Exam Questions 312-49v10

Computer Hacking Forensic Investigator (CHFI-v10)

https://www.2passeasy.com/dumps/312-49v10/

NEW QUESTION 1
- (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 2
- (Exam Topic 3)
Which of the following stand true for BIOS Parameter Block?

A. The BIOS Partition Block describes the physical layout of a data storage volume
B. The BIOS Partition Block is the first sector of a data storage device
C. The length of BIOS Partition Block remains the same across all the file systems
D. The BIOS Partition Block always refers to the 512-byte boot sector

Answer: A

NEW QUESTION 3
- (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 4
- (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 5
- (Exam Topic 3)
What technique is used by JPEGs for compression?

A. TIFF-8
B. ZIP
C. DCT
D. TCD

Answer: C

NEW QUESTION 6
- (Exam Topic 3)
A forensic examiner is examining a Windows system seized from a crime scene. During the examination of a suspect file, he discovered that the file is password protected. He tried guessing the password using the suspect's available information but without any success. Which of the following tool can help the investigator to solve this issue?

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

Answer: A

NEW QUESTION 7
- (Exam Topic 3)
An attacker successfully gained access to a remote Windows system and plans to install persistent backdoors on it. Before that, to avoid getting detected in future, he wants to cover his tracks by disabling the

last-accessed timestamps of the machine. What would he do to achieve this?

A. Set the registry value of HKLM\SYSTEM\CurrentControlSet\Control\FileSystem\NtfsDisableLastAccessUpdate to 0
B. Run the command fsutil behavior set disablelastaccess 0
C. Set the registry value of HKLM\SYSTEM\CurrentControlSet\Control\FileSystem\NtfsDisableLastAccessUpdate to 1
D. Run the command fsutil behavior set enablelastaccess 0

Answer: C

NEW QUESTION 8
- (Exam Topic 3)
Ron, a computer forensics expert, is investigating a case involving corporate espionage. He has recovered several mobile computing devices from the crime scene. One of the evidence that Ron possesses is a mobile phone from Nokia that was left in ON condition. Ron needs to recover the IMEI number of the device to establish the identity of the device owner. Which of the following key combinations can he use to recover the IMEI number?

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

Answer: A

NEW QUESTION 9
- (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 10
- (Exam Topic 3)
In which implementation of RAID will the image of a Hardware RAID volume be different from the image taken separately from the disks?

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

Answer: D

NEW QUESTION 10
- (Exam Topic 3)
Brian needs to acquire data from RAID storage. Which of the following acquisition methods is recommended to retrieve only the data relevant to the investigation?

A. Static Acquisition
B. Sparse or Logical Acquisition
C. Bit-stream disk-to-disk Acquisition
D. Bit-by-bit Acquisition

Answer: B

NEW QUESTION 15
- (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 16
- (Exam Topic 3)
Which of the following attack uses HTML tags like <script></script>?

A. Phishing
B. XSS attack
C. SQL injection
D. Spam

Answer: B

NEW QUESTION 18
- (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 20
- (Exam Topic 3)
What do you call the process in which an attacker uses magnetic field over the digital media device to delete any previously stored data?

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

Answer: C

NEW QUESTION 24
- (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 28
- (Exam Topic 3)
Analyze the hex representation of mysql-bin.000013 file in the screenshot below. Which of the following will be an inference from this analysis?

A. A user with username bad_guy has logged into the WordPress web application
B. A WordPress user has been created with the username anonymous_hacker
C. An attacker with name anonymous_hacker has replaced a user bad_guy in the WordPress database
D. A WordPress user has been created with the username bad_guy

Answer: D

NEW QUESTION 33
- (Exam Topic 3)
The MAC attributes are timestamps that refer to a time at which the file was last modified or last accessed or originally created. Which of the following file systems store MAC attributes in Coordinated Universal Time (UTC) format?

A. File Allocation Table (FAT

B. New Technology File System (NTFS)
C. Hierarchical File System (HFS)
D. Global File System (GFS)

Answer: B

NEW QUESTION 38
- (Exam Topic 3)
Amber, a black hat hacker, has embedded malware into a small enticing advertisement and posted it on a popular ad-network that displays across various websites. What is she doing?

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

Answer: A

NEW QUESTION 40
- (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 43
- (Exam Topic 3)
Which of the following Android libraries are used to render 2D (SGL) or 3D (OpenGL/ES) graphics content to the screen?

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

Answer: A

NEW QUESTION 45
- (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 49
- (Exam Topic 3)
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 the 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. Robust copy
B. Incremental backup copy
C. Bit-stream copy
D. Full backup copy

Answer: C

NEW QUESTION 52
- (Exam Topic 3)
Which of the following Linux command searches through the current processes and lists the process IDs those match the selection criteria to stdout?

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

Answer: B

NEW QUESTION 55
- (Exam Topic 3)
Which of the following statements is TRUE with respect to the Registry settings in the user start-up folder HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce\.

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

Answer: D

NEW QUESTION 59
- (Exam Topic 3)
What is the capacity of Recycle bin in a system running on Windows Vista?

A. 2.99GB
B. 3.99GB
C. Unlimited
D. 10% of the partition space

Answer: C

NEW QUESTION 62
- (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 64
- (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 69
- (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 71
- (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 76
- (Exam Topic 3)
Which command can provide the investigators with details of all the loaded modules on a Linux-based system?

A. list modules -a
B. lsmod
C. plist mod -a
D. lsof -m

Answer: B

NEW QUESTION 79
- (Exam Topic 3)
Hard disk data addressing is a method of allotting addresses to each _____ of data on a hard disk.

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

Answer: A

NEW QUESTION 81
- (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 86
- (Exam Topic 3)
Which list contains the most recent actions performed by a Windows User?

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

Answer: A

NEW QUESTION 90
- (Exam Topic 3)
During forensics investigations, investigators tend to collect the system time at first and compare it with UTC. What does the abbreviation UTC stand for?

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

Answer: A

NEW QUESTION 93
- (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 96
- (Exam Topic 3)
Jacob is a computer forensics investigator with over 10 years of experience in investigations and has written over 50 articles on computer forensics. He has been

called upon as a qualified witness to testify the accuracy and integrity of the technical log files gathered in an investigation into computer fraud. What is the term used for Jacob's testimony in this case?

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

Answer: D

NEW QUESTION 101
- (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 106
- (Exam Topic 3)
If the partition size is 4 GB, each cluster will be 32 K. Even if a file needs only 10 K, the entire 32 K will be allocated, resulting in 22 K of _____ .

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

Answer: A

NEW QUESTION 108
- (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 109
- (Exam Topic 3)
During the trial, an investigator observes that one of the principal witnesses is severely ill and cannot be present for the hearing. He decides to record the evidence and present it to the court. Under which rule should he present such evidence?

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

Answer: B

NEW QUESTION 112
- (Exam Topic 3)
Select the tool appropriate for finding the dynamically linked lists of an application or malware.

A. SysAnalyzer
B. ResourcesExtract
C. PEiD
D. Dependency Walker

Answer: D

NEW QUESTION 116
- (Exam Topic 3)
Examination of a computer by a technically unauthorized person will almost always result in:

A. Rendering any evidence found inadmissible in a court of law
B. Completely accurate results of the examination
C. The chain of custody being fully maintained
D. Rendering any evidence found admissible in a court of law

Answer: A

NEW QUESTION 119
- (Exam Topic 3)
Which Event Correlation approach assumes and predicts what an attacker can do next after the attack by studying statistics and probability?

A. Profile/Fingerprint-Based Approach
B. Bayesian Correlation
C. Time (Clock Time) or Role-Based Approach
D. Automated Field Correlation

Answer: B

NEW QUESTION 123
- (Exam Topic 3)
Self-Monitoring, Analysis, and Reporting Technology (SMART) is built into the hard drives to monitor and report system activity. Which of the following is included in the report generated by SMART?

A. Power Off time
B. Logs of high temperatures the drive has reached
C. All the states (running and discontinued) associated with the OS
D. List of running processes

Answer: B

NEW QUESTION 127
- (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 130
- (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 134
- (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 part of Metasploit framework helps users to hide the data related to a previously deleted file or currently unused by the allocated file.

A. Waffen FS
B. RuneFS
C. FragFS
D. Slacker

Answer: D

NEW QUESTION 139
- (Exam Topic 3)
Buffer overflow vulnerabilities, of web applications, occurs when the application fails to guard its buffer properly and allows writing beyond its maximum size. Thus, it overwrites the _____. There are multiple forms of buffer overflow, including a Heap Buffer Overflow and a Format String Attack.

A. Adjacent buffer locations
B. Adjacent string locations
C. Adjacent bit blocks
D. Adjacent memory locations

Answer: D

NEW QUESTION 142
- (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 145
- (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 149
- (Exam Topic 3)
%3cscript%3ealert(”XXXXXXXX”)%3c/script%3e is a script obtained from a Cross-Site Scripting attack. What type of encoding has the attacker employed?

A. Double encoding
B. Hex encoding
C. Unicode
D. Base64

Answer: B

NEW QUESTION 152
- (Exam Topic 3)
Which of the following statements is incorrect when preserving digital evidence?

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

Answer: B

NEW QUESTION 157
- (Exam Topic 3)
When a user deletes a file, the system creates a $I file to store its details. What detail does the $I file not contain?

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

Answer: B

NEW QUESTION 161
- (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 165
- (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 167
- (Exam Topic 3)
Gill is a computer forensics investigator who has been called upon to examine a seized computer. This computer, according to the police, was used by a hacker who gained access to numerous banking institutions to steal customer information. After preliminary investigations, Gill finds in the computer's log files that the hacker was able to gain access to these banks through the use of Trojan horses. The hacker then used these Trojan horses to obtain remote access to the companies' domain controllers. From this point, Gill found that the hacker pulled off the SAM files from the domain controllers to then attempt and crack network passwords. What is the most likely password cracking technique used by this hacker to break the user passwords from the SAM files?

A. Syllable attack
B. Hybrid attack
C. Brute force attack
D. Dictionary attack

Answer: D

NEW QUESTION 172
- (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 177
- (Exam Topic 3)
In which of these attacks will a steganalyst use a random message to generate a stego-object by using some steganography tool, to find the steganography algorithm used to hide the information?

A. Chosen-message attack
B. Known-cover attack
C. Known-message attack
D. Known-stego attack

Answer: A

NEW QUESTION 180
- (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 183
- (Exam Topic 3)
Which program uses different techniques to conceal a malware's code, thereby making it difficult for security mechanisms to detect or remove it?

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

Answer: D

NEW QUESTION 188
- (Exam Topic 3)
Which of the following commands shows you the username and IP address used to access the system via a remote login session and the type of client from which they are accessing the system?

A. Net config
B. Net sessions
C. Net share
D. Net stat

Answer: B

NEW QUESTION 189
- (Exam Topic 3)
Which of the following is NOT an anti-forensics technique?

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

Answer: A

NEW QUESTION 193
- (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 195
- (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 196
- (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 201
- (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 204
- (Exam Topic 3)
What is the investigator trying to view by issuing the command displayed in the following screenshot?

A. List of services stopped
B. List of services closed recently
C. List of services recently started
D. List of services installed

Answer: D

NEW QUESTION 205
- (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 210
- (Exam Topic 3)
What does the Rule 101 of Federal Rules of Evidence states?

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

Answer: A

NEW QUESTION 215
- (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 216
- (Exam Topic 2)
What type of analysis helps to identify the time and sequence of events in an investigation?

A. Time-based
B. Functional
C. Relational
D. Temporal

Answer: D

NEW QUESTION 221
- (Exam Topic 2)
On an Active Directory network using NTLM authentication, where on the domain controllers are the passwords stored?

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

Answer: A

NEW QUESTION 225
- (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 226

- (Exam Topic 2)
You have been called in to help with an investigation of an alleged network intrusion. After questioning the members of the company IT department, you search through the server log files to find any trace of the intrusion. After that you decide to telnet into one of the company routers to see if there is any evidence to be found. While connected to the router, you see some unusual activity and believe that the attackers are currently connected to that router. You start up an ethereal session to begin capturing traffic on the router that could be used in the investigation. At what layer of the OSI model are you monitoring while watching traffic to and from the router?

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

Answer: A

NEW QUESTION 231
- (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 234
- (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 235
- (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 237
- (Exam Topic 2)
Madison is on trial for allegedly breaking into her university’s internal network. The police raided her dorm room and seized all of her computer equipment. Madison’s lawyer is trying to convince the judge that the seizure was unfounded and baseless. Under which US Amendment is Madison’s lawyer trying to prove the police violated?

A. The 4th Amendment
B. The 1st Amendment
C. The 10th Amendment
D. The 5th Amendment

Answer: A

NEW QUESTION 240
- (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 245
- (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 249
- (Exam Topic 2)
Tyler is setting up a wireless network for his business that he runs out of his home. He has followed all the directions from the ISP as well as the wireless router manual. He does not have any encryption set and the
SSID is being broadcast. On his laptop, he can pick up the wireless signal for short periods of time, but then the connection drops and the signal goes away. Eventually the wireless signal shows back up, but drops intermittently. What could be Tyler issue with his home wireless network?

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

Answer: C

NEW QUESTION 254
- (Exam Topic 2)
Data is striped at a byte level across multiple drives, and parity information is distributed among all member drives.

What RAID level is represented here?

A. RAID Level 0
B. RAID Level 5
C. RAID Level 3
D. RAID Level 1

Answer: B

NEW QUESTION 255
- (Exam Topic 2)
Before performing a logical or physical search of a drive in Encase, what must be added to the program?

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

Answer: B

NEW QUESTION 256
- (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 261
- (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 262
- (Exam Topic 2)
Bob works as information security analyst for a big finance company. One day, the anomaly-based intrusion detection system alerted that a volumetric DDOS targeting the main IP of the main web server was occurring. What kind of attack is it?

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

Answer: D

NEW QUESTION 264
- (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 269
- (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 271
- (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 275
- (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 277
- (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 282
- (Exam Topic 2)
Wireless access control attacks aim to penetrate a network by evading WLAN access control measures such as AP MAC filters and Wi-Fi port access controls. Which of the following wireless access control attacks allow the attacker to set up a rogue access point outside the corporate perimeter and then lure the employees of the organization to connect to it?

A. Ad hoc associations
B. Client mis-association
C. MAC spoofing
D. Rogue access points

Answer: B

NEW QUESTION 283
- (Exam Topic 2)
Which code does the FAT file system use to mark the file as deleted?

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

Answer: D

NEW QUESTION 286
- (Exam Topic 2)
Which of the following tool enables data acquisition and duplication?

A. Colasoft’s Capsa
B. DriveSpy
C. Wireshark
D. Xplico

Answer: B

NEW QUESTION 291
- (Exam Topic 2)
Which of the following files DOES NOT use Object Linking and Embedding (OLE) technology to embed and link to other objects?

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

Answer: A

NEW QUESTION 292
- (Exam Topic 2)
Depending upon the jurisdictional areas, different laws apply to different incidents. Which of the following law is related to fraud and related activity in connection with computers?

A. 18 USC §1029
B. 18 USC §1030
C. 18 USC §1361
D. 18 USC §1371

Answer: B

NEW QUESTION 297
- (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 302
- (Exam Topic 2)
The following is a log file screenshot from a default installation of IIS 6.0.

What time standard is used by IIS as seen in the screenshot?

A. UTC

B. GMT
C. TAI
D. UT

Answer: A

NEW QUESTION 307
- (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 311
- (Exam Topic 2)
What advantage does the tool Evidor have over the built-in Windows search?

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

Answer: C

NEW QUESTION 312
- (Exam Topic 2)
Using Internet logging software to investigate a case of malicious use of computers, the investigator comes across some entries that appear odd.

From the log, the investigator can see where the person in question went on the Internet. From the log, it appears that the user was manually typing in different user ID numbers. What technique this user was trying?

A. Parameter tampering
B. Cross site scripting
C. SQL injection
D. Cookie Poisoning

Answer: A

NEW QUESTION 315
- (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 317
- (Exam Topic 2)
Who is responsible for the following tasks?

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

Answer: A

NEW QUESTION 320
- (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 321
- (Exam Topic 2)
When marking evidence that has been collected with the aa/ddmmyy/nnnn/zz format, what does the nnn denote?

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

Answer: D

NEW QUESTION 322
- (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 325
- (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 328
- (Exam Topic 2)
In Windows Security Event Log, what does an event id of 530 imply?

A. Logon Failure – Unknown user name or bad password
B. Logon Failure – User not allowed to logon at this computer
C. Logon Failure – Account logon time restriction violation
D. Logon Failure – Account currently disabled

Answer: C

NEW QUESTION 330
- (Exam Topic 2)
How will you categorize a cybercrime that took place within a CSP's cloud environment?

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

Answer: D

NEW QUESTION 331
- (Exam Topic 2)
While presenting his case to the court, Simon calls many witnesses to the stand to testify. Simon decides to call Hillary Taft, a lay witness, to the stand. Since Hillary is a lay witness, what field would she be considered an expert in?

A. Technical material related to forensics
B. No particular field

C. Judging the character of defendants/victims
D. Legal issues

Answer: B

NEW QUESTION 335
- (Exam Topic 2)
Which MySQL log file contains information on server start and stop?

A. Slow query log file
B. General query log file
C. Binary log
D. Error log file

Answer: D

NEW QUESTION 337
- (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 340
- (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 343
- (Exam Topic 2)
What is one method of bypassing a system BIOS password?

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

Answer: B

NEW QUESTION 348
- (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 350
- (Exam Topic 2)
What is considered a grant of a property right given to an individual who discovers or invents a new machine, process, useful composition of matter or manufacture?

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

Answer: D

NEW QUESTION 353

- (Exam Topic 2)
Ivanovich, a forensics investigator, is trying to extract complete information about running processes from a system. Where should he look apart from the RAM and virtual memory?

A. Swap space
B. Application data
C. Files and documents
D. Slack space

Answer: A

NEW QUESTION 354
- (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 358
- (Exam Topic 2)
Where is the startup configuration located on a router?

A. Static RAM
B. BootROM
C. NVRAM
D. Dynamic RAM

Answer: C

NEW QUESTION 363
- (Exam Topic 2)
A picture file is recovered from a computer under investigation. During the investigation process, the file is enlarged 500% to get a better view of its contents. The picture quality is not degraded at all from this process. What kind of picture is this file. What kind of picture is this file?

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

Answer: B

NEW QUESTION 366
- (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 371
- (Exam Topic 2)
Jacob is a computer forensics investigator with over 10 years experience in investigations and has written over 50 articles on computer forensics. He has been called upon as a qualified witness to testify the accuracy and integrity of the technical log files gathered in an investigation into computer fraud. What is the term used for Jacob testimony in this case?

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

Answer: B

NEW QUESTION 375
- (Exam Topic 2)
Which of the following acts as a network intrusion detection system as well as network intrusion prevention system?

A. Accunetix

B. Nikto
C. Snort
D. Kismet

Answer: C

NEW QUESTION 376
- (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 377
- (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 379
- (Exam Topic 2)
Which of the following tool captures and allows you to interactively browse the traffic on a network?

A. Security Task Manager
B. Wireshark
C. ThumbsDisplay
D. RegScanner

Answer: B

NEW QUESTION 384
- (Exam Topic 2)
A small law firm located in the Midwest has possibly been breached by a computer hacker looking to obtain information on their clientele. The law firm does not have any on-site IT employees, but wants to search for evidence of the breach themselves to prevent any possible media attention. Why would this not be recommended?

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

Answer: D

NEW QUESTION 386
- (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 389
- (Exam Topic 2)
You have been given the task to investigate web attacks on a Windows-based server. Which of the following commands will you use to look at the sessions the machine has opened with other systems?

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

Answer: D

NEW QUESTION 394
- (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 396
- (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 400
- (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 401
- (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 403
- (Exam Topic 2)
Charles has accidentally deleted an important file while working on his Mac computer. He wants to recover the deleted file as it contains some of his crucial business secrets. Which of the following tool will help Charles?

A. Xplico
B. Colasoft's Capsa
C. FileSalvage
D. DriveSpy

Answer: C

NEW QUESTION 406
- (Exam Topic 2)
Which tool does the investigator use to extract artifacts left by Google Drive on the system?

A. PEBrowse Professional
B. RegScanner
C. RAM Capturer
D. Dependency Walker

Answer: C

NEW QUESTION 407
- (Exam Topic 2)
All Blackberry email is eventually sent and received through what proprietary RIM-operated mechanism?

A. Blackberry Message Center
B. Microsoft Exchange

C. Blackberry WAP gateway
D. Blackberry WEP gateway

Answer: A

NEW QUESTION 408
- (Exam Topic 2)
Heather, a computer forensics investigator, is assisting a group of investigators working on a large computer fraud case involving over 20 people. These 20 people, working in different offices, allegedly siphoned off money from many different client accounts. Heather responsibility is to find out how the accused people communicated between each other. She has searched their email and their computers and has not found any useful evidence. Heather then finds some possibly useful evidence under the desk of one of the accused.
In an envelope she finds a piece of plastic with numerous holes cut out of it. Heather then finds the same exact piece of plastic with holes at many of the other accused peoples desks. Heather believes that the 20 people involved in the case were using a cipher to send secret messages in between each other. What type of cipher was used by the accused in this case?

A. Grill cipher
B. Null cipher
C. Text semagram
D. Visual semagram

Answer: A

NEW QUESTION 412
- (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 413
- (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 416
- (Exam Topic 2)
What technique is used by JPEGs for compression?

A. ZIP
B. TCD
C. DCT
D. TIFF-8

Answer: C

NEW QUESTION 421
- (Exam Topic 2)
Which program is the bootloader when Windows XP starts up?

A. KERNEL.EXE
B. NTLDR
C. LOADER
D. LILO

Answer: B

NEW QUESTION 426
- (Exam Topic 2)
This type of testimony is presented by someone who does the actual fieldwork and does not offer a view in court.

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

Answer: D

NEW QUESTION 429
- (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 434
- (Exam Topic 2)
Shane has started the static analysis of a malware and is using the tool ResourcesExtract to find more details of the malicious program. What part of the analysis is he performing?

A. Identifying File Dependencies
B. Strings search
C. Dynamic analysis
D. File obfuscation

Answer: B

NEW QUESTION 438
- (Exam Topic 2)
Daryl, a computer forensics investigator, has just arrived at the house of an alleged computer hacker. Daryl takes pictures and tags all computer and peripheral equipment found in the house. Daryl packs all the items found in his van and takes them back to his lab for further examination. At his lab, Michael his assistant helps him with the investigation. Since Michael is still in training, Daryl supervises all of his work very carefully. Michael is not quite sure about the procedures to copy all the data off the computer and peripheral devices. How many data acquisition tools should Michael use when creating copies of the evidence for the investigation?

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

Answer: A

NEW QUESTION 442
- (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 447
- (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 449
- (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 451
- (Exam Topic 2)

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

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

Answer: A

NEW QUESTION 453
- (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 458
- (Exam Topic 2)
Which of the following Registry components include offsets to other cells as well as the LastWrite time for the key?

A. Value list cell
B. Value cell
C. Key cell
D. Security descriptor cell

Answer: C

NEW QUESTION 460
- (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 463
- (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 467
- (Exam Topic 2)
Jason discovered a file named $RIYG6VR.doc in the C:\$Recycle.Bin\<USER SID>\ while analyzing a hard disk image for the deleted data. What inferences can he make from the file name?

A. It is a doc file deleted in seventh sequential order
B. RIYG6VR.doc is the name of the doc file deleted from the system
C. It is file deleted from R drive
D. It is a deleted doc file

Answer: D

NEW QUESTION 470
- (Exam Topic 2)
Which of the following is NOT a part of pre-investigation phase?

A. Building forensics workstation
B. Gathering information about the incident
C. Gathering evidence data
D. Creating an investigation team

Answer: C

NEW QUESTION 471
- (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 474
- (Exam Topic 2)
Which file is a sequence of bytes organized into blocks understandable by the system's linker?

A. executable file
B. source file
C. Object file
D. None of these

Answer: C

NEW QUESTION 476
- (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 480
- (Exam Topic 2)
Which of the following Event Correlation Approach checks and compares all the fields systematically and intentionally for positive and negative correlation with each other to determine the correlation across one or multiple fields?

A. Rule-Based Approach
B. Automated Field Correlation
C. Field-Based Approach
D. Graph-Based Approach

Answer: B

NEW QUESTION 484
- (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 489
- (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 491
- (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 493
- (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 497
- (Exam Topic 2)
Under confession, an accused criminal admitted to encrypting child pornography pictures and then hiding them within other pictures. What technique did the accused criminal employ?

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

Answer: D

NEW QUESTION 499
- (Exam Topic 2)
Netstat is a tool for collecting information regarding network connections. It provides a simple view of TCP and UDP connections, and their state and network traffic statistics. Which of the following commands shows you the TCP and UDP network connections, listening ports, and the identifiers?

A. netstat – r
B. netstat – ano
C. netstat – b
D. netstat – s

Answer: B

NEW QUESTION 501
- (Exam Topic 2)
When making the preliminary investigations in a sexual harassment case, how many investigators are you recommended having?

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

Answer: B

NEW QUESTION 504
- (Exam Topic 1)
What happens when a file is deleted by a Microsoft operating system using the FAT file system?

A. only the reference to the file is removed from the FAT
B. the file is erased and cannot be recovered
C. a copy of the file is stored and the original file is erased
D. the file is erased but can be recovered

Answer: A

NEW QUESTION 505
- (Exam Topic 1)
Why should you note all cable connections for a computer you want to seize as evidence?

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

Answer: A

NEW QUESTION 510

- (Exam Topic 1)
You have been asked to investigate the possibility of computer fraud in the finance department of a company. It is suspected that a staff member has been committing finance fraud by printing cheques that have not been authorized. You have exhaustively searched all data files on a bitmap image of the target computer, but have found no evidence. You suspect the files may not have been saved. What should you examine next in this case?

A. The registry
B. The swap file
C. The recycle bin
D. The metadata

Answer: B

NEW QUESTION 515
- (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 519
- (Exam Topic 1)
Why are Linux/Unix based computers better to use than Windows computers for idle scanning?

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

Answer: C

NEW QUESTION 524
- (Exam Topic 1)
Corporate investigations are typically easier than public investigations because:

A. the users have standard corporate equipment and software
B. the investigator does not have to get a warrant
C. the investigator has to get a warrant
D. the users can load whatever they want on their machines

Answer: B

NEW QUESTION 526
- (Exam Topic 1)
Harold is a security analyst who has just run the rdisk /s command to grab the backup SAM files on a computer. Where should Harold navigate on the computer to find the file?

A. %systemroot%\system32\LSA
B. %systemroot%\system32\drivers\etc
C. %systemroot%\repair
D. %systemroot%\LSA

Answer: C

NEW QUESTION 528
- (Exam Topic 1)
You work as a penetration tester for Hammond Security Consultants. You are currently working on a contract for the state government of California. Your next step is to initiate a DoS attack on their network. Why would you want to initiate a DoS attack on a system you are testing?

A. Show outdated equipment so it can be replaced
B. List weak points on their network
C. Use attack as a launching point to penetrate deeper into the network
D. Demonstrate that no system can be protected against DoS attacks

Answer: B

NEW QUESTION 532
- (Exam Topic 1)
Which of the following should a computer forensics lab used for investigations have?

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

Answer: B

NEW QUESTION 534
- (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 536
- (Exam Topic 1)
You are running through a series of tests on your network to check for any security vulnerabilities.
After normal working hours, you initiate a DoS attack against your external firewall. The firewall Quickly freezes up and becomes unusable. You then initiate an FTP connection from an external IP into your internal network. The connection is successful even though you have FTP blocked at the external firewall. What has happened?

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

Answer: D

NEW QUESTION 540
- (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 541
- (Exam Topic 1)
From the following spam mail header, identify the host IP that sent this spam? From jie02@netvigator.com jie02@netvigator.com Tue Nov 27 17:27:11 2001
Received: from viruswall.ie.cuhk.edu.hk (viruswall [137.189.96.52]) by eng.ie.cuhk.edu.hk (8.11.6/8.11.6) with ESMTP id
fAR9RAP23061 for ; Tue, 27 Nov 2001 17:27:10 +0800 (HKT)
Received: from mydomain.com (pcd249020.netvigator.com [203.218.39.20]) by viruswall.ie.cuhk.edu.hk (8.12.1/8.12.1)
with SMTP id fAR9QXwZ018431 for ; Tue, 27 Nov 2001 17:26:36 +0800 (HKT)
Message-Id: >200111270926.fAR9QXwZ018431@viruswall.ie.cuhk.edu.hk From: "china hotel web"
To: "Shlam"
Subject: SHANGHAI (HILTON HOTEL) PACKAGE
Date: Tue, 27 Nov 2001 17:25:58 +0800 MIME-Version: 1.0
X- Priority: 3 X-MSMail- Priority: Normal
Reply-To: "china hotel web"

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

Answer: C

NEW QUESTION 545
- (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 548
- (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 553
- (Exam Topic 1)
Area density refers to:

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

Answer: A

NEW QUESTION 555
- (Exam Topic 1)
You are using DriveSpy, a forensic tool and want to copy 150 sectors where the starting sector is 1709 on the primary hard drive. Which of the following formats correctly specifies these sectors?

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

Answer: B

NEW QUESTION 556
- (Exam Topic 1)
Which federal computer crime law specifically refers to fraud and related activity in connection with access devices like routers?

A. 18 U.S.
B. 1029
C. 18 U.S.
D. 1362
E. 18 U.S.
F. 2511
G. 18 U.S.
H. 2703

Answer: A

NEW QUESTION 560
- (Exam Topic 1)
You have compromised a lower-level administrator account on an Active Directory network of a small company in Dallas, Texas. You discover Domain Controllers through enumeration. You connect to one of the Domain Controllers on port 389 using ldp.exe. What are you trying to accomplish here?

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

Answer: D

NEW QUESTION 565
- (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 567
- (Exam Topic 1)
Item 2If you come across a sheepdip machine at your client site, what would you infer?

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

Answer: C

NEW QUESTION 569
- (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 572
- (Exam Topic 1)
An Employee is suspected of stealing proprietary information belonging to your company that he had no rights to possess. The information was stored on the Employees Computer that was protected with the NTFS Encrypted File System (EFS) and you had observed him copy the files to a floppy disk just before leaving work for the weekend. You detain the Employee before he leaves the building and recover the floppy disks and secure his computer. Will you be able to break the encryption so that you can verify that that the employee was in possession of the proprietary information?

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

Answer: B

NEW QUESTION 574
- (Exam Topic 1)
James is testing the ability of his routers to withstand DoS attacks. James sends ICMP ECHO requests to the broadcast address of his network. What type of DoS attack is James testing against his network?

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

Answer: A

NEW QUESTION 579
- (Exam Topic 1)
Harold wants to set up a firewall on his network but is not sure which one would be the most appropriate. He knows he needs to allow FTP traffic to one of the servers on his network, but he wants to only allow
FTP-PUT. Which firewall would be most appropriate for Harold? needs?

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

Answer: C

NEW QUESTION 582
- (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 586
- (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 591
- (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 595
- (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 599
- (Exam Topic 1)
What header field in the TCP/IP protocol stack involves the hacker exploit known as the Ping of Death?

A. ICMP header field
B. TCP header field
C. IP header field
D. UDP header field

Answer: B

NEW QUESTION 601
- (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 603
- (Exam Topic 1)
You are a computer forensics investigator working with local police department and you are called to assist in an investigation of threatening emails. The complainant has printer out 27 email messages from the suspect and gives the printouts to you. You inform her that you will need to examine her computer because you need access to the _____ in order to track the emails back to the suspect.

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

Answer: D

NEW QUESTION 608
- (Exam Topic 1)
A packet is sent to a router that does not have the packet destination address in its route table. How will the packet get to its proper destination?

A. Root Internet servers
B. Border Gateway Protocol

C. Gateway of last resort
D. Reverse DNS

Answer: C

NEW QUESTION 612
- (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 615
- (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 620
- (Exam Topic 1)
In the context of file deletion process, which of the following statement holds true?

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

Answer: C

NEW QUESTION 624
- (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 625
- (Exam Topic 1)
The newer Macintosh Operating System is based on:

A. OS/2
B. BSD Unix
C. Linux
D. Microsoft Windows

Answer: B

NEW QUESTION 628
- (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 629
- (Exam Topic 1)

You work as an IT security auditor hired by a law firm in Boston to test whether you can gain access to sensitive information about the company clients. You have rummaged through their trash and found very little information. You do not want to set off any alarms on their network, so you plan on performing passive foot printing against their Web servers. What tool should you use?

A. Ping sweep
B. Nmap
C. Netcraft
D. Dig

Answer: C

NEW QUESTION 634
- (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 639
- (Exam Topic 1)
Which part of the Windows Registry contains the user's password file?

A. HKEY_LOCAL_MACHINE
B. HKEY_CURRENT_CONFIGURATION
C. HKEY_USER
D. HKEY_CURRENT_USER

Answer: A

NEW QUESTION 644
- (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 649
- (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 651
- (Exam Topic 1)
Meyer Electronics Systems just recently had a number of laptops stolen out of their office. On these laptops contained sensitive corporate information regarding patents and company strategies. A month after the laptops were stolen, a competing company was found to have just developed products that almost exactly duplicated products that Meyer produces. What could have prevented this information from being stolen from the laptops?

A. EFS Encryption
B. DFS Encryption
C. IPS Encryption
D. SDW Encryption

Answer: A

NEW QUESTION 654
- (Exam Topic 1)
After passing her CEH exam, Carol wants to ensure that her network is completely secure. She implements a DMZ, stateful firewall, NAT, IPSEC, and a packet filtering firewall. Since all security measures were taken, none of the hosts on her network can reach the Internet. Why is that?

A. Stateful firewalls do not work with packet filtering firewalls
B. NAT does not work with stateful firewalls

C. IPSEC does not work with packet filtering firewalls
D. NAT does not work with IPSEC

Answer: D

NEW QUESTION 658
- (Exam Topic 1)
You have used a newly released forensic investigation tool, which doesn't meet the Daubert Test, during a case. The case has ended-up in court. What argument could the defense make to weaken your case?

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

Answer: C

NEW QUESTION 661
- (Exam Topic 1)
Frank is working on a vulnerability assessment for a company on the West coast. The company hired Frank to assess its network security through scanning, pen tests, and vulnerability assessments. After discovering numerous known vulnerabilities detected by a temporary IDS he set up, he notices a number of items that show up as unknown but Questionable in the logs. He looks up the behavior on the Internet, but cannot find anything related. What organization should Frank submit the log to find out if it is a new vulnerability or not?

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

Answer: C

NEW QUESTION 664
- (Exam Topic 1)
Hackers can gain access to Windows Registry and manipulate user passwords, DNS settings, access rights or others features that they may need in order to accomplish their objectives. One simple method for loading an application at startup is to add an entry (Key) to the following Registry Hive:

A. HKEY_LOCAL_MACHINE\hardware\windows\start
B. HKEY_LOCAL_USERS\Software\Microsoft\old\Version\Load
C. HKEY_CURRENT_USER\Microsoft\Default
D. HKEY_LOCAL_MACHINE\Software\Microsoft\CurrentVersion\Run

Answer: D

NEW QUESTION 667
- (Exam Topic 1)
This is original file structure database that Microsoft originally designed for floppy disks. It is written to the outermost track of a disk and contains information about each file stored on the drive.

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

Answer: C

NEW QUESTION 669
- (Exam Topic 1)
After undergoing an external IT audit, George realizes his network is vulnerable to DDoS attacks. What countermeasures could he take to prevent DDoS attacks?

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

Answer: B

NEW QUESTION 670
- (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 671
- (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 675
- (Exam Topic 1)
Kimberly is studying to be an IT security analyst at a vocational school in her town. The school offers many different programming as well as networking languages. What networking protocol language should she learn that routers utilize?

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

Answer: D

NEW QUESTION 679
- (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 681
- (Exam Topic 1)
You are running known exploits against your network to test for possible vulnerabilities. To test the strength of your virus software, you load a test network to mimic your production network. Your software successfully blocks some simple macro and encrypted viruses. You decide to really test the software by using virus code where the code rewrites itself entirely and the signatures change from child to child, but the functionality stays the same. What type of virus is this that you are testing?

A. Polymorphic
B. Metamorphic
C. Oligomorhic
D. Transmorphic

Answer: B

NEW QUESTION 683
- (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 686
- (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 690
- (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 694
- (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 698
- (Exam Topic 1)
As a CHFI professional, which of the following is the most important to your professional reputation?

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

Answer: B

NEW QUESTION 699
- (Exam Topic 1)
Jonathan is a network administrator who is currently testing the internal security of his network. He is attempting to hijack a session, using Ettercap, of a user connected to his Web server. Why will Jonathan not succeed?

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

Answer: B

NEW QUESTION 700
- (Exam Topic 1)
When using Windows acquisitions tools to acquire digital evidence, it is important to use a well-tested hardware write-blocking device to:

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

Answer: D

NEW QUESTION 701
- (Exam Topic 1)
You are carrying out the last round of testing for your new website before it goes live. The website has many dynamic pages and connects to a SQL backend that accesses your product inventory in a database. You come across a web security site that recommends inputting the following code into a search field on web pages to check for vulnerabilities: When you type this and click on search, you receive a pop-up window that says: "This is a test."
What is the result of this test?

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

Answer: A

NEW QUESTION 704
- (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 707
- (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 712
- (Exam Topic 1)
Melanie was newly assigned to an investigation and asked to make a copy of all the evidence from the compromised system. Melanie did a DOS copy of all the files on the system. What would be the primary reason for you to recommend a disk imaging tool?

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

Answer: C

NEW QUESTION 715
- (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 716
- (Exam Topic 1)
You are trying to locate Microsoft Outlook Web Access Default Portal using Google search on the Internet. What search string will you use to locate them?

A. allinurl:"exchange/logon.asp"
B. intitle:"exchange server"
C. locate:"logon page"
D. outlook:"search"

Answer: A

NEW QUESTION 721
- (Exam Topic 1)
In a computer forensics investigation, what describes the route that evidence takes from the time you find it until the case is closed or goes to court?

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

Answer: C

NEW QUESTION 723
- (Exam Topic 1)
Before you are called to testify as an expert, what must an attorney do first?

A. engage in damage control
B. prove that the tools you used to conduct your examination are perfect
C. read your curriculum vitae to the jury
D. qualify you as an expert witness

Answer: D

NEW QUESTION 726

- (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 729
- (Exam Topic 1)
Chris has been called upon to investigate a hacking incident reported by one of his clients. The company suspects the involvement of an insider accomplice in the attack. Upon reaching the incident scene, Chris secures the physical area, records the scene using visual media. He shuts the system down by pulling the power plug so that he does not disturb the system in any way. He labels all cables and connectors prior to disconnecting any. What do you think would be the next sequence of events?

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

Answer: B

NEW QUESTION 730
- (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 732
- (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 735
- (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 739
- (Exam Topic 1)
Kyle is performing the final testing of an application he developed for the accounting department. His last round of testing is to ensure that the program is as secure as possible. Kyle runs the following
command. What is he testing at this point?
#include #include int main(int argc, char
*argv[]) { char buffer[10]; if (argc < 2) { fprintf (stderr, "USAGE: %s string\n", argv[0]); return 1; } strcpy(buffer, argv[1]); return 0; }

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

Answer: A

NEW QUESTION 744
- (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 747
- (Exam Topic 1)
You are assigned to work in the computer forensics lab of a state police agency. While working on a high profile criminal case, you have followed every applicable procedure, however your boss is still concerned that the defense attorney might question whether evidence has been changed while at the lab. What can you do to prove that the evidence is the same as it was when it first entered the lab?

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

Answer: A

NEW QUESTION 752
- (Exam Topic 1)
An Expert witness give an opinion if:

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

Answer: A

NEW QUESTION 754
- (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 755
- (Exam Topic 1)
John and Hillary works at the same department in the company. John wants to find out Hillary's network password so he can take a look at her documents on the file server. He enables Lophtcrack program to sniffing mode. John sends Hillary an email with a link to Error! Reference source not found. What information will he be able to gather from this?

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

Answer: A

NEW QUESTION 756
- (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 761
.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual 312-49v10 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the 312-49v10 Product From:

https://www.2passeasy.com/dumps/312-49v10/

Money Back Guarantee

312-49v10 Practice Exam Features:

* 312-49v10 Questions and Answers Updated Frequently

* 312-49v10 Practice Questions Verified by Expert Senior Certified Staff

* 312-49v10 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* 312-49v10 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year