EC-Council

Exam Questions 312-49v10

Computer Hacking Forensic Investigator (CHFI-v10)

About Exambible

Your Partner of IT Exam

Found in 1998

Exambible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, Exambible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

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

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

Answer: C

NEW QUESTION 2
- (Exam Topic 1)
You are the security analyst working for a private company out of France. Your current assignment is to obtain credit card information from a Swiss bank owned by that company. After initial reconnaissance, you discover that the bank security defenses are very strong and would take too long to penetrate. You decide to get the information by monitoring the traffic between the bank and one of its subsidiaries in London. After monitoring some of the traffic, you see a lot of FTP packets traveling back and forth. You want to sniff the traffic and extract usernames and passwords. What tool could you use to get this information?

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

Answer: C

NEW QUESTION 3
- (Exam Topic 1)
An Employee is suspected of stealing proprietary information belonging to your company that he had no rights to possess. The information was stored on the Employees Computer that was protected with the NTFS Encrypted File System (EFS) and you had observed him copy the files to a floppy disk just before leaving work for the weekend. You detain the Employee before he leaves the building and recover the floppy disks and secure his computer. Will you be able to break the encryption so that you can verify that that the employee was in possession of the proprietary information?

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

Answer: B

NEW QUESTION 4
- (Exam Topic 1)
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 5
- (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 6
- (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 7
- (Exam Topic 1)
It takes mismanaged case/s to ruin your professional reputation as a computer forensics examiner?

A. by law, three
B. quite a few
C. only one
D. at least two

Answer: C

NEW QUESTION 8
- (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 9
- (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 10
- (Exam Topic 1)
George is performing security analysis for Hammond and Sons LLC. He is testing security vulnerabilities of their wireless network. He plans on remaining as "stealthy" as possible during the scan. Why would a scanner like Nessus is not recommended in this situation?

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

Answer: A

NEW QUESTION 10
- (Exam Topic 1)
Law enforcement officers are conducting a legal search for which a valid warrant was obtained.
While conducting the search, officers observe an item of evidence for an unrelated crime that was not included in the warrant. The item was clearly visible to the officers and immediately identified as evidence. What is the term used to describe how this evidence is admissible?

A. Plain view doctrine
B. Corpus delicti
C. Locard Exchange Principle
D. Ex Parte Order

Answer: A

NEW QUESTION 14
- (Exam Topic 1)
After passing her CEH exam, Carol wants to ensure that her network is completely secure. She implements a DMZ, stateful firewall, NAT, IPSEC, and a packet filtering firewall. Since all security measures were taken, none of the hosts on her network can reach the Internet. Why is that?

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

Answer: D

NEW QUESTION 17

- (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 19
- (Exam Topic 1)
You have completed a forensic investigation case. You would like to destroy the data contained in various disks at the forensics lab due to sensitivity of the case. How would you permanently erase the data on the hard disk?

A. Throw the hard disk into the fire
B. Run the powerful magnets over the hard disk
C. Format the hard disk multiple times using a low level disk utility
D. Overwrite the contents of the hard disk with Junk data

Answer: A

NEW QUESTION 20
- (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 21
- (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 22
- (Exam Topic 1)
The following excerpt is taken from a honeypot log. The log captures activities across three days. There are several intrusion attempts; however, a few are successful.
(Note: The objective of this question is to test whether the student can read basic information from log entries and interpret the nature of attack.)
Apr 24 14:46:46 [4663]: spp_portscan: portscan detected from 194.222.156.169
Apr 24 14:46:46 [4663]: IDS27/FIN Scan: 194.222.156.169:56693 -> 172.16.1.107:482
Apr 24 18:01:05 [4663]: IDS/DNS-version-query: 212.244.97.121:3485 -> 172.16.1.107:53
Apr 24 19:04:01 [4663]: IDS213/ftp-passwd-retrieval: 194.222.156.169:1425 -> 172.16.1.107:21
Apr 25 08:02:41 [5875]: spp_portscan: PORTSCAN DETECTED from 24.9.255.53
Apr 25 02:08:07 [5875]: IDS277/DNS-version-query: 63.226.81.13:4499 -> 172.16.1.107:53
Apr 25 02:08:07 [5875]: IDS277/DNS-version-query: 63.226.81.13:4630 -> 172.16.1.101:53
Apr 25 02:38:17 [5875]: IDS/RPC-rpcinfo-query: 212.251.1.94:642 -> 172.16.1.107:111
Apr 25 19:37:32 [5875]: IDS230/web-cgi-space-wildcard: 198.173.35.164:4221 -> 172.16.1.107:80
Apr 26 05:45:12 [6283]: IDS212/dns-zone-transfer: 38.31.107.87:2291 -> 172.16.1.101:53
Apr 26 06:43:05 [6283]: IDS181/nops-x86: 63.226.81.13:1351 -> 172.16.1.107:53
Apr 26 06:44:25 victim7 PAM_pwdb[12509]: (login) session opened for user simple by (uid=0)
Apr 26 06:44:36 victim7 PAM_pwdb[12521]: (su) session opened for user simon by simple(uid=506) Apr 26 06:45:34 [6283]: IDS175/socks-probe: 24.112.167.35:20 -> 172.16.1.107:1080
Apr 26 06:52:10 [6283]: IDS127/telnet-login-incorrect: 172.16.1.107:23 -> 213.28.22.189:4558
From the options given below choose the one which best interprets the following entry: Apr 26 06:43:05 [6283]: IDS181/nops-x86: 63.226.81.13:1351 -> 172.16.1.107:53

A. An IDS evasion technique
B. A buffer overflow attempt
C. A DNS zone transfer
D. Data being retrieved from 63.226.81.13

Answer: A

NEW QUESTION 24
- (Exam Topic 1)

A state department site was recently attacked and all the servers had their disks erased. The incident response team sealed the area and commenced investigation. During evidence collection they came across a zip disks that did not have the standard labeling on it. The incident team ran the disk on an isolated system and found that the system disk was accidentally erased. They decided to call in the FBI for further investigation. Meanwhile, they short listed possible suspects including three summer interns. Where did the incident team go wrong?

A. They examined the actual evidence on an unrelated system
B. They attempted to implicate personnel without proof
C. They tampered with evidence by using it
D. They called in the FBI without correlating with the fingerprint data

Answer: C

NEW QUESTION 25
- (Exam Topic 1)
A packet is sent to a router that does not have the packet destination address in its route table. How will the packet get to its proper destination?

A. Root Internet servers
B. Border Gateway Protocol
C. Gateway of last resort
D. Reverse DNS

Answer: C

NEW QUESTION 27
- (Exam Topic 1)
Michael works for Kimball Construction Company as senior security analyst. As part of yearly security audit, Michael scans his network for vulnerabilities. Using Nmap, Michael conducts XMAS scan and most of the ports scanned do not give a response. In what state are these ports?

A. Closed
B. Open
C. Stealth
D. Filtered

Answer: B

NEW QUESTION 28
- (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 31
- (Exam Topic 1)
When reviewing web logs, you see an entry for resource not found in the HTTP status code filed. What is the actual error code that you would see in the log for resource not found?

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

Answer: B

NEW QUESTION 32
- (Exam Topic 1)
You have been asked to investigate after a user has reported a threatening e-mail they have received from an external source. Which of the following are you most interested in when trying to trace the source of the message?

A. The X509 Address
B. The SMTP reply Address
C. The E-mail Header
D. The Host Domain Name

Answer: C

NEW QUESTION 33
- (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 38
- (Exam Topic 2)
How many times can data be written to a DVD+R disk?

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

Answer: B

NEW QUESTION 41
- (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 42
- (Exam Topic 2)
When making the preliminary investigations in a sexual harassment case, how many investigators are you recommended having?

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

Answer: B

NEW QUESTION 45
- (Exam Topic 2)
John is working as a computer forensics investigator for a consulting firm in Canada. He is called to seize a computer at a local web caf purportedly used as a botnet server. John thoroughly scans the computer and finds nothing that would lead him to think the computer was a botnet server. John decides to scan the virtual memory of the computer to possibly find something he had missed. What information will the virtual memory scan produce?

A. It contains the times and dates of when the system was last patched
B. It is not necessary to scan the virtual memory of a computer
C. It contains the times and dates of all the system files
D. Hidden running processes

Answer: D

NEW QUESTION 50
- (Exam Topic 2)
What will the following command accomplish? dd if=/dev/xxx of=mbr.backup bs=512 count=1

A. Back up the master boot record
B. Restore the master boot record
C. Mount the master boot record on the first partition of the hard drive
D. Restore the first 512 bytes of the first partition of the hard drive

Answer: A

NEW QUESTION 54
- (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 56

- (Exam Topic 2)
What type of attack sends SYN requests to a target system with spoofed IP addresses?

A. SYN flood
B. Ping of death
C. Cross site scripting
D. Land

Answer: A

NEW QUESTION 57
- (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 61
- (Exam Topic 2)
Amber, a black hat hacker, has embedded a malware into a small enticing advertisement and posted it on a popular ad-network that displays across various websites. What is she doing?

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

Answer: D

NEW QUESTION 62
- (Exam Topic 2)
When using an iPod and the host computer is running Windows, what file system will be used?

A. iPod+
B. HFS
C. FAT16
D. FAT32

Answer: D

NEW QUESTION 63
- (Exam Topic 1)
From the following spam mail header, identify the host IP that sent this spam? From jie02@netvigator.com jie02@netvigator.com Tue Nov 27 17:27:11 2001
Received: from viruswall.ie.cuhk.edu.hk (viruswall [137.189.96.52]) by eng.ie.cuhk.edu.hk (8.11.6/8.11.6) with ESMTP id
fAR9RAP23061 for ; Tue, 27 Nov 2001 17:27:10 +0800 (HKT)
Received: from mydomain.com (pcd249020.netvigator.com [203.218.39.20]) by viruswall.ie.cuhk.edu.hk (8.12.1/8.12.1)
with SMTP id fAR9QXwZ018431 for ; Tue, 27 Nov 2001 17:26:36 +0800 (HKT)
Message-Id: >200111270926.fAR9QXwZ018431@viruswall.ie.cuhk.edu.hk From: "china hotel web"
To: "Shlam"
Subject: SHANGHAI (HILTON HOTEL) PACKAGE
Date: Tue, 27 Nov 2001 17:25:58 +0800 MIME-Version: 1.0
X- Priority: 3 X-MSMail- Priority: Normal
Reply-To: "china hotel web"

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

Answer: C

NEW QUESTION 64
- (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. DDoS
B. Sniffer Attack
C. Buffer Overflow
D. Man-in-the-Middle Attack

Answer: A

NEW QUESTION 69
- (Exam Topic 1)
Lance wants to place a honeypot on his network. Which of the following would be your recommendations?

A. Use a system that has a dynamic addressing on the network
B. Use a system that is not directly interacting with the router
C. Use it on a system in an external DMZ in front of the firewall
D. It doesn't matter as all replies are faked

Answer: D

NEW QUESTION 70
- (Exam Topic 1)
What term is used to describe a cryptographic technique for embedding information into something else for the sole purpose of hiding that information from the casual observer?

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

Answer: C

NEW QUESTION 74
- (Exam Topic 1)
You are working as Computer Forensics investigator and are called by the owner of an accounting firm to investigate possible computer abuse by one of the firm's employees. You meet with the owner of the firm and discover that the company has never published a policy stating that they reserve the right to inspect their computing assets at will. What do you do?

A. Inform the owner that conducting an investigation without a policy is not a problem because the company is privately owned
B. Inform the owner that conducting an investigation without a policy is a violation of the 4th amendment
C. Inform the owner that conducting an investigation without a policy is a violation of the employee's expectation of privacy
D. Inform the owner that conducting an investigation without a policy is not a problem because a policy is only necessary for government agencies

Answer: C

NEW QUESTION 75
- (Exam Topic 1)
When an investigator contacts by telephone the domain administrator or controller listed by a Who is lookup to request all e-mails sent and received for a user account be preserved, what U.S.C. statute authorizes this phone call and obligates the ISP to preserve e-mail records?

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

Answer: D

NEW QUESTION 79
- (Exam Topic 1)
Simon is a former employee of Trinitron XML Inc. He feels he was wrongly terminated and wants to hack into his former company's network. Since Simon remembers some of the server names, he attempts to run the axfr and ixfr commands using DIG. What is Simon trying to accomplish here?

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

Answer: C

NEW QUESTION 80
- (Exam Topic 1)
One way to identify the presence of hidden partitions on a suspect's hard drive is to:

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

Answer: A

NEW QUESTION 81
- (Exam Topic 1)
You are running through a series of tests on your network to check for any security vulnerabilities.
After normal working hours, you initiate a DoS attack against your external firewall. The firewall Quickly freezes up and becomes unusable. You then initiate an FTP connection from an external IP into your internal network. The connection is successful even though you have FTP blocked at the external firewall. What has

happened?

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

Answer: D

NEW QUESTION 84
- (Exam Topic 1)
Item 2If you come across a sheepdip machine at your client site, what would you infer?

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

Answer: C

NEW QUESTION 87
- (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 89
- (Exam Topic 1)
When conducting computer forensic analysis, you must guard against So that you remain focused on the primary job and insure that the level of work does not increase beyond what was originally expected.

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

Answer: B

NEW QUESTION 91
- (Exam Topic 1)
Melanie was newly assigned to an investigation and asked to make a copy of all the evidence from the compromised system. Melanie did a DOS copy of all the files on the system. What would be the primary reason for you to recommend a disk imaging tool?

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

Answer: C

NEW QUESTION 93
- (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 95
- (Exam Topic 1)
What method of computer forensics will allow you to trace all ever-established user accounts on a Windows 2000 sever the course of its lifetime?

A. forensic duplication of hard drive
B. analysis of volatile data
C. comparison of MD5 checksums
D. review of SIDs in the Registry

Answer: C

NEW QUESTION 97
- (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 100
- (Exam Topic 1)
George is the network administrator of a large Internet company on the west coast. Per corporate policy, none of the employees in the company are allowed to use FTP or SFTP programs without obtaining approval from the IT department. Few managers are using SFTP program on their computers. Before talking to his boss, George wants to have some proof of their activity. George wants to use Ethereal to monitor network traffic, but only SFTP traffic to and from his network.
What filter should George use in Ethereal?

A. src port 23 and dst port 23
B. udp port 22 and host 172.16.28.1/24
C. net port 22
D. src port 22 and dst port 22

Answer: D

NEW QUESTION 103
- (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)
You are working in the security Department of law firm. One of the attorneys asks you about the topic of sending fake email because he has a client who has been charged with doing just that. His client alleges that he is innocent and that there is no way for a fake email to actually be sent. You inform the attorney that his client is mistaken and that fake email is possibility and that you can prove it. You return to your desk and craft a fake email to the attorney that appears to come from his boss. What port do you send the email to on the company SMTP server?

A. 10
B. 25
C. 110
D. 135

Answer: B

NEW QUESTION 108
- (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 109
- (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 111
- (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 114
- (Exam Topic 1)
What are the security risks of running a "repair" installation for Windows XP?

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

Answer: A

NEW QUESTION 117
- (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 121
- (Exam Topic 1)
The rule of thumb when shutting down a system is to pull the power plug. However, it has certain drawbacks. Which of the following would that be?

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

Answer: A

NEW QUESTION 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 128
- (Exam Topic 1)
A honey pot deployed with the IP 172.16.1.108 was compromised by an attacker. Given below is an excerpt from a Snort binary capture of the attack. Decipher the activity carried out by the attacker by studying the log. Please note that you are required to infer only what is explicit in the excerpt.
(Note: The student is being tested on concepts learnt during passive OS fingerprinting, basic TCP/IP connection concepts and the ability to read packet signatures from a sniff dump.)
03/15-20:21:24.107053 211.185.125.124:3500 -> 172.16.1.108:111
TCP TTL:43 TOS:0x0 ID:29726 IpLen:20 DgmLen:52 DF
A* Seq: 0x9B6338C5 Ack: 0x5820ADD0 Win: 0x7D78 TcpLen: 32 TCP Options (3) => NOP NOP TS: 23678634 2878772
=+= 03/15-20:21:24.452051 211.185.125.124:789 -> 172.16.1.103:111
UDP TTL:43 TOS:0x0 ID:29733 IpLen:20 DgmLen:84
Len: 64
01 0A 8A 0A 00 00 00 00 00 00 00 02 00 01 86 A0 .....
00 00 00 02 00 00 00 03 00 00 00 00 00 00 00 00 .....
00 00 00 00 00 00 00 00 00 01 86 B8 00 00 00 01 .....
00 00 00 11 00 00 00 00 .....
=+= 03/15-20:21:24.730436 211.185.125.124:790 -> 172.16.1.103:32773
UDP TTL:43 TOS:0x0 ID:29781 IpLen:20 DgmLen:1104 Len: 1084
47 F7 9F 63 00 00 00 00 00 00 00 02 00 01 86 B8

A. The attacker has conducted a network sweep on port 111
B. The attacker has scanned and exploited the system using Buffer Overflow

C. The attacker has used a Trojan on port 32773
D. The attacker has installed a backdoor

Answer: A

NEW QUESTION 132
- (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 137
- (Exam Topic 1)
Hackers can gain access to Windows Registry and manipulate user passwords, DNS settings, access rights or others features that they may need in order to accomplish their objectives. One simple method for loading an application at startup is to add an entry (Key) to the following Registry Hive:

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

Answer: D

NEW QUESTION 141
- (Exam Topic 1)
After passively scanning the network of Department of Defense (DoD), you switch over to active scanning to identify live hosts on their network. DoD is a large organization and should respond to any number of scans. You start an ICMP ping sweep by sending an IP packet to the broadcast address. Only five hosts respond to your ICMP pings; definitely not the number of hosts you were expecting. Why did this ping sweep only produce a few responses?

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

Answer: D

NEW QUESTION 143
- (Exam Topic 1)
Volatile Memory is one of the leading problems for forensics. Worms such as code Red are memory resident and do write themselves to the hard drive, if you turn the system off they disappear. In a lab environment, which of the following options would you suggest as the most appropriate to overcome the problem of capturing volatile memory?

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

Answer: C

NEW QUESTION 147
- (Exam Topic 1)
What file structure database would you expect to find on floppy disks?

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

Answer: D

NEW QUESTION 151
- (Exam Topic 1)
Harold is a security analyst who has just run the rdisk /s command to grab the backup SAM files on a computer. Where should Harold navigate on the computer to find the file?

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

Answer: C

NEW QUESTION 152
- (Exam Topic 1)
You are working on a thesis for your doctorate degree in Computer Science. Your thesis is based on HTML, DHTML, and other web-based languages and how they have evolved over the years.
You navigate to archive. org and view the HTML code of news.com. You then navigate to the current news.com website and copy over the source code. While searching through the code, you come across something abnormal: What have you found?

A. Web bug
B. CGI code
C. Trojan.downloader
D. Blind bug

Answer: A

NEW QUESTION 153
- (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 156
- (Exam Topic 1)
E- mail logs contain which of the following information to help you in your investigation? (Choose four.)

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

Answer: ACDE

NEW QUESTION 157
- (Exam Topic 1)
When examining the log files from a Windows IIS Web Server, how often is a new log file created?

A. the same log is used at all times
B. a new log file is created everyday
C. a new log file is created each week
D. a new log is created each time the Web Server is started

Answer: A

NEW QUESTION 161
- (Exam Topic 1)
You are using DriveSpy, a forensic tool and want to copy 150 sectors where the starting sector is 1709 on the primary hard drive. Which of the following formats correctly specifies these sectors?

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

Answer: B

NEW QUESTION 165
- (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 168
- (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 170
- (Exam Topic 1)
What is a good security method to prevent unauthorized users from "tailgating"?

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

Answer: A

NEW QUESTION 173
- (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 178
- (Exam Topic 1)
You are contracted to work as a computer forensics investigator for a regional bank that has four 30 TB storage area networks that store customer data. What method would be most efficient for you to acquire digital evidence from this network?

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

Answer: C

NEW QUESTION 179
- (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 180
- (Exam Topic 1)
To make sure the evidence you recover and analyze with computer forensics software can be admitted in court, you must test and validate the software. What group is actively providing tools and creating procedures for testing and validating computer forensics software?

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

Answer: C

NEW QUESTION 181
- (Exam Topic 1)
A(n) is one that's performed by a computer program rather than the attacker manually performing the steps in the attack sequence.

A. blackout attack
B. automated attack

C. distributed attack
D. central processing attack

Answer: B

NEW QUESTION 186
- (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 191
- (Exam Topic 1)
You are a security analyst performing a penetration tests for a company in the Midwest. After some initial reconnaissance, you discover the IP addresses of some Cisco routers used by the company. You type in the following URL that includes the IP address of one of the routers:
http://172.168.4.131/level/99/exec/show/config
After typing in this URL, you are presented with the entire configuration file for that router. What have you discovered?

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

Answer: A

NEW QUESTION 195
- (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 199
- (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 201
- (Exam Topic 1)
In General, Involves the investigation of data that can be retrieved from the hard disk or other disks of a computer by applying scientific methods to retrieve the data.

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

Answer: D

NEW QUESTION 205
- (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 206
- (Exam Topic 1)
When you carve an image, recovering the image depends on which of the following skills?

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

Answer: A

NEW QUESTION 211
- (Exam Topic 1)
When performing a forensics analysis, what device is used to prevent the system from recording data on an evidence disk?

A. a write-blocker
B. a protocol analyzer
C. a firewall
D. a disk editor

Answer: A

NEW QUESTION 212
- (Exam Topic 1)
The newer Macintosh Operating System is based on:

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

Answer: B

NEW QUESTION 215
- (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 218
- (Exam Topic 1)
What type of file is represented by a colon (:) with a name following it in the Master File Table of NTFS disk?

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

Answer: B

NEW QUESTION 220
- (Exam Topic 1)
Office documents (Word, Excel, PowerPoint) contain a code that allows tracking the MAC, or unique identifier, of the machine that created the document. What is that code called?

A. the Microsoft Virtual Machine Identifier
B. the Personal Application Protocol
C. the Globally Unique ID
D. the Individual ASCII String

Answer: C

NEW QUESTION 221
- (Exam Topic 1)
This is original file structure database that Microsoft originally designed for floppy disks. It is written to the outermost track of a disk and contains information about each file stored on the drive.

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

Answer: C

NEW QUESTION 223
- (Exam Topic 1)
You are carrying out the last round of testing for your new website before it goes live. The website has many dynamic pages and connects to a SQL backend that accesses your product inventory in a database. You come across a web security site that recommends inputting the following code into a search field on web pages to check for vulnerabilities: When you type this and click on search, you receive a pop-up window that says: "This is a test."
What is the result of this test?

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

Answer: A

NEW QUESTION 226
- (Exam Topic 1)
Jason has set up a honeypot environment by creating a DMZ that has no physical or logical access to his production network. In this honeypot, he has placed a server running Windows Active Directory. He has also placed a Web server in the DMZ that services a number of web pages that offer visitors a chance to download sensitive information by clicking on a button. A week later, Jason finds in his network logs how an intruder accessed the honeypot and downloaded sensitive information. Jason uses the logs to try and prosecute the intruder for stealing sensitive corporate information. Why will this not be viable?

A. Entrapment
B. Enticement
C. Intruding into a honeypot is not illegal
D. Intruding into a DMZ is not illegal

Answer: A

NEW QUESTION 229
- (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 233
- (Exam Topic 1)
As a CHFI professional, which of the following is the most important to your professional reputation?

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

Answer: B

NEW QUESTION 237
- (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 240
- (Exam Topic 1)
Kyle is performing the final testing of an application he developed for the accounting department. His last round of testing is to ensure that the program is as secure as possible. Kyle runs the following
command. What is he testing at this point?
#include #include int main(int argc, char
*argv[]) { char buffer[10]; if (argc < 2) { fprintf (stderr, "USAGE: %s string\n", argv[0]); return 1; } strcpy(buffer, argv[1]); return 0; }

A. Buffer overflow

B. SQL injection
C. Format string bug
D. Kernal injection

Answer: A

NEW QUESTION 241
- (Exam Topic 1)
You just passed your ECSA exam and are about to start your first consulting job running security audits for a financial institution in Los Angeles. The IT manager of the company you will be working for tries to see if you remember your ECSA class. He asks about the methodology you will be using to test the company's network. How would you answer?

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

Answer: D

NEW QUESTION 243
- (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 246
- (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 248
- (Exam Topic 4)
Which Federal Rule of Evidence speaks about the Hearsay exception where the availability of the declarant Is immaterial and certain characteristics of the declarant such as present sense Impression, excited utterance, and recorded recollection are also observed while giving their testimony?

A. Rule 801
B. Rule 802
C. Rule 804
D. Rule 803

Answer: D

NEW QUESTION 250
- (Exam Topic 4)
This law sets the rules for commercial email, establishes requirements for commercial messages, gives recipients the right to have you stop emailing them, and spells out tough penalties for violations.

A. The CAN-SPAM act
B. Federal Spam act
C. Telemarketing act
D. European Anti-Spam act

Answer: A

NEW QUESTION 255
- (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 260
- (Exam Topic 4)
According to RFC 3227, which of the following is considered as the most volatile item on a typical system?

A. Registers and cache
B. Temporary system files
C. Archival media
D. Kernel statistics and memory

Answer: A

NEW QUESTION 262
- (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 265
- (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 267
- (Exam Topic 4)
Which of the following tools will allow a forensic Investigator to acquire the memory dump of a suspect machine so that It may be Investigated on a forensic workstation to collect evidentiary data like processes and Tor browser artifacts?

A. DB Browser SQLite
B. Bulk Extractor
C. Belkasoft Live RAM Capturer and AccessData FTK imager
D. Hex Editor

Answer: C

NEW QUESTION 269
- (Exam Topic 4)
Consider a scenario where a forensic investigator is performing malware analysis on a memory dump acquired from a victims computer. The investigator uses Volatility Framework to analyze RAM contents; which plugin helps investigator to identify hidden processes or injected code/DLL in the memory dump?

A. pslist
B. malscan
C. mallist
D. malfind

Answer: D

NEW QUESTION 272
- (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 275

- (Exam Topic 4)
Which of the following statements is true with respect to SSDs (solid-state drives)?

A. Like HDD
B. SSDs also have moving parts
C. SSDs cannot store non-volatile data
D. SSDs contain tracks, clusters, and sectors to store data
E. Faster data access, lower power usage, and higher reliability are some of the m<ijor advantages of SSDs over HDDs

Answer: D

NEW QUESTION 279
- (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 281
- (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 284
- (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 285
- (Exam Topic 4)
An investigator needs to perform data acquisition from a storage media without altering its contents to maintain the Integrity of the content. The approach adopted by the Investigator relies upon the capacity of enabling read-only access to the storage media. Which tool should the Investigator Integrate Into his/her procedures to accomplish this task?

A. BitLocker
B. Data duplication tool
C. Backup tool
D. Write blocker

Answer: D

NEW QUESTION 286
- (Exam Topic 4)
Jeff is a forensics investigator for a government agency's cyber security office. Jeff Is tasked with acquiring a memory dump of a Windows 10 computer that was involved In a DDoS attack on the government agency's web application. Jeff is onsite to collect the memory. What tool could Jeff use?

A. Volatility
B. Autopsy
C. RAM Mapper
D. Memcheck

Answer: A

NEW QUESTION 291
- (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-DTRAI83202Xrelay-bin.index
C. WIN-DTRAI83202Xslow.log
D. WIN-DTRAI83202X-bin.nnnnnn

Answer: C

NEW QUESTION 293
- (Exam Topic 4)
You are an information security analyst at a large pharmaceutical company. While performing a routine review of audit logs, you have noticed a significant amount of egress traffic to various IP addresses on destination port 22 during off-peak hours. You researched some of the IP addresses and found that many of them are in Eastern Europe. What is the most likely cause of this traffic?

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

Answer: C

NEW QUESTION 295
- (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 296
- (Exam Topic 4)
"To ensure that the digital evidence is collected, preserved, examined, or transferred In a manner safeguarding the accuracy and reliability of the evidence, law enforcement, and forensics organizations must establish and maintain an effective quality system" Is a principle established by:

A. NCIS
B. NIST
C. EC-Council
D. SWGDE

Answer: B

NEW QUESTION 298
- (Exam Topic 4)
Fred, a cybercrime Investigator for the FBI, finished storing a solid-state drive In a static resistant bag and filled out the chain of custody form. Two days later. John grabbed the solid-state drive and created a clone of It (with write blockers enabled) In order to Investigate the drive. He did not document the chain of custody though. When John was finished, he put the solid-state drive back in the static resistant and placed it back in the evidence locker. A day later, the court trial began and upon presenting the evidence and the supporting documents, the chief Justice outright rejected them. Which of the following statements strongly support the reason for rejecting the evidence?

A. Block clones cannot be created with solid-state drives
B. Write blockers were used while cloning the evidence
C. John did not document the chain of custody
D. John investigated the clone instead of the original evidence itself

Answer: C

NEW QUESTION 302
- (Exam Topic 4)
Frank, a cloud administrator in his company, needs to take backup of the OS disks of two Azure VMs that store business-critical data. Which type of Azure blob storage can he use for this purpose?

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

Answer: D

NEW QUESTION 307
- (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 312
- (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 315
- (Exam Topic 4)
Which layer in the loT architecture is comprised of hardware parts such as sensors, RFID tags, and devices that play an important role in data collection?

A. Middleware layer
B. Edge technology layer
C. Application layer
D. Access gateway layer

Answer: B

NEW QUESTION 318
- (Exam Topic 4)
Cloud forensic investigations impose challenges related to multi-jurisdiction and multi-tenancy aspects. To have a better understanding of the roles and responsibilities between the cloud service provider (CSP) and the client, which document should the forensic investigator review?

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

Answer: A

NEW QUESTION 323
- (Exam Topic 4)
A breach resulted from a malware attack that evaded detection and compromised the machine memory without installing any software or accessing the hard drive. What technique did the adversaries use to deliver the attack?

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

Answer: A

NEW QUESTION 325
- (Exam Topic 4)
Which among the following acts has been passed by the U.S. Congress to protect investors from the possibility of fraudulent accounting activities by corporations?

A. Federal Information Security Management act of 2002
B. Gramm-Leach-Bliley act
C. Health insurance Probability and Accountability act of 1996
D. Sarbanes-Oxley act of 2002

Answer: D

NEW QUESTION 330
- (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 332
- (Exam Topic 4)
Recently, an Internal web app that a government agency utilizes has become unresponsive, Betty, a network engineer for the government agency, has been tasked to determine the cause of the web application's unresponsiveness. Betty launches Wlreshark and begins capturing the traffic on the local network. While analyzing the results, Betty noticed that a syn flood attack was underway. How did Betty know a syn flood attack was occurring?

A. Wireshark capture shows multiple ACK requests and SYN responses from single/multiple IP address(es)
B. Wireshark capture does not show anything unusual and the issue is related to the web application
C. Wireshark capture shows multiple SYN requests and RST responses from single/multiple IP address(es)
D. Wireshark capture shows multiple SYN requests and ACK responses from single/multiple IP address(es)

Answer: C

NEW QUESTION 334
- (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 335
- (Exam Topic 4)
Identify the location of Recycle Bin on a Windows 7 machine that uses NTFS file system to store and retrieve files on the hard disk.

A. Drive:\$Recycle.Bin
B. DriveARECYCLER
C. C:\RECYCLED
D. DriveARECYCLED

Answer: A

NEW QUESTION 336
- (Exam Topic 4)
A clothing company has recently deployed a website on Its latest product line to Increase Its conversion rate and base of customers. Andrew, the network administrator recently appointed by the company, has been assigned with the task of protecting the website from Intrusion and vulnerabilities. Which of the following tool should Andrew consider deploying in this scenario?

A. ModSecurity
B. CryptaPix
C. Recuva
D. Kon-Boot

Answer: A

NEW QUESTION 337
- (Exam Topic 4)
A computer forensics Investigator or forensic analyst Is a specially trained professional who works with law enforcement as well as private businesses to retrieve Information from computers and other types of data storage devices. For this, the analyst should have an excellent working knowledge of all aspects of the computer. Which of the following is not a duty of the analyst during a criminal investigation?

A. To create an investigation report
B. To fill the chain of custody
C. To recover data from suspect devices
D. To enforce the security of all devices and software in the scene

Answer: D

NEW QUESTION 339
- (Exam Topic 4)
In which loT attack does the attacker use multiple forged identities to create a strong illusion of traffic congestion, affecting communication between neighboring nodes and networks?

A. Replay attack
B. Jamming attack
C. Blueborne attack
D. Sybil attack

Answer: D

NEW QUESTION 344
- (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 347
- (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 348
- (Exam Topic 4)
Malware analysis can be conducted in various manners. An investigator gathers a suspicious executable file and uploads It to VirusTotal in order to confirm whether the file Is malicious, provide information about Its functionality, and provide Information that will allow to produce simple network signatures. What type of malware analysis was performed here?

A. Static
B. Volatile
C. Dynamic
D. Hybrid

Answer: D

NEW QUESTION 351
- (Exam Topic 3)
Which of the following standard represents a legal precedent regarding the admissibility of scientific examinations or experiments in legal cases?

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

Answer: C

NEW QUESTION 353
- (Exam Topic 3)
Which of the following Android libraries are used to render 2D (SGL) or 3D (OpenGL/ES) graphics content to the screen?

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

Answer: A

NEW QUESTION 354
- (Exam Topic 3)
Tasklist command displays a list of applications and services with their Process ID (PID) for all tasks running on either a local or a remote computer. Which of the following tasklist commands provides information about the listed processes, including the image name, PID, name, and number of the session for the process?

A. tasklist /p
B. tasklist /v
C. tasklist /u
D. tasklist /s

Answer: B

NEW QUESTION 358
- (Exam Topic 3)

Rusty, a computer forensics apprentice, uses the command nbtstat –c while analyzing the network information in a suspect system. What information is he looking for?

A. Contents of the network routing table
B. Status of the network carrier
C. Contents of the NetBIOS name cache
D. Network connections

Answer: C

NEW QUESTION 361
- (Exam Topic 3)
Select the data that a virtual memory would store in a Windows-based system.

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

Answer: D

NEW QUESTION 365
- (Exam Topic 3)
Which of the following processes is part of the dynamic malware analysis?

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

Answer: A

NEW QUESTION 369
- (Exam Topic 3)
Buffer overflow vulnerability of a web application occurs when it fails to guard its buffer properly and allows writing beyond its maximum size. Thus, it overwrites the . There are multiple forms of buffer overflow, including a Heap Buffer Overflow and a Format String Attack.

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

Answer: A

NEW QUESTION 373
- (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 375
- (Exam Topic 3)
Hard disk data addressing is a method of allotting addresses to each of data on a hard disk.

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

Answer: A

NEW QUESTION 377
- (Exam Topic 3)
Raw data acquisition format creates of a data set or suspect drive.

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

Answer: B

NEW QUESTION 378
- (Exam Topic 3)
What does the bytes 0x0B-0x53 represent in the boot sector of NTFS volume on Windows 2000?

A. Jump instruction and the OEM ID
B. BIOS Parameter Block (BPB) and the OEM ID
C. BIOS Parameter Block (BPB) and the extended BPB
D. Bootstrap code and the end of the sector marker

Answer: C

NEW QUESTION 382
- (Exam Topic 3)
What is cold boot (hard boot)?

A. It is the process of restarting a computer that is already in sleep mode
B. It is the process of shutting down a computer from a powered-on or on state
C. It is the process of restarting a computer that is already turned on through the operating system
D. It is the process of starting a computer from a powered-down or off state

Answer: D

NEW QUESTION 384
- (Exam Topic 3)
A company's policy requires employees to perform file transfers using protocols which encrypt traffic. You suspect some employees are still performing file transfers using unencrypted protocols because the employees don't like changes. You have positioned a network sniffer to capture traffic from the laptops used by employees in the data ingest department. Using Wireshark to examine the captured traffic, which command can be used as a display filter to find unencrypted file transfers?

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

Answer: B

NEW QUESTION 387
- (Exam Topic 3)
Amber, a black hat hacker, has embedded malware into a small enticing advertisement and posted it on a popular ad-network that displays across various websites. What is she doing?

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

Answer: A

NEW QUESTION 392
- (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 394
- (Exam Topic 3)
What document does the screenshot represent?

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

Answer: D

NEW QUESTION 399
- (Exam Topic 3)
Ron, a computer forensics expert, is investigating a case involving corporate espionage. He has recovered several mobile computing devices from the crime scene. One of the evidence that Ron possesses is a mobile phone from Nokia that was left in ON condition. Ron needs to recover the IMEI number of the device to establish the identity of the device owner. Which of the following key combinations can he use to recover the IMEI number?

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

Answer: A

NEW QUESTION 403
- (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 405
- (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 408
- (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 409
- (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 414
- (Exam Topic 3)
Which of the following files store the MySQL database data permanently, including the data that had been deleted, helping the forensic investigator in examining the case and finding the culprit?

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

Answer: D

NEW QUESTION 415
- (Exam Topic 3)
In a Linux-based system, what does the command “Last -F” display?

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

Answer: A

NEW QUESTION 419
- (Exam Topic 3)
Which type of attack is possible when attackers know some credible information about the victim's password, such as the password length, algorithms involved, or the strings and characters used in its creation?

A. Rule-Based Attack
B. Brute-Forcing Attack
C. Dictionary Attack
D. Hybrid Password Guessing Attack

Answer: A

NEW QUESTION 421
- (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 425
- (Exam Topic 3)
Which of the following is a non-zero data that an application allocates on a hard disk cluster in systems running on Windows OS?

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

Answer: B

NEW QUESTION 426
- (Exam Topic 3)
companyXYZ has asked you to assess the security of their perimeter email gateway. From your office in New York you craft a specially formatted email message and send it across the Internet to an employee of CompanyXYZ. The employee of CompanyXYZ is aware.

A. Source code review
B. Reviewing the firewalls configuration

C. Data items and vulnerability scanning
D. Interviewing employees and network engineers

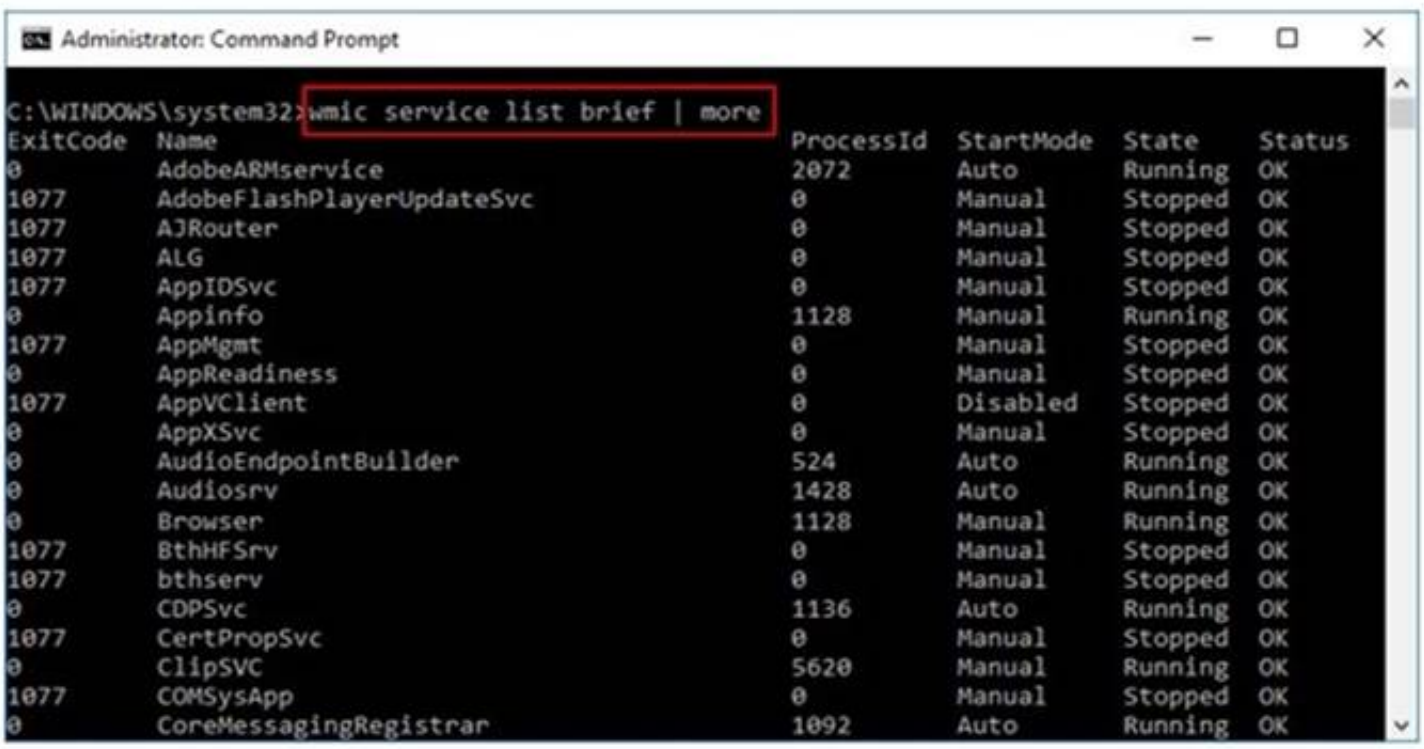
Answer: A

NEW QUESTION 430
- (Exam Topic 3)
What is the name of the first reserved sector in File allocation table?

A. Volume Boot Record
B. Partition Boot Sector
C. Master Boot Record
D. BIOS Parameter Block

Answer: C

NEW QUESTION 435
- (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 440
- (Exam Topic 3)
In Linux OS, different log files hold different information, which help the investigators to analyze various issues during a security incident. What information can the investigators obtain from the log file var/log/dmesg?

A. Kernel ring buffer information
B. All mail server message logs
C. Global system messages
D. Debugging log messages

Answer: A

NEW QUESTION 445
- (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 447
- (Exam Topic 3)
A section of your forensics lab houses several electrical and electronic equipment. Which type of fire extinguisher you must install in this area to contain any fire incident?

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

Answer: C

NEW QUESTION 451
- (Exam Topic 3)
Which of the following is NOT an anti-forensics technique?

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

Answer: A

NEW QUESTION 454
- (Exam Topic 3)
A Linux system is undergoing investigation. In which directory should the investigators look for its current state data if the system is in powered on state?

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

Answer: B

NEW QUESTION 457
- (Exam Topic 3)
Gill is a computer forensics investigator who has been called upon to examine a seized computer. This computer, according to the police, was used by a hacker who gained access to numerous banking institutions to steal customer information. After preliminary investigations, Gill finds in the computer's log files that the hacker was able to gain access to these banks through the use of Trojan horses. The hacker then used these Trojan horses to obtain remote access to the companies' domain controllers. From this point, Gill found that the hacker pulled off the SAM files from the domain controllers to then attempt and crack network passwords. What is the most likely password cracking technique used by this hacker to break the user passwords from the SAM files?

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

Answer: D

NEW QUESTION 460
- (Exam Topic 3)
Which command can provide the investigators with details of all the loaded modules on a Linux-based system?

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

Answer: B

NEW QUESTION 461
- (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 464
- (Exam Topic 3)
Which of the following ISO standard defines file systems and protocol for exchanging data between optical disks?

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

Answer: A

NEW QUESTION 469
- (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 471
- (Exam Topic 3)
POP3 is an Internet protocol, which is used to retrieve emails from a mail server. Through which port does an email client connect with a POP3 server?

A. 110
B. 143
C. 25
D. 993

Answer: A

NEW QUESTION 475
- (Exam Topic 3)
Consider that you are investigating a machine running an Windows OS released prior to Windows Vista. You are trying to gather information about the deleted files by examining the master database file named INFO2 located at C:\Recycler\<USER SID>\. You read an entry named "Dd5.exe". What does Dd5.exe mean?

A. D driv
B. fifth file deleted, a .exe file
C. D drive, fourth file restored, a .exe file
D. D drive, fourth file deleted, a .exe file
E. D drive, sixth file deleted, a .exe file

Answer: B

NEW QUESTION 480
- (Exam Topic 3)
Which of the following components within the android architecture stack take care of displaying windows owned by different applications?

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

Answer: D

NEW QUESTION 485
- (Exam Topic 3)
You are a Penetration Tester and are assigned to scan a server. You need to use a scanning technique wherein the TCP Header is split into many packets so that it becomes difficult to detect what the packets are meant for. Which of the below scanning technique will you use?

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

Answer: D

NEW QUESTION 490
- (Exam Topic 3)
Which of the following statements is TRUE with respect to the Registry settings in the user start-up folder HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce\.

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

Answer: D

NEW QUESTION 495
- (Exam Topic 3)
Which of the following Linux command searches through the current processes and lists the process IDs those match the selection criteria to stdout?

A. pstree
B. pgrep

C. ps
D. grep

Answer: B

NEW QUESTION 498
- (Exam Topic 3)
What do you call the process in which an attacker uses magnetic field over the digital media device to delete any previously stored data?

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

Answer: C

NEW QUESTION 500
- (Exam Topic 3)
Which of the following is a precomputed table containing word lists like dictionary files and brute force lists and their hash values?

A. Directory Table
B. Rainbow Table
C. Master file Table (MFT)
D. Partition Table

Answer: B

NEW QUESTION 503
- (Exam Topic 3)
Which layer of iOS architecture should a forensics investigator evaluate to analyze services such as Threading, File Access, Preferences, Networking and high-level features?

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

Answer: D

NEW QUESTION 506
- (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 509
- (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 512
- (Exam Topic 3)
Amelia has got an email from a well-reputed company stating in the subject line that she has won a prize money, whereas the email body says that she has to pay a certain amount for being eligible for the contest. Which of the following acts does the email breach?

A. CAN-SPAM Act
B. HIPAA
C. GLBA
D. SOX

Answer: A

NEW QUESTION 515

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

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

Answer: D

NEW QUESTION 519
- (Exam Topic 3)
What is the role of Alloc.c in Apache core?

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

Answer: A

NEW QUESTION 524
- (Exam Topic 3)
What is the capacity of Recycle bin in a system running on Windows Vista?

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

Answer: C

NEW QUESTION 529
- (Exam Topic 3)
Which among the following web application threats is resulted when developers expose various internal implementation objects, such as files, directories, database records, or key-through references?

A. Remote File Inclusion
B. Cross Site Scripting
C. Insecure Direct Object References
D. Cross Site Request Forgery

Answer: C

NEW QUESTION 531
- (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 536
- (Exam Topic 3)
In which of these attacks will a steganalyst use a random message to generate a stego-object by using some steganography tool, to find the steganography algorithm used to hide the information?

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

Answer: A

NEW QUESTION 538
- (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 539
- (Exam Topic 3)
When analyzing logs, it is important that the clocks of all the network devices are synchronized. Which protocol will help in synchronizing these clocks?

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

Answer: D

NEW QUESTION 543
- (Exam Topic 3)
The MAC attributes are timestamps that refer to a time at which the file was last modified or last accessed or originally created. Which of the following file systems store MAC attributes in Coordinated Universal Time (UTC) format?

A. File Allocation Table (FAT
B. New Technology File System (NTFS)
C. Hierarchical File System (HFS)
D. Global File System (GFS)

Answer: B

NEW QUESTION 545
- (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 550
- (Exam Topic 3)
Which of the following attack uses HTML tags like <script></script>?

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

Answer: B

NEW QUESTION 555
- (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 560
- (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 561
- (Exam Topic 3)

Report writing is a crucial stage in the outcome of an investigation. Which information should not be included in the report section?

A. Speculation or opinion as to the cause of the incident
B. Purpose of the report
C. Author of the report
D. Incident summary

Answer: A

NEW QUESTION 563
- (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 565
- (Exam Topic 3)
Which of the following stand true for BIOS Parameter Block?

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

Answer: A

NEW QUESTION 570
- (Exam Topic 3)
Graphics Interchange Format (GIF) is a RGB bitmap image format for images with up to 256 distinct colors per frame.

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

Answer: A

NEW QUESTION 575
- (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 577
- (Exam Topic 3)
Which of the following tools is not a data acquisition hardware tool?

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

Answer: C

NEW QUESTION 580
- (Exam Topic 3)
Which of the following is NOT an anti-forensics technique?

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

Answer: A

NEW QUESTION 583
- (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 585
- (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 588
- (Exam Topic 3)
Jacob is a computer forensics investigator with over 10 years of experience in investigations and has written over 50 articles on computer forensics. He has been called upon as a qualified witness to testify the accuracy and integrity of the technical log files gathered in an investigation into computer fraud. What is the term used for Jacob's testimony in this case?

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

Answer: D

NEW QUESTION 589
- (Exam Topic 3)
Lynne receives the following email:
Dear lynne@gmail.com! We are sorry to inform you that your ID has been temporarily frozen due to incorrect or missing information saved at 2016/11/10 20:40:24
You have 24 hours to fix this problem or risk to be closed permanently! To proceed Please Connect >> My Apple ID
Thank You The link to My Apple ID shows http://byggarbetsplatsen.se/backup/signon/ What type of attack is this?

A. Mail Bombing
B. Phishing
C. Email Spamming
D. Email Spoofing

Answer: B

NEW QUESTION 591
- (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 594
- (Exam Topic 3)
Which of these ISO standards define the file system for optical storage media, such as CD-ROM and DVD-ROM?

A. ISO 9660
B. ISO 13346
C. ISO 9960
D. ISO 13490

Answer: A

NEW QUESTION 598
- (Exam Topic 3)

To reach a bank web site, the traffic from workstations must pass through a firewall. You have been asked to review the firewall configuration to ensure that workstations in network 10.10.10.0/24 can only reach the bank web site 10.20.20.1 using https. Which of the following firewall rules meets this requirement?

A. if (source matches 10.10.10.0/24 and destination matches 10.20.20.1 and port matches 443) then permit
B. if (source matches 10.10.10.0/24 and destination matches 10.20.20.1 and port matches 80 or 443) then permit
C. if (source matches 10.10.10.0 and destination matches 10.20.20.1 and port matches 443) then permit

Answer: A

NEW QUESTION 600
- (Exam Topic 3)
Which of the following statements is TRUE about SQL Server error logs?

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

Answer: B

NEW QUESTION 604
- (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 609
- (Exam Topic 3)
> NMAP -sn 192.168.11.200-215 The NMAP command above performs which of the following?

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

Answer: C

NEW QUESTION 613
- (Exam Topic 3)
Examination of a computer by a technically unauthorized person will almost always result in:

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

Answer: A

NEW QUESTION 618
- (Exam Topic 3)
Which of the following is found within the unique instance ID key and helps investigators to map the entry from USBSTOR key to the MountedDevices key?

A. ParentIDPrefix
B. LastWrite
C. UserAssist key
D. MRUListEx key

Answer: A

NEW QUESTION 620
- (Exam Topic 3)
UEFI is a specification that defines a software interface between an OS and platform firmware. Where does this interface store information about files present on a disk?

A. BIOS-MBR
B. GUID Partition Table (GPT)
C. Master Boot Record (MBR)
D. BIOS Parameter Block

Answer: B

NEW QUESTION 621
- (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 624
- (Exam Topic 3)
In Windows, prefetching is done to improve system performance. There are two types of prefetching: boot prefetching and application prefetching. During boot prefetching, what does the Cache Manager do?

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

Answer: C

NEW QUESTION 627
- (Exam Topic 3)
Which part of Metasploit framework helps users to hide the data related to a previously deleted file or currently unused by the allocated file.

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

Answer: D

NEW QUESTION 632
- (Exam Topic 3)
Which of the following is NOT a physical evidence?

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

Answer: C

NEW QUESTION 634
- (Exam Topic 3)
An attacker successfully gained access to a remote Windows system and plans to install persistent backdoors on it. Before that, to avoid getting detected in future, he wants to cover his tracks by disabling the
last-accessed timestamps of the machine. What would he do to achieve this?

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

Answer: C

NEW QUESTION 635
- (Exam Topic 3)
Which of the following file formats allows the user to compress the acquired data as well as keep it randomly accessible?

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

Answer: B

NEW QUESTION 640
- (Exam Topic 2)
Which password cracking technique uses every possible combination of character sets?

A. Rainbow table attack
B. Brute force attack
C. Rule-based attack

D. Dictionary attack

Answer: B

NEW QUESTION 642
- (Exam Topic 2)
Given the drive dimensions as follows and assuming a sector has 512 bytes, what is the capacity of the described hard drive?
22,164 cylinders/disk
80 heads/cylinder
63 sectors/track

A. 53.26 GB
B. 57.19 GB
C. 11.17 GB
D. 10 GB

Answer: A

NEW QUESTION 643
- (Exam Topic 2)
What does the part of the log, “% SEC-6-IPACCESSLOGP”, extracted from a Cisco router represent?

A. The system was not able to process the packet because there was not enough room for all of the desired IP header options
B. Immediate action required messages
C. Some packet-matching logs were missed because the access list log messages were rate limited, or no access list log buffers were available
D. A packet matching the log criteria for the given access list has been detected (TCP or UDP)

Answer: D

NEW QUESTION 644
- (Exam Topic 2)
Smith, a forensic examiner, was analyzing a hard disk image to find and acquire deleted sensitive files. He stumbled upon a $Recycle.Bin folder in the root directory of the disk. Identify the operating system in use.

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

Answer: D

NEW QUESTION 645
- (Exam Topic 2)
What must an investigator do before disconnecting an iPod from any type of computer?

A. Unmount the iPod
B. Mount the iPod
C. Disjoin the iPod
D. Join the iPod

Answer: A

NEW QUESTION 650
- (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 654
- (Exam Topic 2)
Depending upon the jurisdictional areas, different laws apply to different incidents. Which of the following law is related to fraud and related activity in connection with computers?

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

Answer: B

NEW QUESTION 655
- (Exam Topic 2)
Billy, a computer forensics expert, has recovered a large number of DBX files during the forensic investigation of a laptop. Which of the following email clients can he use to analyze the DBX files?

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

Answer: D

NEW QUESTION 657
- (Exam Topic 2)
Stephen is checking an image using Compare Files by The Wizard, and he sees the file signature is shown as FF D8 FF E1. What is the file type of the image?

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

Answer: C

NEW QUESTION 661
- (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 665
- (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 669
- (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 672
- (Exam Topic 2)
Harold is a computer forensics investigator working for a consulting firm out of Atlanta Georgia. Harold is called upon to help with a corporate espionage case in Miami Florida. Harold assists in the investigation by
pulling all the data from the computers allegedly used in the illegal activities. He finds that two suspects in the company where stealing sensitive corporate information and selling it to competing companies. From the email and instant messenger logs recovered, Harold has discovered that the two employees notified the buyers by writing symbols on the back of specific stop signs. This way, the buyers knew when and where to meet with the alleged suspects to buy the stolen material. What type of steganography did these two suspects use?

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

Answer: B

NEW QUESTION 677
- (Exam Topic 2)

Which of the following files stores information about a local Google Drive installation such as User email ID, Local Sync Root Path, and Client version installed?

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

Answer: D

NEW QUESTION 682
- (Exam Topic 2)
Charles has accidentally deleted an important file while working on his Mac computer. He wants to recover the deleted file as it contains some of his crucial business secrets. Which of the following tool will help Charles?

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

Answer: C

NEW QUESTION 683
- (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 686
- (Exam Topic 2)
What will the following Linux command accomplish? dd if=/dev/mem of=/home/sam/mem.bin bs=1024

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

Answer: C

NEW QUESTION 688
- (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 691
- (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 695
- (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 697
- (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 700
- (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 702
- (Exam Topic 2)
Which of the following tool can the investigator use to analyze the network to detect Trojan activities?

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

Answer: D

NEW QUESTION 703
- (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 706
- (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 711
- (Exam Topic 2)
What is the primary function of the tool CHKDSK in Windows that authenticates the file system reliability of a volume?

A. Repairs logical file system errors
B. Check the disk for hardware errors
C. Check the disk for connectivity errors
D. Check the disk for Slack Space

Answer: A

NEW QUESTION 714
- (Exam Topic 2)
Jacky encrypts her documents using a password. It is known that she uses her daughter’s year of birth as part of the password. Which password cracking

technique would be optimal to crack her password?

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

Answer: A

NEW QUESTION 719
- (Exam Topic 2)
Which of the following standard represents a legal precedent sent in 1993 by the Supreme Court of the United States regarding the admissibility of expert witnesses' testimony during federal legal proceedings?

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

Answer: D

NEW QUESTION 724
- (Exam Topic 2)
Sniffers that place NICs in promiscuous mode work at what layer of the OSI model?

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

Answer: C

NEW QUESTION 728
- (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 732
- (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 735
- (Exam Topic 2)
Which of the following reports are delivered under oath to a board of directors/managers/panel of the jury?

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

Answer: B

NEW QUESTION 736
- (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 741
- (Exam Topic 2)
All Blackberry email is eventually sent and received through what proprietary RIM-operated mechanism?

A. Blackberry Message Center
B. Microsoft Exchange
C. Blackberry WAP gateway
D. Blackberry WEP gateway

Answer: A

NEW QUESTION 746
- (Exam Topic 2)
Which among the following is an act passed by the U.S. Congress in 2002 to protect investors from the possibility of fraudulent accounting activities by corporations?

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

Answer: C

NEW QUESTION 747
- (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 751
- (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

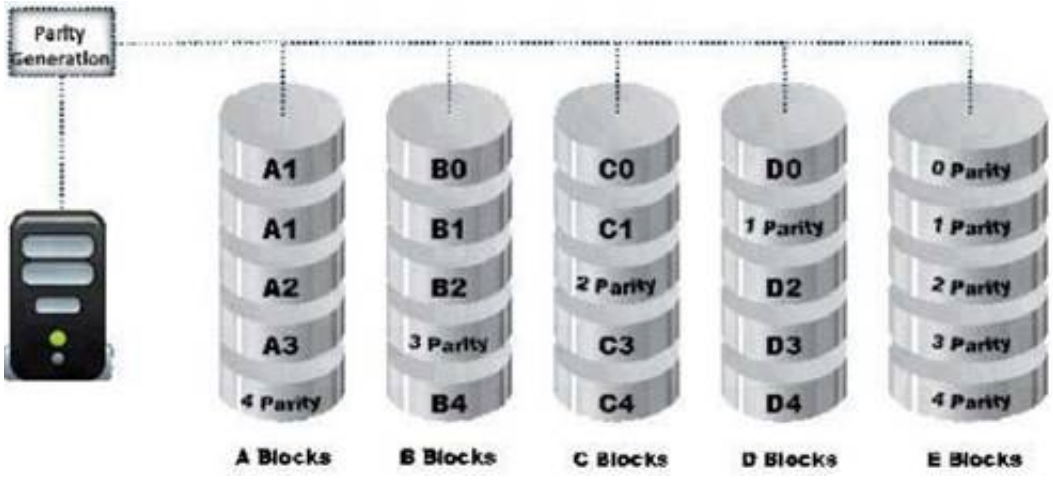
Answer: D

NEW QUESTION 753
- (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 758
- (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 762
- (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 765
- (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 767
- (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 770
- (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 775
- (Exam Topic 2)
Which of the following refers to the process of the witness being questioned by the attorney who called the latter to the stand?

A. Witness Authentication
B. Direct Examination
C. Expert Witness
D. Cross Questioning

Answer: B

NEW QUESTION 776
- (Exam Topic 2)
Why would a company issue a dongle with the software they sell?

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

Answer: C

NEW QUESTION 777
- (Exam Topic 2)
What layer of the OSI model do TCP and UDP utilize?

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

Answer: C

NEW QUESTION 778
.....

Relate Links

100% Pass Your 312-49v10 Exam with Exambible Prep Materials

https://www.exambible.com/312-49v10-exam/

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - https://www.exambible.com/