

# EC-Council

## Exam Questions 312-49v10

Computer Hacking Forensic Investigator (CHFI-v10)



#### NEW QUESTION 1

- (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 2

- (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 3

- (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 4

- (Exam Topic 1)

A suspect is accused of violating the acceptable use of computing resources, as he has visited adult websites and downloaded images. The investigator wants to demonstrate that the suspect did indeed visit these sites. However, the suspect has cleared the search history and emptied the cookie cache. Moreover, he has removed any images he might have downloaded. What can the investigator do to prove the violation?

- A. Image the disk and try to recover deleted files
- B. Seek the help of co-workers who are eye-witnesses
- C. Check the Windows registry for connection data (you may or may not recover)
- D. Approach the websites for evidence

**Answer: A**

#### NEW QUESTION 5

- (Exam Topic 1)

Area density refers to:

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

**Answer: A**

#### NEW QUESTION 6

- (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_pwd[12509]: (login) session opened for user simple by (uid=0)
Apr 26 06:44:36 victim7 PAM_pwd[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 7

- (Exam Topic 1)

You are working as an independent computer forensics investigator and received a call from a systems administrator for a local school system requesting your assistance. One of the students at the local high school is suspected of downloading inappropriate images from the Internet to a PC in the Computer lab. When you arrive at the school, the systems administrator hands you a hard drive and tells you that he made a “simple backup copy” of the hard drive in the PC and put it on this drive and requests that you examine that drive for evidence of the suspected images. You inform him that a “simple backup copy” will not provide deleted files or recover file fragments.

What type of copy do you need to make to ensure that the evidence found is complete and admissible in future proceeding?

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

**Answer:** C

#### NEW QUESTION 8

- (Exam Topic 1)

Corporate investigations are typically easier than public investigations because:

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

**Answer:** B

#### NEW QUESTION 9

- (Exam Topic 2)

Preparing an image drive to copy files to is the first step in Linux forensics. For this purpose, what would the following command accomplish?

`dcflddd if=/dev/zero of=/dev/hda bs=4096 conv=noerror, sync`

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

**Answer:** A

#### NEW QUESTION 10

- (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 10

- (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 13

- (Exam Topic 2)

Steven has been given the task of designing a computer forensics lab for the company he works for. He has found documentation on all aspects of how to design a lab except the number of exits needed. How many exits should Steven include in his design for the computer forensics lab?

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

**Answer:** B

#### NEW QUESTION 18

- (Exam Topic 2)

Which of the following commands shows you the names of all open shared files on a server and the number of file locks on each file?

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

**Answer:** B

#### NEW QUESTION 19

- (Exam Topic 1)

Software firewalls work at which layer of the OSI model?

- A. Application
- B. Network
- C. Transport
- D. Data Link

**Answer:** D

#### NEW QUESTION 21

- (Exam Topic 1)

What does ICMP Type 3/Code 13 mean?

- A. Host Unreachable
- B. Administratively Blocked
- C. Port Unreachable
- D. Protocol Unreachable

**Answer:** B

#### NEW QUESTION 24

- (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 26

- (Exam Topic 1)

Under which Federal Statutes does FBI investigate for computer crimes involving e-mail scams and mail fraud?

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

**Answer:** B

#### NEW QUESTION 28

- (Exam Topic 1)

What should you do when approached by a reporter about a case that you are working on or have worked on?

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

**Answer:** A

#### NEW QUESTION 29

- (Exam Topic 1)

In conducting a computer abuse investigation you become aware that the suspect of the investigation is using ABC Company as his Internet Service Provider (ISP). You contact ISP and request that they provide you assistance with your investigation. What assistance can the ISP provide?

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

**Answer:** B

#### NEW QUESTION 33

- (Exam Topic 1)

When examining a hard disk without a write-blocker, you should not start windows because Windows will write data to the:

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

**Answer:** A

#### NEW QUESTION 37

- (Exam Topic 1)

In a computer forensics investigation, what describes the route that evidence takes from the time you find it until the case is closed or goes to court?

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

**Answer:** C

#### NEW QUESTION 41

- (Exam Topic 1)

In the context of file deletion process, which of the following statement holds true?

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

**Answer:** C

#### NEW QUESTION 44

- (Exam Topic 1)

Study the log given below and answer the following question:

```
Apr 24 14:46:46 [4663]: spp_portscan: portscan detected from 194.222.156.169
Apr 24 14:46:46 [4663]: IDS27/FIN Scan: 194.222.156.169:56693 -> 172.16.1.107:482
Apr 24 18:01:05 [4663]: IDS/DNS-version-query: 212.244.97.121:3485 -> 172.16.1.107:53
Apr 24 19:04:01 [4663]: IDS213/ftp-passwd-retrieval: 194.222.156.169:1425 -> 172.16.1.107:21
Apr 25 08:02:41 [5875]: spp_portscan: PORTSCAN DETECTED from 24.9.255.53
Apr 25 02:08:07 [5875]: IDS277/DNS-version-query: 63.226.81.13:4499 -> 172.16.1.107:53
Apr 25 02:08:07 [5875]: IDS277/DNS-version-query: 63.226.81.13:4630 -> 172.16.1.101:53
Apr 25 02:38:17 [5875]: IDS/RPC-rpcinfo-query: 212.251.1.94:642 -> 172.16.1.107:111
Apr 25 19:37:32 [5875]: IDS230/web-cgi-space-wildcard: 198.173.35.164:4221 -> 172.16.1.107:80
Apr 26 05:45:12 [6283]: IDS212/dns-zone-transfer: 38.31.107.87:2291 -> 172.16.1.101:53
Apr 26 06:43:05 [6283]: IDS181/nops-x86: 63.226.81.13:1351 -> 172.16.1.107:53
Apr 26 06:44:25 victim7 PAM_pwd[12509]: (login) session opened for user simple by (uid=0)
Apr 26 06:44:36 victim7 PAM_pwd[12521]: (su) session opened for user simon by simple(uid=506) Apr 26 06:45:34 [6283]: IDS175/socks-probe:
24.112.167.35:20 -> 172.16.1.107:1080
Apr 26 06:52:10 [6283]: IDS127/telnet-login-incorrect: 172.16.1.107:23 -> 213.28.22.189:4558
```

Precautionary measures to prevent this attack would include writing firewall rules. Of these firewall rules, which among the following would be appropriate?

- A. Disallow UDP53 in from outside to DNS server
- B. Allow UDP53 in from DNS server to outside
- C. Disallow TCP53 in from secondaries or ISP server to DNS server
- D. Block all UDP traffic

**Answer:** A

**NEW QUESTION 48**

- (Exam Topic 1)

What does the acronym POST mean as it relates to a PC?

- A. Primary Operations Short Test
- B. PowerOn Self Test
- C. Pre Operational Situation Test
- D. Primary Operating System Test

**Answer:** B

**NEW QUESTION 51**

- (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 56**

- (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 57**

- (Exam Topic 1)

How many sectors will a 125 KB file use in a FAT32 file system?

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

**Answer:** C

**NEW QUESTION 58**

- (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 63**

- (Exam Topic 1)

Office Documents (Word, Excel and PowerPoint) contain a code that allows tracking the MAC or unique identifier of the machine that created the document. What is that code called?

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

**Answer:** A

**NEW QUESTION 64**

- (Exam Topic 1)

During the course of an investigation, you locate evidence that may prove the innocence of the suspect of the investigation. You must maintain an unbiased opinion and be objective in your entire fact finding process. Therefore, you report this evidence. This type of evidence is known as:

- A. Inculpatory evidence



- B. Mandatory evidence
- C. Exculpatory evidence
- D. Terrible evidence

**Answer:** C

#### NEW QUESTION 65

- (Exam Topic 1)

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

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

**Answer:** A

#### NEW QUESTION 67

- (Exam Topic 1)

Why are Linux/Unix based computers better to use than Windows computers for idle scanning?

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

**Answer:** C

#### NEW QUESTION 70

- (Exam Topic 1)

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

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

**Answer:** D

#### NEW QUESTION 71

- (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 74

- (Exam Topic 1)

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

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

**Answer:** C

#### NEW QUESTION 75

- (Exam Topic 1)

When examining a file with a Hex Editor, what space does the file header occupy?

- A. the last several bytes of the file
- B. the first several bytes of the file
- C. none, file headers are contained in the FAT
- D. one byte at the beginning of the file

**Answer:** D

**NEW QUESTION 80**

- (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 81**

- (Exam Topic 1)

In Linux, what is the smallest possible shellcode?

- A. 24 bytes
- B. 8 bytes
- C. 800 bytes
- D. 80 bytes

**Answer:** A

**NEW QUESTION 86**

- (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 90**

- (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 93**

- (Exam Topic 1)

Which of the following should a computer forensics lab used for investigations have?

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

**Answer:** B

**NEW QUESTION 96**

- (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 98**



- (Exam Topic 1)

What is the target host IP in the following command?

- A. 172.16.28.95
- B. 10.10.150.1
- C. Firewall does not scan target hosts
- D. This command is using FIN packets, which cannot scan target hosts

**Answer:** A

#### NEW QUESTION 101

- (Exam Topic 1)

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

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

**Answer:** A

#### NEW QUESTION 106

- (Exam Topic 1)

Which response organization tracks hoaxes as well as viruses?

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

**Answer:** D

#### NEW QUESTION 108

- (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 113

- (Exam Topic 1)

How many characters long is the fixed-length MD5 algorithm checksum of a critical system file?

- A. 128
- B. 64
- C. 32
- D. 16

**Answer:** C

#### NEW QUESTION 117

- (Exam Topic 1)

When using Windows acquisitions tools to acquire digital evidence, it is important to use a well-tested hardware write-blocking device to:

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

**Answer:** D

#### NEW QUESTION 121

- (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 123

- (Exam Topic 1)

What will the following command produce on a website login page? SELECT email, passwd, login\_id, full\_name FROM members WHERE email = 'someone@somehwere.com'; DROP TABLE members; --'

- A. Deletes the entire members table
- B. Inserts the Error! Reference source not found.email address into the members table
- C. Retrieves the password for the first user in the members table
- D. This command will not produce anything since the syntax is incorrect

**Answer:** A

#### NEW QUESTION 124

- (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 127

- (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 131

- (Exam Topic 1)

Sectors in hard disks typically contain how many bytes?

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

**Answer:** B

#### NEW QUESTION 132

- (Exam Topic 1)

One technique for hiding information is to change the file extension from the correct one to one that might not be noticed by an investigator. For example, changing a .jpg extension to a .doc extension so that a picture file appears to be a document. What can an investigator examine to verify that a file has the correct extension?

- A. the File Allocation Table
- B. the file header
- C. the file footer
- D. the sector map

**Answer:** B

#### NEW QUESTION 135

- (Exam Topic 1)

Before you are called to testify as an expert, what must an attorney do first?

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

**Answer:** D

#### NEW QUESTION 140

- (Exam Topic 1)

What header field in the TCP/IP protocol stack involves the hacker exploit known as the Ping of Death?

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

**Answer:** B

#### NEW QUESTION 143

- (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 146

- (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 149

- (Exam Topic 4)

To which phase of the computer forensics investigation process does "planning and budgeting of a forensics lab" belong?

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

**Answer:** C

#### NEW QUESTION 153

- (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 157

- (Exam Topic 4)

Which of the following is considered as the starting point of a database and stores user data and database objects in an MS SQL server?

- A. Ibdatabase1
- B. Application data files (ADF)
- C. Transaction log data files (LDF)
- D. Primary data files (MDF)

**Answer:** C

#### NEW QUESTION 161

- (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-zA-Z0-9\%I*((\%3E)|>)/lx`. 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 164

- (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 169

- (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 SFTP 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 171

- (Exam Topic 4)

Cybercriminals sometimes use compromised computers to commit other crimes, which may involve using computers or networks to spread malware or illegal information. Which type of cybercrime stops users from using a device or network, or prevents a company from providing a software service to its customers?

- A. Denial-of-Service (DoS) attack
- B. Malware attack
- C. Ransomware attack
- D. Phishing

**Answer: C**

#### NEW QUESTION 172

- (Exam Topic 4)

William is examining a log entry that reads 192.168.0.1 - - [18/Jun/2020:12:42:29 +0000] "GET / HTTP/1.1" 200 1861. Which of the following logs does the log entry belong to?

- A. The combined log format of Apache access log
- B. The common log format of Apache access log
- C. Apache error log
- D. IIS log

**Answer: A**

#### NEW QUESTION 173

- (Exam Topic 4)

A cybercriminal is attempting to remove evidence from a Windows computer. He deletes the file evidence1.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 175

- (Exam Topic 4)

Which layer in the IoT 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 179

- (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 184

- (Exam Topic 4)

An EC2 instance storing critical data of a company got infected with malware. The forensics team took the EBS volume snapshot of the affected Instance to perform further analysis and collected other data of evidentiary value. What should be their next step?

- A. They should pause the running instance
- B. They should keep the instance running as it stores critical data
- C. They should terminate all instances connected via the same VPC
- D. They should terminate the instance after taking necessary backup

**Answer:** D

#### NEW QUESTION 186

- (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 Wireshark 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 189

- (Exam Topic 4)

An Investigator Is checking a Cisco firewall log that reads as follows:

Aug 21 2019 09:16:44: %ASA-1-106021: Deny ICMP reverse path check from 10.0.0.44 to 10.0.0.33 on Interface outside

What does %ASA-1-106021 denote?

- A. Mnemonic message
- B. Type of traffic
- C. Firewall action
- D. Type of request

**Answer:** C

#### NEW QUESTION 190

- (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 194

- (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 196

- (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 199

- (Exam Topic 3)

In a computer that has Dropbox client installed, which of the following files related to the Dropbox client store information about local Dropbox installation and the Dropbox user account, along with email IDs linked with the account?

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

**Answer:** A

#### NEW QUESTION 204

- (Exam Topic 4)

Data density of a disk drive is calculated by using

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

**Answer:** D

#### NEW QUESTION 206

- (Exam Topic 3)

An investigator is analyzing a checkpoint firewall log and comes across symbols. What type of log is he looking at?



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

**Answer:** C

#### NEW QUESTION 208

- (Exam Topic 3)

You are assigned a task to examine the log files pertaining to MyISAM storage engine. While examining, you are asked to perform a recovery operation on a MyISAM log file. Which among the following MySQL Utilities allow you to do so?

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

**Answer:** C

#### NEW QUESTION 209

- (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 214

- (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 219

- (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 224

- (Exam Topic 3)

An investigator has found certain details after analysis of a mobile device. What can reveal the manufacturer information?

- A. Equipment Identity Register (EIR)
- B. Electronic Serial Number (ESN)
- C. International mobile subscriber identity (IMSI)
- D. Integrated circuit card identifier (ICCID)

**Answer:** B

#### NEW QUESTION 227

- (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 229

- (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 231

- (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 236

- (Exam Topic 3)

In which implementation of RAID will the image of a Hardware RAID volume be different from the image taken separately from the disks?

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

**Answer:** D

#### NEW QUESTION 239

- (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 242

- (Exam Topic 3)

Which of these Windows utility help you to repair logical file system errors?

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

**Answer: D**

#### NEW QUESTION 247

- (Exam Topic 3)

What document does the screenshot represent?



The screenshot shows a form for evidence collection. It has several fields with folder icons: 'Laboratory or Agency Name', 'Case Number', 'Received from (Name and Title)', 'Address and Telephone Number', 'Location from where Evidence Obtained', 'Reason Evidence Was Obtained', and 'Date and Time Evidence Was Obtained'. At the bottom, there is a table with three columns: 'Item Number', 'Quantity', and 'Description of Item'.

Item Number	Quantity	Description of Item

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

**Answer: D**

#### NEW QUESTION 249

- (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 251

- (Exam Topic 3)

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

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

**Answer:** B

**NEW QUESTION 252**

- (Exam Topic 3)

Which of the following tool is used to locate IP addresses?

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

**Answer:** A

**NEW QUESTION 254**

- (Exam Topic 3)

Which of the following web browser uses the Extensible Storage Engine (ESE) database format to store browsing records, including history, cache, and cookies?

- A. Safari
- B. Mozilla Firefox
- C. Microsoft Edge
- D. Google Chrome

**Answer:** C

**NEW QUESTION 256**

- (Exam Topic 3)

Brian needs to acquire data from RAID storage. Which of the following acquisition methods is recommended to retrieve only the data relevant to the investigation?

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

**Answer:** B

**NEW QUESTION 258**

- (Exam Topic 3)

Where should the investigator look for the Edge browser's browsing records, including history, cache, and cookies?

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

**Answer:** A

**NEW QUESTION 261**

- (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 263**

- (Exam Topic 3)

%3cscript%3ealert("XXXXXXXX")%3c/script%3e is a script obtained from a Cross-Site Scripting attack.

What type of encoding has the attacker employed?

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

**Answer:** B

**NEW QUESTION 265**

- (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 270**

- (Exam Topic 3)

Which of the following examinations refers to the process of providing the opposing side in a trial the opportunity to question a witness?

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

**Answer:** A

**NEW QUESTION 272**

- (Exam Topic 3)

Select the tool appropriate for examining the dynamically linked libraries of an application or malware.

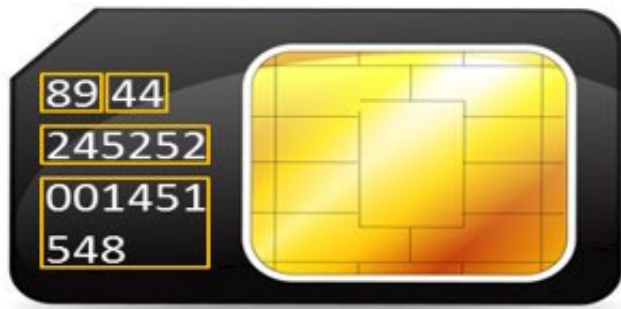
- A. DependencyWalker
- B. SysAnalyzer
- C. PEiD
- D. ResourcesExtract

**Answer:** A

**NEW QUESTION 277**

- (Exam Topic 3)

During an investigation, Noel found the following SIM card from the suspect's mobile. What does the code 89 44 represent?



- A. Issuer Identifier Number and TAC
- B. Industry Identifier and Country code
- C. Individual Account Identification Number and Country Code
- D. TAC and Industry Identifier

**Answer:** B

**NEW QUESTION 282**

- (Exam Topic 3)

Which among the following search warrants allows the first responder to search and seize the victim's computer components such as hardware, software, storage devices, and documentation?

- A. John Doe Search Warrant
- B. Citizen Informant Search Warrant
- C. Electronic Storage Device Search Warrant
- D. Service Provider Search Warrant

**Answer:** C

**NEW QUESTION 286**

- (Exam Topic 3)

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

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

**Answer:** A

**NEW QUESTION 289**

- (Exam Topic 3)

As part of extracting the system data, Jenifer has used the netstat command. What does this tool reveal?

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

**Answer:** C

**NEW QUESTION 292**

- (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 294**

- (Exam Topic 3)

If the partition size is 4 GB, each cluster will be 32 K. Even if a file needs only 10 K, the entire 32 K will be allocated, resulting in 22 K of .

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

**Answer:** A

**NEW QUESTION 298**

- (Exam Topic 3)

Which of the following standard represents a legal precedent set in 1993 by the Supreme Court of the United States regarding the admissibility of expert witnesses' testimony during federal legal proceedings?

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

**Answer:** D

**NEW QUESTION 301**

- (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 306**

- (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 307**

- (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 310

- (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 311

- (Exam Topic 3)

In both pharming and phishing attacks an attacker can create websites that look similar to legitimate sites with the intent of collecting personal identifiable information from its victims. What is the difference between pharming and phishing attacks?

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

**Answer:** B

#### NEW QUESTION 314

- (Exam Topic 3)

Identify the file system that uses \$BitMap file to keep track of all used and unused clusters on a volume.

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

**Answer:** A

#### NEW QUESTION 315

- (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 319

- (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 (gfwzip)
- C. Advanced Forensic Framework 4
- D. Advanced Forensics Format (AFF)

**Answer:** B

#### NEW QUESTION 323

- (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 328

- (Exam Topic 2)

What is one method of bypassing a system BIOS password?

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



**Answer:** B

#### NEW QUESTION 329

- (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 331

- (Exam Topic 2)

Using Internet logging software to investigate a case of malicious use of computers, the investigator comes across some entries that appear odd.

```
File Edit Format View Help
Begin log; 2007-04-24
http://www.somewhere.com/
http://www.somewhere.com/default.aspx?userid=566466
http://www.somewhere.com/default.aspx?userid=566467
http://www.somewhere.com/default.aspx?userid=566468
http://www.somewhere.com/default.aspx?userid=566469
http://www.somewhere.com/default.aspx?userid=566470
http://www.somewhere.com/default.aspx?userid=566471
```

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

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

**Answer:** A

#### NEW QUESTION 332

- (Exam Topic 2)

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

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

**Answer:** A

#### NEW QUESTION 334

- (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 337

- (Exam Topic 2)

Where is the default location for Apache access logs on a Linux computer?

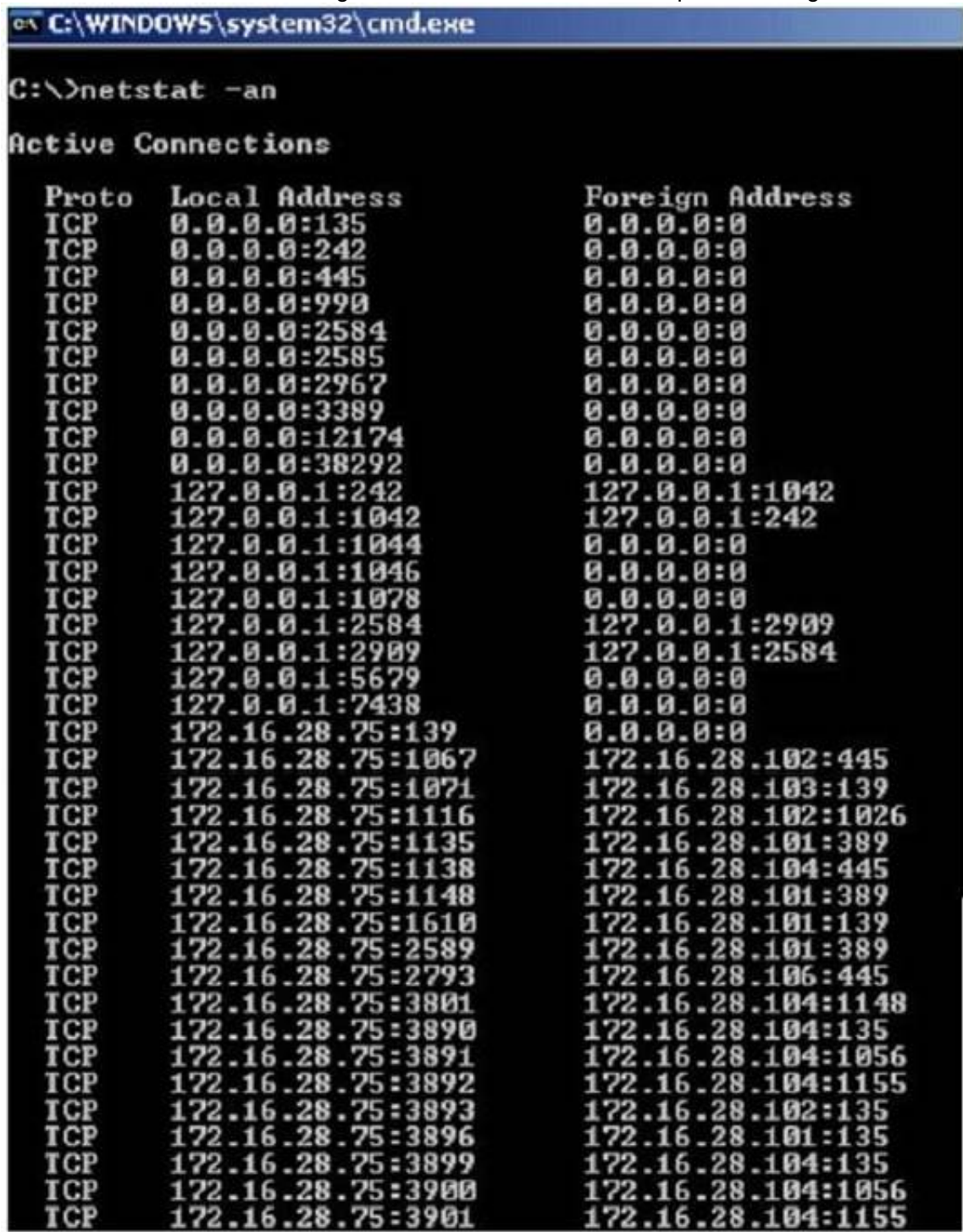
- A. `usr/local/apache/logs/access_log`
- B. `bin/local/home/apache/logs/access_log`
- C. `usr/logs/access_log`
- D. `logs/usr/apache/access_log`

**Answer:** A

NEW QUESTION 342

- (Exam Topic 2)

Jack Smith is a forensics investigator who works for Mason Computer Investigation Services. He is investigating a computer that was infected by Ramen Virus.



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

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

Answer: B

NEW QUESTION 347

- (Exam Topic 2)

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

Answer: B

NEW QUESTION 348

- (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 353

- (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 357

- (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 360

- (Exam Topic 2)

Which of the following techniques can be used to beat steganography?

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

**Answer:** B

#### NEW QUESTION 364

- (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 368

- (Exam Topic 2)

Which of the following files gives information about the client sync sessions in Google Drive on Windows?

- A. sync\_log.log
- B. Sync\_log.log
- C. sync.log
- D. Sync.log

**Answer:** B

#### NEW QUESTION 373

- (Exam Topic 2)

The process of restarting a computer that is already turned on through the operating system is called?

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

**Answer:** A

#### NEW QUESTION 376

- (Exam Topic 2)

Your company's network just finished going through a SAS 70 audit. This audit reported that overall, your network is secure, but there are some areas that needs improvement. The major area was SNMP security. The audit company recommended turning off SNMP, but that is not an option since you have so many remote nodes to keep track of. What step could you take to help secure SNMP on your network?

- A. Block all internal MAC address from using SNMP
- B. Block access to UDP port 171
- C. Block access to TCP port 171

D. Change the default community string names

**Answer:** D

**NEW QUESTION 378**

- (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 379**

- (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 383**

- (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 385**

- (Exam Topic 2)

Which rule requires an original recording to be provided to prove the content of a recording?

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

**Answer:** B

**NEW QUESTION 390**

- (Exam Topic 2)

During an investigation, an employee was found to have deleted harassing emails that were sent to someone else. The company was using Microsoft Exchange and had message tracking enabled. Where could the investigator search to find the message tracking log file on the Exchange server?

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

**Answer:** A

**NEW QUESTION 391**

- (Exam Topic 2)

Which forensic investigating concept trails the whole incident from how the attack began to how the victim was affected?

- A. Point-to-point
- B. End-to-end
- C. Thorough
- D. Complete event analysis

**Answer:** B

**NEW QUESTION 392**

- (Exam Topic 2)

Which of the following commands shows you all of the network services running on Windows-based servers?

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

**Answer:** A

**NEW QUESTION 396**

- (Exam Topic 2)

In Steganalysis, which of the following describes a Known-stego attack?

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

**Answer:** C

**NEW QUESTION 397**

- (Exam Topic 2)

Wireless access control attacks aim to penetrate a network by evading WLAN access control measures such as AP MAC filters and Wi-Fi port access controls. Which of the following wireless access control attacks allow the attacker to set up a rogue access point outside the corporate perimeter and then lure the employees of the organization to connect to it?

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

**Answer:** B

**NEW QUESTION 401**

- (Exam Topic 2)

Which of the following is a database in which information about every file and directory on an NT File System (NTFS) volume is stored?

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

**Answer:** D

**NEW QUESTION 404**

- (Exam Topic 2)

What type of attack sends spoofed UDP packets (instead of ping packets) with a fake source address to the IP broadcast address of a large network?

- A. Fraggle
- B. Smurf scan
- C. SYN flood
- D. Teardrop

**Answer:** A

**NEW QUESTION 406**

- (Exam Topic 2)

What file is processed at the end of a Windows XP boot to initialize the logon dialog box?

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

**Answer:** A

**NEW QUESTION 409**

- (Exam Topic 2)

Which code does the FAT file system use to mark the file as deleted?

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

**Answer:** D

**NEW QUESTION 413**



- (Exam Topic 2)

Tyler is setting up a wireless network for his business that he runs out of his home. He has followed all the directions from the ISP as well as the wireless router manual. He does not have any encryption set and the SSID is being broadcast. On his laptop, he can pick up the wireless signal for short periods of time, but then the connection drops and the signal goes away.

Eventually the wireless signal shows back up, but drops intermittently. What could be Tyler issue with his home wireless network?

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

**Answer: C**

#### NEW QUESTION 418

- (Exam Topic 2)

Which of the following attacks allows an attacker to access restricted directories, including application source code, configuration and critical system files, and to execute commands outside of the web server's root directory?

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

**Answer: C**

#### NEW QUESTION 419

- (Exam Topic 2)

While presenting his case to the court, Simon calls many witnesses to the stand to testify. Simon decides to call Hillary Taft, a lay witness, to the stand. Since Hillary is a lay witness, what field would she be considered an expert in?

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

**Answer: B**

#### NEW QUESTION 420

- (Exam Topic 2)

Julie is a college student majoring in Information Systems and Computer Science. She is currently writing an essay for her computer crimes class. Julie paper focuses on white-collar crimes in America and how forensics investigators investigate the cases. Julie would like to focus the subject. Julie would like to focus the subject of the essay on the most common type of crime found in corporate America. What crime should Julie focus on?

- A. Physical theft
- B. Copyright infringement
- C. Industrial espionage
- D. Denial of Service attacks

**Answer: C**

#### NEW QUESTION 424

- (Exam Topic 2)

Which of the following tool creates a bit-by-bit image of an evidence media?

- A. Recuva
- B. FileMerlin
- C. AccessData FTK Imager
- D. Xplico

**Answer: C**

#### NEW QUESTION 426

- (Exam Topic 2)

The following is a log file screenshot from a default installation of IIS 6.0.



```
#Software: Microsoft Internet Information Services 6.0
#Version: 1.0
#Date: 2007-01-22 15:42:36
#Fields: date time s-sitename s-ip cs-method cs-uri-stem cs-uri-query s-port cs-user
2007-01-22 15:42:36 W3SVC1 172.16.28.102 GET /index.html - 80 - 172.16.28.80
Mozilla/4.0+(compatible;+MSIE+6.0;+windows+NT+5.1;+SV1;+Avant+Browser;+.NET+CLR+1.1.
2007-01-22 15:42:36 W3SVC1 172.16.28.102 GET /development/index.asp - 80 - 172.16.28
Mozilla/4.0+(compatible;+MSIE+6.0;+windows+NT+5.1;+SV1;+Avant+Browser;+.NET+CLR+1.1.
2007-01-22 15:42:36 W3SVC1 172.16.28.102 GET /development/css/olcstyle.css - 80 - 17
Mozilla/4.0+(compatible;+MSIE+6.0;+windows+NT+5.1;+SV1;+Avant+Browser;+.NET+CLR+1.1.
2007-01-22 15:42:36 W3SVC1 172.16.28.102 GET /favicon.ico - 80 - 172.16.28.80 Avant+
2007-01-22 15:42:36 W3SVC1 172.16.28.102 GET /development/css/dhtml_horiz.css - 80 -
Mozilla/4.0+(compatible;+MSIE+6.0;+windows+NT+5.1;+SV1;+Avant+Browser;+.NET+CLR+1.1.
2007-01-22 15:42:36 W3SVC1 172.16.28.102 GET /development/images/index_01.jpg - 80 -
Mozilla/4.0+(compatible;+MSIE+6.0;+windows+NT+5.1;+SV1;+Avant+Browser;+.NET+CLR+1.1.
2007-01-22 15:42:36 W3SVC1 172.16.28.102 GET /development/images/index_02.jpg - 80 -
Mozilla/4.0+(compatible;+MSIE+6.0;+windows+NT+5.1;+SV1;+Avant+Browser;+.NET+CLR+1.1.
2007-01-22 15:42:36 W3SVC1 172.16.28.102 GET /development/images/index_03.jpg - 80 -
Mozilla/4.0+(compatible;+MSIE+6.0;+windows+NT+5.1;+SV1;+Avant+Browser;+.NET+CLR+1.1.
2007-01-22 15:42:36 W3SVC1 172.16.28.102 GET /development/images/index_04.jpg - 80 -
Mozilla/4.0+(compatible;+MSIE+6.0;+windows+NT+5.1;+SV1;+Avant+Browser;+.NET+CLR+1.1.
2007-01-22 15:42:36 W3SVC1 172.16.28.102 GET /development/images/index_05.jpg - 80 -
Mozilla/4.0+(compatible;+MSIE+6.0;+windows+NT+5.1;+SV1;+Avant+Browser;+.NET+CLR+1.1.
2007-01-22 15:42:36 W3SVC1 172.16.28.102 GET /development/images/index_06.jpg - 80 -
Mozilla/4.0+(compatible;+MSIE+6.0;+windows+NT+5.1;+SV1;+Avant+Browser;+.NET+CLR+1.1.
2007-01-22 15:42:36 W3SVC1 172.16.28.102 GET /development/images/index_07.jpg - 80 -
Mozilla/4.0+(compatible;+MSIE+6.0;+windows+NT+5.1;+SV1;+Avant+Browser;+.NET+CLR+1.1.
2007-01-22 15:42:36 W3SVC1 172.16.28.102 GET /development/images/index_08.jpg - 80 -
Mozilla/4.0+(compatible;+MSIE+6.0;+windows+NT+5.1;+SV1;+Avant+Browser;+.NET+CLR+1.1.
2007-01-22 15:42:36 W3SVC1 172.16.28.102 GET /development/script/dhtml.js - 80 - 172
Mozilla/4.0+(compatible;+MSIE+6.0;+windows+NT+5.1;+SV1;+Avant+Browser;+.NET+CLR+1.1.
2007-01-22 15:42:36 W3SVC1 172.16.28.102 GET /development/images/greenArrow.jpg - 80
Mozilla/4.0+(compatible;+MSIE+6.0;+windows+NT+5.1;+SV1;+Avant+Browser;+.NET+CLR+1.1.
2007-01-22 15:42:36 W3SVC1 172.16.28.102 GET /development/images/board_01.jpg - 80 -
Mozilla/4.0+(compatible;+MSIE+6.0;+windows+NT+5.1;+SV1;+Avant+Browser;+.NET+CLR+1.1.
2007-01-22 15:42:36 W3SVC1 172.16.28.102 GET /development/images/board_02.jpg - 80 -
Mozilla/4.0+(compatible;+MSIE+6.0;+windows+NT+5.1;+SV1;+Avant+Browser;+.NET+CLR+1.1.
2007-01-22 15:42:36 W3SVC1 172.16.28.102 GET /development/images/flash_bar.jpg -
```

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

- A. UTC  
B. GMT  
C. TAI  
D. UT

**Answer: A**

### NEW QUESTION 429

- (Exam Topic 2)

What is the size value of a nibble?

- A. 0.5 kilo byte  
B. 0.5 bit  
C. 0.5 byte  
D. 2 bits

**Answer: C**

## NEW QUESTION 432

- (Exam Topic 2)

Richard is extracting volatile data from a system and uses the command `doskey/history`. What is he trying to extract?

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

**Answer: B**

**NEW QUESTION 437**

- (Exam Topic 2)

In handling computer-related incidents, which IT role should be responsible for recovery, containment, and prevention to constituents?

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

**Answer: B**

## NEW QUESTION 439

- (Exam Topic 2)

Which of the following acts as a network intrusion detection system as well as network intrusion prevention system?

- A. Accunetix  
B. Nikto  
C. Snort  
D. Kismet

**Answer:** C

**NEW QUESTION 442**

- (Exam Topic 2)

At what layer does a cross site scripting attack occur on?

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

**Answer:** B

**NEW QUESTION 444**

- (Exam Topic 2)

Before performing a logical or physical search of a drive in Encase, what must be added to the program?

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

**Answer:** B

**NEW QUESTION 446**

- (Exam Topic 2)

Which of the following tools will help the investigator to analyze web server logs?

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

**Answer:** D

**NEW QUESTION 449**

- (Exam Topic 2)

If you are concerned about a high level of compression but not concerned about any possible data loss, what type of compression would you use?

- A. Lossful compression
- B. Lossy compression
- C. Lossless compression
- D. Time-loss compression

**Answer:** B

**NEW QUESTION 454**

- (Exam Topic 2)

Which of the following is an iOS Jailbreaking tool?

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

**Answer:** D

**NEW QUESTION 457**

.....

## Thank You for Trying Our Product

### We offer two products:

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

2nd - Questions and Answers in PDF Format

### 312-49v10 Practice Exam Features:

- \* 312-49v10 Questions and Answers Updated Frequently
- \* 312-49v10 Practice Questions Verified by Expert Senior Certified Staff
- \* 312-49v10 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- \* 312-49v10 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

**100% Actual & Verified — Instant Download, Please Click**  
**[Order The 312-49v10 Practice Test Here](#)**