion Detection System (IDS) usually produces the most false alarms due to the unpredictable behaviors of users and networks?

A. network-based IDS systems (NIDS)
B. host-based IDS systems (HIDS)
C. anomaly detection
D. signature recognition

Answer: B

NEW QUESTION 727
- (Exam Topic 1)

You are working as an independent computer forensics investigator and received a call from a systems administrator for a local school system requesting your assistance. One of the students at the local high school is suspected of downloading inappropriate images from the Internet to a PC in the Computer lab. When you arrive at the school, the systems administrator hands you a hard drive and tells you that he made a “simple backup copy” of the hard drive in the PC and put it on this drive and requests that you examine that drive for evidence of the suspected images. You inform him that a “simple backup copy” will not provide deleted files or recover file fragments.
What type of copy do you need to make to ensure that the evidence found is complete and admissible in future proceeding?

A. Bit-stream Copy
B. Robust Copy
C. Full backup Copy
D. Incremental Backup Copy

Answer: A

NEW QUESTION 731
- (Exam Topic 1)
Jim performed a vulnerability analysis on his network and found no potential problems. He runs another utility that executes exploits against his system to verify the results of the vulnerability test.
The second utility executes five known exploits against his network in which the vulnerability analysis said were not exploitable. What kind of results did Jim receive from his vulnerability analysis?

A. False negatives
B. False positives
C. True negatives
D. True positives

Answer: A

NEW QUESTION 736
- (Exam Topic 1)
The use of warning banners helps a company avoid litigation by overcoming an employee assumed ______. When connecting to the company's intranet, network or Virtual Private Network(VPN) and will allow the company's investigators to monitor, search and retrieve information stored within the network.

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

Answer: D

NEW QUESTION 738
- (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 741
- (Exam Topic 1)
When a file is deleted by Windows Explorer or through the MS-DOS delete command, the operating system inserts ______ in the first letter position of the filename in the FAT database.

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

Answer: D

NEW QUESTION 742
- (Exam Topic 1)
John is using Firewalk to test the security of his Cisco PIX firewall. He is also utilizing a sniffer located on a subnet that resides deep inside his network. After analyzing the sniffer log files, he does not see any of the traffic produced by Firewalk. Why is that?

A. Firewalk cannot pass through Cisco firewalls
B. Firewalk sets all packets with a TTL of zero
C. Firewalk cannot be detected by network sniffers
D. Firewalk sets all packets with a TTL of one

Answer: D

NEW QUESTION 745
- (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 748
- (Exam Topic 1)
What is a good security method to prevent unauthorized users from "tailgating"?

A. Man trap
B. Electronic combination locks
C. Pick-resistant locks
D. Electronic key systems

Answer: A

NEW QUESTION 751
- (Exam Topic 1)
George is performing security analysis for Hammond and Sons LLC. He is testing security vulnerabilities of their wireless network. He plans on remaining as "stealthy" as possible during the scan. Why would a scanner like Nessus is not recommended in this situation?

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

Answer: A

NEW QUESTION 755
- (Exam Topic 1)
This organization maintains a database of hash signatures for known software.

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

Answer: C

NEW QUESTION 757
- (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 759
- (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 760
- (Exam Topic 1)
In Linux, what is the smallest possible shellcode?

A. 24 bytes

B. 8 bytes
C. 800 bytes
D. 80 bytes

Answer: A

NEW QUESTION 761
- (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 762
- (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 763
- (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 765
- (Exam Topic 1)
When investigating a potential e-mail crime, what is your first step in the investigation?

A. Trace the IP address to its origin
B. Write a report
C. Determine whether a crime was actually committed
D. Recover the evidence

Answer: A

NEW QUESTION 768
- (Exam Topic 1)
You are called by an author who is writing a book and he wants to know how long the copyright for his book will last after he has the book published?

A. 70 years
B. the life of the author
C. the life of the author plus 70 years
D. copyrights last forever

Answer: C

NEW QUESTION 772
- (Exam Topic 1)
Which of the following refers to the data that might still exist in a cluster even though the original file has been overwritten by another file?

A. Sector
B. Metadata
C. MFT
D. Slack Space

Answer: D

NEW QUESTION 777

- (Exam Topic 1)
An employee is attempting to wipe out data stored on a couple of compact discs (CDs) and digital video discs (DVDs) by using a large magnet. You inform him that this method will not be effective in wiping out the data because CDs and DVDs are _______ media used to store large amounts of data and are not affected by the magnet.

A. logical
B. anti-magnetic
C. magnetic
D. optical

Answer: D

NEW QUESTION 778
- (Exam Topic 1)
You setup SNMP in multiple offices of your company. Your SNMP software manager is not receiving data from other offices like it is for your main office. You suspect that firewall changes are to blame. What ports should you open for SNMP to work through Firewalls? (Choose two.)

A. 162
B. 161
C. 163
D. 160

Answer: AB

NEW QUESTION 780
- (Exam Topic 1)
A(n) _______ is one that's performed by a computer program rather than the attacker manually performing the steps in the attack sequence.

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

Answer: B

NEW QUESTION 785
- (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 786
- (Exam Topic 1)
What type of attack occurs when an attacker can force a router to stop forwarding packets by flooding the router with many open connections simultaneously so that all the hosts behind the router are effectively disabled?

A. digital attack
B. denial of service
C. physical attack
D. ARP redirect

Answer: B

NEW QUESTION 790
- (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 795
- (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 799
- (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 803
- (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 807
......