EC-Council

Exam Questions 312-49v10

Computer Hacking Forensic Investigator (CHFI-v10)

NEW QUESTION 1
- (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 2
- (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 3
- (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 4
- (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 5
- (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 6
- (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 7
- (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 8
- (Exam Topic 1)
George is performing security analysis for Hammond and Sons LLC. He is testing security vulnerabilities of their wireless network. He plans on remaining as "stealthy" as possible during the scan. Why would a scanner like Nessus is not recommended in this situation?

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

Answer: A

NEW QUESTION 9
- (Exam Topic 1)
Jason is the security administrator of ACMA metal Corporation. One day he notices the company's Oracle database server has been compromised and the customer information along with financial data has been stolen. The financial loss will be in millions of dollars if the database gets into the hands of the competitors. Jason wants to report this crime to the law enforcement agencies immediately.
Which organization coordinates computer crimes investigations throughout the United States?

A. Internet Fraud Complaint Center
B. Local or national office of the U.
C. Secret Service
D. National Infrastructure Protection Center
E. CERT Coordination Center

Answer: B

NEW QUESTION 10
- (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 10
- (Exam Topic 1)
The following excerpt is taken from a honeypot log. The log captures activities across three days. There are several intrusion attempts; however, a few are successful.
(Note: The objective of this question is to test whether the student can read basic information from log entries and interpret the nature of attack.)
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
From the options given below choose the one which best interprets the following entry: Apr 26 06:43:05 [6283]: IDS181/nops-x86: 63.226.81.13:1351 -> 172.16.1.107:53

A. An IDS evasion technique
B. A buffer overflow attempt
C. A DNS zone transfer

D. Data being retrieved from 63.226.81.13

Answer: A

NEW QUESTION 14
- (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: C

NEW QUESTION 15
- (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 18
- (Exam Topic 1)
You are employed directly by an attorney to help investigate an alleged sexual harassment case at a large pharmaceutical manufacture. While at the corporate office of the company, the CEO demands to know the status of the investigation. What prevents you from discussing the case with the CEO?

A. the attorney-work-product rule
B. Good manners
C. Trade secrets
D. ISO 17799

Answer: A

NEW QUESTION 20
- (Exam Topic 1)
Paul's company is in the process of undergoing a complete security audit including logical and physical security testing. After all logical tests were performed; it is now time for the physical round to begin. None of the employees are made aware of this round of testing. The security-auditing firm sends in a technician dressed as an electrician. He waits outside in the lobby for some employees to get to work and follows behind them when they access the restricted areas. After entering the main office, he is able to get into the server room telling the IT manager that there is a problem with the outlets in that room. What type of attack has the technician performed?

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

Answer: A

NEW QUESTION 25
- (Exam Topic 2)
Which of the following file contains the traces of the applications installed, run, or uninstalled from a system?

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

Answer: A

NEW QUESTION 27
- (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 30
- (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 33
- (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 37
- (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 39
- (Exam Topic 2)
Which of the following commands shows you the names of all open shared files on a server and the number of file locks on each file?

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

Answer: B

NEW QUESTION 41
- (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 46
- (Exam Topic 1)
What will the following command accomplish?

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

Answer: A

NEW QUESTION 50

- (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 52
- (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 54
- (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 57
- (Exam Topic 1)
Which Intrusion Detection System (IDS) usually produces the most false alarms due to the unpredictable behaviors of users and networks?

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

Answer: B

NEW QUESTION 60
- (Exam Topic 1)
The rule of thumb when shutting down a system is to pull the power plug. However, it has certain drawbacks. Which of the following would that be?

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

Answer: A

NEW QUESTION 61
- (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 62
- (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 63
- (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 68
- (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 71
- (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 72
- (Exam Topic 1)
With Regard to using an Antivirus scanner during a computer forensics investigation, You should:

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

Answer: D

NEW QUESTION 75
- (Exam Topic 1)
You are contracted to work as a computer forensics investigator for a regional bank that has four 30 TB storage area networks that store customer data.
What method would be most efficient for you to acquire digital evidence from this network?

A. create a compressed copy of the file with DoubleSpace
B. create a sparse data copy of a folder or file
C. make a bit-stream disk-to-image file
D. make a bit-stream disk-to-disk file

Answer: C

NEW QUESTION 78
- (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 79
- (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 82
- (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 84
- (Exam Topic 1)
The police believe that Melvin Matthew has been obtaining unauthorized access to computers belonging to numerous computer software and computer operating systems manufacturers, cellular telephone manufacturers, Internet Service Providers and Educational Institutions. They also suspect that he has been stealing, copying and misappropriating proprietary computer software belonging to the several victim companies. What is preventing the police from breaking down the suspects door and searching his home and seizing all of his computer equipment if they have not yet obtained a warrant?

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

Answer: A

NEW QUESTION 86
- (Exam Topic 1)
What is the name of the Standard Linux Command that is also available as windows application that can be used to create bit-stream images?

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

Answer: D

NEW QUESTION 91
- (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 94
- (Exam Topic 1)
Sectors in hard disks typically contain how many bytes?

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

Answer: B

NEW QUESTION 99
- (Exam Topic 1)
When obtaining a warrant, it is important to:

A. particularlydescribe the place to be searched and particularly describe the items to be seized
B. generallydescribe the place to be searched and particularly describe the items to be seized
C. generallydescribe the place to be searched and generally describe the items to be seized
D. particularlydescribe the place to be searched and generally describe the items to be seized

Answer: A

NEW QUESTION 102
- (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 105
- (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 109
- (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 112
- (Exam Topic 4)
This is a statement, other than one made by the declarant while testifying at the trial or hearing, offered in evidence to prove the truth of the matter asserted. Which among the following is suitable for the above statement?

A. Testimony by the accused
B. Limited admissibility
C. Hearsay rule
D. Rule 1001

Answer: C

NEW QUESTION 117
- (Exam Topic 4)
Mark works for a government agency as a cyber-forensic investigator. He has been given the task of restoring data from a hard drive. The partition of the hard drive was deleted by a disgruntled employee In order to hide their nefarious actions. What tool should Mark use to restore the data?

A. EFSDump
B. Diskmon D
C. iskvlew
D. R-Studio

Answer: D

NEW QUESTION 120

- (Exam Topic 4)
Storage location of Recycle Bin for NTFS file systems (Windows Vista and later) is located at:

A. Drive:\$ Recycl
B. Bin
C. DriveARECYCIE.BIN
D. Drive:\RECYCLER
E. Drive:\REYCLED

Answer: C

NEW QUESTION 125
- (Exam Topic 4)
Which "Standards and Criteria" under SWDGE states that "the agency must use hardware and software that are appropriate and effective for the seizure or examination procedure"?

A. Standards and Criteria 1.7
B. Standards and Criteria 1.6
C. Standards and Criteria 1.4
D. Standards and Criteria 1.5

Answer: D

NEW QUESTION 127
- (Exam Topic 4)
Simona has written a regular expression for the detection of web application-specific attack attempt that reads as /((\%3C)|<K(\%2F)|V)*[a-zO-9\%I*((\%3E)|>)/Ix. Which of the following does the part (|\%3E)|>) look for?

A. Alphanumeric string or its hex equivalent
B. Opening angle bracket or its hex equivalent
C. Closing angle bracket or its hex equivalent
D. Forward slash for a closing tag or its hex equivalent

Answer: D

NEW QUESTION 130
- (Exam Topic 4)
Rule 1002 of Federal Rules of Evidence (US) talks about

A. Admissibility of original
B. Admissibility of duplicates
C. Requirement of original
D. Admissibility of other evidence of contents

Answer: C

NEW QUESTION 132
- (Exam Topic 4)
You are an information security analyst at a large pharmaceutical company. While performing a routine review of audit logs, you have noticed a significant amount of egress traffic to various IP addresses on destination port 22 during off-peak hours. You researched some of the IP addresses and found that many of them are in Eastern Europe. What is the most likely cause of this traffic?

A. Malicious software on internal system is downloading research data from partner 5FTP servers in Eastern Europe
B. Internal systems are downloading automatic Windows updates
C. Data is being exfiltrated by an advanced persistent threat (APT)
D. The organization's primary internal DNS server has been compromised and is performing DNS zone transfers to malicious external entities

Answer: C

NEW QUESTION 137
- (Exam Topic 4)
A call detail record (CDR) provides metadata about calls made over a phone service. From the following data fields, which one Is not contained in a CDR.

A. The call duration
B. A unique sequence number identifying the record
C. The language of the call
D. Phone number receiving the call

Answer: C

NEW QUESTION 138
- (Exam Topic 4)
Which of the following is the most effective tool for acquiring volatile data from a Windows-based system?

A. Coreography
B. Datagrab
C. Ethereal

D. Helix

Answer: D

NEW QUESTION 139
- (Exam Topic 4)
Which of the following directory contains the binary files or executables required for system maintenance and administrative tasks on a Linux system?

A. /sbin
B. /bin
C. /usr
D. /lib

Answer: A

NEW QUESTION 140
- (Exam Topic 4)
Assume there Is a file named myflle.txt In C: drive that contains hidden data streams. Which of the following commands would you Issue to display the contents of a data stream?

A. echo text > program: source_file
B. myfile.dat: st ream 1
C. C:\MORE < myfile.txt:siream1
D. C:\>ECHO text_message > myfile.txt:stream1

Answer: A

NEW QUESTION 141
- (Exam Topic 4)
Harry has collected a suspicious executable file from an infected system and seeks to reverse its machine code to Instructions written in assembly language. Which tool should he use for this purpose?

A. Ollydbg
B. oledump
C. HashCalc
D. BinText

Answer: A

NEW QUESTION 146
- (Exam Topic 4)
Frank, a cloud administrator in his company, needs to take backup of the OS disks of two Azure VMs that store business-critical data. Which type of Azure blob storage can he use for this purpose?

A. Append blob
B. Medium blob
C. Block blob
D. Page blob

Answer: D

NEW QUESTION 149
- (Exam Topic 4)
Williamson is a forensic investigator. While investigating a case of data breach at a company, he is maintaining a document that records details such as the forensic processes applied on the collected evidence, particulars of people handling It. the dates and times when it Is being handled, and the place of storage of the evidence. What do you call this document?

A. Consent form
B. Log book
C. Authorization form
D. Chain of custody

Answer: D

NEW QUESTION 151
- (Exam Topic 4)
Cloud forensic investigations impose challenges related to multi-jurisdiction and multi-tenancy aspects. To have a better understanding of the roles and responsibilities between the cloud service provider (CSP) and the client, which document should the forensic investigator review?

A. Service level agreement
B. Service level management
C. National and local regulation
D. Key performance indicator

Answer: A

NEW QUESTION 153
- (Exam Topic 4)
Donald made an OS disk snapshot of a compromised Azure VM under a resource group being used by the affected company as a part of forensic analysis process. He then created a vhd file out of the snapshot and stored it in a file share and as a page blob as backup in a storage account under different region. What Is the next thing he should do as a security measure?

A. Recommend changing the access policies followed by the company
B. Delete the snapshot from the source resource group
C. Delete the OS disk of the affected VM altogether
D. Create another VM by using the snapshot

Answer: C

NEW QUESTION 155
- (Exam Topic 4)
A breach resulted from a malware attack that evaded detection and compromised the machine memory without installing any software or accessing the hard drive. What technique did the adversaries use to deliver the attack?

A. Fileless
B. Trojan
C. JavaScript
D. Spyware

Answer: A

NEW QUESTION 159
- (Exam Topic 4)
When installed on a Windows machine, which port does the Tor browser use to establish a network connection via Tor nodes?

A. 7680
B. 49667/49668
C. 9150/9151
D. 49664/49665

Answer: C

NEW QUESTION 162
- (Exam Topic 4)
"In exceptional circumstances, where a person finds it necessary to access original data held on a computer or on storage media, that person must be competent to do so and be able to explain his/her actions and the impact of those actions on the evidence, in the court." Which ACPO principle states this?

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

Answer: D

NEW QUESTION 165
- (Exam Topic 4)
allows a forensic investigator to identify the missing links during investigation.

A. Evidence preservation
B. Chain of custody
C. Evidence reconstruction
D. Exhibit numbering

Answer: C

NEW QUESTION 167
- (Exam Topic 4)
Place the following In order of volatility from most volatile to the least volatile.

A. Registers and cache, routing tables, temporary file systems, disk storage, archival media
B. Register and cache, temporary file systems, routing tables, disk storage, archival media
C. Registers and cache, routing tables, temporary file systems, archival media, disk storage
D. Archival media, temporary file systems, disk storage, archival media, register and cache

Answer: B

NEW QUESTION 170
- (Exam Topic 4)
Data density of a disk drive is calculated by using

A. Slack space, bit density, and slack density.
B. Track space, bit area, and slack space.
C. Track density, areal density, and slack density.

D. Track density, areal density, and bit density.

Answer: D

NEW QUESTION 171
- (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 176
- (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 177
- (Exam Topic 3)
You are assigned a task to examine the log files pertaining to MyISAM storage engine. While examining, you are asked to perform a recovery operation on a MyISAM log file. Which among the following MySQL Utilities allow you to do so?

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

Answer: C

NEW QUESTION 181
- (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 182
- (Exam Topic 3)
Bob has encountered a system crash and has lost vital data stored on the hard drive of his Windows computer. He has no cloud storage or backup hard drives. He wants to recover all the data, which includes his personal photos, music, documents, videos, official emails, etc. Which of the following tools shall resolve Bob's purpose?

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

Answer: B

NEW QUESTION 186
- (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 191

- (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 192
- (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 194
- (Exam Topic 3)
What technique is used by JPEGs for compression?

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

Answer: C

NEW QUESTION 195
- (Exam Topic 3)
Buffer overflow vulnerability of a web application occurs when it 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 memory locations
B. Adjacent bit blocks
C. Adjacent buffer locations
D. Adjacent string locations

Answer: A

NEW QUESTION 197
- (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 199
- (Exam Topic 3)
Raw data acquisition format creates of a data set or suspect drive.

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

Answer: B

NEW QUESTION 200
- (Exam Topic 3)
Joshua is analyzing an MSSQL database for finding the attack evidence and other details, where should he look for the database logs?

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

Answer: C

NEW QUESTION 203
- (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 204
- (Exam Topic 3)
Which of these Windows utility help you to repair logical file system errors?

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

Answer: D

NEW QUESTION 209
- (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

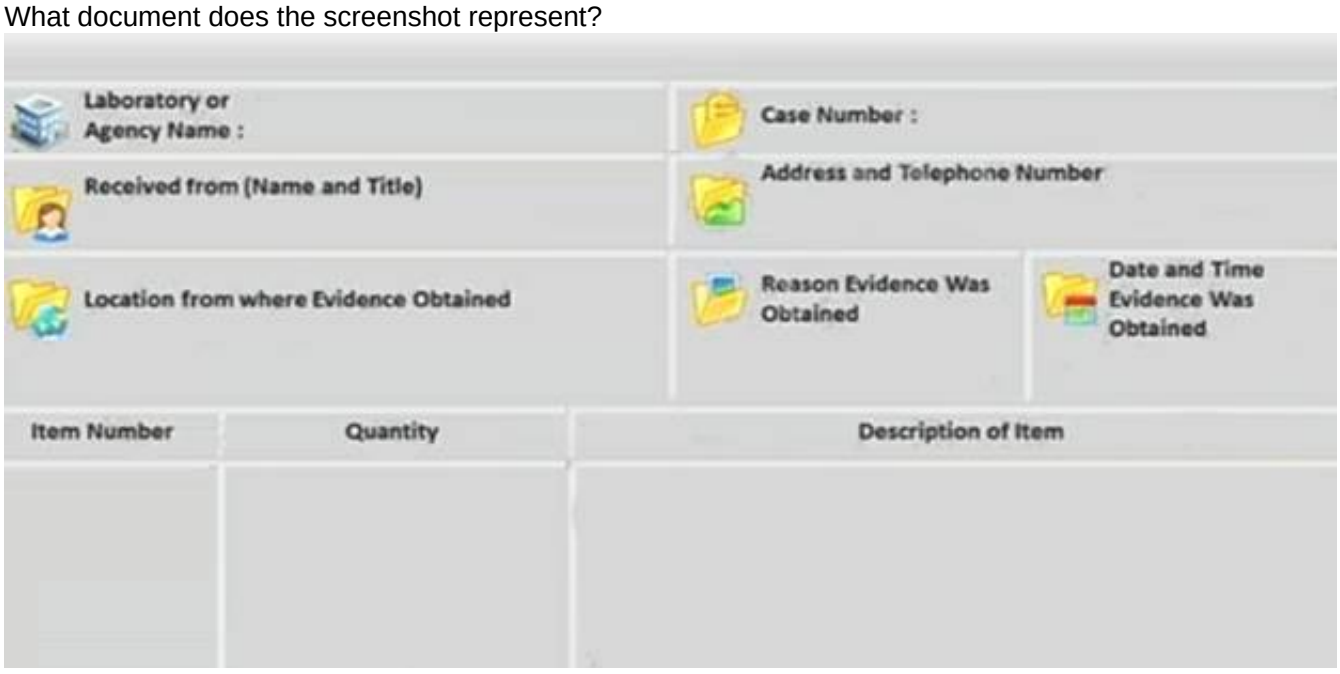
Answer: B

NEW QUESTION 213
- (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 214
- (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 216
- (Exam Topic 3)
Which forensic investigation methodology believes that criminals commit crimes solely to benefit their criminal enterprises?

A. Scientific Working Group on Digital Evidence
B. Daubert Standard
C. Enterprise Theory of Investigation
D. Fyre Standard

Answer: C

NEW QUESTION 221
- (Exam Topic 3)
Email archiving is a systematic approach to save and protect the data contained in emails so that it can be accessed fast at a later date. There are two main archive types, namely Local Archive and Server Storage Archive. Which of the following statements is correct while dealing with local archives?

A. Server storage archives are the server information and settings stored on a local system, whereas the local archives are the local email client information stored on the mail server
B. It is difficult to deal with the webmail as there is no offline archive in most case
C. So consult your counsel on the case as to the best way to approach and gain access to the required data on servers
D. Local archives should be stored together with the server storage archives in order to be admissible in a court of law
E. Local archives do not have evidentiary value as the email client may alter the message data

Answer: B

NEW QUESTION 222
- (Exam Topic 3)
Which of the following tool is used to locate IP addresses?

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

Answer: A

NEW QUESTION 226
- (Exam Topic 3)
What is the purpose of using Obfuscator in malware?

A. Execute malicious code in the system
B. Avoid encryption while passing through a VPN
C. Avoid detection by security mechanisms
D. Propagate malware to other connected devices

Answer: C

NEW QUESTION 228
- (Exam Topic 3)
Which one of the following is not a first response procedure?

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

Answer: C

NEW QUESTION 230
- (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 235
- (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 238
- (Exam Topic 3)
An investigator enters the command sqlcmd -S WIN-CQQMK62867E -e -s"," -E as part of collecting the primary data file and logs from a database. What does the "WIN-CQQMK62867E" represent?

A. Name of the Database
B. Name of SQL Server
C. Operating system of the system
D. Network credentials of the database

Answer: B

NEW QUESTION 242
- (Exam Topic 3)
A Linux system is undergoing investigation. In which directory should the investigators look for its current state data if the system is in powered on state?

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

Answer: B

NEW QUESTION 245
- (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 248
- (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 252
- (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 257
- (Exam Topic 3)
Which of the following examinations refers to the process of providing the opposing side in a trial the opportunity to question a witness?

A. Cross Examination
B. Direct Examination
C. Indirect Examination
D. Witness Examination

Answer: A

NEW QUESTION 262

- (Exam Topic 3)
Select the tool appropriate for examining the dynamically linked libraries of an application or malware.

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

Answer: A

NEW QUESTION 264
- (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 265
- (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 266
- (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 268
- (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 272
- (Exam Topic 3)
As part of extracting the system data, Jenifer has used the netstat command. What does this tool reveal?

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

Answer: C

NEW QUESTION 275
- (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 280
- (Exam Topic 3)
When analyzing logs, it is important that the clocks of all the network devices are synchronized. Which protocol will help in synchronizing these clocks?

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

Answer: D

NEW QUESTION 285
- (Exam Topic 3)
Pick the statement which does not belong to the Rule 804. Hearsay Exceptions; Declarant Unavailable.

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

Answer: D

NEW QUESTION 289
- (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 292
- (Exam Topic 3)
Which Linux command when executed displays kernel ring buffers or information about device drivers loaded into the kernel?

A. pgrep
B. dmesg
C. fsck
D. grep

Answer: B

NEW QUESTION 293
- (Exam Topic 3)
What does Locard's Exchange Principle state?

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

Answer: C

NEW QUESTION 296
- (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 299
- (Exam Topic 3)
Korey, a data mining specialist in a knowledge processing firm DataHub.com, reported his CISO that he has lost certain sensitive data stored on his laptop. The CISO wants his forensics investigation team to find if the data loss was accident or intentional. In which of the following category this case will fall?

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

Answer: B

NEW QUESTION 301
- (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 305
- (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 306
- (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 URL that 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 309
- (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 311
- (Exam Topic 3)
Which of the following is NOT a physical evidence?

A. Removable media
B. Cables
C. Image file on a hard disk
D. Publications

Answer: C

NEW QUESTION 316
- (Exam Topic 3)
NTFS sets a flag for the file once you encrypt it and creates an EFS attribute where it stores Data Decryption Field (DDF) and Data Recovery Field (DDR). Which of the following is not a part of DDF?

A. Encrypted FEK
B. Checksum
C. EFS Certificate Hash
D. Container Name

Answer: B

NEW QUESTION 317
- (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 319
- (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 321
- (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 325
- (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 330
- (Exam Topic 2)
What will the following Linux command accomplish? dd if=/dev/mem of=/home/sam/mem.bin bs=1024

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

Answer: C

NEW QUESTION 333
- (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 337
- (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 338
- (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 342
- (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 343
- (Exam Topic 2)
Which of the following tool can the investigator use to analyze the network to detect Trojan activities?

A. Regshot
B. TRIPWIRE
C. RAM Computer
D. Capsa

Answer: D

NEW QUESTION 346
- (Exam Topic 2)
Harold is finishing up a report on a case of network intrusion, corporate spying, and embezzlement that he has been working on for over six months. He is trying to find the right term to use in his report to describe network-enabled spying. What term should Harold use?

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

Answer: C

NEW QUESTION 349
- (Exam Topic 2)
Jacky encrypts her documents using a password. It is known that she uses her daughter’s year of birth as part of the password. Which password cracking technique would be optimal to crack her password?

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

Answer: A

NEW QUESTION 352
- (Exam Topic 2)
What feature of Decryption Collection allows an investigator to crack a password as quickly as possible?

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

Answer: B

NEW QUESTION 357
- (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 362
- (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 364
- (Exam Topic 2)
What does 254 represent in ICCID 89254021520014515744?

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

Answer: B

NEW QUESTION 369
- (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 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 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 376
- (Exam Topic 2)
What does the 63.78.199.4(161) denotes in a Cisco router log?
Mar 14 22:57:53.425 EST: %SEC-6-IPACCESSLOGP: list internet-inbound denied udp 66.56.16.77(1029) -> 63.78.199.4(161), 1 packet

A. Destination IP address

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

Answer: A

NEW QUESTION 377
- (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 379
- (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 381
- (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 382
- (Exam Topic 2)
Which of the following commands shows you all of the network services running on Windows-based servers?

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

Answer: A

NEW QUESTION 387
- (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 390
- (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 393

- (Exam Topic 2)
Which among the following files provides email header information in the Microsoft Exchange server?

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

Answer: B

NEW QUESTION 397
- (Exam Topic 2)
Which network attack is described by the following statement? "At least five Russian major banks came under a continuous hacker attack, although online client services were not disrupted. The attack came from a wide-scale botnet involving at least 24,000 computers, located in 30 countries."

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

Answer: D

NEW QUESTION 401
- (Exam Topic 2)
Which of the following tasks DOES NOT come under the investigation phase of a cybercrime forensics investigation case?

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

Answer: C

NEW QUESTION 404
- (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 408
- (Exam Topic 2)
What is the default IIS log location?

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

Answer: B

NEW QUESTION 412
- (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 414
- (Exam Topic 2)
What must be obtained before an investigation is carried out at a location?

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

Answer: A

NEW QUESTION 418
- (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 423
- (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 426
- (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 429
- (Exam Topic 2)
When investigating a computer forensics case where Microsoft Exchange and Blackberry Enterprise server are used, where would investigator need to search to find email sent from a Blackberry device?

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

Answer: C

NEW QUESTION 431
- (Exam Topic 2)
At what layer does a cross site scripting attack occur on?

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

Answer: B

NEW QUESTION 436
- (Exam Topic 2)
Casey has acquired data from a hard disk in an open source acquisition format that allows her to generate compressed or uncompressed image files. What format did she use?

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

Answer: B

NEW QUESTION 437
- (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 438
- (Exam Topic 2)
Pagefile.sys is a virtual memory file used to expand the physical memory of a computer. Select the registry path for the page file:

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

Answer: A

NEW QUESTION 439
- (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 444
- (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 445
- (Exam Topic 2)
Which of the following tools will help the investigator to analyze web server logs?

A. XRY LOGICAL
B. LanWhois
C. Deep Log Monitor
D. Deep Log Analyzer

Answer: D

NEW QUESTION 447
- (Exam Topic 2)
While looking through the IIS log file of a web server, you find the following entries:

```
2007-01-23 14:18:39 W3SVC1 172.16.28.102 GET /Development/index.asp
2007-01-23 14:18:39 W3SVC1 172.16.28.102 GET /login.asp?username=if ((select user)='sa' OR (select user)='dbo')
select 1 else select 1/0
2007-01-23 14:18:39 W3SVC1 172.16.28.102 GET /Developments/index_02.jpg
2007-01-23 14:18:39 W3SVC1 172.16.28.102 GET /Development/index_04.jpg
```

What is evident from this log file?

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

Answer: D

NEW QUESTION 452
- (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 454
- (Exam Topic 2)
What is the smallest physical storage unit on a hard drive?

A. Track
B. Cluster
C. Sector
D. Platter

Answer: C

NEW QUESTION 457
.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

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