EC-COUNCIL.312-49v9.v2022-11-15.q347

Exam Code:	312-49v9
Exam Name:	ECCouncil Computer Hacking Forensic Investigator (V9)
Certification Provider:	EC-COUNCIL
Free Question Number:	347
Version:	v2022-11-15
# of views:	3500
# of Questions views:	3470
https://www.freeqas.com/qa/EC-COUNCIL/312-49v9/EC-COUNCIL.312-49v9.v2022-11-15.q347.html	

NEW QUESTION: 1
Which of the following is NOT an anti-forensics technique?
A. Password Protection
B. Steganography
C. Encryption
D. Data Deduplication
Answer: (SHOW ANSWER)

NEW QUESTION: 2
Kimberly is studying to be an IT security analyst at a vocational school in her town. The school offers many different programming as well as networking languages. What networking protocol language should she learn that routers utilize?
A. UDP
B. ATM
C. BPG
D. OSPF
Answer: (SHOW ANSWER)

NEW QUESTION: 3
When obtaining a warrant, it is important to:
A. particularlydescribe the place to be searched and particularly describe the items to be seized
B. generallydescribe the place to be searched and generally describe the items to be seized
C. generallydescribe the place to be searched and particularly describe the items to be seized
D. particularlydescribe the place to be searched and generally describe the items to be seized
Answer: A (LEAVE A REPLY)

NEW QUESTION: 4
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 config
B. Net stat
C. Net sessions
D. Net share
Answer: (SHOW ANSWER)

NEW QUESTION: 5
Smith, a forensic examiner, was analyzing a hard disk image to find and acquire deleted sensitive files. He stumbled upon a $Recycle.Bin folder in the root directory of the disk. Identify the operating system in use.
A. Windows XP
B. Windows 98
C. Linux
D. Windows 8.1
Answer: A (LEAVE A REPLY)

NEW QUESTION: 6
You have compromised a lower-level administrator account on an Active Directory network of a small company in Dallas, Texas. You discover Domain Controllers through enumeration. You connect to one of the Domain Controllers on port 389 using ldp.exe. What are you trying to accomplish here?
A. Establish a remote connection to the Domain Controller
B. Enumerate domain user accounts and built-in groups
C. Enumerate MX and A records from DNS
D. Poison the DNS records with false records
Answer: B (LEAVE A REPLY)

NEW QUESTION: 7
Paraben Lockdown device uses which operating system to write hard drive data?
A. Red Hat
B. Windows
C. Mac OS
D. Unix
Answer: B (LEAVE A REPLY)

NEW QUESTION: 8

Before performing a logical or physical search of a drive in Encase, what must be added to the program?
A. Keywords
B. Hash sets
C. Bookmarks
D. File signatures
Answer: A (LEAVE A REPLY)

NEW QUESTION: 9
What is the first step that needs to be carried out to investigate wireless attacks?
A. Identify wireless devices at crime scene
B. Document the scene and maintain a chain of custody
C. Detect the wireless connections
D. Obtain a search warrant
Answer: D (LEAVE A REPLY)

NEW QUESTION: 10
You are a security analyst performing reconnaissance on a company you will be carrying out a penetration test for. You conduct a search for IT jobs on Dice.com and find the following information for an open position: 7+ years experience in Windows Server environment 5+ years experience in Exchange 2000/2003 environment Experience with
Cisco Pix Firewall, Linksys 1376 router, Oracle 11i and MYOB v3.4 Accounting software are reQuired MCSA desired, MCSE, CEH preferred No Unix/Linux Experience needed
What is this information posted on the job website considered?
A. Competitive exploit
B. Information vulnerability
C. Trade secret
D. Social engineering exploit
Answer: B (LEAVE A REPLY)

NEW QUESTION: 11
On an Active Directory network using NTLM authentication, where on the domain controllers are the passwords stored?
A. SAM
B. Shadow file
C. AMS
D. Password.conf
Answer: A (LEAVE A REPLY)

NEW QUESTION: 12
Before you are called to testify as an expert, what must an attorney do first?

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

NEW QUESTION: 13
What is the target host IP in the following command?
A. 172.16.28.95
B. 10.10.150.1
C. This command is using FIN packets, which cannot scan target hosts
D. Firewalk does not scan target hosts
Answer: A (LEAVE A REPLY)

NEW QUESTION: 14
Mobile phone forensics is the science of recovering digital evidence from a mobile phone under forensically sound conditions.
A. False
B. True
Answer: B (LEAVE A REPLY)

NEW QUESTION: 15
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:\ALCSetup.log
C. C:\hiberfil.sys
D. C:\config.sys
Answer: A (LEAVE A REPLY)

NEW QUESTION: 16
John is working on his company policies and guidelines. The section he is currently working on covers company documents; how they should be handled, stored, and eventually destroyed. John is concerned about the process whereby outdated documents are destroyed. What type of shredder should John write in the guidelines to be used when destroying documents?
A. Cross-cut shredder
B. Cross-hatch shredder
C. Cris-cross shredder
D. Strip-cut shredder
Answer: (SHOW ANSWER)

NEW QUESTION: 17
The surface of a hard disk consists of several concentric rings known as tracks; each of these tracks has smaller partitions called disk blocks. What is the size of each block?
A. 512 bytes
B. 512 bits
C. 256 bits
D. 256 bytes
Answer: A (LEAVE A REPLY)

NEW QUESTION: 18
Which of the following options will help users to enable or disable the last access time on a system running Windows 10 OS?
A. Reg.exe
B. Devcon
C. wmic service
D. fsutil
Answer: D (LEAVE A REPLY)

NEW QUESTION: 19
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. HTML tags
B. Single pipe character
C. Multiple pipe characters
D. Plaintext
Answer: (SHOW ANSWER)

NEW QUESTION: 20
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. Cross-hatch shredder
B. Cris-cross shredder
C. Cross-cut shredder
D. Strip-cut shredder
Answer: (SHOW ANSWER)

NEW QUESTION: 21
Madison is on trial for allegedly breaking into her university internal network. The police raided her dorm room and seized all of her computerMadison 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 isequipment.
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?Madison? lawyer trying to prove the police violated?
A. The 10th Amendment
B. The 4th Amendment
C. The 5th Amendment
D. The 1st Amendment
Answer: (SHOW ANSWER)

NEW QUESTION: 22
When investigating a computer forensics case where Microsoft Exchange and Blackberry Enterprise server are used, where would investigator need to search to find email sent from a Blackberry device?
A. RIM Messaging center
B. Blackberry Enterprise server
C. Microsoft Exchange server
D. Blackberry desktop redirector
Answer: C (LEAVE A REPLY)

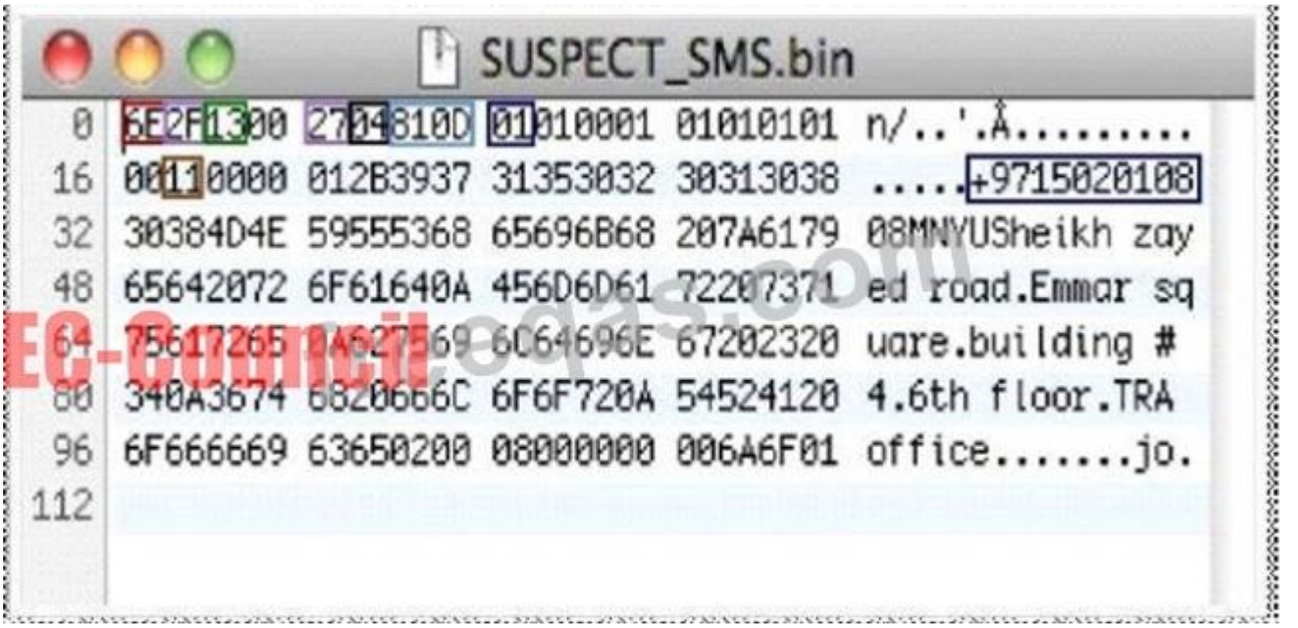
NEW QUESTION: 23
Which of the following standard represents a legal precedent set in 1993 by the Supreme Court of the United States regarding the admissibility of expert witnesses' testimony during federal legal proceedings?
A. SWGDE & SWGIT
B. IOCE
C. Frye

D. Daubert

Answer: D (LEAVE A REPLY)

NEW QUESTION: 24

Determine the message length from following hex viewer record:



A. 810D

B. 6E2F

C. 27

D. 13

Answer: (SHOW ANSWER)

NEW QUESTION: 25

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

A. Visual cipher

B. Visual semagram

C. Text semagram

D. Grill cipher

Answer: B (LEAVE A REPLY)

NEW QUESTION: 26

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. dir

C. vim

D. grep

Answer: D (LEAVE A REPLY)

NEW QUESTION: 27

Pick the statement which does not belong to the Rule 804. Hearsay Exceptions; Declarant Unavailable.

A. Prior statement by witness

B. Statement under belief of impending death

C. Statement against interest

D. Statement of personal or family history

Answer: B (LEAVE A REPLY)

NEW QUESTION: 28

Email spoofing refers to:

A. The forgery of an email header so that the message appears to have originated from someone or somewhere other than the actual source

B. A sudden spike of "Reply All" messages on an email distribution list, caused by one misdirected message

C. Sending huge volumes of email to an address in an attempt to overflow the mailbox or overwhelm the server where the email address Is hosted to cause a denial-of-service attack

D. The criminal act of sending an illegitimate email, falsely claiming to be from a legitimate site in an attempt to acquire the user's personal or account information

Answer: A (LEAVE A REPLY)

NEW QUESTION: 29

Buffer Overflow occurs when an application writes more data to a block of memory, or buffer, than the buffer is allocated to hold. Buffer overflow attacks allow an attacker to modify the _____in order to control the process execution, crash the process and modify internal variables.

A. Target rainbow table

B. Target process's address space

C. Target SAM file

D. Target remote access

Answer: B (LEAVE A REPLY)

NEW QUESTION: 30
An investigator has extracted the device descriptor for a 1 GB thumb drive that looks like: Disk&Ven_Best_Buy&Prod_Geek_Squad_U3&Rev 6.15. What does the "Geek_Squad" part represent?
A. Developer description
B. Product description
C. Software or OS used
D. Manufacturer Details
Answer: B (LEAVE A REPLY)

NEW QUESTION: 31
Which of the following is not correct when documenting an electronic crime scene?
A. Write down the color of shirt and pant the suspect was wearing
B. Document related electronic components that are difficult to find
C. Document the physical scene, such as the position of the mouse and the location of components near the system
D. Record the condition of the computer system, storage media, electronic devices and conventional evidence, including power status of the computer
Answer: (SHOW ANSWER)

NEW QUESTION: 32
CAN-SPAM Act requires that you:
A. Don't use true header information
B. Don't use deceptive subject lines
C. Don't tell the recipients where you are located
D. Don't identify the message as an ad
Answer: B (LEAVE A REPLY)

NEW QUESTION: 33
Digital photography helps in correcting the perspective of the Image which Is used In taking the measurements of the evidence. Snapshots of the evidence and incident-prone areas need to be

taken to help in the forensic process. Is digital photography accepted as evidence in the court of law?
A. Yes
B. No
Answer: A (LEAVE A REPLY)

NEW QUESTION: 34
You are employed directly by an attorney to help investigate an alleged sexual harassment case at a large pharmaceutical manufacture. While at the corporate office of the company, the CEO demands to know the status of the investigation. What prevents you from discussing the case with the CEO?
A. the attorney-work-product rule
B. Good manners
C. ISO 17799
D. Trade secrets
Answer: (SHOW ANSWER)

NEW QUESTION: 35
Which of the following email headers specifies an address for mailer-generated errors, like "no such user" bounce messages (instead of the sender's address)?
A. Content-Transfer-Encoding header
B. Content-Type header
C. Errors-To header
D. Mime-Version header
Answer: (SHOW ANSWER)

NEW QUESTION: 36
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. The life of the author
B. Copyrights last forever
C. The life of the author plus 70 years
D. 70 years
Answer: C (LEAVE A REPLY)

NEW QUESTION: 37
Which U.S. law sets the rules for sending emails for commercial purposes, establishes the minimum requirements for commercial messaging, gives the recipients of emails the right to ask the senders to stop emailing them, and spells out the penalties in case the above said rules are violated?
A. American: NAVSO P-5239-26 (RLL)

B. NO-SPAM Act
C. American: DoD 5220.22-M
D. CAN-SPAM Act
Answer: (SHOW ANSWER)

NEW QUESTION: 38
When should an MD5 hash check be performed when processing evidence?
A. On an hourly basis during the evidence examination
B. After the evidence examination has been completed
C. Before and after evidence examination
D. Before the evidence examination has been completed
Answer: C (LEAVE A REPLY)

NEW QUESTION: 39
Which of the following is a non-zero data that an application allocates on a hard disk cluster in systems running on Windows OS?
A. Sparse File
B. Meta Block Group
C. Master File Table
D. Slack Space
Answer: C (LEAVE A REPLY)

NEW QUESTION: 40
Davidson Trucking is a small transportation company that has three local offices in Detroit Michigan. Ten female employees that work for the company have gone to an attorney reporting that male employees repeatedly harassed them and that management did nothing to stop the problem. Davidson has employee policies that outline all company guidelines, including awareness on harassment and how it will not be tolerated. When the case is brought to court, whom should the prosecuting attorney call upon for not upholding company policy?
A. Administrative assistant in charge of writing policies
B. IT personnel
C. Employees themselves
D. Supervisors
Answer: D (LEAVE A REPLY)

NEW QUESTION: 41
What does the 63.78.199.4(161) denotes in a Cisco router log?
Mar 14 22:57:53.425 EST: %SEC-6-IPACCESSLOGP: list internet-inbound denied udp 66.56.16.77(1029) ->
63.78.199.4(161), 1 packet
A. Login IP address

B. None of the above
C. Destination IP address
D. Source IP address
Answer: (SHOW ANSWER)

NEW QUESTION: 42
Which of the following attacks allows an attacker to access restricted directories, including application source code, configuration and critical system files, and to execute commands outside of the web server's root directory?
A. Parameter/form tampering
B. Directory traversal
C. Unvalidated input
D. Security misconfiguration
Answer: (SHOW ANSWER)

NEW QUESTION: 43
What will the following command accomplish in Linux? fdisk /dev/hda
A. Delete all files under the /dev/hda folder
B. Partition the hard drive
C. Format the hard drive
D. Fill the disk with zeros
Answer: B (LEAVE A REPLY)

NEW QUESTION: 44
At what layer does a cross site scripting attack occur on?
A. Session
B. Presentation
C. Data Link
D. Application
Answer: D (LEAVE A REPLY)

NEW QUESTION: 45
Volatile information can be easily modified or lost when the system is shut down or rebooted. It helps to determine a logical timeline of the security incident and the users who would be responsible.
A. False
B. True
Answer: (SHOW ANSWER)

NEW QUESTION: 46

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 it is collected by other members of your team. 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 the report file because they are now primary evidence in the case.
B. All forms should be placed in an approved secure container because they are now primary evidence in the case.
C. The multi-evidence form should be placed in the report file and the single-evidence forms should be kept with each hard drive in an approved secure container.
D. 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.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 47
The investigator wants to examine changes made to the system's registry by the suspect program. Which of the following tool can help the investigator?
A. What's Running
B. RAM Capturer
C. Regshot
D. TRIPWIRE
Answer: C (LEAVE A REPLY)

NEW QUESTION: 48
What does the 56.58.152.114(445) denote in a Cisco router log?
Jun 19 23:25:46.125 EST: %SEC-4-IPACCESSLOGP: list internet-inbound denied udp 67.124.115.35(8084) -> 56.58.152.114(445), 1 packet
A. Login IP address
B. Source IP address
C. None of the above

D. Destination IP address
Answer: D (LEAVE A REPLY)

NEW QUESTION: 49
Which of the following files gives information about the client sync sessions in Google Drive on Windows?
A. Sync_log.log
B. sync, log Q Sync, log
C. sync_log.log
Answer: C (LEAVE A REPLY)

NEW QUESTION: 50
An investigator is analyzing a checkpoint firewall log and comes across symbols. What type of log is he looking at?

A. Connection rejected
B. Malicious URL detected
C. An email marked as potential spam
D. Security event was monitored but not stopped
Answer: C (LEAVE A REPLY)

NEW QUESTION: 51
How many sectors will a 125 KB file use in a FAT32 file system?
A. 32
B. 16
C. 250
D. 25
Answer: C (LEAVE A REPLY)
If you assume that we are using 512 bytes sectors, then 125x1024/512 = 250 sectors would be needed.
Actually, this is the same for a FAT16 file system as well.

NEW QUESTION: 52
Which of the following does Microsoft Exchange E-mail Server use for collaboration of various e-mail applications?
A. Simple Mail Transfer Protocol (SMTP)
B. Post Office Protocol version 3 (POP3)
C. Internet Message Access Protocol (IMAP)
D. Messaging Application Programming Interface (MAPI)

Answer: (SHOW ANSWER)

NEW QUESTION: 53

If the partition size is 4 GB, each cluster will be 32 K.

Even if a file needs only 10 K, the entire

32 K will be allocated, resulting in 22 K of ____

A. Slack space

B. Sector space

C. Cluster space

D. Deleted space

Answer: A (LEAVE A REPLY)

NEW QUESTION: 54

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

A. Somedomain.com

B. Smtp1.somedomain.com

C. Simon1.state.ok.gov.us

D. David1.state.ok.gov.us

Answer: C (LEAVE A REPLY)

NEW QUESTION: 55

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

A. Slack file

B. White space
C. ADS
D. AFS
Answer: C (LEAVE A REPLY)

NEW QUESTION: 56
What must be obtained before an investigation is carried out at a location?
A. Search warrant
B. Subpoena
C. Modus operandi
D. Habeas corpus
Answer: A (LEAVE A REPLY)

NEW QUESTION: 57
What must an attorney do first before you are called to testify as an expert?
A. Engage in damage control
B. Qualify you as an expert witness
C. Read your curriculum vitae to the jury
D. Prove that the tools you used to conduct your examination are perfect
Answer: B (LEAVE A REPLY)

NEW QUESTION: 58
Digital evidence is not fragile in nature.
A. True
B. False
Answer: B (LEAVE A REPLY)

NEW QUESTION: 59
Lance wants to place a honeypot on his network. Which of the following would be your recommendations?
A. Use it on a system in an external DMZ in front of the firewall
B. Use a system that has a dynamic addressing on the network
C. Use a system that is not directly interacting with the router
D. It doesn't matter as all replies are faked
Answer: D (LEAVE A REPLY)

NEW QUESTION: 60
When collecting evidence from the RAM, where do you look for data?
A. Swap file
B. SAM file
C. Log file

D. Data file
Answer: A (LEAVE A REPLY)

NEW QUESTION: 61
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 retrievecompany? 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 of free speech
B. Right to work
C. Right of privacy
D. Right to Internet access
Answer: C (LEAVE A REPLY)

NEW QUESTION: 62
What is the location of the binary files required for the functioning of the OS in a Linux system?
A. /run
B. /root
C. /sbin
D. /bin
Answer: D (LEAVE A REPLY)

NEW QUESTION: 63
Graphics Interchange Format (GIF) is a ____ RGB bitmap image format for images with up to 256 distinct colors per frame.
A. 8-bit
B. 24-bit
C. 16-bit
D. 32-bit
Answer: A (LEAVE A REPLY)

NEW QUESTION: 64
Which of the following file system is used by Mac OS X?
A. HFS+
B. EFS
C. NFS
D. EXT2
Answer: A (LEAVE A REPLY)

NEW QUESTION: 65
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.

What can the investigator infer from the screenshot seen below?
A. Buffer overflow attempt on the firewall.
B. Network intrusion has occurred
C. A smurf attack has been attempted
D. A denial of service has been attempted
Answer: (SHOW ANSWER)

NEW QUESTION: 66
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 lots of allocation units per block or cluster
B. one who has NTFS 4 or 5 partitions
C. one who uses hard disk writes on IRQ 13 and 21
D. one who uses dynamic swap file capability
Answer: A (LEAVE A REPLY)

NEW QUESTION: 67
You are carrying out the last round of testing for your new website before it goes live. The website has many dynamic pages and connects to a SQL backend that accesses your product inventory in a database. You come across a web security site that recommends inputting the following code

into a search field on web pages to check for vulnerabilities: When you type this and click on search, you receive a pop-up window that says:
"This is a test."
What is the result of this test?
A. Your website is vulnerable to CSS
B. Your website is vulnerable to web bugs
C. Your website is not vulnerable
D. Your website is vulnerable to SQL injection
Answer: A (LEAVE A REPLY)

NEW QUESTION: 68
You are a security analyst performing a penetration tests for a company in the Midwest.
After some initial reconnaissance, you discover the IP addresses of some Cisco routers used by the company. You type in the following URL that includes the IP address of one of the routers:
http://172.168.4.131/level/99/exec/show/config
After typing in this URL, you are presented with the entire configuration file for that router.
What have you discovered?
A. HTTP Configuration Arbitrary Administrative Access Vulnerability
B. Cisco IOS Arbitrary Administrative Access Online Vulnerability
C. HTML Configuration Arbitrary Administrative Access Vulnerability
D. URL Obfuscation Arbitrary Administrative Access Vulnerability
Answer: A (LEAVE A REPLY)

NEW QUESTION: 69
Where does Encase search to recover NTFS files and folders?
A. MFT
B. HAL
C. MBR
D. Slack space
Answer: A (LEAVE A REPLY)

NEW QUESTION: 70
An employee is suspected of stealing proprietary information belonging to your company that he had no rights to possess. The information was stored on the employee computer that was protected with the NTFS Encrypted File System (EFS) and you had observed him copy the files to astored on the employee? computer that was protected with the NTFS
Encrypted File System (EFS) and you had observed him copy the files to a floppy disk just before leaving work for the weekend. You detain the employee before he leaves the building and recover the floppy disk and secure his computer. Will you be able to break the encryption so that you can verify that the employee was in possession of the proprietary information?

A. EFS uses a 128-bit key that cannot be cracked, so you will not be able to recover the information
B. When the encrypted file was copied to the floppy disk, the EFS private key was also copied to the floppy disk, so you can recover the information
C. The EFS Revoked Key Agent can be used on the computer to recover the information
D. When the encrypted file was copied to the floppy disk, it was automatically unencrypted, so you can recover the information
Answer: D (LEAVE A REPLY)

NEW QUESTION: 71
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 config
B. Net share
C. Net file
D. Net sessions
Answer: D (LEAVE A REPLY)

NEW QUESTION: 72
In Linux, what is the smallest possible shellcode?
A. 8 bytes
B. 24 bytes
C. 800 bytes
D. 80 bytes
Answer: B (LEAVE A REPLY)

NEW QUESTION: 73
In a virtual test environment, Michael is testing the strength and security of BGP using multiple routers to mimic the backbone of the Internet. This project will help him write his doctoral thesis on "bringing down the Internet". Without sniffing the traffic between the routers, Michael sends millions of RESET packets to the routers in an attempt to shut one or all of them down. After a few hours, one of the routers finally shuts itself down. What will the other routers communicate between themselves?
A. RESTART packets to the affected router to get it to power back up
B. STOP packets to all other routers warning of where the attack originated
C. More RESET packets to the affected router to get it to power back up
D. The change in the routing fabric to bypass the affected router
Answer: (SHOW ANSWER)

NEW QUESTION: 74

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

A. TAC and Industry Identifier
B. Individual Account Identification Number and Country Code
C. Industry Identifier and Country code
D. Issuer Identifier Number and TAC
Answer: C (LEAVE A REPLY)

NEW QUESTION: 75
Which of the following statements is incorrect when preserving digital evidence?
A. Remove the power cable depending on the power state of the computer i.e., in on. off, or in sleep mode
B. Document the actions and changes that you observe in the monitor, computer, printer, or in other peripherals
C. Turn on the computer and extract Windows event viewer log files
D. Verily if the monitor is in on, off, or in sleep mode
Answer: (SHOW ANSWER)

NEW QUESTION: 76
While presenting his case to the court, Simon calls many witnesses to the stand to testify. Simon decides to call Hillary Taft, a lay witness, to the stand. Since Hillary is a lay witness, what field would she be considered an expert in?
A. No particular field
B. Legal issues
C. Technical material related to forensics
D. Judging the character of defendants/victims
Answer: A (LEAVE A REPLY)

NEW QUESTION: 77
What value of the "Boot Record Signature" is used to indicate that the boot-loader exists?
A. AA55
B. A100
C. AA00
D. 00AA
Answer: A (LEAVE A REPLY)

NEW QUESTION: 78
With Regard to using an Antivirus scanner during a computer forensics investigation, You should:
A. Never run a scan on your forensics workstation because it could change your systems configuration
B. Scan your Forensics workstation before beginning an investigation
C. Scan the suspect hard drive before beginning an investigation
D. Scan your forensics workstation at intervals of no more than once every five minutes during an investigation
Answer: (SHOW ANSWER)

NEW QUESTION: 79
How many sectors will a 125 KB file use in a FAT32 file system?
A. 25
B. 16
C. 256
D. 32
Answer: C (LEAVE A REPLY)

NEW QUESTION: 80
Bob has encountered a system crash and has lost vital data stored on the hard drive of his Windows computer.
He has no cloud storage or backup hard drives. he wants to recover all those data, which includes his personal photos, music, documents, videos, official email, etc. Which of the following tools shall resolve Bob's purpose?
A. Colasoft's Capsa
B. Xplico
C. Cain & Abel
D. Recuva
Answer: B (LEAVE A REPLY)

NEW QUESTION: 81

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

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

A. Those connections are in closed/waiting mode

B. Those connections are in listening mode

C. Those connections are in timed out/waiting mode

D. Those connections are established

Answer: (SHOW ANSWER)

NEW QUESTION: 82

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. Write information to the subject hard driveWrite information to the subject? hard drive

B. Violate your contract

C. Cause network congestion

D. Make you an agent of law enforcement

Answer: D (LEAVE A REPLY)

NEW QUESTION: 83

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 simple DOS copy will not include deleted files, file slack and other information

B. 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

C. A disk imaging tool would check for CRC32s for internal self checking and validation and have MD5 checksum

D. Evidence file format will contain case data entered by the examiner and encrypted at the beginning of the evidence file

Answer: A (LEAVE A REPLY)

NEW QUESTION: 84

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

A. Globally unique ID

B. Individual ASCII string
C. Microsoft Virtual Machine Identifier
D. Personal Application Protocol
Answer: A (LEAVE A REPLY)

NEW QUESTION: 85
Which response organization tracks hoaxes as well as viruses?
A. CERT
B. CIAC
C. NIPC
D. FEDCIRC
Answer: B (LEAVE A REPLY)

NEW QUESTION: 86
Which type of attack is possible when attackers know some credible information about the victim's password, such as the password length, algorithms involved, or the strings and characters used in its creation?
A. Rule-Based Attack
B. Hybrid Password Guessing Attack
C. Brute-Forcing Attack
D. Dictionary Attack
Answer: A (LEAVE A REPLY)

NEW QUESTION: 87
Stephen is checking an image using Compare Files by The Wizard, and he sees the file signature is shown as FF D8 FF E1. What is the file type of the image?
A. png
B. gif
C. Jpeg
D. bmp
Answer: (SHOW ANSWER)

NEW QUESTION: 88
What information do you need to recover when searching a victim computer for a crime committed with specific e-mail message?What information do you need to recover when searching a victim? computer for a crime committed with specific e-mail message?
A. E-mail header
B. Firewall log
C. Internet service provider information
D. Username and password
Answer: A (LEAVE A REPLY)

NEW QUESTION: 89
Which of the following should a computer forensics lab used for investigations have?
A. open access
B. restricted access
C. an entry log
D. isolation
Answer: (SHOW ANSWER)

NEW QUESTION: 90
Why is it a good idea to perform a penetration test from the inside?
A. It is easier to hack from the inside
B. To attack a network from a hacker's perspective
C. It is never a good idea to perform a penetration test from the inside
D. Because 70% of attacks are from inside the organization
Answer: (SHOW ANSWER)

NEW QUESTION: 91
You are working in the security Department of law firm. One of the attorneys asks you about the topic of sending fake email because he has a client who has been charged with doing just that. His client alleges that he is innocent and that there is no way for a fake email to actually be sent. You inform the attorney that his client is mistaken and that fake email is possibility and that you can prove it. You return to your desk and craft a fake email to the attorney that appears to come from his boss. What port do you send the email to on the company SMTP server?
A. 25
B. 135
C. 10
D. 110
Answer: A (LEAVE A REPLY)

NEW QUESTION: 92

Subscriber Identity Module (SIM) is a removable component that contains essential information about the subscriber. Its main function entails authenticating the user of the cell phone to the network to gain access to subscribed services. SIM contains a 20-digit long
Integrated Circuit Card identification (ICCID) number, identify the issuer identifier Number from the ICCID below.

A. 001451548
B. 44
C. 89
D. 245252
Answer: (SHOW ANSWER)

NEW QUESTION: 93
What is the first step that needs to be carried out to crack the password?
A. If it matches, that password has been cracked and the password cracker displays the unencrypted version of the password
B. The list of dictionary words is hashed or encrypted
C. A word list is created using a dictionary generator program or dictionaries
D. The hashed wordlist is compared against the target hashed password, generally one word at a time
Answer: (SHOW ANSWER)

NEW QUESTION: 94
File deletion is a way of removing a file from a computer's file system. What happens when a file is deleted in windows7?
A. Corresponding clusters in FAT are marked as used
B. The computer looks at the clusters occupied by that file and does not avails space to store a new file
C. The last letter of a file name is replaced by a hex byte code E5h
D. The operating system marks the file's name in the MFT with a special character that indicates that the file has been deleted
Answer: D (LEAVE A REPLY)

NEW QUESTION: 95

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. Approach the websites for evidence
D. Check the Windows registry for connection data (You may or may not recover)
Answer: A (LEAVE A REPLY)

NEW QUESTION: 96
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 (LEAVE A REPLY)

NEW QUESTION: 97
In Windows 7 system files, which file reads the Boot.ini file and loads Ntoskrnl.exe.
Bootvid.dll. Hal.dll, and boot-start device drivers?
A. Gdi32.dll
B. Ntldr
C. Boot.in
D. Kernel32.dll
Answer: (SHOW ANSWER)

NEW QUESTION: 98
When investigating a Windows System, it is important to view the contents of the page or swap file because:
A. This is file that windows use to communicate directly with Registry
B. A Large volume of data can exist within the swap file of which the computer user has no knowledge
C. Windows stores all of the systems configuration information in this file
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: (SHOW ANSWER)

NEW QUESTION: 99
What method of computer forensics will allow you to trace all ever-established user accounts on a Windows 2000 server the course of its lifetime?

A. forensic duplication of hard drive
B. analysis of volatile data
C. comparison of MD5 checksums
D. review of SIDs in the Registry
Answer: D (LEAVE A REPLY)
Not MD5: MD5 checksums are used as integrity checks
User accounts are assigned a unique SID, and the SID are not reused.

NEW QUESTION: 100
Select the data that a virtual memory would store in a Windows-based system.
A. Running processes
B. Documents and other files
C. Information or metadata of the files
D. Application data
Answer: (SHOW ANSWER)

NEW QUESTION: 101
TCP/IP (Transmission Control Protocol/Internet Protocol) is a communication protocol used to connect different hosts in the Internet. It contains four layers, namely the network interface layer. Internet layer, transport layer, and application layer.
Which of the following protocols works under the transport layer of TCP/IP?
A. SNMP
B. FTP
C. UDP
D. HTTP
Answer: (SHOW ANSWER)

NEW QUESTION: 102
Smith, an employee of a reputed forensic investigation firm, has been hired by a private organization to investigate a laptop that is suspected to be involved in the hacking of the organization's DC server. Smith wants to find all the values typed into the Run box in the Start menu. Which of the following registry keys will Smith check to find the above information?
A. TypedURLs key
B. MountedDevices key
C. RunMRU key
D. UserAssist Key
Answer: C (LEAVE A REPLY)

NEW QUESTION: 103
Which one of the following is not a consideration in a forensic readiness planning checklist?
A. Define the business states that need digital evidence

B. Identify the potential evidence available
C. Decide the procedure for securely collecting the evidence that meets the requirement fn a forensically sound manner
D. Take permission from all employees of the organization
Answer: D (LEAVE A REPLY)

NEW QUESTION: 104
Which among the following search warrants allows the first responder to get the victim's computer information such as service records, billing records, and subscriber information from the service provider?
A. Electronic Storage Device Search Warrant
B. Citizen Informant Search Warrant
C. Service Provider Search Warrant
D. IT Bench Search Warrant
Answer: C (LEAVE A REPLY)

NEW QUESTION: 105
Which ISO Standard enables laboratories to demonstrate that they comply with quality assurance and provide valid results?
A. ISO/IEC 17025
B. ISO/IEC 16025
C. ISO/IEC 18025
D. ISO/IEC 19025
Answer: A (LEAVE A REPLY)

NEW QUESTION: 106
To which phase of the Computer Forensic Investigation Process does the Planning and Budgeting of a Forensics Lab belong?
A. Investigation Phase
B. Pre-investigation Phase
C. Reporting Phase
D. Post-investigation Phase
Answer: B (LEAVE A REPLY)

NEW QUESTION: 107
Annie is searching for certain deleted files on a system running Windows XP OS. Where will she find the files if they were not completely deleted from the system?
A. C:\$RECYCLER
B. C: \$Recycle.Bin
C. C: $Recycled.Bin
D. C:\RECYCLER
Answer: B (LEAVE A REPLY)

NEW QUESTION: 108
You are working for a large clothing manufacturer as a computer forensics investigator and are called in to investigate an unusual case of an employee possibly stealing clothing designs from the company and selling them under a different brand name for a different company. What you discover during the course of the investigation is that the clothing designs are actually original products of the employee and the company has no policy against an employee selling his own designs on his own time. The only thing that you can find that the employee is doing wrong is that his clothing design incorporates the same graphic symbol as that of the company with only the wording in the graphic being different.
What area of the law is the employee violating?
A. Trademark law
B. Copyright law
C. Printright law
D. Brandmark law
Answer: A (LEAVE A REPLY)

NEW QUESTION: 109
Data files from original evidence should be used for forensics analysis
A. True
B. False
Answer: (SHOW ANSWER)

NEW QUESTION: 110
Which federal computer crime law specifically refers to fraud and related activity in connection with access devices like routers?
A. 18 U.S.C. 1362
B. 18 U.S. 2511
C. 18 U.S.C. 2703
D. 18 U.S.C. 1029

Answer: D (LEAVE A REPLY)

NEW QUESTION: 111
Which of the following processes is part of the dynamic malware analysis?
A. Process Monitoring
B. Malware disassembly
C. File fingerprinting
D. Searching for the strings
Answer: (SHOW ANSWER)

NEW QUESTION: 112
Which of the following Android libraries are used to render 2D (SGL) or 3D (OpenGL/ES) graphics content to the screen?
A. Media framework
B. OpenGL/ES and SGL
C. WebKit
D. Surface Manager
Answer: B (LEAVE A REPLY)

NEW QUESTION: 113
Volatile Memory is one of the leading problems for forensics. Worms such as code Red are memory resident and do write themselves to the hard drive, if you turn the system off they disappear. In a lab environment, which of the following options would you suggest as the most appropriate to overcome the problem of capturing volatile memory?
A. Give the Operating System a minimal amount of memory, forcing it to use a swap file
B. Create a Separate partition of several hundred megabytes and place the swap file there
C. Use intrusion forensic techniques to study memory resident infections
D. Use VMware to be able to capture the data in memory and examine it
Answer: B (LEAVE A REPLY)

NEW QUESTION: 114
The offset in a hexadecimal code is:
A. The 0x at the beginning of the code
B. The 0x at the end of the code
C. The first byte after the colon
D. The last byte after the colon
Answer: (SHOW ANSWER)

NEW QUESTION: 115
When a router receives an update for its routing table, what is the metric value change to that path?

A. Decreased by 1
B. Decreased by 2
C. Increased by 2
D. Increased by 1
Answer: D (LEAVE A REPLY)

NEW QUESTION: 116
Hackers can gain access to Windows Registry and manipulate user passwords, DNS settings, access rights or others features that they may need in order to accomplish their objectives. One simple method for loading an application at startup is to add an entry (Key) to the following Registry Hive:
A. HKEY_LOCAL_MACHINE\hardware\windows\start
B. HKEY_LOCAL_MACHINE\Software\Microsoft\CurrentVersion\Run
C. HKEY_CURRENT_USER\Microsoft\Default
D. HKEY_LOCAL_USERS\Software\Microsoft\old\Version\Load
Answer: (SHOW ANSWER)

NEW QUESTION: 117
What type of analysis helps to identify the time and sequence of events in an investigation?
A. Time-based
B. Functional
C. Relational
D. Temporal
Answer: (SHOW ANSWER)

NEW QUESTION: 118
POP3 (Post Office Protocol 3) is a standard protocol for receiving an email that deletes mail on the server as soon as the user downloads it. When a message arrives, the POP3 server appends it to the bottom of the recipient's account file, which can be retrieved by the email client at any preferred time. Email client connects to the POP3 server at _____ by default to fetch emails.
A. Port 109
B. Port 123
C. Port 110
D. Port 115
Answer: (SHOW ANSWER)

NEW QUESTION: 119
Jacky encrypts her documents using a password. It is known that she uses her daughter's year of birth as part of the password. Which password cracking technique would be optimal to crack her password?

A. Rule-based attack
B. Syllable attack
C. Hybrid attack
D. Brute force attack
Answer: (SHOW ANSWER)

NEW QUESTION: 120
What will the following command accomplish?
dd if=/dev/xxx of=mbr.backup bs=512 count=1
A. Restore the first 512 bytes of the first partition of the hard drive
B. Mount the master boot record on the first partition of the hard drive
C. Back up the master boot record
D. Restore the master boot record
Answer: C (LEAVE A REPLY)

NEW QUESTION: 121
An Expert witness gives an opinion if:
A. To deter the witness form expanding the scope of his or her investigation beyond the requirements of the case
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. The Opinion, inferences or conclusions depend on special knowledge, skill or training not within the ordinary experience of lay jurors
Answer: (SHOW ANSWER)

NEW QUESTION: 122
What will the following command produce on a website login page?
SELECT email, passwd, login_id, full_name FROM members
WHERE email = 'someone@somehwere.com';
DROP TABLE members; --'
A. Retrieves the password for the first user in the members table
B. This command will not produce anything since the syntax is incorrect

C. Deletes the entire members table
D. Inserts the Error! Reference source not found. email address into the members table
Answer: C (LEAVE A REPLY)
The third line deletes the table named members.

NEW QUESTION: 123
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 tampered with evidence by using it
B. They attempted to implicate personnel without proof
C. They examined the actual evidence on an unrelated system
D. They called in the FBI without correlating with the fingerprint data
Answer: A (LEAVE A REPLY)

NEW QUESTION: 124
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. Change the default community string names
B. Block access to UDP port 171
C. Block all internal MAC address from using SNMP
D. Block access to TCP port 171
Answer: A (LEAVE A REPLY)

NEW QUESTION: 125
What is the investigator trying to analyze if the system gives the following image as output?

A. All the logon sessions

B. Currently active logon sessions

C. Inactive logon sessions

D. Details of users who can logon

Answer: (SHOW ANSWER)

NEW QUESTION: 126

Investigators can use the Type Allocation Code (TAC) to find the model and origin of a mobile device. Where is TAC located in mobile devices?
A. Integrated circuit card identifier (ICCID)
B. International Mobile Equipment Identifier (IMEI)
C. International mobile subscriber identity (IMSI)
D. Equipment Identity Register (EIR)
Answer: D (LEAVE A REPLY)

NEW QUESTION: 127
When you carve an image, recovering the image depends on which of the following skills?
A. Recovering the image from a tape backup
B. Recovering the image from the tape backup
C. Recognizing the pattern of the header content
D. Recognizing the pattern of a corrupt file
Answer: C (LEAVE A REPLY)

NEW QUESTION: 128
Which of the following files gives information about the client sync sessions in Google Drive on Windows?
A. Sync.log
B. sync_log.log
C. Sync_log.log
D. sync.log
Answer: C (LEAVE A REPLY)

NEW QUESTION: 129
Which of the following should a computer forensics lab used for investigations have?
A. isolation
B. open access
C. an entry log
D. restricted access
Answer: (SHOW ANSWER)

NEW QUESTION: 130
Jacob is a computer forensics investigator with over 10 years experience in investigations and has written over 50 articles on computer forensics. He has been called upon as a qualified witness to testify the accuracy and integrity of the technical log files gathered in an investigation into computer fraud. What is the term used for Jacob testimony in this case?
A. Justification
B. Authentication
C. Certification

D. Reiteration
Answer: (SHOW ANSWER)

NEW QUESTION: 131
Which of the following acts as a network intrusion detection system as well as network intrusion prevention system?
A. Snort
B. Nikto
C. Accunetix
D. Kismet
Answer: A (LEAVE A REPLY)

NEW QUESTION: 132
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. D:\Exchsrvr\Message Tracking\servername.log
B. C:\Program Files\Microsoft Exchange\srvr\servername.log
C. C:\Program Files\Exchsrvr\servername.log
D. C:\Exchsrvr\Message Tracking\servername.log
Answer: (SHOW ANSWER)

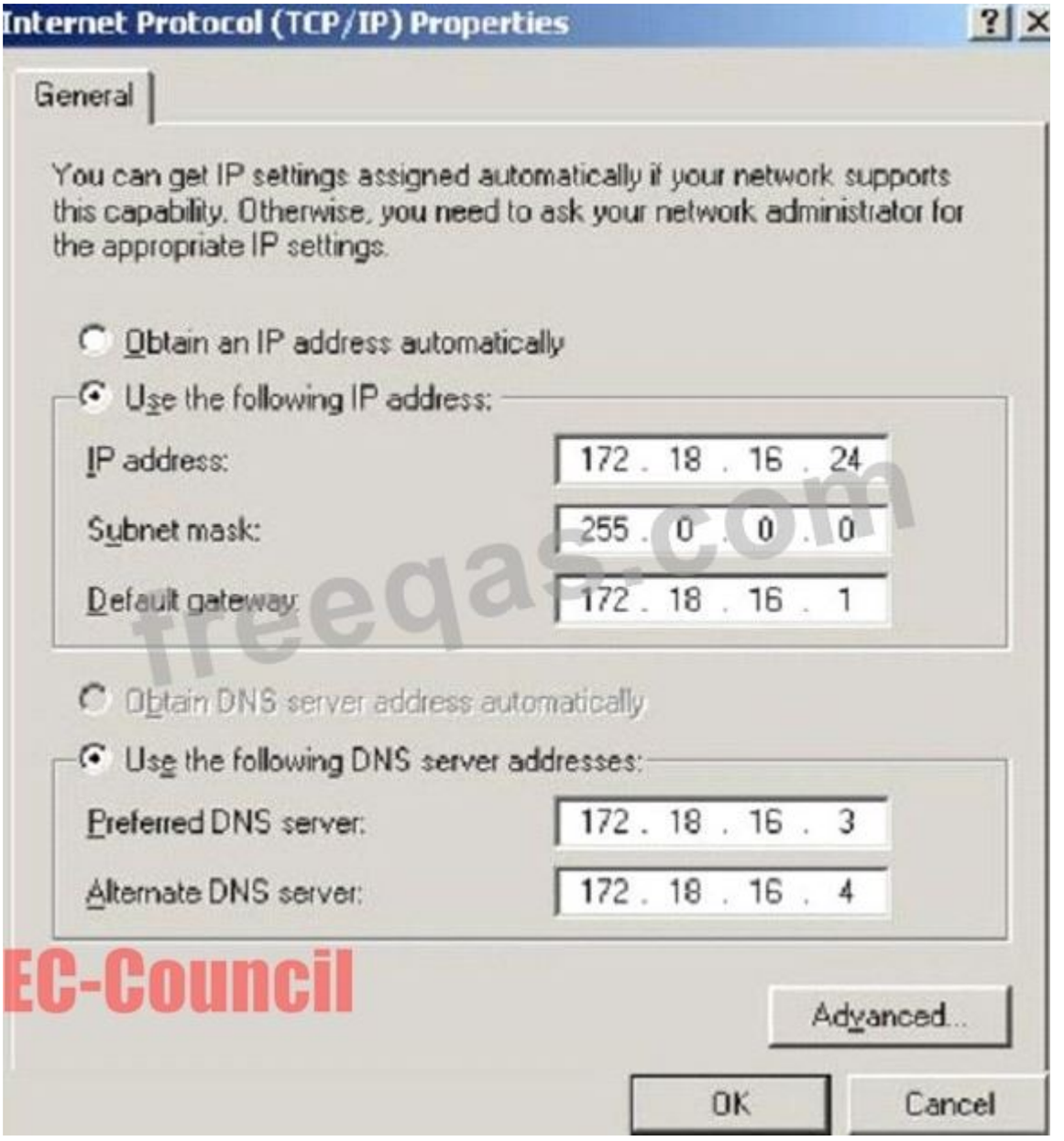
NEW QUESTION: 133
The ARP table of a router comes in handy for Investigating network attacks, as the table contains IP addresses associated with the respective MAC addresses.
The ARP table can be accessed using the _____command in Windows 7.
A. C:\arp -d
B. C:\arp -a
C. C:\arp -b
D. C:\arp -s
Answer: B (LEAVE A REPLY)

NEW QUESTION: 134
An investigator has extracted the device descriptor for a 1GB thumb drive that looks like: Disk&Ven_Best_Buy&Prod_Geek_Squad_U3&Rev_6.15. What does the "Geek_Squad" part represent?
A. Developer description
B. Product description
C. Software or OS used
D. Manufacturer Details

Answer: (SHOW ANSWER)

NEW QUESTION: 135
What stage of the incident handling process involves reporting events?
A. Follow-up
B. Identification
C. Containment
D. Recovery
Answer: B (LEAVE A REPLY)

NEW QUESTION: 136
What is the CIDR from the following screenshot?



A. /8D./8D./8
B. /16 C./16 C./16
C. /32 B./32 B./32

D. /24A./24A./24
Answer: A (LEAVE A REPLY)

NEW QUESTION: 137
What type of equipment would a forensics investigator store in a StrongHold bag?
A. Hard drives
B. PDAPDA?
C. Wireless cards
D. Backup tapes
Answer: (SHOW ANSWER)

NEW QUESTION: 138
Bob works as an Information Security Analyst for a big finance company. One day, the anomaly-based intrusion detection system alerted that a volumetric DDOS targeting the main IP of the main web server was occurring. What kind of attack is it?
A. Advanced Persistent Threat (APT)
B. IDS Attack
C. Network Attack
D. Web Application Attack
Answer: C (LEAVE A REPLY)

NEW QUESTION: 139
Lynne receives the following email:
Dear lynne@gmail.com!
We are sorry to inform you that your ID has been temporarily frozen due to incorrect or missing information saved at 2016/11 /1 O 20:40:24 You have 24 hours to fix this problem or risk to be closed permanently!
To proceed Please Connect>> My Apple ID
Thank You
The
link to My Apple ID shows http://byggarbetsplatsen.se/backup/signon/
What type of attack is this?

A. Email Spoofing
B. Email Spamming
C. Mail Bombing
D. Phishing
Answer: D (LEAVE A REPLY)

NEW QUESTION: 140
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. Because 70% of attacks are from inside the organization
C. It is easier to hack from the inside
D. To attack a network from a hacker's perspective
Answer: B (LEAVE A REPLY)

NEW QUESTION: 141
Which of the following file system uses Master File Table (MFT) database to store information about every file and directory on a volume?
A. FAT File System
B. NTFS File System
C. ReFS
D. exFAT
Answer: B (LEAVE A REPLY)

NEW QUESTION: 142
What does the 56.58.152.114(445) denote in a Cisco router log?
Jun 19 23:25:46.125 EST: %SEC-4-IPACCESSLOGP: list internet-inbound denied udp 67.124.115.35(8084)
-> 56.58.152.114(445), 1 packet
A. None of the above
B. Destination IP address
C. Login IP address
D. Source IP address
Answer: (SHOW ANSWER)

NEW QUESTION: 143
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 haveis 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 Federal Rules of Evidence

C. The Good Samaritan Laws

D. The Fourth Amendment

Answer: D (LEAVE A REPLY)

NEW QUESTION: 144

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. Audit logs

D. Security software logs

Answer: D (LEAVE A REPLY)

NEW QUESTION: 145

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. Change the default community string names

B. Block all internal MAC address from using SNMP

C. Block access to TCP port 171

D. Block access to UDP port 171

Answer: (SHOW ANSWER)

NEW QUESTION: 146

What is the purpose of using Obfuscator in malware?

A. Propagate malware to other connected devices

B. Execute malicious code in the system

C. Avoid encryption while passing through a VPN

D. Avoid detection by security mechanisms

Answer: (SHOW ANSWER)

NEW QUESTION: 147

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

A. The RGBQUAD array

B. Information header

C. Image data

D. Header

Answer: A (LEAVE A REPLY)

NEW QUESTION: 148

Which of the following files stores information about local Dropbox installation and account, email IDs linked with the account, current version/build for the local application, the host_id, and local path information?

A. filecache.db

B. sigstore.db

C. host.db

D. config.db

Answer: (SHOW ANSWER)

NEW QUESTION: 149

After suspecting a change in MS-Exchange Server storage archive, the investigator has analyzed it. Which of the following components is not an actual part of the archive?

A. PUB.STM

B. PUB.EDB

C. PRIV.STM

D. PRIV.EDB

Answer: C (LEAVE A REPLY)

NEW QUESTION: 150

Volatile Memory is one of the leading problems for forensics.

Worms such as code Red are memory resident and do not write themselves to the hard drive, if you turn the system off they disappear.

In a lab environment, which of the following options would you suggest as the most appropriate to overcome the problem of capturing volatile memory?

A. Use intrusion forensic techniques to study memory resident infections

B. Use Vmware to be able to capture the data in memory and examine it

C. Create a Separate partition of several hundred megabytes and place the swap file there

D. Give the Operating System a minimal amount of memory, forcing it to use a swap file

Answer: B,C (LEAVE A REPLY)

NEW QUESTION: 151
When investigating a computer forensics case where Microsoft Exchange and Blackberry Enterprise server are used, where would investigator need to search to find email sent from a Blackberry device?
A. Blackberry desktop redirector
B. Blackberry Enterprise server
C. Microsoft Exchange server
D. RIM Messaging center
Answer: C (LEAVE A REPLY)

NEW QUESTION: 152
Preparing an image drive to copy files to is the first step in Linux forensics. For this purpose, what would the following command accomplish?
dcfldd if=/dev/zero of=/dev/hda bs=4096 conv=noerror, sync
A. Copy files from the master disk to the slave disk on the secondary IDE controller
B. Low-level format
C. Fill the disk with 4096 zeros
D. Fill the disk with zeros
Answer: (SHOW ANSWER)

NEW QUESTION: 153
Which network attack is described by the following statement?
"At least five Russian major banks came under a continuous hacker attack, although online client services were not disrupted. The attack came from a wide-scale botnet involving at least 24,000 computers, located in
30 countries."
A. DDoS
B. Man-in-the-Middle Attack
C. Sniffer Attack
D. Buffer Overflow
Answer: A (LEAVE A REPLY)

NEW QUESTION: 154
Which of the following tools is not a data acquisition hardware tool?
A. Triage-Responder
B. F-Response Imager
C. Atola Insight Forensic
D. UltraKit
Answer: (SHOW ANSWER)

NEW QUESTION: 155
A picture file is recovered from a computer under investigation. During the investigation process, the file is enlarged 500% to get a better view of its contents. The picture quality is not degraded at all from this process.
What kind of picture is this file. What kind of picture is this file?
A. Raster image
B. Metafile image
C. Catalog image
D. Vector image
Answer: (SHOW ANSWER)

NEW QUESTION: 156
You are a security analyst performing reconnaissance on a company you will be carrying out a penetration test for. You conduct a search for IT jobs on Dice.com and find the following information for an open position: 7+ years experience in Windows Server environment 5+ years experience in Exchange 2000/2003 environment Experience with Cisco Pix Firewall, Linksys 1376 router, Oracle 11i and MYOB v3.4 Accounting software are required MCSA desired, MCSE, CEH preferred No Unix/Linux Experience needed What is this information posted on the job website considered?
A. Social engineering exploit
B. Trade secret
C. Competitive exploit
D. Information vulnerability
Answer: D (LEAVE A REPLY)

NEW QUESTION: 157
Jacob is a computer forensics investigator with over 10 years experience in investigations and has written over
50 articles on computer forensics. He has been called upon as a qualified witness to testify the accuracy and integrity of the technical log files gathered in an investigation into computer fraud. What is the term used for Jacob testimony in this case?
A. Justification

B. Certification
C. Reiteration
D. Authentication
Answer: D (LEAVE A REPLY)

NEW QUESTION: 158
What layer of the OSI model do TCP and UDP utilize?
A. Session
B. Data Link
C. Transport
D. Network
Answer: C (LEAVE A REPLY)

NEW QUESTION: 159
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. In the DHCP Server log files
B. In the Web Server log files
C. On the individual computer ARP cacheOn the individual computer? ARP cache
D. There is no way to determine the specific IP address
Answer: A (LEAVE A REPLY)

NEW QUESTION: 160
Which principle states that "anyone or anything, entering a crime scene takes something of the scene with them, and leaves something of themselves behind when they leave"?
A. Evidence Theory of Investigation
B. Enterprise Theory of Investigation
C. Locard's Exchange Principle
D. Locard's Evidence Principle
Answer: C (LEAVE A REPLY)

NEW QUESTION: 161
Which of the following information is displayed when Netstat is used with -ano switch?
A. Ethernet statistics
B. Details of TCP and UDP connections
C. Details of routing table
D. Contents of IP routing table
Answer: B (LEAVE A REPLY)

NEW QUESTION: 162

During the course of a corporate investigation, you find that an employee is committing a federal crime. Can the employer file a criminal complain with the police?
A. No, because the investigation was conducted without a warrant
B. Yes, and all evidence can be turned over to the police
C. No, because the investigation was conducted without following standard police procedures
D. Yes, but only if you turn the evidence over to a district judge
Answer: B (LEAVE A REPLY)

NEW QUESTION: 163
Which wireless standard has bandwidth up to 54 Mbps and signals in a regulated frequency spectrum around 5 GHz?
A. 802.11b
B. 802.11g
C. 802.11a
D. 802.11i
Answer: (SHOW ANSWER)

NEW QUESTION: 164
Damaged portions of a disk on which no read/Write operation can be performed is known as _____.
A. Unused sector
B. Empty sector
C. Bad sector
D. Lost sector
Answer: C (LEAVE A REPLY)

NEW QUESTION: 165
Jones had been trying to penetrate a remote production system for the past two weeks.
This time however, he is able to get into the system. He was able to use the system for a period of three weeks. However law enforcement agencies were recording his every activity and this was later presented as evidence. The organization had used a virtual environment to trap Jones. What is a virtual environment?
A. An environment set up before an user logs in
B. A system using Trojaned commands
C. An environment set up after the user logs in
D. A honeypot that traps hackers
Answer: D (LEAVE A REPLY)

NEW QUESTION: 166

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. Lawyers
B. Forensic laboratory staff
C. Local managers or other non-forensic staff
D. System administrators
Answer: B (LEAVE A REPLY)

NEW QUESTION: 167
The offset in a hexadecimal code is:
A. The first byte after the colon
B. The 0x at the beginning of the code
C. The last byte after the colon
D. The 0x at the end of the code
Answer: B (LEAVE A REPLY)

NEW QUESTION: 168
What does the 63.78.199.4(161) denotes in a Cisco router log?
Mar 14 22:57:53.425 EST: %SEC-6-IPACCESSLOGP: list internet-inbound denied udp 66.56.16.77(1029) -> 63.78.199.4(161), 1 packet
A. Source IP address
B. Login IP address
C. None of the above
D. Destination IP address
Answer: D (LEAVE A REPLY)

NEW QUESTION: 169
Self-Monitoring, Analysis, and Reporting Technology (SMART) is built into the hard drives to monitor and report system activity. Which of the following is included in the report generated by SMART?
A. All the states (running and discontinued) associated with the OS

B. List of running processes
C. Power Off time
D. Logs of high temperatures the drive has reached
Answer: D (LEAVE A REPLY)

NEW QUESTION: 170
In Steganalysis, which of the following describes a Known-stego attack?
A. During the communication process, active attackers can change cover
B. Only the steganography medium is available for analysis
C. The hidden message and the corresponding stego-image are known
D. Original and stego-object are available and the steganography algorithm is known
Answer: (SHOW ANSWER)

NEW QUESTION: 171
The process of restarting a computer that is already turned on through the operating system is called?
A. Ice boot
B. Warm boot
C. Cold boot
D. Hot Boot
Answer: B (LEAVE A REPLY)

NEW QUESTION: 172
Which component in the hard disk moves over the platter to read and write information?
A. Spindle
B. Actuator Axis
C. Actuator
D. Head
Answer: D (LEAVE A REPLY)

NEW QUESTION: 173
Which of the following statements is not a part of securing and evaluating electronic crime scene checklist?
A. Transmit additional flash messages to other responding units
B. Request additional help at the scene if needed
C. Blog about the incident on the internet
D. Locate and help the victim
Answer: (SHOW ANSWER)

NEW QUESTION: 174
What happens when a file is deleted by a Microsoft operating system using the FAT file system?

A. The file is erased but can be recovered partially
B. Only the reference to the file is removed from the FAT and can be recovered
C. A copy of the file is stored and the original file is erased
D. The file is erased and cannot be recovered
Answer: B (LEAVE A REPLY)

NEW QUESTION: 175
The pagefile.sys is a virtual memory file used to expand the physical memory of a computer. Select the registry path for the page file:
A. HKLM\SYSTEM\CurrentControlSet\Control\SessionManager\MemoryManagement
B. HKLM\SYSTEM\CurrentControlSet\Control\SessionManager\MemoryManagement \PrefetchParameter
C. HKLM\SYSTEM\CurrentControlSet\Control\SessionManager\SystemManagemen
D. HKLM\SYSTEM\CurrentControlSet\Control\SessionManager\DeviceManagement
Answer: D (LEAVE A REPLY)

NEW QUESTION: 176
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: (SHOW ANSWER)
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: 177
Gary is checking for the devices connected to USB ports of a suspect system during an investigation. Select the appropriate tool that will help him document all the connected devices.
A. Reg.exe
B. Devcon
C. DevScan
D. fsutil
Answer: B (LEAVE A REPLY)

NEW QUESTION: 178
When conducting computer forensic analysis, you must guard against

_____ So that you remain focused on the primary job and insure that the level of work does not increase beyond what was originally expected.

A. Hard Drive Failure

B. Unauthorized expenses

C. Scope Creep

D. Overzealous marketing

Answer: C (LEAVE A REPLY)

NEW QUESTION: 179

Which Is a Linux journaling file system?

A. HFS

B. BFS

C. FAT

D. Ext3

Answer: D (LEAVE A REPLY)

NEW QUESTION: 180

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 Lophtcrack 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. Hillary network username and password hash

C. The SAM file from Hillary computer

D. The network shares that Hillary has permissions

Answer: B (LEAVE A REPLY)

NEW QUESTION: 181

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

A. the sector map

B. the file header

C. the File Allocation Table

D. the file footer

Answer: B (LEAVE A REPLY)

NEW QUESTION: 182
Kimberly is studying to be an IT security analyst at a vocational school in her town. The school offers many different programming as well as networking languages. What networking protocol language should she learn that routers utilize?
A. UDP
B. ATM
C. BPG
D. OSPF
Answer: (SHOW ANSWER)

NEW QUESTION: 183
How many characters long is the fixed-length MD5 algorithm checksum of a critical system file?
A. 16
B. 128
C. 32
D. 64
Answer: C (LEAVE A REPLY)

NEW QUESTION: 184
How do you define Technical Steganography?
A. Steganography that utilizes visual symbols or signs to hide secret messages
B. Steganography that utilizes written natural language to hide the message in the carrier in some non-obvious ways
C. Steganography that utilizes written JAVA language to hide the message in the carrier in some non-obvious ways
D. Steganography that uses physical or chemical means to hide the existence of a message
Answer: D (LEAVE A REPLY)

NEW QUESTION: 185
Which of the following is a device monitoring tool?
A. RAM Capturer
B. Regshot
C. Driver Detective

D. Capsa
Answer: D (LEAVE A REPLY)

NEW QUESTION: 186
If you see the files Zer0.tar.gz and copy.tar.gz on a Linux system while doing an investigation, what can you conclude?
A. Nothing in particular as these can be operational files
B. The system files have been copied by a remote attacker
C. The system has been compromised using a t0rnrootkit
D. The system administrator has created an incremental backup
Answer: (SHOW ANSWER)

NEW QUESTION: 187
A packet is sent to a router that does not have the packet destination address in its route table, how will the packet get to its properA packet is sent to a router that does not have the packet? destination address in its route table, how will the packet get to its proper destination?
A. Root Internet servers
B. Border Gateway Protocol
C. Gateway of last resort
D. Reverse DNS
Answer: (SHOW ANSWER)

NEW QUESTION: 188
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: (SHOW ANSWER)

NEW QUESTION: 189
You are asked to build a forensic lab and your manager has specifically informed you to use copper for lining the walls, ceilings, and floor. What is the main purpose of lining the walls, ceilings, and floor with copper?
A. To avoid electromagnetic emanations
B. To control the room temperature
C. To strengthen the walls, ceilings, and floor
D. To make the lab sound proof
Answer: (SHOW ANSWER)

NEW QUESTION: 190

You are a security analyst performing a penetration tests for a company in the Midwest. After some initial reconnaissance, you discover the IP addresses of some Cisco routers used by the company. You type in the following URL that includes the IP address of one of the routers:
http://172.168.4.131/level/99/exec/show/config
After typing in this URL, you are presented with the entire configuration file for that router. What have you discovered?
A. HTML Configuration Arbitrary Administrative Access Vulnerability
B. Cisco IOS Arbitrary Administrative Access Online Vulnerability
C. URL Obfuscation Arbitrary Administrative Access Vulnerability
D. HTTP Configuration Arbitrary Administrative Access Vulnerability
Answer: D (LEAVE A REPLY)

NEW QUESTION: 191
While looking through the IIS log file of a web server, you find the following entries:

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

What is evident from this log file?
A. Cross site scripting
B. SQL injection is possible
C. Web bugs
D. Hidden fields
Answer: B (LEAVE A REPLY)

NEW QUESTION: 192
An employee is attempting to wipe out data stored on a couple of compact discs (CDs) and digital video discs (DVDs) by using a large magnet. You inform him that this method will not be effective in wiping out the data because CDs and DVDs are _____ media used to store large amounts of data and are not affected by the magnet.
A. optical
B. anti-magnetic
C. logical
D. magnetic
Answer: A (LEAVE A REPLY)

NEW QUESTION: 193
What is static executable file analysis?
A. It is a process that consists of collecting information about and from an executable file without actually launching an executable file in a controlled and monitored environment
B. It is a process that consists of collecting information about and from an executable file by launching the file under any circumstances

C. It is a process that consists of collecting information about and from an executable file by launching an executable file in a controlled and monitored environment
D. It is a process that consists of collecting information about and from an executable file without actually launching the file under any circumstances
Answer: D (LEAVE A REPLY)

NEW QUESTION: 194
Ron, a computer forensics expert, is investigating a case involving corporate espionage. He has recovered several mobile computing devices from the crime scene. One of the evidence that Ron possesses is a mobile phone from Nokia that was left in ON condition. Ron needs to recover the IMEI number of the device to establish the identity of the device owner. Which of the following key combinations can he use to recover the IMEI number?
A. #*06*#
B. #06#*
C. *#06#
D. *IMEI#
Answer: A (LEAVE A REPLY)

NEW QUESTION: 195
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. The Quotation mark (? is a valid username
B. SQL injection is not possible
C. SQL injection is possible
D. The user for line 3306 in the SQL database has a weak password
Answer: (SHOW ANSWER)

NEW QUESTION: 196
Which of the following would you consider an aspect of organizational security, especially focusing on IT security?
A. Application security
B. Information copyright security
C. Biometric information security
D. Security from frauds
Answer: (SHOW ANSWER)

NEW QUESTION: 197
Centralized binary logging is a process in which many websites write binary and unformatted log data to a single log file. What extension should the investigator look to find its log file?
A. .ibl
B. .txt
C. .cbl
D. .log
Answer: A (LEAVE A REPLY)

NEW QUESTION: 198
Shane has started the static analysis of a malware and is using the tool ResourcesExtract to find more details of the malicious program. What part of the analysis is he performing?
A. File obfuscation
B. Identifying File Dependencies
C. Dynamic analysis
D. Strings search
Answer: D (LEAVE A REPLY)

NEW QUESTION: 199
MAC filtering is a security access control methodology, where a _____ is assigned to each network card to determine access to the network
A. 24-bit address
B. 16-bit address
C. 32-bit address
D. 48-bit address
Answer: D (LEAVE A REPLY)

NEW QUESTION: 200
John is working as a computer forensics investigator for a consulting firm in Canada. He is called to seize a computer at a local web caf purportedly used as a botnet server. John thoroughly scans the computer and finds nothing that would lead him to think the computer was a botnet server. John decides to scan the virtual memory of the computer to possibly find something he had missed. What information will the virtual memory scan produce?
A. It is not necessary to scan the virtual memory of a computer
B. Hidden running processes
C. It contains the times and dates of when the system was last patched

D. It contains the times and dates of all the system files
Answer: B (LEAVE A REPLY)

NEW QUESTION: 201
Windows identifies which application to open a file with by examining which of the following?
A. The File extension
B. The file Signature at the end of the file
C. The file attributes
D. The file signature at the beginning of the file
Answer: A (LEAVE A REPLY)

NEW QUESTION: 202
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 running memory to a file
C. Copy the contents of the system folder em?to a fileCopy the contents of the system folder ? em?to a file
D. Copy the memory dump file to an image file
Answer: (SHOW ANSWER)

NEW QUESTION: 203
You have used a newly released forensic investigation tool, which doesn't meet the Daubert Test, during a case. The case has ended-up in court. What argument could the defense make to weaken your case?
A. You are not certified for using the tool
B. Only the local law enforcement should use the tool
C. The total has not been reviewed and accepted by your peers
D. The tool hasn't been tested by the International Standards Organization (ISO)
Answer: (SHOW ANSWER)

NEW QUESTION: 204
Which of the following tool creates a bit-by-bit image of an evidence media?
A. AccessData FTK Imager
B. Xplico
C. Recuva
D. FileMerlin
Answer: A (LEAVE A REPLY)

NEW QUESTION: 205

Which of the following tool enables a user to reset his/her lost admin password in a Windows system?
A. Smartkey Password Recovery Bundle Standard
B. Advanced Office Password Recovery
C. Passware Kit Forensic
D. Active@ Password Changer
Answer: D (LEAVE A REPLY)

NEW QUESTION: 206
In which of these attacks will a steganalyst use a random message to generate a stego-object by using some steganography tool, to find the steganography algorithm used to hide the information?
A. Chosen-message attack
B. Known-stego attack
C. Known-message attack
D. Known-cover attack
Answer: (SHOW ANSWER)

NEW QUESTION: 207
How often must a company keep log files for them to be admissible in a court of law?
A. Continuously
B. Monthly
C. Weekly
D. All log files are admissible in court no matter their frequency
Answer: A (LEAVE A REPLY)

NEW QUESTION: 208
NTFS sets a flag for the file once you encrypt it and creates an EFS attribute where it stores Data Decryption Field (DDF) and Data Recovery Field (DDR). Which of the following is not a part of DDF?
A. Checksum
B. EFS Certificate Hash
C. Container Name
D. Encrypted FEK
Answer: (SHOW ANSWER)

NEW QUESTION: 209
Lynne receives the following email:
Dear lynne@gmail.com! We are sorry to inform you that your ID has been temporarily frozen due to incorrect or missing information saved at 2016/11/10 20:40:24 You have 24 hours to fix this problem or risk to be closed permanently!

To proceed Please Connect >> My Apple ID
Thank
You The link to My Apple ID shows http://byggarbetsplatsen.se/backup/signon/ What type of attack is this?
A. Mail Bombing
B. Email Spoofing
C. Email Spamming
D. Phishing
Answer: D (LEAVE A REPLY)

NEW QUESTION: 210
Jack Smith is a forensics investigator who works for Mason Computer Investigation Services. He is investigating a computer that was infected by Ramen Virus.

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

A. Those connections are in timed out/waiting mode

B. Those connections are in closed/waiting mode
C. Those connections are in listening mode
D. Those connections are established
Answer: C (LEAVE A REPLY)

NEW QUESTION: 211
How many times can data be written to a DVD+R disk?
A. Zero
B. Infinite
C. Twice
D. Once
Answer: D (LEAVE A REPLY)

NEW QUESTION: 212
Which legal document allows law enforcement to search an office, place of business, or other locale for evidence relating to an alleged crime?
A. Subpoena
B. Wire tap
C. Search warrant
D. Bench warrant
Answer: C (LEAVE A REPLY)

NEW QUESTION: 213
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. HTTP redirect attack
B. ARP Poisoning

C. DNS Poisoning

D. IP Spoofing

Answer: C (LEAVE A REPLY)

NEW QUESTION: 214

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.

What can the investigator infer from the screenshot seen below?

A. Network intrusion has occurred

B. A denial of service has been attempted

C. A smurf attack has been attempted

D. Buffer overflow attempt on the firewall.

Answer: A (LEAVE A REPLY)

NEW QUESTION: 215

What is the First Step required in preparing a computer for forensics investigation?

A. Do not turn the computer off or on, run any programs, or attempt to access data on a computer

B. Suspend automated document destruction and recycling policies that may pertain to any relevant media or users at Issue

C. Secure any relevant media

D. Identify the type of data you are seeking, the Information you are looking for, and the urgency level of the examination

Answer: A (LEAVE A REPLY)

NEW QUESTION: 216
What will the following URL produce in an unpatched IIS Web Server?
http://www.thetargetsite.com/scripts/..%
co%af../..%co%af../windows/system32/cmd.exe?/c+dir+c:\
A. Execute a buffer flow in the C: drive of the web server
B. Insert a Trojan horse into the C: drive of the web server
C. Directory listing of the C:\windows\system32 folder on the web server
D. Directory listing of C: drive on the web server
Answer: D (LEAVE A REPLY)

NEW QUESTION: 217
Chong-lee, a forensics executive, suspects that a malware is continuously making copies of files and folders on a victim system to consume the available disk space. What type of test would confirm his claim?
A. File fingerprinting
B. Dynamic analysis
C. Identifying file obfuscation
D. Static analysis
Answer: A (LEAVE A REPLY)

NEW QUESTION: 218
When is it appropriate to use computer forensics?
A. If employees do not care for their boss?management techniques
B. If copyright and intellectual property theft/misuse has occurred
C. If a financial institution is burglarized by robbers
D. If sales drop off for no apparent reason for an extended period of time
Answer: B (LEAVE A REPLY)

NEW QUESTION: 219
Why should you note all cable connections for a computer you want to seize as evidence?
A. to know what outside connections existed
B. to know what hardware existed
C. in case other devices were connected
D. to know what peripheral devices exist
Answer: A (LEAVE A REPLY)

NEW QUESTION: 220
In Microsoft file structures, sectors are grouped together to form:
A. Partitions
B. Bitstreams
C. Clusters

D. Drives
Answer: C (LEAVE A REPLY)

NEW QUESTION: 221
Which tool allows dumping the contents of process memory without stopping the process?
A. psdump.exe
B. pdump.exe
C. processdump.exe
D. pmdump.exe
Answer: D (LEAVE A REPLY)

NEW QUESTION: 222
What must be obtained before an investigation is carried out at a location?
A. Modus operandi
B. Search warrant
C. Habeas corpus
D. Subpoena
Answer: (SHOW ANSWER)

NEW QUESTION: 223
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. 4
C. 2
D. 1
Answer: B (LEAVE A REPLY)

NEW QUESTION: 224
What is a first sector ("sector zero") of a hard disk?
A. Hard disk boot record
B. Master boot record
C. System boot record
D. Secondary boot record
Answer: (SHOW ANSWER)

NEW QUESTION: 225
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. Enable tunneling feature on the switch

B. Crash the switch with aDoS attack since switches cannot send ACK bits

C. Poison the switch's MAC address table by flooding it with ACK bits

D. Trick the switch into thinking it already has a session with Terri's computer

Answer: D (LEAVE A REPLY)

NEW QUESTION: 226

It takes _____ mismanaged case/s to ruin your professional reputation as a computer forensics examiner?

A. at least two

B. only one

C. by law, three

D. quite a few

Answer: B (LEAVE A REPLY)

NEW QUESTION: 227

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

A. The Host Domain Name

B. The E-mail Header

C. The SMTP reply Address

D. The X509 Address

Answer: B (LEAVE A REPLY)

NEW QUESTION: 228

Area density refers to:

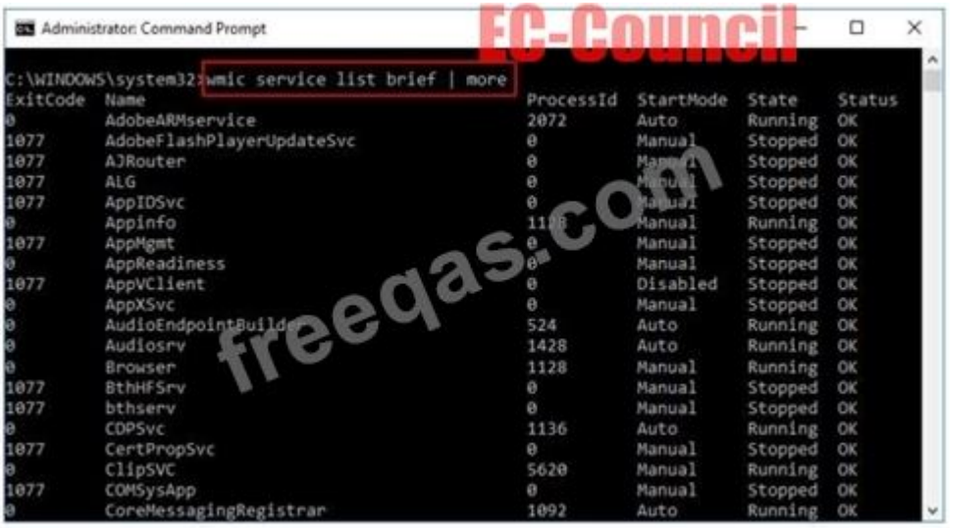
A. the amount of data per square inch

B. the amount of data per disk

C. the amount of data per partition

D. the amount of data per platter
Answer: B (LEAVE A REPLY)

NEW QUESTION: 229
What is the investigator trying to view by issuing the command displayed in the following screenshot?



A. List of services stopped
B. List of services installed
C. List of services closed recently
D. List of services recently started
Answer: B (LEAVE A REPLY)

NEW QUESTION: 230
What is cold boot (hard boot)?
A. It is the process of shutting down a computer from a powered-on or on state
B. It is the process of restarting a computer that is already in sleep mode
C. It is the process of restarting a computer that is already turned on through the operating system
D. It is the process of starting a computer from a powered-down or off state
Answer: D (LEAVE A REPLY)

NEW QUESTION: 231
Billy, a computer forensics expert, has recovered a large number of DBX files during forensic investigation of a laptop. Which of the following email clients he can use to analyze the DBX files?
A. Microsoft Outlook Express
B. Mozilla Thunderoird
C. Eudora
D. Microsoft Outlook
Answer: A (LEAVE A REPLY)

NEW QUESTION: 232

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

A. HKEY_LOCAL_MACHINE

B. HKEY_CURRENT_CONFIGURATION

C. HKEY_USER

D. HKEY_CURRENT_USER

Answer: A,D (LEAVE A REPLY)

The answer is HKEY_CURRENT_USER\Identities\{VALUE}

Note the "user's" password file will be user specific, the Local Machine is the machine information

NEW QUESTION: 233

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

A. Something other than root

B. You cannot determine what privilege runs the daemon service

C. Root

D. Guest

Answer: A (LEAVE A REPLY)

NEW QUESTION: 234

A honey pot deployed with the IP 172.16.1.108 was compromised by an attacker. Given below is an excerpt from a Snort binary capture of the attack. Decipher the activity carried out by the attacker by studying the log.

Please note that you are required to infer only what is explicit in the excerpt.

(Note: The student is being tested on concepts learnt during passive OS fingerprinting, basic TCP/IP connection concepts and the ability to read packet signatures from a sniff dump.)

03/15-20:21:24.107053 211.185.125.124:3500 -> 172.16.1.108:111

TCP TTL:43 TOS:0x0 ID:29726 IpLen:20 DgmLen:52 DF

A* Seq: 0x9B6338C5 Ack: 0x5820ADD0 Win: 0x7D78 TcpLen: 32

TCP Options (3) => NOP NOP TS: 23678634 2878772

=+=

03/15-20:21:24.452051 211.185.125.124:789 -> 172.16.1.103:111

UDP TTL:43 TOS:0x0 ID:29733 IpLen:20 DgmLen:84

Len: 64

01 0A 8A 0A 00 00 00 00 00 00 00 02 00 01 86 A0 ....

00 00 00 02 00 00 00 03 00 00 00 00 00 00 00 00 ....

00 00 00 00 00 00 00 00 00 01 86 B8 00 00 00 01 ....

00 00 00 11 00 00 00 00 ....

=+=

03/15-20:21:24.730436 211.185.125.124:790 -> 172.16.1.103:32773

UDP TTL:43 TOS:0x0 ID:29781 IpLen:20 DgmLen:1104

Len: 1084

47 F7 9F 63 00 00 00 00 00 00 00 02 00 01 86 B8

A. The attacker has scanned and exploited the system using Buffer Overflow

B. The attacker has installed a backdoor

C. The attacker has used a Trojan on port 32773

D. The attacker has conducted a network sweep on port 111

Answer: (SHOW ANSWER)

NEW QUESTION: 235

Under confession, an accused criminal admitted to encrypting child pornography pictures and then hiding them within other pictures. What technique did the accused criminal employ?

A. Steganalysis

B. Picture encoding

C. Steganography

D. Typography

Answer: C (LEAVE A REPLY)

NEW QUESTION: 236

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

A. Closed

B. Filtered

C. Open

D. Stealth

Answer: (SHOW ANSWER)

NEW QUESTION: 237

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. outlook:"search"

B. allinurl:"exchange/logon.asp"

C. locate:"logon page"

D. intitle:"exchange server"

Answer: (SHOW ANSWER)

NEW QUESTION: 238

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

A. Events history

B. Previously typed commands

C. History of the browser

D. Passwords used across the system
Answer: B (LEAVE A REPLY)

NEW QUESTION: 239
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. Enable tunneling feature on the switch
C. Crash the switch with a DoS attack since switches cannot send ACK bits
D. Trick the switch into thinking it already has a session with Terri's computer
Answer: D (LEAVE A REPLY)

NEW QUESTION: 240
If an attacker's computer sends an IPID of 31400 to a zombie computer on an open port in IDLE scanning, what will be the response?
A. 31399
B. The zombie will not send a response
C. 31402
D. 31401
Answer: (SHOW ANSWER)

NEW QUESTION: 241
As a part of the investigation, Caroline, a forensic expert, was assigned the task to examine the transaction logs pertaining to a database named Transfers. She used SQL Server Management Studio to collect the active transaction log files of the database. Caroline wants to extract detailed information on the logs, including AllocUnitId, page id, slot id, etc. Which of the following commands does she need to execute in order to extract the desired information?
A. DBCC LOG(Transfers, 2)
B. DBCC LOG(Transfers, 3)
C. DBCC LOG(Transfers, 1)
D. DBCC LOG(Transfers, 0)
Answer: (SHOW ANSWER)

NEW QUESTION: 242
Microsoft Security IDs are available in Windows Registry Editor. The path to locate IDs in Windows 7 is:
A. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList
B. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Profilelist
C. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Reglist
D. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Regedit
Answer: A (LEAVE A REPLY)

NEW QUESTION: 243
Identify the attack from following sequence of actions?
Step 1: A user logs in to a trusted site and creates a new session
Step 2: The trusted site stores a session identifier for the session in a cookie in the web browser
Step 3: The user is tricked to visit a malicious site
Step 4: the malicious site sends a request from the user's browser using his session cookie
A. Web Application Denial-of-Service (DoS) Attack
B. Cross-Site Scripting (XSS) Attacks
C. Cross-Site Request Forgery (CSRF) Attack
D. Hidden Field Manipulation Attack
Answer: (SHOW ANSWER)

NEW QUESTION: 244
When should an MD5 hash check be performed when processing evidence?
A. On an hourly basis during the evidence examination
B. After the evidence examination has been completed
C. Before and after evidence examination
D. Before the evidence examination has been completed
Answer: C (LEAVE A REPLY)

NEW QUESTION: 245
Bob has encountered a system crash and has lost vital data stored on the hard drive of his Windows computer.
He has no cloud storage or backup hard drives. He wants to recover all the data, which includes his personal photos, music, documents, videos, official emails, etc. Which of the following tools shall resolve Bob's purpose?
A. Colasoft's Capsa
B. Xplico
C. Cain & Abel

D. Recuva
Answer: (SHOW ANSWER)

NEW QUESTION: 246
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 in a civil case must be secured more tightly than in a criminal case
B. evidence in a criminal case must be secured more tightly than in a civil case
C. evidence must be handled in the same way regardless of the type of case
D. evidence procedures are not important unless you work for a law enforcement agency
Answer: B (LEAVE A REPLY)

NEW QUESTION: 247
What encryption technology is used on Blackberry devices?Password Keeper?
A. AES
B. 3DES
C. RC5
D. Blowfish
Answer: A (LEAVE A REPLY)

NEW QUESTION: 248
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. Hybrid attack
B. Syllable attack
C. Brute forcing attack
D. Rule-based attack
Answer: (SHOW ANSWER)

NEW QUESTION: 249
The use of warning banners helps a company avoid litigation by overcoming an employee assumed _____. When connecting to the company's intranet, network or Virtual Private Network(VPN) and will allow the company's investigators to monitor, search and retrieve information stored within the network.
A. Right of Privacy
B. Right to Internet Access
C. Right to work
D. Right of free speech
Answer: A (LEAVE A REPLY)

NEW QUESTION: 250

As a CHFI professional, which of the following is the most important to your professional reputation?
A. The free that you charge
B. The friendship of local law enforcement officers
C. Your Certifications
D. The correct, successful management of each and every case
Answer: (SHOW ANSWER)

NEW QUESTION: 251
Which of the following standard is based on a legal precedent regarding the admissibility of scientific examinations or experiments in legal cases?
A. FERPA standard
B. Daubert Standard
C. Schneiderman Standard
D. Frye Standard
Answer: (SHOW ANSWER)

NEW QUESTION: 252
When a user deletes a file or folder, the system stores complete path including the original filename in a special hidden file called "INF02" in the Recycled folder. If the INF02 file is deleted, it is recovered when you _____
A. Undo the last act ion performed on the system
B. Reboot Windows
C. Download the file from Microsoft website
D. Use a recovery tool to undelete the file
Answer: B (LEAVE A REPLY)

NEW QUESTION: 253
Lynne receives the following email:
Dear lynne@gmail.com! We are sorry to inform you that your ID has been temporarily frozen due to incorrect or missing information saved at 2016/11/10 20:40:24 You have 24 hours to fix this problem or risk to be closed permanently!
To proceed Please Connect >> My Apple ID
Thank You The link to My Apple ID shows http://byggarbetsplatsen.se/backup/signon/ What type of attack is this?
A. Mail Bombing
B. Phishing
C. Email Spamming
D. Email Spoofing
Answer: B (LEAVE A REPLY)

NEW QUESTION: 254
Microsoft Security IDs are available in Windows Registry Editor. The path to locate IDs in Windows 7 is:
A. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion \NetworkList
B. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\Currentversion \ProfileList
C. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule
D. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentsVersion \setup
Answer: B (LEAVE A REPLY)

NEW QUESTION: 255
Which Intrusion Detection System (IDS) usually produces the most false alarms due to the unpredictable behaviors of users and networks?
A. anomaly detection
B. network-based IDS systems (NIDS)
C. signature recognition
D. host-based IDS systems (HIDS)
Answer: D (LEAVE A REPLY)

NEW QUESTION: 256
When investigating a potential e-mail crime, what is your first step in the investigation?
A. Determine whether a crime was actually committed
B. Write a report
C. Trace the IP address to its origin
D. Recover the evidence
Answer: (SHOW ANSWER)

NEW QUESTION: 257
Why should you never power on a computer that you need to acquire digital evidence from?
A. When the computer boots up, files are written to the computer rendering the data nclean

B. When the computer boots up, the system cache is cleared which could destroy evidence
C. When the computer boots up, data in the memory buffer is cleared which could destroy evidence
D. Powering on a computer has no affect when needing to acquire digital evidence from it
Answer: (SHOW ANSWER)

NEW QUESTION: 258
What does the acronym POST mean as it relates to a PC?
A. Primary Operations Short Test
B. PowerOn Self Test
C. Pre Operational Situation Test
D. Primary Operating System Test
Answer: B (LEAVE A REPLY)

NEW QUESTION: 259
In handling computer-related incidents, which IT role should be responsible for recovery, containment, and prevention to constituents?
A. Director of Administration
B. Director of Information Technology
C. Security Administrator
D. Network Administrator
Answer: D (LEAVE A REPLY)

NEW QUESTION: 260
Dumpster Diving refers to:
A. Creating a set of dictionary words and names, and trying all the possible combinations to crack the password
B. Convincing people to reveal the confidential information
C. Looking at either the user's keyboard or screen while he/she is logging in
D. Searching for sensitive information in the user's trash bins and printer trash bins, and searching the user's desk for sticky notes
Answer: D (LEAVE A REPLY)

NEW QUESTION: 261
What is the size value of a nibble?
A. 2 bits
B. 0.5 byte
C. 0.5 kilo byte
D. 0.5 bit
Answer: B (LEAVE A REPLY)

NEW QUESTION: 262

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

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

What is evident from this log file?

A. Web bugs

B. Hidden fields

C. SQL injection is possible

D. Cross site scripting

Answer: C (LEAVE A REPLY)

NEW QUESTION: 263

Which US law does the interstate or international transportation and receiving of child pornography fall under?

A. 18 U.S. Code § 146A

B. 18 U.S. Code § 1466A

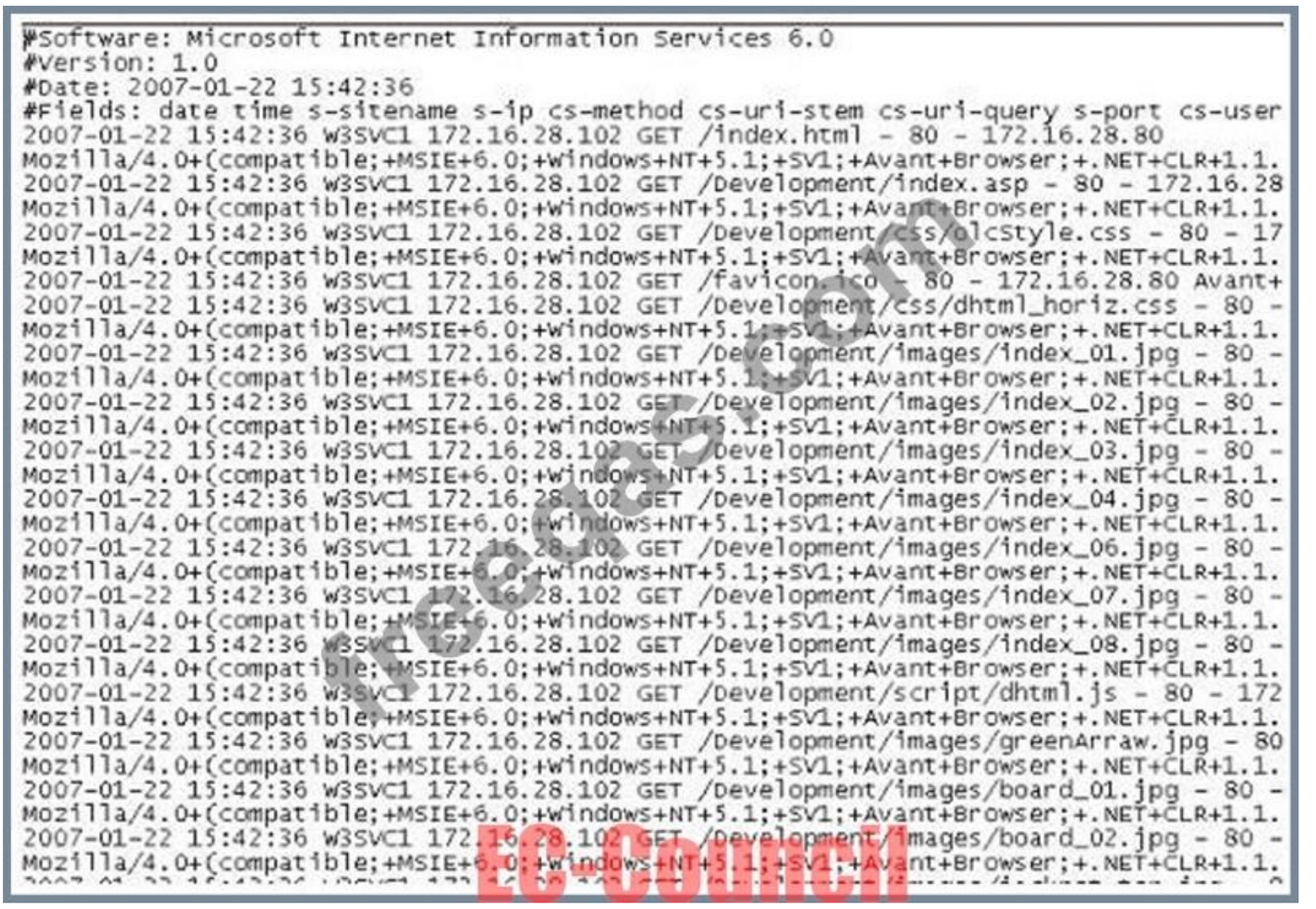
C. 18 U.S. Code § 2252

D. 18 U.S. Code § 252

Answer: C (LEAVE A REPLY)

NEW QUESTION: 264

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



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

A. UT

B. GMT

C. UTC

D. TAI

Answer: (SHOW ANSWER)

NEW QUESTION: 265

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

A. 162

B. 160

C. 161

D. 163

Answer: A,C (LEAVE A REPLY)

NEW QUESTION: 266

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

A. 4 billion

B. 32 million

C. 320 billion
D. 1 billion
Answer: A (LEAVE A REPLY)

NEW QUESTION: 267
A small law firm located in the Midwest has possibly been breached by a computer hacker who was looking to obtain information on their clientele. The law firm does not have any onsite IT employees but wants to search for evidence of the breach themselves to prevent any possible media attention. Why would this not be recommended?
A. Searching creates cache Files that would hinder the investigation
B. Searching for evidence themselves would not have any ill effects
C. Searching could possibly crash the machine or device
D. Searching can change date/time stamps
Answer: D (LEAVE A REPLY)

NEW QUESTION: 268
Which table is used to convert huge word lists (i .e. dictionary files and brute-force lists) into password hashes?
A. Master file tables
B. Rainbow tables
C. Database tables
D. Hash tables
Answer: B (LEAVE A REPLY)

NEW QUESTION: 269
The Apache server saves diagnostic information and error messages that it encounters while processing requests. The default path of this file is usr/local/apache/logs/error.log in Linux. Identify the Apache error log from the following logs.
A. 127.0.0.1 - - [10/Apr/2007:1 0:39:11 +0300]] [error] "GET I apache_pb.gif HTTP/ 1.0" 200 2326
B. 127.0.0.1 - frank [10/0ct/2000:13:55:36 -0700]"GET I apache_pb.gif HTTP/ 1.0" 200 2326
C. http://victim.com/scripts/..%c0%af../..%cOo/oaf
../..%c0%af../..%c0%af../..%c0%af../..
%c0%af../ ..
%c0%af../..%c0%af../winnt/system32/cmd.exe?/c+dir+C:\Winnt\system32\Logfiles\W3S VC1
D. [Wed Oct 11 14:32:52 2000] [error] [client 127.0.0.1] client denied by server configuration: /export/ home/live/ap/htdocs/test
Answer: D (LEAVE A REPLY)

NEW QUESTION: 270

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

A. It contains the times and dates of when the system was last patched

B. It contains the times and dates of all the system files

C. It is not necessary to scan the virtual memory of a computer

D. Hidden running processes

Answer: D (LEAVE A REPLY)

NEW QUESTION: 271

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

A. International Mobile Equipment Identifier (IMEI)

B. Integrated circuit card identifier (ICCID)

C. Equipment Identity Register (EIR)

D. International mobile subscriber identity (IMSI)

Answer: A (LEAVE A REPLY)

NEW QUESTION: 272

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

A. image

B. mcopy

C. dd

D. MD5

Answer: C (LEAVE A REPLY)

NEW QUESTION: 273

Smith, as a part his forensic investigation assignment, seized a mobile device. He was asked to recover the Subscriber Identity Module (SIM card) data in 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 made three unsuccessful attempts, which blocked the SIM card. What can Jason do in this scenario to reset the PIN and access SIM data?

A. He should contact the network operator for Personal Unlock Number (PUK)

B. He should contact the network operator for a Temporary Unlock Code (TUK)

C. Use system and hardware tools to gain access

D. He can attempt PIN guesses after 24 hours

Answer: A (LEAVE A REPLY)

NEW QUESTION: 274

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

A. RIYG6VR.doc is the name of the doc file deleted from the system

B. It is a deleted doc file

C. It is file deleted from R drive

D. It is a doc file deleted in seventh sequential order

Answer: (SHOW ANSWER)

NEW QUESTION: 275

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

A. Lsproc

B. Registry

C. EProcess

D. Dun1pChk

Answer: C (LEAVE A REPLY)

NEW QUESTION: 276

Which US law does the interstate or international transportation and receiving of child pornography fall under?

A. §18. U.S.C 146A

B. §18. U.S.C 2252

C. §18. U.S.C. 1466A

D. §18. U.S.C 252

Answer: B (LEAVE A REPLY)

NEW QUESTION: 277

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 (LEAVE A REPLY)

NEW QUESTION: 278
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 metadata
B. The recycle bin
C. The swapfile
D. The registry
Answer: C (LEAVE A REPLY)

NEW QUESTION: 279
Which of the following refers to the data that might still exist in a cluster even though the original file has been overwritten by another file?
A. Sector
B. Metadata
C. MFT
D. Slack Space
Answer: (SHOW ANSWER)

NEW QUESTION: 280
What TCP/UDP port does the toolkit program netstat use?
A. Port 7
B. Port 23
C. Port 69
D. Port 15
Answer: D (LEAVE A REPLY)

NEW QUESTION: 281
What type of file is represented by a colon (:) with a name following it in the Master File Table (MFT) of an NTFS disk?
A. Reserved file
B. Encrypted file

C. Data stream file
D. Compressed file
Answer: C (LEAVE A REPLY)

NEW QUESTION: 282
When you are running a vulnerability scan on a network and the IDS cuts off your connection, what type of IDS is being used?
A. Active IDS
B. NIPS
C. Progressive IDS
D. Passive IDS
Answer: (SHOW ANSWER)

NEW QUESTION: 283
The IIS log file format is a fixed (cannot be customized) ASCII text-based format. The IIS format includes basic items, such as client IP address, user name, date and time, service and instance, server name and IP address, request type, target of operation, etc. Identify the service status code from the following IIS log.
1 92.168.100.150, -, 03/6/11, 8:45:30, W3SVC2, SERVER, 172.15.10.30, 4210, 125, 3524,
1 00, 0, GET, /dollerlogo.gif,
A. 3524
B. 100
C. 4210
D. W3SVC2
Answer: B (LEAVE A REPLY)

NEW QUESTION: 284
Robert, a cloud architect, received a huge bill from the cloud service provider, which usually doesn't happen. After analyzing the bill, he found that the cloud resource consumption was very high. He then examined the cloud server and discovered that a malicious code was running on the server, which was generating huge but harmless traffic from the server. This means that the server has been compromised by an attacker with the sole intention to hurt the cloud customer financially. Which attack is described in the above scenario?
A. Man-in-the-cloud Attack
B. EDoS Attack (Economic Denial of Service)
C. DDoS Attack (Distributed Denial of Service)
D. XSS Attack
Answer: C (LEAVE A REPLY)

NEW QUESTION: 285

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

NEW QUESTION: 286
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. 404
B. 999
C. 202
D. 606
Answer: (SHOW ANSWER)

NEW QUESTION: 287
When performing a forensics analysis, what device is used to prevent the system from recording data on an evidence disk?
A. Protocol analyzer
B. Firewall
C. Disk editor
D. Write-blocker
Answer: (SHOW ANSWER)

NEW QUESTION: 288
Which of the following is the certifying body of forensics labs that investigate criminal cases by analyzing evidence?
A. The American Forensics Laboratory for Computer Forensics (AFLCF)

B. International Society of Forensics Laboratory (ISFL)
C. The American Forensics Laboratory Society (AFLS)
D. The American Society of Crime Laboratory Directors (ASCLD)
Answer: D (LEAVE A REPLY)

NEW QUESTION: 289
Why would a company issue a dongle with the software they sell?
A. To provide copyright protection
B. To provide source code protection
C. To ensure that keyloggers cannot be used
D. To provide wireless functionality with the software
Answer: (SHOW ANSWER)

NEW QUESTION: 290
LBA (Logical Block Address) addresses data by allotting a _____to each sector of the hard disk.
A. Sector number
B. Index number
C. Sequential number
D. Operating system number
Answer: C (LEAVE A REPLY)

NEW QUESTION: 291
An attack vector is a path or means by which an attacker can gain access to computer or network resources in order to deliver an attack payload or cause a malicious outcome.
A. False
B. True
Answer: B (LEAVE A REPLY)

NEW QUESTION: 292
You are assisting a Department of Defense contract company to become compliant with the stringent security policies set by the DoD. One such strict rule is that firewalls must only allow incoming connections that were first initiated by internal computers. What type of firewall must you implement to abide by this policy?
A. Statefull firewall
B. Application-level proxy firewall
C. Circuit-level proxy firewall
D. Packet filtering firewall
Answer: A (LEAVE A REPLY)

NEW QUESTION: 293

What must an investigator do before disconnecting an iPod from any type of computer?
A. Disjoin the iPod
B. Unmount the iPod
C. Mount the iPod
D. Join the iPod
Answer: B (LEAVE A REPLY)

NEW QUESTION: 294
When investigating a wireless attack, what information can be obtained from the DHCP logs?
A. MAC address of the attacker
If any computers on the network are running in promiscuous mode
B. IP traffic between the attacker and the victim
C. The operating system of the attacker and victim computersThe operating system of the attacker and victim? computers
Answer: A (LEAVE A REPLY)

NEW QUESTION: 295
After passing her CEH exam, Carol wants to ensure that her network is completely secure. She implements a DMZ, stateful firewall, NAT, IPSEC, and a packet filtering firewall. Since all security measures were taken, none of the hosts on her network can reach the Internet. Why is that?
A. NAT does not work with IPSEC
B. IPSEC does not work with packet filtering firewalls
C. NAT does not work with stateful firewalls
D. Stateful firewalls do not work with packet filtering firewalls
Answer: (SHOW ANSWER)

NEW QUESTION: 296
How often must a company keep log files for them to be admissible in a court of law?
A. Continuously
B. Weekly
C. All log files are admissible in court no matter their frequency
D. Monthly
Answer: A (LEAVE A REPLY)

NEW QUESTION: 297
You have completed a forensic investigation case. You would like to destroy the data contained in various disks at the forensics lab due to sensitivity of the case. How would you permanently erase the data on the hard disk?
A. Overwrite the contents of the hard disk with Junk data
B. Format the hard disk multiple times using a low level disk utility
C. Throw the hard disk into the fire

D. Run the powerful magnets over the hard disk
Answer: C (LEAVE A REPLY)

NEW QUESTION: 298
Which program uses different techniques to conceal a malware's code, thereby making it difficult for security mechanisms to detect or remove it?
A. Obfuscator
B. Dropper
C. Packer
D. Injector
Answer: A (LEAVE A REPLY)

NEW QUESTION: 299
If you come across a sheepdip machine at your client site, what would you infer?
A. A sheepdip coordinates several honeypots
B. A sheepdip computer defers a denial of service attack
C. A sheepdip computer is another name for a honeypot
D. A sheepdip computer is used only for virus-checking.
Answer: (SHOW ANSWER)

NEW QUESTION: 300
Under which Federal Statutes does FBI investigate for computer crimes involving e-mail scams and mail fraud?
A. 18 U.S.C. 1029 Possession of Access Devices
B. 18 U.S.C. 1361 Injury to Government Property
C. 18 U.S.C. 1831 Economic Espionage Act
D. 18 U.S.C. 1343 Fraud by wire, radio or television
E. 18 U.S.C. 1030 Fraud and related activity in connection with computers
F. 18 U.S.C. 1832 Trade Secrets Act
G. 18 U.S.C. 1362 Government communication systems
Answer: (SHOW ANSWER)

NEW QUESTION: 301
Chris has been called upon to investigate a hacking incident reported by one of his clients. The company suspects the involvement of an insider accomplice in the attack. Upon reaching the incident scene, Chris secures the physical area, records the scene using visual media. He shuts the system down by pulling the power plug so that he does not disturb the system in any way. He labels all cables and connectors prior to disconnecting any. What do you think would be the next sequence of events?
A. Connect the target media; prepare the system for acquisition; Secure the evidence; Copy the media

B. Connect the target media; Prepare the system for acquisition; Secure the evidence; Copy the media
C. Prepare the system for acquisition; Connect the target media; copy the media; Secure the evidence
D. Secure the evidence; prepare the system for acquisition; Connect the target media; copy the media
Answer: C (LEAVE A REPLY)

NEW QUESTION: 302
Which among the following U.S. laws requires financial institutions/companies that offer consumers financial products or services such as loans, financial or investment advice, or insurance to protect their customers' information against security threats?
A. FISMA
B. GLBA
C. HIPAA
D. SOX
Answer: (SHOW ANSWER)

NEW QUESTION: 303
Network forensics allows Investigators to inspect network traffic and logs to identify and locate the attack system
Network forensics can reveal: (Select three answers)
A. Hardware configuration of the attacker's system
B. Source of security incidents' and network attacks
C. Path of the attack
D. Intrusion techniques used by attackers
Answer: (SHOW ANSWER)

NEW QUESTION: 304
Kyle is performing the final testing of an application he developed for the accounting department. His last round of testing is to ensure that the program is as secure as possible. Kyle runs the following command. What is he testing at this point?

#include #include int main(int argc, char
*argv[]) { char buffer[10]; if (argc < 2) { fprintf (stderr, "USAGE: %s string\n", argv[0]); return 1; }
strcpy(buffer, argv[1]); return 0; }

A. Buffer overflow

B. Format string bug

C. SQL injection

D. Kernal injection

Answer: (SHOW ANSWER)

NEW QUESTION: 305

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

A. assume the suspect machine is contaminated

B. do not enter alone

C. determine a way to obtain the suspect computer

D. coordinate with the HAZMAT team

Answer: (SHOW ANSWER)

NEW QUESTION: 306

What is one method of bypassing a system BIOS password?

A. Remove all the system memory

B. Removing the CMOS battery

C. Login to Windows and disable the BIOS password

D. Removing the processor

Answer: (SHOW ANSWER)

NEW QUESTION: 307

The police believe that Melvin Matthew has been obtaining unauthorized access to computers belonging to numerous computer software and computer operating systems manufacturers, cellular telephone manufacturers, Internet Service Providers and Educational Institutions. They also suspect that he has been stealing, copying and misappropriating proprietary computer software belonging to the several victim companies. What is preventing the police from breaking down the suspects door and searching his home and seizing all of his computer equipment if they have not yet obtained a warrant?

A. The Federal Rules of Evidence

B. The Good Samaritan Laws

C. The USA patriot Act

D. The Fourth Amendment

Answer: (SHOW ANSWER)

NEW QUESTION: 308

When searching through file headers for picture file formats, what should be searched to find a JPEG file in hexadecimal format?
A. FF 00 FF 00 FF 00
B. EF 00 EF 00 EF 00
C. FF D8 FF E0 00 10
D. FF FF FF FF FF FF
Answer: C (LEAVE A REPLY)

NEW QUESTION: 309
Jason is the security administrator of ACMA metal Corporation. One day he notices the company's Oracle database server has been compromised and the customer information along with financial data has been stolen. The financial loss will be in millions of dollars if the database gets into the hands of the competitors. Jason wants to report this crime to the law enforcement agencies immediately.
Which organization coordinates computer crimes investigations throughout the United States?
A. Internet Fraud Complaint Center
B. Local or national office of the U.S. Secret Service
C. CERT Coordination Center
D. National Infrastructure Protection Center
Answer: B (LEAVE A REPLY)

NEW QUESTION: 310
Microsoft Outlook maintains email messages in a proprietary format in what type of file?
A. .pst
B. .email
C. .doc
D. .mail
Answer: A (LEAVE A REPLY)

NEW QUESTION: 311
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. Footprinting
B. Password brute force
C. Nmap Scanning
D. SQL Injection
Answer: D (LEAVE A REPLY)

NEW QUESTION: 312
Which of the following file in Novel GroupWise stores information about user accounts?
A. gwcheck.db
B. PRIV.STM
C. PRIV.EDB
D. ngwguard.db
Answer: (SHOW ANSWER)

NEW QUESTION: 313
Which of the following registry hive gives the configuration information about which application was used to open various files on the system?
A. HKEY_LOCAL_MACHINE
B. HKEY_USERS
C. HKEY_CURRENT_CONFIG
D. HKEY_CLASSES_ROOT
Answer: (SHOW ANSWER)

NEW QUESTION: 314
When searching through file headers for picture file formats, what should be searched to find a JPEG file in hexadecimal format?
A. FF FF FF FF FF FF
B. FF 00 FF 00 FF 00
C. EF 00 EF 00 EF 00
D. FF D8 FF E0 00 10
Answer: D (LEAVE A REPLY)

NEW QUESTION: 315
During forensics investigations, investigators tend to first collect the system time and then compare it with UTC. What does the abbreviation UTC stand for?
A. Universal Time for Computers
B. Correlated Universal Time
C. Coordinated Universal Time
D. Universal Computer Time
Answer: C (LEAVE A REPLY)

NEW QUESTION: 316
Amelia has got an email from a well-reputed company stating in the subject line that she has won a prize money, whereas the email body says that she has to pay a certain amount for being eligible for the contest.
Which of the following acts does the email breach?
A. SOX

B. GLBA
C. CAN-SPAM Act
D. HIPAA
Answer: C (LEAVE A REPLY)

NEW QUESTION: 317
To calculate the number of bytes on a disk, the formula is: CHS**
A. number of circles x number of halves x number of sides x 512 bytes per sector
B. number of cylinders x number of halves x number of shims x 512 bytes per sector
C. number of cells x number of heads x number of sides x 512 bytes per sector
D. number of cylinders x number of heads x number of sides x 512 bytes per sector
Answer: D (LEAVE A REPLY)
Although D in this question is probably the closest, the answer may have been transcribed incorrectly. CHS stands for Cylinder Head Sector, and S is not sides. Each side of a platter of a disk has its own head.
A cylinder is an alignment of all tracks under one head position. So the answer is number of cylinders x number of heads x number of sectors (per track) x 512 bytes per sector (assuming that is the sector size as some disks may have larger sector sizes). The number of tracks per side of disk, or the number of tracks that a single head can access is equal to the number of cylinders.

NEW QUESTION: 318
A steganographic file system is a method to store the files in a way that encrypts and hides the data without the knowledge of others
A. True
B. False
Answer: (SHOW ANSWER)

NEW QUESTION: 319
What type of equipment would a forensics investigator store in a StrongHold bag?
A. Backup tapes
B. PDAPDA?
C. Hard drives

D. Wireless cards
Answer: (SHOW ANSWER)

NEW QUESTION: 320
A packet is sent to a router that does not have the packet destination address in its route table. How will the packet get to its proper destination?
A. Reverse DNS
B. Root Internet servers
C. Border Gateway Protocol
D. Gateway of last resort
Answer: (SHOW ANSWER)

NEW QUESTION: 321
George is performing security analysis for Hammond and Sons LLC. He is testing security vulnerabilities of their wireless network. He plans on remaining as "stealthy" as possible during the scan. Why would a scanner like Nessus is not recommended in this situation?
A. Nessus is too loud
B. Nessus is not a network scanner
C. Nessus cannot perform wireless testing
D. There are no ways of performing a "stealthy" wireless scan
Answer: A (LEAVE A REPLY)

NEW QUESTION: 322
Which of the following tool is used to locate IP addresses?
A. Towelroot
B. Deep Log Analyzer
C. SmartWhois
D. XRY LOGICAL
Answer: C (LEAVE A REPLY)

NEW QUESTION: 323
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. The /tmp directory will be flushed
B. All running processes will be lost
C. Power interruption will corrupt the pagefile
D. Any data not yet flushed to the system will be lost
Answer: D (LEAVE A REPLY)

NEW QUESTION: 324

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. Power off all devices if currently on
B. Unplug all connected devices
C. Photograph and document the peripheral devices
D. Place PDA, including all devices, in an antistatic bag
Answer: C (LEAVE A REPLY)

NEW QUESTION: 325
Bob has encountered a system crash and has lost vital data stored on the hard drive of his Windows computer. He has no cloud storage or backup hard drives. He wants to recover all the data, which includes his personal photos, music, documents, videos, official emails, etc. Which of the following tools shall resolve Bob's purpose?
A. Xplico
B. Recuva
C. Colasoft's Capsa
D. Cain & Abel
Answer: B (LEAVE A REPLY)

NEW QUESTION: 326
To check for POP3 traffic using Ethereal, what port should an investigator search by?
A. 125
B. 25
C. 110
D. 143
Answer: C (LEAVE A REPLY)

NEW QUESTION: 327
Lance wants to place a honeypot on his network. Which of the following would be your recommendations?
A. It doesn't matter as all replies are faked
B. Use a system that is not directly interacing with the router
C. Use a system that has a dynamic addressing on the network
D. Use it on a system in an external DMZ in front of the firewall
Answer: A (LEAVE A REPLY)

NEW QUESTION: 328

As a Certified Ethical Hacker, you were contracted by a private firm to conduct an external security assessment through penetration testing . What document describes the specifics of the testing, the associated violations, and essentially protects both the organization's interest and your liabilities as a tester?

A. Project Scope

B. Rules of Engagement

C. Service Level Agreement

D. Non-Disclosure Agreement

Answer: B (LEAVE A REPLY)

NEW QUESTION: 329

A picture file is recovered from a computer under investigation. During the investigation process, the file is enlarged 500% to get a better view of its contents. The picture quality is not degraded at all from this process. What kind of picture is this file. What kind of picture is this file?

A. Vector image

B. Metafile image

C. Raster image

D. Catalog image

Answer: A (LEAVE A REPLY)

NEW QUESTION: 330

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

A. #06#*

B. *#06#

C. *IMEI#

D. #*06*#

Answer: D (LEAVE A REPLY)

NEW QUESTION: 331

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

A. IP header field

B. ICMP header field

C. TCP header field

D. UDP header field

Answer: C (LEAVE A REPLY)

NEW QUESTION: 332
Printing under a Windows Computer normally requires which one of the following files types to be created?
A. MEM
B. EMF
C. EME
D. CME
Answer: B (LEAVE A REPLY)

NEW QUESTION: 333
Wi-Fi Protected Access (WPA) is a data encryption method for WLANs based on 802.11 standards. Temporal Key Integrity Protocol (TKIP) enhances WEP by adding a rekeying mechanism to provide fresh encryption and integrity keys. Temporal keys are changed for every_____.
A. 20.000 packets
B. 5,000 packets
C. 15,000 packets
D. 10.000 packets
Answer: D (LEAVE A REPLY)

NEW QUESTION: 334
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 (LEAVE A REPLY)
The Ping of Death occurs when the ICMP Header field contains a packet size lager than 65507 bytes.

NEW QUESTION: 335

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

A. Grill cipher

B. Visual semagram

C. Text semagram

D. Null cipher

Answer: A (LEAVE A REPLY)

NEW QUESTION: 336

What malware analysis operation can the investigator perform using the jv16 tool?

A. Registry Analysis/Monitoring

B. Installation Monitor

C. Network Traffic Monitoring/Analysis

D. Files and Folder Monitor

Answer: (SHOW ANSWER)

NEW QUESTION: 337

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

A. Title 18, Section 1030

B. Title 18, Section 2703(d)

C. Title 18, Section Chapter 90

D. Title 18, Section 2703(f)

Answer: D (LEAVE A REPLY)

1 8 U.S.C. S 1029 Fraud and Related Activity in Connection with Access Devices

1 8 U.S.C. S 1030 Fraud and Related Activity in Connection with Computers

1 8 U.S.C. S 2703 Required Disclosure of Customer Communications Records

1 8 U.S.C. S 2703(d) Requirements for Court Order

1 8 U.S.C. S 2703(f) Requirement to Preserve Evidence

NEW QUESTION: 338
Which Intrusion Detection System (IDS) usually produces the most false alarms due to the unpredictable behaviors of users and networks?
A. network-based IDS systems (NIDS)
B. host-based IDS systems (HIDS)
C. anomaly detection
D. signature recognition
Answer: B,C (LEAVE A REPLY)
NIDS and HIDS are types of IDS systems, Host or Network, and addresses placement of the probe.
Anomaly detection is based on behavior analysis, and if you read the question, the question says "behavior" and if the behavior is unporedictable, then the IDS won't know what is normal and what is bad.

NEW QUESTION: 339
The following excerpt is taken from a honeypot log. The log captures activities across three days. There are several intrusion attempts; however, a few are successful.
(Note: The objective of this question is to test whether the student can read basic information from log entries and interpret the nature of attack.) Apr 24 14:46:46 [4663]: spp_portscan: portscan detected from 194.222.156.169 Apr 24 14:46:46 [4663]: IDS27/FIN Scan: 194.222.156.169:56693 -> 172.16.1.107:482 Apr 24 18:01:05 [4663]: IDS/DNS-version-query: 212.244.97.121:3485 -> 172.16.1.107:53 Apr 24 19:04:01 [4663]: IDS213/ftp-passwd-retrieval: 194.222.156.169:1425 -> 172.16.1.107:21 Apr 25 08:02:41 [5875]: spp_portscan: PORTSCAN DETECTED from 24.9.255.53 Apr 25 02:08:07 [5875]: IDS277/DNS-version-query: 63.226.81.13:4499 -> 172.16.1.107:53 Apr 25 02:08:07 [5875]: IDS277/DNS-version-query: 63.226.81.13:4630 -> 172.16.1.101:53 Apr 25 02:38:17 [5875]: IDS/RPC-rpcinfo-query: 212.251.1.94:642 -> 172.16.1.107:111 Apr 25 19:37:32 [5875]: IDS230/web-cgi-space-wildcard: 198.173.35.164:4221 -> 172.16.1.107:80 Apr 26 05:45:12 [6283]: IDS212/dns-zone-transfer: 38.31.107.87:2291 -> 172.16.1.101:53 Apr 26 06:43:05 [6283]: IDS181/nops-x86: 63.226.81.13:1351 -> 172.16.1.107:53 Apr 26 06:44:25 victim7 PAM_pwdb[12509]: (login) session opened for user simple by (uid=0) Apr 26 06:44:36 victim7 PAM_pwdb[12521]: (su) session opened for user simon by simple(uid=506) Apr 26 06:45:34 [6283]: IDS175/socks-probe: 24.112.167.35:20 -> 172.16.1.107:1080 Apr 26 06:52:10 [6283]: IDS127/telnet-login-incorrect: 172.16.1.107:23 -> 213.28.22.189:4558 From the options given below choose the one which best interprets the following entry:
Apr 26 06:43:05 [6283]: IDS181/nops-x86: 63.226.81.13:1351 -> 172.16.1.107:53
A. An IDS evasion technique
B. A buffer overflow attempt
C. A DNS zone transfer
D. Data being retrieved from 63.226.81.13
Answer: A (LEAVE A REPLY)

NEW QUESTION: 340
Harold is a security analyst who has just run the rdisk /s command to grab the backup SAM files on a computer. Where should Harold navigate on the computer to find the file?
A. %systemroot%\repair
B. %systemroot%\LSA
C. %systemroot%\system32\LSA
D. %systemroot%\system32\drivers\etc
Answer: A (LEAVE A REPLY)

NEW QUESTION: 341
Harold is a computer forensics investigator working for a consulting firm out of Atlanta Georgia. Harold is called upon to help with a corporate espionage case in Miami Florida. Harold assists in the investigation by pulling all the data from the computers allegedly used in the illegal activities. He finds that two suspects in the company where stealing sensitive corporate information and selling it to competing companies. From the email and instant messenger logs recovered, Harold has discovered that the two employees notified the buyers by writing symbols on the back of specific stop signs. This way, the buyers knew when and where to meet with the alleged suspects to buy the stolen material. What type of steganography did these two suspects use?
A. Text semagram
B. Grill cipher
C. Visual semagram
D. Visual cipher
Answer: C (LEAVE A REPLY)

NEW QUESTION: 342
Which of the following network attacks refers to sending huge volumes of email to an address in an attempt to overflow the mailbox or overwhelm the server where the email address is hosted so as to cause a denial-of-service attack?
A. Email spoofing
B. Email spamming
C. Mail bombing
D. Phishing
Answer: C (LEAVE A REPLY)

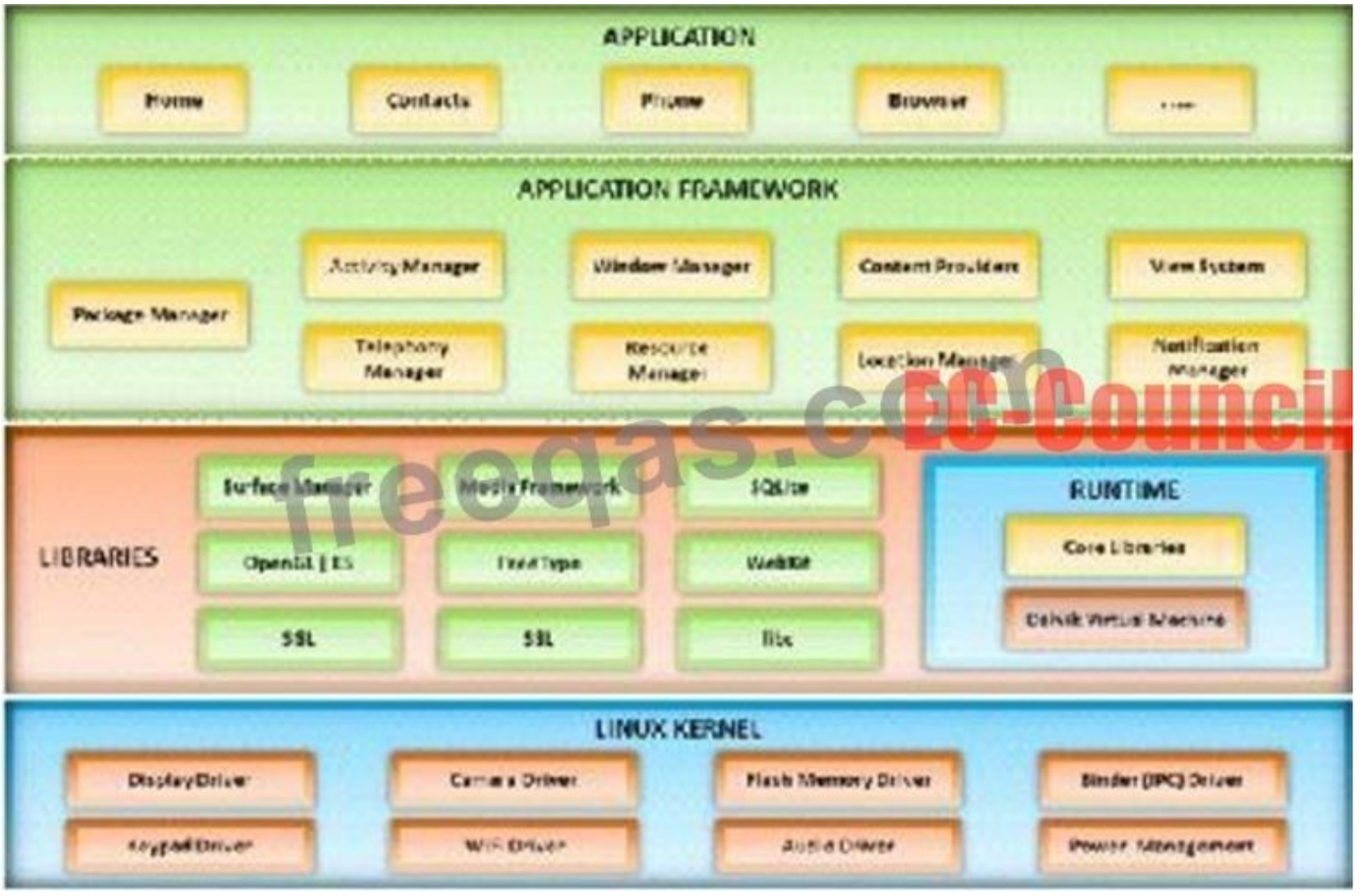
NEW QUESTION: 343
Gary, a computer technician, is facing allegations of abusing children online by befriending them and sending them illicit adult images from his office computer. What type of investigation does this case require?
A. Both Criminal and Administrative Investigation
B. Civil Investigation

C. Administrative Investigation
D. Criminal Investigation
Answer: D (LEAVE A REPLY)

NEW QUESTION: 344
When making the preliminary investigations in a sexual harassment case, how many investigators are you recommended having?
A. Four
B. Two
C. Three
D. One
Answer: B (LEAVE A REPLY)

NEW QUESTION: 345
Which of the following web browser uses the Extensible Storage Engine (ESE) database format to store browsing records, including history, cache, and cookies?
A. Safari
B. Mozilla Firefox
C. Microsoft Edge
D. Google Chrome
Answer: C (LEAVE A REPLY)

NEW QUESTION: 346
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. Windows Phone 7 Architecture

C. Symbian OS Architecture

D. Android OS Architecture

Answer: D (LEAVE A REPLY)

NEW QUESTION: 347

The status of the network interface cards (NICs) connected to a system gives information about whether the system is connected to a wireless access point and what IP address is being used. Which command displays the network configuration of the NICs on the system?

A. netstat

B. net session

C. tasklist
D. ipconfig /all
Answer: D (LEAVE A REPLY)