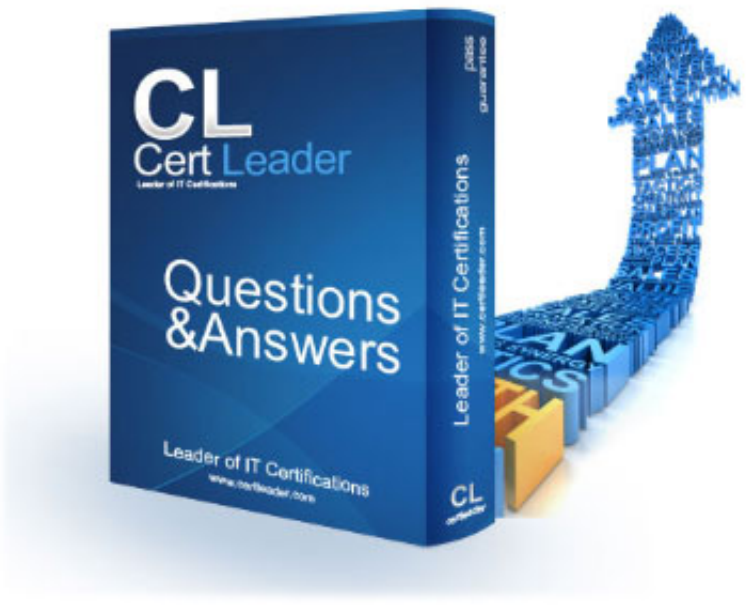
312-49v10 Dumps

Computer Hacking Forensic Investigator (CHFI-v10)

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



NEW QUESTION 1
- (Exam Topic 3)
The given image displays information about date and time of installation of the OS along with service packs, patches, and sub-directories. What command or tool did the investigator use to view this output?

A. dir /o:d
B. dir /o:s
C. dir /o:e
D. dir /o:n

Answer: A

NEW QUESTION 2
- (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 3
- (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 4
- (Exam Topic 3)
Steve, a forensic investigator, was asked to investigate an email incident in his organization. The organization has Microsoft Exchange Server deployed for email communications. Which among the following files will Steve check to analyze message headers, message text, and standard attachments?

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

Answer: B

NEW QUESTION 5
- (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 6
- (Exam Topic 3)
Where should the investigator look for the Edge browser's browsing records, including history, cache, and cookies?

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

Answer: A

NEW QUESTION 7
- (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 8
- (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 9
- (Exam Topic 3)
Which of the following statements is TRUE about SQL Server error logs?

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

Answer: B

NEW QUESTION 10
- (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 10
- (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 13
- (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 16
- (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 19
- (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 23
- (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 24
- (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 27
- (Exam Topic 3)
Select the data that a virtual memory would store in a Windows-based system.

A. Information or metadata of the files
B. Documents and other files
C. Application data
D. Running processes

Answer: D

NEW QUESTION 30
- (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 33
- (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 34
- (Exam Topic 3)
A company’s policy requires employees to perform file transfers using protocols which encrypt traffic. You suspect some employees are still performing file transfers using unencrypted protocols because the employees don’t like changes. You have positioned a network sniffer to capture traffic from the laptops used by employees in the data ingest department. Using Wireshark to examine the captured traffic, which command can be used as a display filter to find unencrypted file transfers?

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

Answer: B

NEW QUESTION 35
- (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 39
- (Exam Topic 3)
Which ISO Standard enables laboratories to demonstrate that they comply with quality assurance and provide valid results?

A. ISO/IEC 16025
B. ISO/IEC 18025
C. ISO/IEC 19025
D. ISO/IEC 17025

Answer: D

NEW QUESTION 40
- (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 44
- (Exam Topic 3)
What is the investigator trying to analyze if the system gives the following image as output?

A. All the logon sessions
B. Currently active logon sessions
C. Inactive logon sessions
D. Details of users who can logon

Answer: B

NEW QUESTION 47
- (Exam Topic 3)
Which of the following files store the MySQL database data permanently, including the data that had been deleted, helping the forensic investigator in examining the case and finding the culprit?

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

Answer: D

NEW QUESTION 52
- (Exam Topic 3)
You are a Penetration Tester and are assigned to scan a server. You need to use a scanning technique wherein the TCP Header is split into many packets so that it becomes difficult to detect what the packets are meant for. Which of the below scanning technique will you use?

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

Answer: D

NEW QUESTION 54
- (Exam Topic 3)
Checkpoint Firewall logs can be viewed through a Check Point Log viewer that uses icons and colors in the log table to represent different security events and their severity. What does the icon in the checkpoint logs represent?

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

Answer: C

NEW QUESTION 58
- (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 59
- (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 64
- (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 67
- (Exam Topic 3)
You are asked to build a forensic lab and your manager has specifically informed you to use copper for lining the walls, ceilings, and floor. What is the main purpose of lining the walls, ceilings, and floor with copper?

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

Answer: D

NEW QUESTION 72
- (Exam Topic 3)
In both pharming and phishing attacks an attacker can create websites that look similar to legitimate sites with the intent of collecting personal identifiable information from its victims. What is the difference between pharming and phishing attacks?

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

Answer: B

NEW QUESTION 75
- (Exam Topic 3)
As a Certified Ethical Hacker, you were contracted by a private firm to conduct an external security assessment through penetration testing . What document describes the specifics of the testing, the associated violations, and essentially protects both the organization’s interest and your liabilities as a tester?

A. Project Scope
B. Rules of Engagement
C. Non-Disclosure Agreement
D. Service Level Agreement

Answer: B

NEW QUESTION 77
- (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 78
- (Exam Topic 3)
Which among the following U.S. laws requires financial institutions—companies that offer consumers financial products or services such as loans, financial or investment advice, or insurance—to protect their customers' information against security threats?

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

Answer: C

NEW QUESTION 83
- (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 86
- (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 88
- (Exam Topic 3)
What does the command "C:\>wevtutil gl <log name>" display?

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

Answer: A

NEW QUESTION 90
- (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 91
- (Exam Topic 3)
Which command line tool is used to determine active network connections?

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

Answer: D

NEW QUESTION 92
- (Exam Topic 3)
Which among the following tools can help a forensic investigator to access the registry files during postmortem analysis?

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

Answer: C

NEW QUESTION 95
- (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 100
- (Exam Topic 3)
Which of the following registry hive gives the configuration information about which application was used to open various files on the system?

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

Answer: A

NEW QUESTION 104
- (Exam Topic 3)
Randy has extracted data from an old version of a Windows-based system and discovered info file Dc5.txt in the system recycle bin. What does the file name denote?

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

Answer: B

NEW QUESTION 109
- (Exam Topic 3)
companyXYZ has asked you to assess the security of their perimeter email gateway. From your office in New York you craft a specially formatted email message and send it across the Internet to an employee of CompanyXYZ. The employee of CompanyXYZ is aware.

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

Answer: A

NEW QUESTION 111
- (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 112
- (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 117
- (Exam Topic 3)
Identify the file system that uses $BitMap file to keep track of all used and unused clusters on a volume.

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

Answer: A

NEW QUESTION 118
- (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 120
- (Exam Topic 3)
An investigator has acquired packed software and needed to analyze it for the presence of malice. Which of the following tools can help in finding the packaging software used?

A. SysAnalyzer
B. PEiD
C. Comodo Programs Manager
D. Dependency Walker

Answer: B

NEW QUESTION 121
- (Exam Topic 3)
Which of the following does not describe the type of data density on a hard disk?

A. Volume density
B. Track density
C. Linear or recording density
D. Areal density

Answer: A

NEW QUESTION 123
- (Exam Topic 3)
While analyzing a hard disk, the investigator finds that the file system does not use UEFI-based interface. Which of the following operating systems is present on the hard disk?

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

Answer: C

NEW QUESTION 128
- (Exam Topic 3)
Gary is checking for the devices connected to USB ports of a suspect system during an investigation. Select the appropriate tool that will help him document all the connected devices.

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

Answer: B

NEW QUESTION 130
- (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 131
- (Exam Topic 3)
Sheila is a forensics trainee and is searching for hidden image files on a hard disk. She used a forensic investigation tool to view the media in hexadecimal code for simplifying the search process. Which of the following hex codes should she look for to identify image files?

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

Answer: A

NEW QUESTION 133
- (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 138
- (Exam Topic 3)
Which of the following is a federal law enacted in the US to control the ways that financial institutions deal with the private information of individuals?

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

Answer: C

NEW QUESTION 141
- (Exam Topic 3)
In a Linux-based system, what does the command “Last -F” display?

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

Answer: A

NEW QUESTION 144
- (Exam Topic 3)
Which of the following Perl scripts will help an investigator to access the executable image of a process?

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

Answer: D

NEW QUESTION 149
- (Exam Topic 3)
Which of the following tool can reverse machine code to assembly language?

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

Answer: C

NEW QUESTION 154
- (Exam Topic 3)
What system details can an investigator obtain from the NetBIOS name table cache?

A. List of files opened on other systems
B. List of the system present on a router
C. List of connections made to other systems
D. List of files shared between the connected systems

Answer: C

NEW QUESTION 157
- (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 159
- (Exam Topic 3)
Which of the following techniques delete the files permanently?

A. Steganography
B. Artifact Wiping
C. Data Hiding
D. Trail obfuscation

Answer: B

NEW QUESTION 162
- (Exam Topic 3)
Which of the following file formats allows the user to compress the acquired data as well as keep it randomly accessible?

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

Answer: B

NEW QUESTION 163
- (Exam Topic 3)
What must an attorney do first before you are called to testify as an expert?

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

Answer: A

NEW QUESTION 165
- (Exam Topic 3)
Centralized binary logging is a process in which many websites write binary and unformatted log data to a single log file. What extension should the investigator look to find its log file?

A. .cbl
B. .log
C. .ibl
D. .txt

Answer: C

NEW QUESTION 170
- (Exam Topic 3)
As a part of the investigation, Caroline, a forensic expert, was assigned the task to examine the transaction logs pertaining to a database named Transfers. She used SQL Server Management Studio to collect the active transaction log files of the database. Caroline wants to extract detailed information on the logs, including AllocUnitId, page id, slot id, etc. Which of the following commands does she need to execute in order to extract the desired information?

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

Answer: D

NEW QUESTION 174
- (Exam Topic 3)
Which of the following standard represents a legal precedent regarding the admissibility of scientific examinations or experiments in legal cases?

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

Answer: C

NEW QUESTION 177
- (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 180
- (Exam Topic 3)
Graphics Interchange Format (GIF) is a _____ RGB bitmap image format for images with up to 256 distinct colors per frame.

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

Answer: A

NEW QUESTION 182
- (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 186
- (Exam Topic 2)
Which of the following attacks allows an attacker to access restricted directories, including application source code, configuration and critical system files, and to execute commands outside of the web server's root directory?

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

Answer: C

NEW QUESTION 188
- (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 189
- (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 194
- (Exam Topic 2)
A computer forensics investigator is inspecting the firewall logs for a large financial institution that has employees working 24 hours a day, 7 days a week.

What can the investigator infer from the screenshot seen below?

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

Answer: C

NEW QUESTION 197
- (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 201
- (Exam Topic 2)
Which of the following is a database in which information about every file and directory on an NT File System (NTFS) volume is stored?

A. Volume Boot Record
B. Master Boot Record
C. GUID Partition Table
D. Master File Table

Answer: D

NEW QUESTION 206
- (Exam Topic 2)
Which of the following are small pieces of data sent from a website and stored on the user's computer by the user's web browser to track, validate, and maintain specific user information?

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

Answer: C

NEW QUESTION 207
- (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 211
- (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 213
- (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 217
- (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 219
- (Exam Topic 2)
Paraben Lockdown device uses which operating system to write hard drive data?

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

Answer: D

NEW QUESTION 220
- (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 221
- (Exam Topic 2)
An executive has leaked the company trade secrets through an external drive. What process should the investigation team take if they could retrieve his system?

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

Answer: A

NEW QUESTION 222
- (Exam Topic 2)
Company ABC has employed a firewall, IDS, Antivirus, Domain Controller, and SIEM. The company's domain controller goes down. From which system would you begin your investigation?

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

Answer: C

NEW QUESTION 226
- (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 230
- (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 235
- (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 239
- (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 240
- (Exam Topic 2)
Which rule requires an original recording to be provided to prove the content of a recording?

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

Answer: B

NEW QUESTION 242
- (Exam Topic 2)
The process of restarting a computer that is already turned on through the operating system is called?

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

Answer: A

NEW QUESTION 244
- (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 246
- (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 250
- (Exam Topic 2)
Which of the following options will help users to enable or disable the last access time on a system running Windows 10 OS?

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

Answer: C

NEW QUESTION 254
- (Exam Topic 2)
When carrying out a forensics investigation, why should you never delete a partition on a dynamic disk?

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

Answer: C

NEW QUESTION 256
- (Exam Topic 2)
What feature of Windows is the following command trying to utilize?

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

Answer: C

NEW QUESTION 261
- (Exam Topic 2)
Adam, a forensic investigator, is investigating an attack on Microsoft Exchange Server of a large organization. As the first step of the investigation, he examined the PRIV.EDB file and found the source from where the mail originated and the name of the file that disappeared upon execution. Now, he wants to examine the MIME stream content. Which of the following files is he going to examine?

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

Answer: A

NEW QUESTION 263
- (Exam Topic 2)
Smith, a forensic examiner, was analyzing a hard disk image to find and acquire deleted sensitive files. He stumbled upon a $Recycle.Bin folder in the root directory of the disk. Identify the operating system in use.

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

Answer: D

NEW QUESTION 264
- (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 265
- (Exam Topic 2)
If a PDA is seized in an investigation while the device is turned on, what would be the proper procedure?

A. Keep the device powered on
B. Turn off the device immediately
C. Remove the battery immediately
D. Remove any memory cards immediately

Answer: A

NEW QUESTION 267
- (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 272
- (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 277
- (Exam Topic 2)
What is the first step taken in an investigation for laboratory forensic staff members?

A. Packaging the electronic evidence
B. Securing and evaluating the electronic crime scene
C. Conducting preliminary interviews
D. Transporting the electronic evidence

Answer: B

NEW QUESTION 279
- (Exam Topic 2)
In Steganalysis, which of the following describes a Known-stego attack?

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

Answer: C

NEW QUESTION 281
- (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 284
- (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 285
- (Exam Topic 2)
Which of the following stages in a Linux boot process involve initialization of the system’s hardware?

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

Answer: A

NEW QUESTION 286
- (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 287
- (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 288
- (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 291
- (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 295
- (Exam Topic 2)
Which of the following reports are delivered under oath to a board of directors/managers/panel of the jury?

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

Answer: B

NEW QUESTION 297
- (Exam Topic 2)
When should an MD5 hash check be performed when processing evidence?

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

Answer: C

NEW QUESTION 301
- (Exam Topic 2)
To which phase of the Computer Forensics Investigation Process does the Planning and Budgeting of a Forensics Lab belong?

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

Answer: C

NEW QUESTION 304
- (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 306
- (Exam Topic 2)
Which password cracking technique uses every possible combination of character sets?

A. Rainbow table attack

B. Brute force attack
C. Rule-based attack
D. Dictionary attack

Answer: B

NEW QUESTION 311
- (Exam Topic 2)
Why would a company issue a dongle with the software they sell?

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

Answer: C

NEW QUESTION 315
- (Exam Topic 2)
When marking evidence that has been collected with the “aaa/ddmmyy/nnnn/zz” format, what does the “nnnn” denote?

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

Answer: D

NEW QUESTION 318
- (Exam Topic 2)
What method of copying should always be performed first before carrying out an investigation?

A. Parity-bit copy
B. Bit-stream copy
C. MS-DOS disc copy
D. System level copy

Answer: B

NEW QUESTION 323
- (Exam Topic 2)
When searching through file headers for picture file formats, what should be searched to find a JPEG file in hexadecimal format?

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

Answer: A

NEW QUESTION 328
- (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 333
- (Exam Topic 2)
What technique is used by JPEGs for compression?

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

Answer: C

NEW QUESTION 336
- (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 339
- (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 341
- (Exam Topic 2)
In handling computer-related incidents, which IT role should be responsible for recovery, containment, and prevention to constituents?

A. Security Administrator
B. Network Administrator
C. Director of Information Technology
D. Director of Administration

Answer: B

NEW QUESTION 346
- (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 349
- (Exam Topic 2)
Jack Smith is a forensics investigator who works for Mason Computer Investigation Services. He is investigating a computer that was infected by Ramen Virus.

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

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

Answer: B

NEW QUESTION 352
- (Exam Topic 2)
What stage of the incident handling process involves reporting events?

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

Answer: C

NEW QUESTION 356
- (Exam Topic 2)
Smith, as a part his forensic investigation assignment, seized a mobile device. He was asked to recover the Subscriber Identity Module (SIM card) data in the mobile device. Smith found that the SIM was protected by a Personal Identification Number (PIN) code, but he was also aware that people generally leave the PIN numbers to the defaults or use easily guessable numbers such as 1234. He made three unsuccessful attempts, which blocked the SIM card. What can Jason do in this scenario to reset the PIN and access SIM data?

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

Answer: D

NEW QUESTION 357
- (Exam Topic 2)
Files stored in the Recycle Bin in its physical location are renamed as Dxy.ext, where “x” represents the _____.

A. Drive name
B. Original file name’s extension
C. Sequential number
D. Original file name

Answer: A

NEW QUESTION 359
- (Exam Topic 2)
In a virtual test environment, Michael is testing the strength and security of BGP using multiple routers to mimic the backbone of the Internet. This project will help him write his doctoral thesis on "bringing down the Internet". Without sniffing the traffic between the routers, Michael sends millions of RESET packets to the routers in an attempt to shut one or all of them down. After a few hours, one of the routers finally shuts itself down. What will the other routers communicate between themselves?

A. The change in the routing fabric to bypass the affected router
B. More RESET packets to the affected router to get it to power back up
C. RESTART packets to the affected router to get it to power back up
D. STOP packets to all other routers warning of where the attack originated

Answer: A

NEW QUESTION 364
- (Exam Topic 2)
Why should you never power on a computer that you need to acquire digital evidence from?

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

Answer: A

NEW QUESTION 365
- (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 370
- (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 371
- (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 373
- (Exam Topic 2)

Which of the following is an iOS Jailbreaking tool?

A. Kingo Android ROOT
B. Towelroot
C. One Click Root
D. Redsn0w

Answer: D

NEW QUESTION 376
- (Exam Topic 2)
Why would you need to find out the gateway of a device when investigating a wireless attack?

A. The gateway will be the IP of the proxy server used by the attacker to launch the attack
B. The gateway will be the IP of the attacker computer
C. The gateway will be the IP used to manage the RADIUS server
D. The gateway will be the IP used to manage the access point

Answer: D

NEW QUESTION 379
- (Exam Topic 2)
Paul is a computer forensics investigator working for Tyler & Company Consultants. Paul has been called upon to help investigate a computer hacking ring broken up by the local police. Paul begins to inventory the PCs found in the hackers hideout. Paul then comes across a PDA left by them that is attached to a number of different peripheral devices. What is the first step that Paul must take with the PDA to ensure the integrity of the investigation?

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

Answer: D

NEW QUESTION 380
- (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 384
- (Exam Topic 2)
Watson, a forensic investigator, is examining a copy of an ISO file stored in CDFS format. What type of evidence is this?

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

Answer: A

NEW QUESTION 386
- (Exam Topic 1)
Volatile Memory is one of the leading problems for forensics. Worms such as code Red are memory resident and do write themselves to the hard drive, if you turn the system off they disappear. In a lab environment, which of the following options would you suggest as the most appropriate to overcome the problem of capturing volatile memory?

A. Use VMware to be able to capture the data in memory and examine it
B. Give the Operating System a minimal amount of memory, forcing it to use a swap file
C. Create a Separate partition of several hundred megabytes and place the swap file there
D. Use intrusion forensic techniques to study memory resident infections

Answer: C

NEW QUESTION 390
- (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 392
- (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 397
- (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 398
- (Exam Topic 1)
After passively scanning the network of Department of Defense (DoD), you switch over to active scanning to identify live hosts on their network. DoD is a large organization and should respond to any number of scans. You start an ICMP ping sweep by sending an IP packet to the broadcast address. Only five hosts respond to your ICMP pings; definitely not the number of hosts you were expecting. Why did this ping sweep only produce a few responses?

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

Answer: D

NEW QUESTION 402
- (Exam Topic 1)
When examining a hard disk without a write-blocker, you should not start windows because Windows will write data to the:

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

Answer: A

NEW QUESTION 405
- (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 407
- (Exam Topic 1)
How many bits is Source Port Number in TCP Header packet?

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

Answer: A

NEW QUESTION 408
- (Exam Topic 1)
You are a security analyst performing a penetration tests for a company in the Midwest. After some initial reconnaissance, you discover the IP addresses of some

Cisco routers used by the company. You type in the following URL that includes the IP address of one of the routers:
http://172.168.4.131/level/99/exec/show/config
After typing in this URL, you are presented with the entire configuration file for that router. What have you discovered?

A. HTTP Configuration Arbitrary Administrative Access Vulnerability
B. HTML Configuration Arbitrary Administrative Access Vulnerability
C. Cisco IOS Arbitrary Administrative Access Online Vulnerability
D. URL Obfuscation Arbitrary Administrative Access Vulnerability

Answer: A

NEW QUESTION 412
- (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 416
- (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 421
- (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 424
- (Exam Topic 1)
George is a senior security analyst working for a state agency in Florida. His state's congress just passed a bill mandating every state agency to undergo a security audit annually. After learning what will be required, George needs to implement an IDS as soon as possible before the first audit occurs. The state bill requires that an IDS with a "time-based induction machine" be used.
What IDS feature must George implement to meet this requirement?

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

Answer: C

NEW QUESTION 429
- (Exam Topic 1)
When investigating a network that uses DHCP to assign IP addresses, where would you look to determine which system (MAC address) had a specific IP address at a specific time?

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

Answer: C

NEW QUESTION 433
- (Exam Topic 1)
In a FAT32 system, a 123 KB file will use how many sectors?

A. 34
B. 25

C. 11
D. 56

Answer: B

NEW QUESTION 437
- (Exam Topic 1)
Which of the following is NOT a graphics file?

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

Answer: C

NEW QUESTION 440
- (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 444
- (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 447
- (Exam Topic 1)
What binary coding is used most often for e-mail purposes?

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

Answer: A

NEW QUESTION 450
- (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 455
- (Exam Topic 1)
Printing under a Windows Computer normally requires which one of the following files types to be created?

A. EME
B. MEM

C. EMF
D. CME

Answer: C

NEW QUESTION 458
- (Exam Topic 1)
You are working for a large clothing manufacturer as a computer forensics investigator and are called in to investigate an unusual case of an employee possibly stealing clothing designs from the company and selling them under a different brand name for a different company. What you discover during the course of the investigation is that the clothing designs are actually original products of the employee and the company has no policy against an employee selling his own designs on his own time. The only thing that you can find that the employee is doing wrong is that his clothing design incorporates the same graphic symbol as that of the company with only the wording in the graphic being different. What area of the law is the employee violating?

A. trademark law
B. copyright law
C. printright law
D. brandmark law

Answer: A

NEW QUESTION 459
- (Exam Topic 1)
What is kept in the following directory? HKLM\SECURITY\Policy\Secrets

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

Answer: B

NEW QUESTION 461
- (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 464
- (Exam Topic 1)
When an investigator contacts by telephone the domain administrator or controller listed by a Who is lookup to request all e-mails sent and received for a user account be preserved, what U.S.C. statute authorizes this phone call and obligates the ISP to preserve e-mail records?

A. Title 18, Section 1030
B. Title 18, Section 2703(d)
C. Title 18, Section Chapter 90
D. Title 18, Section 2703(f)

Answer: D

NEW QUESTION 468
- (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 470
- (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 472
- (Exam Topic 1)
When investigating a Windows System, it is important to view the contents of the page or swap file because:

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

Answer: C

NEW QUESTION 473
- (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 476
- (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 478
- (Exam Topic 1)
Office Documents (Word, Excel and PowerPoint) contain a code that allows tracking the MAC or unique identifier of the machine that created the document. What is that code called?

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

Answer: A

NEW QUESTION 480
- (Exam Topic 1)
Bob has been trying to penetrate a remote production system for the past two weeks. This time however, he is able to get into the system. He was able to use the System for a period of three weeks. However, law enforcement agencies were recoding his every activity and this was later presented as evidence.
The organization had used a Virtual Environment to trap Bob. What is a Virtual Environment?

A. A Honeypot that traps hackers
B. A system Using Trojaned commands
C. An environment set up after the user logs in
D. An environment set up before a user logs in

Answer: A

NEW QUESTION 485

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

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

Answer: B

NEW QUESTION 487
- (Exam Topic 1)

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

Answer: B

NEW QUESTION 492
- (Exam Topic 1)
Under which Federal Statutes does FBI investigate for computer crimes involving e-mail scams and mail fraud?

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

Answer: B

NEW QUESTION 493
- (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 494
- (Exam Topic 1)
To make sure the evidence you recover and analyze with computer forensics software can be admitted in court, you must test and validate the software. What group is actively providing tools and creating procedures for testing and validating computer forensics software?

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

Answer: C

NEW QUESTION 497
- (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 498
- (Exam Topic 1)
What type of file is represented by a colon (:) with a name following it in the Master File Table of NTFS disk?

A. A compressed file
B. A Data stream file
C. An encrypted file
D. A reserved file

Answer: B

NEW QUESTION 500
- (Exam Topic 1)
Microsoft Outlook maintains email messages in a proprietary format in what type of file?

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

Answer: C

NEW QUESTION 505
- (Exam Topic 1)
You are called in to assist the police in an investigation involving a suspected drug dealer. The suspects house was searched by the police after a warrant was obtained and they located a floppy disk in the suspects bedroom. The disk contains several files, but they appear to be password protected. What are two common methods used by password cracking software that you can use to obtain the password?

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

Answer: B

NEW QUESTION 509
- (Exam Topic 1)
What is the following command trying to accomplish?

A. Verify that UDP port 445 is open for the 192.168.0.0 network
B. Verify that TCP port 445 is open for the 192.168.0.0 network
C. Verify that NETBIOS is running for the 192.168.0.0 network
D. Verify that UDP port 445 is closed for the 192.168.0.0 network

Answer: A

NEW QUESTION 514
- (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 515
- (Exam Topic 1)
What should you do when approached by a reporter about a case that you are working on or have worked on?

A. Refer the reporter to the attorney that retained you
B. Say, "no comment"
C. Answer all the reporter’s questions as completely as possible
D. Answer only the questions that help your case

Answer: A

NEW QUESTION 519
- (Exam Topic 1)
What file structure database would you expect to find on floppy disks?

A. NTFS
B. FAT32
C. FAT16
D. FAT12

Answer: D

NEW QUESTION 524
- (Exam Topic 1)
Larry is an IT consultant who works for corporations and government agencies. Larry plans on shutting down the city's network using BGP devices and zombies? What type of Penetration Testing is Larry planning to carry out?

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

Answer: B

NEW QUESTION 528
- (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 530
- (Exam Topic 1)
The MD5 program is used to:

A. wipe magnetic media before recycling it
B. make directories on an evidence disk
C. view graphics files on an evidence drive
D. verify that a disk is not altered when you examine it

Answer: D

NEW QUESTION 531
- (Exam Topic 1)
What does mactime, an essential part of the coroner's toolkit do?

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

Answer: A

NEW QUESTION 533
- (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 535
- (Exam Topic 1)
Bill is the accounting manager for Grummon and Sons LLC in Chicago. On a regular basis, he needs to send PDF documents containing sensitive information through E-mail to his customers.
Bill protects the PDF documents with a password and sends them to their intended recipients. Why PDF passwords do not offer maximum protection?

A. PDF passwords can easily be cracked by software brute force tools
B. PDF passwords are converted to clear text when sent through E-mail
C. PDF passwords are not considered safe by Sarbanes-Oxley
D. When sent through E-mail, PDF passwords are stripped from the document completely

Answer: A

NEW QUESTION 539
- (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 542
- (Exam Topic 1)
What term is used to describe a cryptographic technique for embedding information into something else for the sole purpose of hiding that information from the casual observer?

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

Answer: C

NEW QUESTION 547
- (Exam Topic 1)
If a suspect computer is located in an area that may have toxic chemicals, you must:

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

Answer: A

NEW QUESTION 551
- (Exam Topic 1)
Which is a standard procedure to perform during all computer forensics investigations?

A. with the hard drive removed from the suspect PC, check the date and time in the system's CMOS
B. with the hard drive in the suspect PC, check the date and time in the File Allocation Table
C. with the hard drive removed from the suspect PC, check the date and time in the system's RAM
D. with the hard drive in the suspect PC, check the date and time in the system's CMOS

Answer: A

NEW QUESTION 555
- (Exam Topic 1)
A honey pot deployed with the IP 172.16.1.108 was compromised by an attacker. Given below is an excerpt from a Snort binary capture of the attack. Decipher the activity carried out by the attacker by studying the log. Please note that you are required to infer only what is explicit in the excerpt.
(Note: The student is being tested on concepts learnt during passive OS fingerprinting, basic TCP/IP connection concepts and the ability to read packet signatures from a sniff dump.)
03/15-20:21:24.107053 211.185.125.124:3500 -> 172.16.1.108:111
TCP TTL:43 TOS:0x0 ID:29726 IpLen:20 DgmLen:52 DF
A* Seq: 0x9B6338C5 Ack: 0x5820ADD0 Win: 0x7D78 TcpLen: 32 TCP Options (3) => NOP NOP TS: 23678634 2878772
=+= 03/15-20:21:24.452051 211.185.125.124:789 -> 172.16.1.103:111
UDP TTL:43 TOS:0x0 ID:29733 IpLen:20 DgmLen:84
Len: 64
01 0A 8A 0A 00 00 00 00 00 00 00 02 00 01 86 A0 .....
00 00 00 02 00 00 00 03 00 00 00 00 00 00 00 00 .....
00 00 00 00 00 00 00 00 00 01 86 B8 00 00 00 01 .....
00 00 00 11 00 00 00 00 .....
=+= 03/15-20:21:24.730436 211.185.125.124:790 -> 172.16.1.103:32773
UDP TTL:43 TOS:0x0 ID:29781 IpLen:20 DgmLen:1104 Len: 1084
47 F7 9F 63 00 00 00 00 00 00 00 02 00 01 86 B8

A. The attacker has conducted a network sweep on port 111
B. The attacker has scanned and exploited the system using Buffer Overflow
C. The attacker has used a Trojan on port 32773
D. The attacker has installed a backdoor

Answer: A

NEW QUESTION 559
- (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 560
- (Exam Topic 1)
What will the following URL produce in an unpatched IIS Web Server? http://www.thetargetsite.com/scripts/..%co%af../..%co%af../windows/system32/cmd.exe?/c+dir+c:\

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

Answer: A

NEW QUESTION 564
- (Exam Topic 1)
You should make at least how many bit-stream copies of a suspect drive?

A. 1
B. 2
C. 3
D. 4

Answer: B

NEW QUESTION 565
- (Exam Topic 1)
When you carve an image, recovering the image depends on which of the following skills?

A. Recognizing the pattern of the header content
B. Recovering the image from a tape backup
C. Recognizing the pattern of a corrupt file
D. Recovering the image from the tape backup

Answer: A

NEW QUESTION 567
- (Exam Topic 1)
Jim performed a vulnerability analysis on his network and found no potential problems. He runs another utility that executes exploits against his system to verify the results of the vulnerability test.
The second utility executes five known exploits against his network in which the vulnerability analysis said were not exploitable. What kind of results did Jim receive from his vulnerability analysis?

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

Answer: A

NEW QUESTION 570
- (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 571
- (Exam Topic 1)
When setting up a wireless network with multiple access points, why is it important to set each access point on a different channel?

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

Answer: D

NEW QUESTION 575
- (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 580
- (Exam Topic 1)
What is a good security method to prevent unauthorized users from "tailgating"?

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

Answer: A

NEW QUESTION 583
- (Exam Topic 1)
This organization maintains a database of hash signatures for known software.

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

Answer: C

NEW QUESTION 585
- (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 589
- (Exam Topic 1)
Harold is a web designer who has completed a website for ghttech.net. As part of the maintenance agreement he signed with the client, Harold is performing research online and seeing how much exposure the site has received so far. Harold navigates to google.com and types in the following search. link:www.ghttech.net What will this search produce?

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

Answer: B

NEW QUESTION 594
- (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 595
- (Exam Topic 1)
_____ is simply the application of Computer Investigation and analysis techniques in the interests of determining potential legal evidence.

A. Network Forensics
B. Computer Forensics
C. Incident Response

D. Event Reaction

Answer: B

NEW QUESTION 599
- (Exam Topic 1)
You are the security analyst working for a private company out of France. Your current assignment is to obtain credit card information from a Swiss bank owned by that company. After initial reconnaissance, you discover that the bank security defenses are very strong and would take too long to penetrate. You decide to get the information by monitoring the traffic between the bank and one of its subsidiaries in London. After monitoring some of the traffic, you see a lot of FTP packets traveling back and forth. You want to sniff the traffic and extract usernames and passwords. What tool could you use to get this information?

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

Answer: C

NEW QUESTION 601
- (Exam Topic 1)
Profiling is a forensics technique for analyzing evidence with the goal of identifying the perpetrator from their various activity. After a computer has been compromised by a hacker, which of the following would be most important in forming a profile of the incident?

A. The manufacturer of the system compromised
B. The logic, formatting and elegance of the code used in the attack
C. The nature of the attack
D. The vulnerability exploited in the incident

Answer: B

NEW QUESTION 603
- (Exam Topic 1)
An employee is attempting to wipe out data stored on a couple of compact discs (CDs) and digital video discs (DVDs) by using a large magnet. You inform him that this method will not be effective in wiping out the data because CDs and DVDs are _____ media used to store large amounts of data and are not affected by the magnet.

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

Answer: D

NEW QUESTION 607
- (Exam Topic 1)
Simon is a former employee of Trinitron XML Inc. He feels he was wrongly terminated and wants to hack into his former company's network. Since Simon remembers some of the server names, he attempts to run the axfr and ixfr commands using DIG. What is Simon trying to accomplish here?

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

Answer: C

NEW QUESTION 612
- (Exam Topic 1)
Diskcopy is:

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

Answer: B

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

NEW QUESTION 615
- (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 616
- (Exam Topic 1)
What type of attack occurs when an attacker can force a router to stop forwarding packets by flooding the router with many open connections simultaneously so that all the hosts behind the router are effectively disabled?

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

Answer: B

NEW QUESTION 619
- (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 623
- (Exam Topic 1)
If you discover a criminal act while investigating a corporate policy abuse, it becomes a publicsector investigation and should be referred to law enforcement?

A. true
B. false

Answer: A

NEW QUESTION 627
.....

Thank You for Trying Our Product

* 100% Pass or Money Back

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

* One year free update

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

* Trusted by Millions

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

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your 312-49v10 Exam with Our Prep Materials Via below:

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