Untitled Exam

Number: 000-000
Passing Score: 800
Time Limit: 120 min
File Version: 1.0

Exam A

QUESTION 1
What information do you need to recover when searching a victim's computer for a crime committed with specific e-mail message?

A. Internet service provider information
B. E-mail header
C. Username and password
D. Firewall log

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 2
Melanie was newly assigned to an investigation and asked to make a copy of all the evidence from the compromised system. Melanie did a DOS copy of all the files on the system. What would be the primary reason for you to recommend a disk imaging tool?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 3
You are employed directly by an attorney to help investigate an alleged sexual harassment case at a large pharmaceutical manufacture. While at the corporate office of the company, the CEO demands to know the status of the investigation. What prevents you from discussing the case with the CEO?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 4
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 5
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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 6
The _____ refers to handing over the results of private investigations to the authorities because of indications of criminal activity.

A. Locard Exchange Principle
B. Clark Standard
C. Kelly Policy
D. Silver-Platter Doctrine

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 7
You are working as Computer Forensics investigator and are called by the owner of an accounting firm to investigate possible computer abuse by one of the firm's employees. You meet with the owner of the firm and discover that the company has never published a policy stating that they reserve the right to inspect their computing assets at will. What do you do?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 8
During the course of a corporate investigation, you find that an Employee is committing a crime.
Can the Employer file a criminal complaint with Police?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 9
_____ is simply the application of Computer Investigation and analysis techniques in the interests of determining potential legal evidence.

A. Network Forensics
B. Computer Forensics
C. Incident Response
D. Event Reaction

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 10
What is the name of the Standard Linux Command that is also available as windows application that can be used to create bit-stream images?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 11
To preserve digital evidence, an investigator should _____.

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 12
Profiling is a forensics technique for analyzing evidence with the goal of identifying the perpetrator from their various activity. After a computer has been compromised by a hacker, which of the following would be most important in forming a profile of the incident?

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

Correct Answer: B
Section: (none)

Explanation

Explanation/Reference:

QUESTION 13
Printing under a Windows Computer normally requires which one of the following files types to be created?

A. EME
B. MEM
C. EMF
D. CME

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 14
An Expert witness give an opinion if:

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 15
When using Windows acquisitions tools to acquire digital evidence, it is important to use a well-tested hardware write-blocking device to:

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 16
Office Documents (Word, Excel and PowerPoint) contain a code that allows tracking the MAC or unique identifier of the machine that created the document. What is that code called?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 17
You have completed a forensic investigation case. You would like to destroy the data contained in various disks at the forensics lab due to sensitivity of the case. How would you permanently erase the data on the hard disk?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 18
You have been asked to investigate after a user has reported a threatening e-mail they have received from an external source. Which of the following are you most interested in when trying to trace the source of the message?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 19
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 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's computer. You inform the officer that you will not be able to comply with that request because doing so would:

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 20
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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 21
The police believe that Melvin Matthew has been obtaining unauthorized access to computers belonging to numerous computer software and computer operating systems manufacturers, cellular telephone manufacturers, Internet Service Providers and Educational Institutions. They also suspect that he has been stealing, copying and misappropriating proprietary computer software belonging to the several victim companies. What is preventing the police from breaking down the suspects door and searching his home and seizing all of his computer equipment if they have not yet obtained a warrant?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 22
When cataloging digital evidence, the primary goal is to

A. Make bit-stream images of all hard drives
B. Preserve evidence integrity
C. Not remove the evidence from the scene
D. Not allow the computer to be turned off

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 23
You are conducting an investigation of fraudulent claims in an insurance company that involves complex text searches through large numbers of documents. Which of the following tools would allow you to quickly and efficiently search for a string within a file on the bitmap image of the target computer?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 24
As a CHFI professional, which of the following is the most important to your professional reputation?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 25
In conducting a computer abuse investigation you become aware that the suspect of the investigation is using ABC Company as his Internet Service Provider (ISP). You contact ISP and request that they provide you assistance with your investigation. What assistance can the ISP provide?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

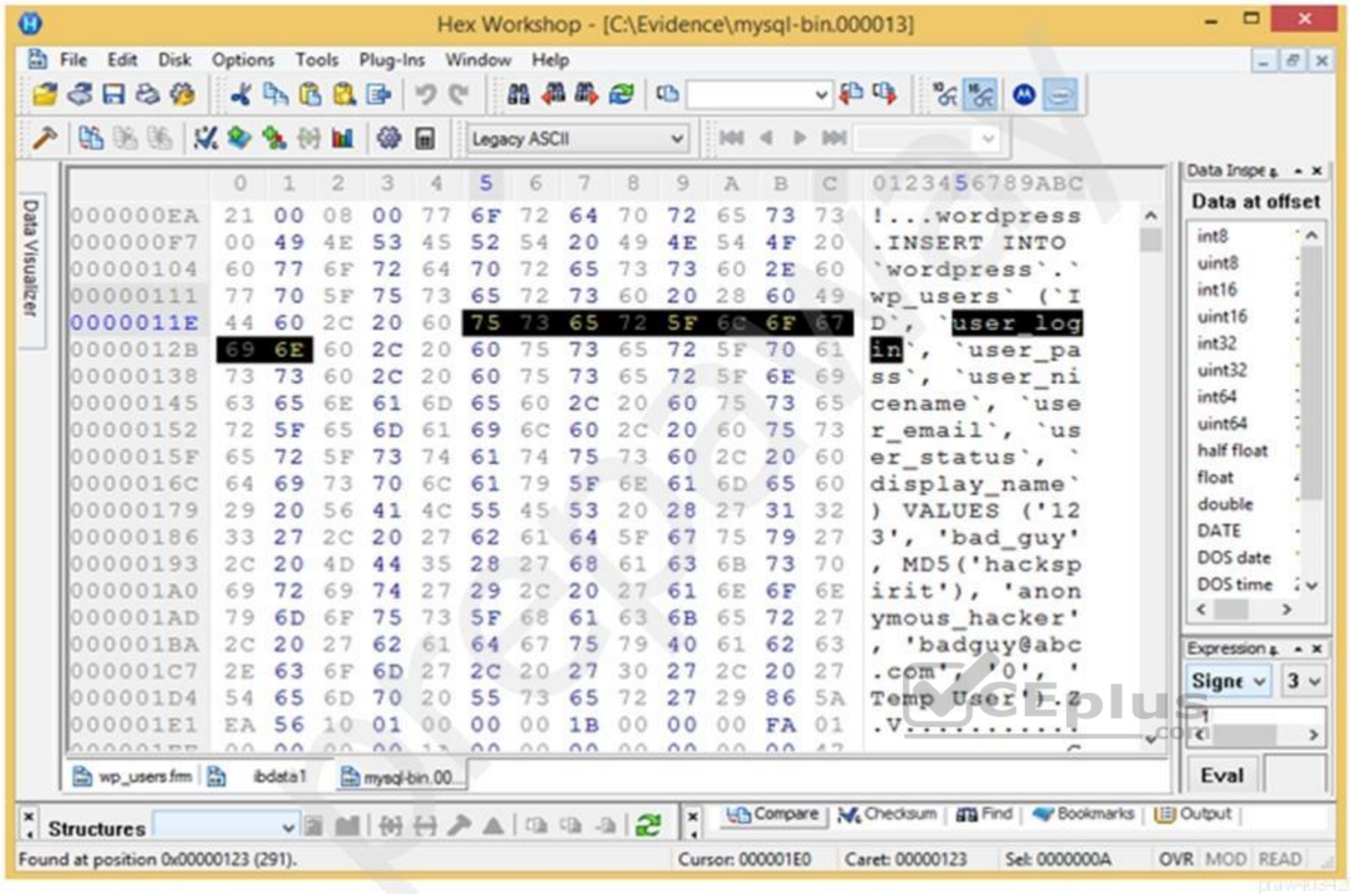
QUESTION 26
You are assisting in the investigation of a possible Web Server Hack. The company who called you stated that customers reported to them that whenever they entered the web address of the company in their browser, what they received was a porno graphic web site. The company checked the web server and nothing appears wrong. When you type in the IP address of the web site in your browser everything appears normal. What is the name of the attack that affects the DNS cache of the name resolution servers, resulting in those servers directing users to the wrong web site?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 27
Analyze the hex representation of mysql-bin.000013 file in the screenshot below. Which of the following will be an inference from this analysis?



A. A user with username bad_guy has logged into the WordPress web application
B. A WordPress user has been created with the username anonymous_hacker
C. An attacker with name anonymous_hacker has replaced a user bad_guy in the WordPress database
D. A WordPress user has been created with the username bad_guy

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 28
Law enforcement officers are conducting a legal search for which a valid warrant was obtained.
While conducting the search, officers observe an item of evidence for an unrelated crime that was not included in the warrant. The item was clearly visible to the officers and immediately identified as evidence. What is the term used to describe how this evidence is admissible?

A. Plain view doctrine
B. Corpus delicti
C. Locard Exchange Principle

D. Ex Parte Order

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 29
Microsoft Outlook maintains email messages in a proprietary format in what type of file?

A. .email
B. .mail
C. .pst
D. .doc

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 30
The efforts to obtain information before a trail by demanding documents, depositions, questioned and answers written under oath, written requests for admissions of fact and examination of the scene is a description of what legal term?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 31
The rule of thumb when shutting down a system is to pull the power plug. However, it has certain drawbacks. Which of the following would that be?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 32
You are a computer forensics investigator working with local police department and you are called to assist in an investigation of threatening emails. The complainant has printer out 27 email messages from the suspect and gives the printouts to you. You inform her that you will need to examine her computer because you need access to the _____ in order to track the emails back to the suspect.

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 33
Hackers can gain access to Windows Registry and manipulate user passwords, DNS settings, access rights or others features that they may need in order to accomplish their objectives. One simple method for loading an application at startup is to add an entry (Key) to the following Registry Hive:

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 34
Which of the following file system is used by Mac OS X?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 35
When you are running a vulnerability scan on a network and the IDS cuts off your connection, what type of IDS is being used?

A. Passive IDS
B. Active IDS
C. Progressive IDS
D. NIPS

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 36
Simon is a former employee of Trinitron XML Inc. He feels he was wrongly terminated and wants to hack into his former company's network. Since Simon remembers some of the server names, he attempts to run the axfr and ixfr commands using DIG. What is Simon trying to accomplish here?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 37
What will the following command produce on a website login page? SELECT email, passwd, login_id, full_name FROM members WHERE email = 'someone@somehwere.com'; DROP TABLE members; --'

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 38
You setup SNMP in multiple offices of your company. Your SNMP software manager is not receiving data from other offices like it is for your main office. You suspect that firewall changes are to blame. What ports should you open for SNMP to work through Firewalls? (Choose two.)

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

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 39
You are carrying out the last round of testing for your new website before it goes live. The website has many dynamic pages and connects to a SQL backend that accesses your product inventory in a database. You come across a web security site that recommends inputting the following code into a search field on web pages to check for vulnerabilities: When you type this and click on search, you receive a pop-up window that says: "This is a test."

What is the result of this test?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 40
If an attacker's computer sends an IPID of 31400 to a zombie computer on an open port in IDLE scanning, what will be the response?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 41
Michael works for Kimball Construction Company as senior security analyst. As part of yearly security audit, Michael scans his network for vulnerabilities. Using Nmap, Michael conducts XMAS scan and most of the ports scanned do not give a response. In what state are these ports?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 42
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. Packet filtering firewall
B. Circuit-level proxy firewall
C. Application-level proxy firewall
D. Stateful firewall

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 43
Jessica works as systems administrator for a large electronics firm. She wants to scan her network quickly to detect live hosts by using ICMP ECHO Requests. What type of scan is Jessica going to perform?

A. Tracert
B. Smurf scan

C. Ping trace
D. ICMP ping sweep

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 44
You work as an IT security auditor hired by a law firm in Boston to test whether you can gain access to sensitive information about the company clients. You have rummaged through their trash and found very little information. You do not want to set off any alarms on their network, so you plan on performing passive foot printing against their Web servers. What tool should you use?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 45
You are a security analyst performing a penetration tests for a company in the Midwest. After some initial reconnaissance, you discover the IP addresses of some Cisco routers used by the company. You type in the following URL that includes the IP address of one of the routers:
http://172.168.4.131/level/99/exec/show/config

After typing in this URL, you are presented with the entire configuration file for that router. What have you discovered?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 46
What is the following command trying to accomplish?

C:> nmap –sU –p445 192.168.0.0/24

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 47
You are the network administrator for a small bank in Dallas, Texas. To ensure network security, you enact a security policy that requires all users to have 14 character passwords. After giving your users 2 weeks notice, you change the Group Policy to force 14 character passwords. A week later you dump the SAM database from the standalone server and run a password-cracking tool against it. Over 99% of the passwords are broken within an hour. Why were these passwords cracked so Quickly?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 48
An "idle" system is also referred to as what?

A. PC not connected to the Internet
B. Zombie
C. PC not being used
D. Bot

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 49
Larry is an IT consultant who works for corporations and government agencies. Larry plans on shutting down the city's network using BGP devices and zombies? What type of Penetration Testing is Larry planning to carry out?

A. Router Penetration Testing
B. DoS Penetration Testing
C. Firewall Penetration Testing
D. Internal Penetration Testing

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 50
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. Hillary network username and password hash
B. The SID of Hillary network account
C. The SAM file from Hillary computer
D. The network shares that Hillary has permissions

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 51
Bill is the accounting manager for Grummon and Sons LLC in Chicago. On a regular basis, he needs to send PDF documents containing sensitive information through E-mail to his customers.
Bill protects the PDF documents with a password and sends them to their intended recipients.
Why PDF passwords do not offer maximum protection?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 52
Meyer Electronics Systems just recently had a number of laptops stolen out of their office. On these laptops contained sensitive corporate information regarding patents and company strategies. A month after the laptops were stolen, a competing company was found to have just developed products that almost exactly duplicated products that Meyer produces. What could have prevented this information from being stolen from the laptops?

A. EFS Encryption
B. DFS Encryption
C. IPS Encryption
D. SDW Encryption

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 53
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. ATM
B. UDP
C. BPG
D. OSPF

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 54
What is the target host IP in the following command?

c:\>firewalk -F 80 10.10.150.1 172.16.28.95 -p UDP

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 55
George is a senior security analyst working for a state agency in Florida. His state's congress just passed a bill mandating every state agency to undergo a security audit annually. After learning what will be required, George needs to implement an IDS as soon as possible before the first audit occurs. The state bill requires that an IDS with a "time-based induction machine" be used.

What IDS feature must George implement to meet this requirement?

A. Signature-based anomaly detection
B. Pattern matching
C. Real-time anomaly detection
D. Statistical-based anomaly detection

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 56
John is using Firewalk to test the security of his Cisco PIX firewall. He is also utilizing a sniffer located on a subnet that resides deep inside his network. After analyzing the sniffer log files, he does not see any of the traffic produced by Firewalk. Why is that?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 57
After undergoing an external IT audit, George realizes his network is vulnerable to DDoS attacks.
What countermeasures could he take to prevent DDoS attacks?

A. Enable direct broadcasts
B. Disable direct broadcasts
C. Disable BGP
D. Enable BGP

Correct Answer: B

Section: (none)
Explanation

Explanation/Reference:

QUESTION 58
George is performing security analysis for Hammond and Sons LLC. He is testing security vulnerabilities of their wireless network. He plans on remaining as "stealthy" as possible during the scan. Why would a scanner like Nessus is not recommended in this situation?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 59
At what layer of the OSI model do routers function on?

A. 4
B. 3
C. 1
D. 5

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 60
Frank is working on a vulnerability assessment for a company on the West coast. The company hired Frank to assess its network security through scanning, pen tests, and vulnerability assessments. After discovering numerous known vulnerabilities detected by a temporary IDS he set up, he notices a number of items that show up as unknown but Questionable in the logs. He looks up the behavior on the Internet, but cannot find anything related. What organization should Frank submit the log to find out if it is a new vulnerability or not?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 61
George is the network administrator of a large Internet company on the west coast. Per corporate policy, none of the employees in the company are allowed to use FTP or SFTP programs without obtaining approval from the IT department. Few managers are using SFTP program on their computers. Before talking to his boss, George wants to have some proof of their activity. George wants to use Ethereal to monitor network traffic, but only SFTP traffic to and from his network.
What filter should George use in Ethereal?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 62
Your company uses Cisco routers exclusively throughout the network. After securing the routers to the best of your knowledge, an outside security firm is brought in to assess the network security. Although they found very few issues, they were able to enumerate the model, OS version, and capabilities for all your Cisco routers with very little effort. Which feature will you disable to eliminate the ability to enumerate this information on your Cisco routers?

A. Border Gateway Protocol
B. Cisco Discovery Protocol
C. Broadcast System Protocol
D. Simple Network Management Protocol

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 63
In Linux, what is the smallest possible shellcode?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 64
Jim performed a vulnerability analysis on his network and found no potential problems. He runs another utility that executes exploits against his system to verify the results of the vulnerability test. The second utility executes five known exploits against his network in which the vulnerability analysis said were not exploitable. What kind of results did Jim receive from his vulnerability analysis?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 65
You work as a penetration tester for Hammond Security Consultants. You are currently working on a contract for the state government of California. Your next step is to initiate a DoS attack on their network. Why would you want to initiate a DoS attack on a system you are testing?

A. Show outdated equipment so it can be replaced
B. List weak points on their network
C. Use attack as a launching point to penetrate deeper into the network
D. Demonstrate that no system can be protected against DoS attacks

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 66
Why are Linux/Unix based computers better to use than Windows computers for idle scanning?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 67
What operating system would respond to the following command?

c:\> nmap -sW 10.10.145.65

A. Windows 95
B. FreeBSD
C. Windows XP
D. Mac OS X

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 68
Paul's company is in the process of undergoing a complete security audit including logical and physical security testing. After all logical tests were performed; it is now time for the physical round to begin. None of the employees are made aware of this round of testing. The security-auditing firm sends in a technician dressed as an electrician. He waits outside in the lobby for some employees to get to work and follows behind them when they access the restricted areas. After entering the main office, he is able to get into the server room telling the IT manager that there is a problem with the outlets in that room. What type of attack has the technician performed?

A. Tailgating
B. Backtrapping

C. Man trap attack
D. Fuzzing

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 69
On Linux/Unix based Web servers, what privilege should the daemon service be run under?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 70
What will the following URL produce in an unpatched IIS Web Server?

http://www.thetargetsite.com/scripts/..% co%af../..%co%af../windows/system32/cmd.exe?/c+dir+c:\

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 71
What is kept in the following directory? HKLM\SECURITY\Policy\Secrets

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 72
Harold is a security analyst who has just run the rdisk /s command to grab the backup SAM files on a computer. Where should Harold navigate on the computer to find the file?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 73
You are trying to locate Microsoft Outlook Web Access Default Portal using Google search on the Internet. What search string will you use to locate them?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 74
When setting up a wireless network with multiple access points, why is it important to set each access point on a different channel?

A. Multiple access points can be set up on the same channel without any issues
B. Avoid over-saturation of wireless signals
C. So that the access points will work on different frequencies
D. Avoid cross talk

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 75
You are running through a series of tests on your network to check for any security vulnerabilities.
After normal working hours, you initiate a DoS attack against your external firewall. The firewall Quickly freezes up and becomes unusable. You then initiate an FTP connection from an external IP into your internal network. The connection is successful even though you have FTP blocked at the external firewall. What has happened?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 76
You just passed your ECSA exam and are about to start your first consulting job running security audits for a financial institution in Los Angeles. The IT manager of the company you will be working for tries to see if you remember your ECSA class. He asks about the methodology you will be using to test the company's network. How would you answer?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 77
Software firewalls work at which layer of the OSI model?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 78
After passing her CEH exam, Carol wants to ensure that her network is completely secure. She implements a DMZ, stateful firewall, NAT, IPSEC, and a packet filtering firewall. Since all security measures were taken, none of the hosts on her network can reach the Internet. Why is that?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 79
Jason has set up a honeypot environment by creating a DMZ that has no physical or logical access to his production network. In this honeypot, he has placed a server running Windows Active Directory. He has also placed a Web server in the DMZ that services a number of web pages that offer visitors a chance to download sensitive information by clicking on a button. A week later, Jason finds in his network logs how an intruder accessed the honeypot and downloaded sensitive information. Jason uses the logs to try and prosecute the intruder for stealing sensitive corporate information. Why will this not be viable?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 80
You have compromised a lower-level administrator account on an Active Directory network of a small company in Dallas, Texas. You discover Domain Controllers through enumeration. You connect to one of the Domain Controllers on port 389 using ldp.exe. What are you trying to accomplish here?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 81
What are the security risks of running a "repair" installation for Windows XP?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 82
Terri works for a security consulting firm that is currently performing a penetration test on First National Bank in Tokyo. Terri's duties include bypassing firewalls and switches to gain access to the network. Terri sends an IP packet to one of the company's switches with ACK bit and the source address of her machine set. What is Terri trying to accomplish by sending this IP packet?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 83
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. Competitive exploit
C. Information vulnerability
D. Trade secret

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 84
The objective of this act was to protect consumers' personal financial information held by financial institutions and their service providers.

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 85
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. To attack a network from a hacker's perspective
D. It is easier to hack from the inside

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 86
Harold is a web designer who has completed a website for ghttech.net. As part of the maintenance agreement he signed with the client, Harold is performing research online and seeing how much exposure the site has received so far. Harold navigates to google.com and types in the following search. link:www.ghttech.net What will this search produce?

A. All sites that ghttech.net links to
B. All sites that link to ghttech.net
C. All search engines that link to .net domains
D. Sites that contain the code: link:www.ghttech.net

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 87
Jonathan is a network administrator who is currently testing the internal security of his network. He is attempting to hijack a session, using Ettercap, of a user connected to his Web server. Why will Jonathan not succeed?

A. Only an HTTPS session can be hijacked
B. HTTP protocol does not maintain session
C. Only FTP traffic can be hijacked
D. Only DNS traffic can be hijacked

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 88
A packet is sent to a router that does not have the packet destination address in its route table.
How will the packet get to its proper destination?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 89
James is testing the ability of his routers to withstand DoS attacks. James sends ICMP ECHO requests to the broadcast address of his network. What type of DoS attack is James testing against his network?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 90
Kyle is performing the final testing of an application he developed for the accounting department.
His last round of testing is to ensure that the program is as secure as possible. Kyle runs the following command. What is he testing at this point?

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

A. Buffer overflow
B. SQL injection
C. Format string bug

D. Kernal injection

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 91
You are running known exploits against your network to test for possible vulnerabilities. To test the strength of your virus software, you load a test network to mimic your production network. Your software successfully blocks some simple macro and encrypted viruses. You decide to really test the software by using virus code where the code rewrites itself entirely and the signatures change from child to child, but the functionality stays the same. What type of virus is this that you are testing?

A. Polymorphic
B. Metamorphic
C. Oligomorhic
D. Transmorphic

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 92
What is a good security method to prevent unauthorized users from "tailgating"?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 93
You are the security analyst working for a private company out of France. Your current assignment is to obtain credit card information from a Swiss bank owned by that company. After initial reconnaissance, you discover that the bank security defenses are very strong and would take too long to penetrate. You decide to get the information by monitoring the traffic between the bank and one of its subsidiaries in London. After monitoring some of the traffic, you see a lot of FTP packets traveling back and forth. You want to sniff the traffic and extract usernames and passwords. What tool could you use to get this information?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 94

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

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 95
Julia is a senior security analyst for Berber Consulting group. She is currently working on a contract for a small accounting firm in Florid a. They have given her permission to perform social engineering attacks on the company to see if their in-house training did any good. Julia calls the main number for the accounting firm and talks to the receptionist. Julia says that she is an IT technician from the company's main office in Iowa. She states that she needs the receptionist's network username and password to troubleshoot a problem they are having. Julia says that Bill Hammond, the CEO of the company, requested this information. After hearing the name of the CEO, the receptionist gave Julia all the information she asked for. What principal of social engineering did Julia use?

A. Social Validation
B. Scarcity
C. Friendship/Liking
D. Reciprocation

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 96
Harold wants to set up a firewall on his network but is not sure which one would be the most appropriate. He knows he needs to allow FTP traffic to one of the servers on his network, but he wants to only allow FTP-PUT. Which firewall would be most appropriate for Harold? needs?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 97
What will the following command accomplish?

C:\ nmap -v -sS -Po <ip> -data_length 6600 0-packet_trace

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 98
What does ICMP Type 3/Code 13 mean?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 99
How many bits is Source Port Number in TCP Header packet?

A. 16
B. 32
C. 48
D. 64

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 100
In Linux OS, different log files hold different information, which help the investigators to analyze various issues during a security incident. What information can the investigators obtain from the log file var/log/dmesg?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://superuser.com/questions/565927/differences-in-var-log-syslog-dmesg-messages-log-files#:~:text=%2Fvar%2Flog%2Fdmesg%20%E2%80%93,kernel%20detects%20during%20boot%20process

QUESTION 101
Which of the following hives in Windows registry contain configuration information related to the application type that is used to open various files on the system?

A. HKEY_CURRENT_CONFIG
B. HKEY_CLASSES_ROOT
C. HKEY_CURRENT_USER

D. HKEY_LOCAL MACHINE

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: https://what-when-how.com/windows-forensic-analysis/registry-analysis-windows-forensic-analysis-part-1/#:~:text=Each%20of%20these%20hives%20plays,the%20function%20of%20the%20system.&text=The%20HKEY_CURRENT_CONFIG%20hive%20contains%20the,various%20files%20on%20the%20system

QUESTION 102
Which of these ISO standards define the file system for optical storage media, such as CD-ROM and DVD-ROM?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://en.wikipedia.org/wiki/ISO_9660#:~:text=ISO%209660%20is%20a%20file%20system%20for%20optical%20disc%20media

QUESTION 103
Which of the following Linux command searches through the current processes and lists the process IDs those match the selection criteria to stdout?

A. pstree
B. pgrep
C. ps
D. grep

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: https://askubuntu.com/questions/180336/how-to-find-the-process-id-pid-of-a-running-terminal-program

QUESTION 104
Which forensic investigation methodology believes that criminals commit crimes solely to benefit their criminal enterprises?

A. Scientific Working Group on Digital Evidence
B. Daubert Standard
C. Enterprise Theory of Investigation
D. Fyre Standard

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: https://info-savvy.com/rules-of-forensics-investigation/

QUESTION 105
Which of these rootkit detection techniques function by comparing a snapshot of the file system, boot records, or memory with a known and trusted baseline?

A. Signature-Based Detection
B. Integrity-Based Detection
C. Cross View-Based Detection
D. Heuristic/Behavior-Based Detection

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: https://info-savvy.com/anti-forensics-techniques-rootkits/

QUESTION 106
Which program uses different techniques to conceal a malware's code, thereby making it difficult for security mechanisms to detect or remove it?

A. Dropper
B. Packer
C. Injector
D. Obfuscator

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.sciencedirect.com/topics/computer-science/obfuscation-technique

QUESTION 107
What does the bytes 0x0B-0x53 represent in the boot sector of NTFS volume on Windows 2000?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: http://ntfs.com/ntfs-partition-boot-sector.htm

QUESTION 108
What does the Rule 101 of Federal Rules of Evidence states?

A. Scope of the Rules, where they can be applied
B. Purpose of the Rules
C. Limited Admissibility of the Evidence
D. Rulings on Evidence

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://law.indiana.edu/instruction/tanford/b723/02obj/R02.pdf

QUESTION 109

What document does the screenshot represent?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 110
You are asked to build a forensic lab and your manager has specifically informed you to use copper for lining the walls, ceilings, and floor. What is the main purpose of lining the walls, ceilings, and floor with copper?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://info-savvy.com/physical-security-recommendations-of-computer-forensics-lab/

QUESTION 111
James is dealing with a case regarding a cybercrime that has taken place in Arizona, USA. James needs to lawfully seize the evidence from an electronic device without affecting the user's anonymity. Which of the following law should he comply with, before retrieving the evidence?

A. First Amendment of the U.S. Constitution
B. Fourth Amendment of the U.S. Constitution

C. Third Amendment of the U.S. Constitution
D. Fifth Amendment of the U.S. Constitution

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.law.cornell.edu/constitution/fifth_amendment

QUESTION 112
Which of the following stand true for BIOS Parameter Block?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://handwiki.org/wiki/BIOS_parameter_block

QUESTION 113
Which Event Correlation approach assumes and predicts what an attacker can do next after the attack by studying statistics and probability?

A. Profile/Fingerprint-Based Approach
B. Bayesian Correlation
C. Time (Clock Time) or Role-Based Approach
D. Automated Field Correlation

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: https://info-savvy.com/summarize-the-event-correlation/#:~:text=Bayesian%20Correlation%20Approach,by%20studying%20statistics%20and%20probability

QUESTION 114
MAC filtering is a security access control methodology, where a _____ is assigned to each network card to determine access to the network.

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.geeksforgeeks.org/mac-filtering-in-computer-network/#:~:text=MAC%20filtering%20is%20a%20security,access%20a%20network%20or%20not.&text=It%20helps%20in%20preventing%20unwanted%20access%20to%20the%20network

QUESTION 115
Which of the following files store the MySQL database data permanently, including the data that had been deleted, helping the forensic investigator in examining the case and finding the culprit?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.stellarinfo.com/blog/recover-mysql-database-from-ibdata1/

QUESTION 116
Which tool allows dumping the contents of process memory without stopping the process?

A. psdump.exe
B. pmdump.exe
C. processdump.exe
D. pdump.exe

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.sciencedirect.com/topics/computer-science/memory-dump-file#:~:text=Post%20Mortem%20Dump%20or%20PMDump,analysis%20of%20a%20dump%20file

QUESTION 117
Which component in the hard disk moves over the platter to read and write information?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://cs.stanford.edu/people/nick/how-hard-drive-works/#:~:text=A%20%22head%22%20moves%20over%20the,the%20stored%200's%20and%201's