Exam Questions 312-49v10

Computer Hacking Forensic Investigator (CHFI-v10)

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

NEW QUESTION 1
- (Exam Topic 1)
It takes mismanaged case/s to ruin your professional reputation as a computer forensics examiner?

A. by law, three
B. quite a few
C. only one
D. at least two

Answer: C

NEW QUESTION 2
- (Exam Topic 1)
What will the following URL produce in an unpatched IIS Web Server? http://www.thetargetsite.com/scripts/..%co%af../..%co%af../windows/system32/cmd.exe?/c+dir+c:\

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

Answer: A

NEW QUESTION 3
- (Exam Topic 1)
John is using Firewalk to test the security of his Cisco PIX firewall. He is also utilizing a sniffer located on a subnet that resides deep inside his network. After analyzing the sniffer log files, he does not see any of the traffic produced by Firewalk. Why is that?

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

Answer: D

NEW QUESTION 4
- (Exam Topic 1)
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

Answer: A

NEW QUESTION 5
- (Exam Topic 1)
Area density refers to:

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

Answer: A

NEW QUESTION 6
- (Exam Topic 1)
The following excerpt is taken from a honeypot log. The log captures activities across three days. There are several intrusion attempts; however, a few are successful.
(Note: The objective of this question is to test whether the student can read basic information from log entries and interpret the nature of attack.)
Apr 24 14:46:46 [4663]: spp_portscan: portscan detected from 194.222.156.169
Apr 24 14:46:46 [4663]: IDS27/FIN Scan: 194.222.156.169:56693 -> 172.16.1.107:482
Apr 24 18:01:05 [4663]: IDS/DNS-version-query: 212.244.97.121:3485 -> 172.16.1.107:53
Apr 24 19:04:01 [4663]: IDS213/ftp-passwd-retrieval: 194.222.156.169:1425 -> 172.16.1.107:21
Apr 25 08:02:41 [5875]: spp_portscan: PORTSCAN DETECTED from 24.9.255.53
Apr 25 02:08:07 [5875]: IDS277/DNS-version-query: 63.226.81.13:4499 -> 172.16.1.107:53
Apr 25 02:08:07 [5875]: IDS277/DNS-version-query: 63.226.81.13:4630 -> 172.16.1.101:53
Apr 25 02:38:17 [5875]: IDS/RPC-rpcinfo-query: 212.251.1.94:642 -> 172.16.1.107:111
Apr 25 19:37:32 [5875]: IDS230/web-cgi-space-wildcard: 198.173.35.164:4221 -> 172.16.1.107:80
Apr 26 05:45:12 [6283]: IDS212/dns-zone-transfer: 38.31.107.87:2291 -> 172.16.1.101:53
Apr 26 06:43:05 [6283]: IDS181/nops-x86: 63.226.81.13:1351 -> 172.16.1.107:53
Apr 26 06:44:25 victim7 PAM_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

NEW QUESTION 7
- (Exam Topic 1)
On Linux/Unix based Web servers, what privilege should the daemon service be run under?

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

Answer: D

NEW QUESTION 8
- (Exam Topic 1)
You are working as an independent computer forensics investigator and received a call from a systems administrator for a local school system requesting your assistance. One of the students at the local high school is suspected of downloading inappropriate images from the Internet to a PC in the Computer lab. When you arrive at the school, the systems administrator hands you a hard drive and tells you that he made a “simple backup copy” of the hard drive in the PC and put it on this drive and requests that you examine that drive for evidence of the suspected images. You inform him that a “simple backup copy” will not provide deleted files or recover file fragments.
What type of copy do you need to make to ensure that the evidence found is complete and admissible in future proceeding?

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

Answer: C

NEW QUESTION 9
- (Exam Topic 1)
What TCP/UDP port does the toolkit program netstat use?

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

Answer: B

NEW QUESTION 10
- (Exam Topic 1)
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

Answer: D

NEW QUESTION 10
- (Exam Topic 1)
You are employed directly by an attorney to help investigate an alleged sexual harassment case at a large pharmaceutical manufacture. While at the corporate office of the company, the CEO demands to know the status of the investigation. What prevents you from discussing the case with the CEO?

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

Answer: A

NEW QUESTION 15
- (Exam Topic 2)
Preparing an image drive to copy files to is the first step in Linux forensics. For this purpose, what would the following command accomplish?
dcfldd if=/dev/zero of=/dev/hda bs=4096 conv=noerror, sync

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

Answer: A

NEW QUESTION 17
- (Exam Topic 2)
What technique is used by JPEGs for compression?

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

Answer: C

NEW QUESTION 21
- (Exam Topic 2)
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 is not necessary to scan the virtual memory of a computer
C. It contains the times and dates of all the system files
D. Hidden running processes

Answer: D

NEW QUESTION 26
- (Exam Topic 2)
What stage of the incident handling process involves reporting events?

A. Containment
B. Follow-up
C. Identification
D. Recovery

Answer: C

NEW QUESTION 30
- (Exam Topic 2)
What type of attack sends SYN requests to a target system with spoofed IP addresses?

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

Answer: A

NEW QUESTION 35
- (Exam Topic 2)
Which of the following commands shows you the names of all open shared files on a server and the number of file locks on each file?

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

Answer: B

NEW QUESTION 36
- (Exam Topic 2)
Amber, a black hat hacker, has embedded a malware into a small enticing advertisement and posted it on a popular ad-network that displays across various websites. What is she doing?

A. Click-jacking
B. Compromising a legitimate site
C. Spearphishing
D. Malvertising

Answer: D

NEW QUESTION 40
- (Exam Topic 1)
From the following spam mail header, identify the host IP that sent this spam? From jie02@netvigator.com jie02@netvigator.com Tue Nov 27 17:27:11 2001
Received: from viruswall.ie.cuhk.edu.hk (viruswall [137.189.96.52]) by eng.ie.cuhk.edu.hk (8.11.6/8.11.6) with ESMTP id
fAR9RAP23061 for ; Tue, 27 Nov 2001 17:27:10 +0800 (HKT)
Received: from mydomain.com (pcd249020.netvigator.com [203.218.39.20]) by viruswall.ie.cuhk.edu.hk (8.12.1/8.12.1)
with SMTP id fAR9QXwZ018431 for ; Tue, 27 Nov 2001 17:26:36 +0800 (HKT)
Message-Id: >200111270926.fAR9QXwZ018431@viruswall.ie.cuhk.edu.hk From: "china hotel web"
To: "Shlam"
Subject: SHANGHAI (HILTON HOTEL) PACKAGE
Date: Tue, 27 Nov 2001 17:25:58 +0800 MIME-Version: 1.0
X- Priority: 3 X-MSMail- Priority: Normal
Reply-To: "china hotel web"

A. 137.189.96.52
B. 8.12.1.0
C. 203.218.39.20
D. 203.218.39.50

Answer: C

NEW QUESTION 42
- (Exam Topic 1)
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 to work
B. Right of free speech
C. Right to Internet Access
D. Right of Privacy

Answer: D

NEW QUESTION 45
- (Exam Topic 1)
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

Answer: C

NEW QUESTION 46
- (Exam Topic 1)
When an investigator contacts by telephone the domain administrator or controller listed by a Who is lookup to request all e-mails sent and received for a user account be preserved, what U.S.C. statute authorizes this phone call and obligates the ISP to preserve e-mail records?

A. Title 18, Section 1030
B. Title 18, Section 2703(d)
C. Title 18, Section Chapter 90
D. Title 18, Section 2703(f)

Answer: D

NEW QUESTION 48
- (Exam Topic 1)
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

Answer: D

NEW QUESTION 51
- (Exam Topic 1)
If a suspect computer is located in an area that may have toxic chemicals, you must:

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

Answer: A

NEW QUESTION 56
- (Exam Topic 1)
In the context of file deletion process, which of the following statement holds true?

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

Answer: C

NEW QUESTION 59
- (Exam Topic 1)
What does the acronym POST mean as it relates to a PC?

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

Answer: B

NEW QUESTION 61
- (Exam Topic 1)
You are conducting an investigation of fraudulent claims in an insurance company that involves complex text searches through large numbers of documents. Which of the following tools would allow you to quickly and efficiently search for a string within a file on the bitmap image of the target computer?

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

Answer: B

NEW QUESTION 66
- (Exam Topic 1)
As a security analyst, you setup a false survey website that will require users to create a username and a strong password. You send the link to all the employees of the company. What information will you be able to gather?

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

Answer: C

NEW QUESTION 68
- (Exam Topic 1)
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

Answer: D

NEW QUESTION 70
- (Exam Topic 1)
After passively scanning the network of Department of Defense (DoD), you switch over to active scanning to identify live hosts on their network. DoD is a large organization and should respond to any number of scans. You start an ICMP ping sweep by sending an IP packet to the broadcast address. Only five hosts respond to your ICMP pings; definitely not the number of hosts you were expecting. Why did this ping sweep only produce a few responses?

A. Only IBM AS/400 will reply to this scan
B. Only Windows systems will reply to this scan
C. A switched network will not respond to packets sent to the broadcast address
D. Only Unix and Unix-like systems will reply to this scan

Answer: D

NEW QUESTION 72
- (Exam Topic 1)

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

Answer: B

NEW QUESTION 74
- (Exam Topic 1)
You are the network administrator for a small bank in Dallas, Texas. To ensure network security, you enact a security policy that requires all users to have 14 character passwords. After giving your users 2 weeks notice, you change the Group Policy to force 14 character passwords. A week later you dump the SAM database from the standalone server and run a password-cracking tool against it. Over 99% of the passwords are broken within an hour. Why were these passwords cracked so Quickly?

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

Answer: A

NEW QUESTION 79
- (Exam Topic 1)
You are a computer forensics investigator working with local police department and you are called to assist in an investigation of threatening emails. The complainant has printer out 27 email messages from the suspect and gives the printouts to you. You inform her that you will need to examine her computer because you need access to the in order to track the emails back to the suspect.

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

Answer: D

NEW QUESTION 83
- (Exam Topic 1)
In Linux, what is the smallest possible shellcode?

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

Answer: A

NEW QUESTION 87
- (Exam Topic 1)
Profiling is a forensics technique for analyzing evidence with the goal of identifying the perpetrator from their various activity. After a computer has been compromised by a hacker, which of the following would be most important in forming a profile of the incident?

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

Answer: B

NEW QUESTION 89
- (Exam Topic 1)
A(n) is one that's performed by a computer program rather than the attacker manually performing the steps in the attack sequence.

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

Answer: B

NEW QUESTION 91
- (Exam Topic 1)
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. The system files have been copied by a remote attacker
B. The system administrator has created an incremental backup
C. The system has been compromised using a t0rnrootkit

D. Nothing in particular as these can be operational files

Answer: D

NEW QUESTION 93
- (Exam Topic 1)
During the course of a corporate investigation, you find that an Employee is committing a crime. Can the Employer file a criminal complaint with Police?

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

Answer: A

NEW QUESTION 95
- (Exam Topic 1)
You are called in to assist the police in an investigation involving a suspected drug dealer. The suspects house was searched by the police after a warrant was obtained and they located a floppy disk in the suspects bedroom. The disk contains several files, but they appear to be password protected. What are two common methods used by password cracking software that you can use to obtain the password?

A. Limited force and library attack
B. Brute Force and dictionary Attack
C. Maximum force and thesaurus Attack
D. Minimum force and appendix Attack

Answer: B

NEW QUESTION 99
- (Exam Topic 1)
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

Answer: A

NEW QUESTION 104
- (Exam Topic 1)
John and Hillary works at the same department in the company. John wants to find out Hillary's network password so he can take a look at her documents on the file server. He enables 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

Answer: A

NEW QUESTION 107
- (Exam Topic 1)
How many characters long is the fixed-length MD5 algorithm checksum of a critical system file?

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

Answer: C

NEW QUESTION 109
- (Exam Topic 1)
Bob has 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 recoding his every activity and this was later presented as evidence.
The organization had used a Virtual Environment to trap Bob. What is a Virtual Environment?

A. A Honeypot that traps hackers
B. A system Using Trojaned commands
C. An environment set up after the user logs in
D. An environment set up before a user logs in

Answer: A

NEW QUESTION 111
- (Exam Topic 1)
What type of file is represented by a colon (:) with a name following it in the Master File Table of NTFS disk?

A. A compressed file
B. A Data stream file
C. An encrypted file
D. A reserved file

Answer: B

NEW QUESTION 115
- (Exam Topic 1)
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

Answer: B

NEW QUESTION 116
- (Exam Topic 1)
Jim performed a vulnerability analysis on his network and found no potential problems. He runs another utility that executes exploits against his system to verify the results of the vulnerability test.
The second utility executes five known exploits against his network in which the vulnerability analysis said were not exploitable. What kind of results did Jim receive from his vulnerability analysis?

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

Answer: A

NEW QUESTION 119
- (Exam Topic 1)
What header field in the TCP/IP protocol stack involves the hacker exploit known as the Ping of Death?

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

Answer: B

NEW QUESTION 122
- (Exam Topic 1)
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

Answer: D

NEW QUESTION 127
- (Exam Topic 4)
When Investigating a system, the forensics analyst discovers that malicious scripts were Injected Into benign and trusted websites. The attacker used a web application to send malicious code. In the form of a browser side script, to a different end-user. What attack was performed here?

A. Brute-force attack
B. Cookie poisoning attack
C. Cross-site scripting attack
D. SQL injection attack

Answer: C

NEW QUESTION 131
- (Exam Topic 4)
An investigator Is examining a file to identify any potentially malicious content. To avoid code execution and still be able to uncover hidden indicators of

compromise (IOC), which type of examination should the investigator perform:

A. Threat hunting
B. Threat analysis
C. Static analysis
D. Dynamic analysis

Answer: B

NEW QUESTION 132
- (Exam Topic 4)
A forensic analyst has been tasked with investigating unusual network activity Inside a retail company's network. Employees complain of not being able to access services, frequent rebooting, and anomalies In log files. The Investigator requested log files from the IT administrator and after carefully reviewing them, he finds the following log entry:

```
12:34:35 192.2.3.4 HEAD GET /login.asp?username=blah" or 1=1 – 12:34:35 192.2.3.4 HEAD GET
/login.asp?username=blah"  or )1=1  (--  12:34:35 192.2.3.4  HEAD  GET
/login.asp?username+blah" or exec master..xp_cmdshell 'net user test testpass - -
```

What type of attack was performed on the companies' web application?

A. Directory transversal
B. Unvalidated input
C. Log tampering
D. SQL injection

Answer: D

NEW QUESTION 136
- (Exam Topic 4)
Which of the following tools will allow a forensic Investigator to acquire the memory dump of a suspect machine so that It may be Investigated on a forensic workstation to collect evidentiary data like processes and Tor browser artifacts?

A. DB Browser SQLite
B. Bulk Extractor
C. Belkasoft Live RAM Capturer and AccessData FTK imager
D. Hex Editor

Answer: C

NEW QUESTION 138
- (Exam Topic 4)
In Java, when multiple applications are launched, multiple Dalvik Virtual Machine instances occur that consume memory and time. To avoid that. Android Implements a process that enables low memory consumption and quick start-up time. What is the process called?

A. init
B. Media server
C. Zygote
D. Daemon

Answer: C

NEW QUESTION 141
- (Exam Topic 4)
On NTFS file system, which of the following tools can a forensic Investigator use In order to identify timestomping of evidence files?

A. wbStego
B. Exiv2
C. analyzeMFT
D. Timestomp

Answer: D

NEW QUESTION 143
- (Exam Topic 4)
Which set of anti-forensic tools/techniques allows a program to compress and/or encrypt an executable file to hide attack tools from being detected by reverse-engineering or scanning?

A. Packers
B. Emulators
C. Password crackers
D. Botnets

Answer: A

NEW QUESTION 144
- (Exam Topic 4)

Which of the following statements pertaining to First Response is true?

A. First Response is a part of the investigation phase
B. First Response is a part of the post-investigation phase
C. First Response is a part of the pre-investigation phase
D. First Response is neither a part of pre-investigation phase nor a part of investigation phas
E. It only involves attending to a crime scene first and taking measures that assist forensic investigators in executing their tasks in the investigation phase more efficiently

Answer: A

NEW QUESTION 145
- (Exam Topic 4)
A call detail record (CDR) provides metadata about calls made over a phone service. From the following data fields, which one Is not contained in a CDR.

A. The call duration
B. A unique sequence number identifying the record
C. The language of the call
D. Phone number receiving the call

Answer: C

NEW QUESTION 149
- (Exam Topic 4)
Cybercriminals sometimes use compromised computers to commit other crimes, which may involve using computers or networks to spread malware or Illegal Information. Which type of cybercrime stops users from using a device or network, or prevents a company from providing a software service to its customers?

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

Answer: C

NEW QUESTION 152
- (Exam Topic 4)
Which of the following is the most effective tool for acquiring volatile data from a Windows-based system?

A. Coreography
B. Datagrab
C. Ethereal
D. Helix

Answer: D

NEW QUESTION 153
- (Exam Topic 4)
Which of the following directory contains the binary files or executables required for system maintenance and administrative tasks on a Linux system?

A. /sbin
B. /bin
C. /usr
D. /lib

Answer: A

NEW QUESTION 155
- (Exam Topic 4)
Assume there Is a file named myflle.txt In C: drive that contains hidden data streams. Which of the following commands would you Issue to display the contents of a data stream?

A. echo text > program: source_file
B. myfile.dat: st ream 1
C. C:\MORE < myfile.txt:siream1
D. C:\>ECHO text_message > myfile.txt:stream1

Answer: A

NEW QUESTION 158
- (Exam Topic 4)
"To ensure that the digital evidence is collected, preserved, examined, or transferred In a manner safeguarding the accuracy and reliability of the evidence, law enforcement, and forensics organizations must establish and maintain an effective quality system" Is a principle established by:

A. NCIS
B. NIST
C. EC-Council
D. SWGDE

Answer: B

NEW QUESTION 162
- (Exam Topic 4)
Which following forensic tool allows investigator to detect and extract hidden streams on NTFS drive?

A. Stream Detector
B. TimeStomp
C. Autopsy
D. analyzeMFT

Answer: A

NEW QUESTION 167
- (Exam Topic 4)
Harry has collected a suspicious executable file from an infected system and seeks to reverse its machine code to Instructions written in assembly language. Which tool should he use for this purpose?

A. Ollydbg
B. oledump
C. HashCalc
D. BinText

Answer: A

NEW QUESTION 169
- (Exam Topic 4)
A cybercriminal is attempting to remove evidence from a Windows computer. He deletes the file evldence1.doc. sending it to Windows Recycle Bin. The cybercriminal then empties the Recycle Bin. After having been removed from the Recycle Bin. what will happen to the data?

A. The data will remain in its original clusters until it is overwritten
B. The data will be moved to new clusters in unallocated space
C. The data will become corrupted, making it unrecoverable
D. The data will be overwritten with zeroes

Answer: A

NEW QUESTION 174
- (Exam Topic 4)
Which layer in the loT architecture is comprised of hardware parts such as sensors, RFID tags, and devices that play an important role in data collection?

A. Middleware layer
B. Edge technology layer
C. Application layer
D. Access gateway layer

Answer: B

NEW QUESTION 176
- (Exam Topic 4)
Williamson is a forensic investigator. While investigating a case of data breach at a company, he is maintaining a document that records details such as the forensic processes applied on the collected evidence, particulars of people handling It. the dates and times when it Is being handled, and the place of storage of the evidence. What do you call this document?

A. Consent form
B. Log book
C. Authorization form
D. Chain of custody

Answer: D

NEW QUESTION 177
- (Exam Topic 4)
Which among the following acts has been passed by the U.S. Congress to protect investors from the possibility of fraudulent accounting activities by corporations?

A. Federal Information Security Management act of 2002
B. Gramm-Leach-Bliley act
C. Health insurance Probability and Accountability act of 1996
D. Sarbanes-Oxley act of 2002

Answer: D

NEW QUESTION 178
- (Exam Topic 4)
Chloe is a forensic examiner who is currently cracking hashed passwords for a crucial mission and hopefully solve the case. She is using a lookup table used for

recovering a plain text password from cipher text; it contains word list and brute-force list along with their computed hash values. Chloe Is also using a graphical generator that supports SHA1.
* a. What password technique is being used?
* b. What tool is Chloe using?

A. Dictionary attack
B. Cisco PIX
C. Cain & Able
D. Rten
E. Brute-force
F. MScache
G. Rainbow Tables
H. Winrtgen

Answer: D

NEW QUESTION 182
- (Exam Topic 4)
Edgar is part of the FBI's forensic media and malware analysis team; he Is analyzing a current malware and Is conducting a thorough examination of the suspect system, network, and other connected devices. Edgar's approach Is to execute the malware code to know how It Interacts with the host system and Its Impacts on It. He is also using a virtual machine and a sandbox environment.
What type of malware analysis is Edgar performing?

A. Malware disassembly
B. VirusTotal analysis
C. Static analysis
D. Dynamic malware analysis/behavioral analysis

Answer: D

NEW QUESTION 187
- (Exam Topic 4)
Consider a scenario where the perpetrator of a dark web crime has unlnstalled Tor browser from their computer after committing the crime. The computer has been seized by law enforcement so they can Investigate It for artifacts of Tor browser usage. Which of the following should the Investigators examine to establish the use of Tor browser on the suspect machine?

A. Swap files
B. Files in Recycle Bin
C. Security logs
D. Prefetch files

Answer: A

NEW QUESTION 190
- (Exam Topic 4)
Which of the following attacks refers to unintentional download of malicious software via the Internet? Here, an attacker exploits flaws in browser software to install malware merely by the user visiting the malicious website.

A. Malvertising
B. Internet relay chats
C. Drive-by downloads
D. Phishing

Answer: C

NEW QUESTION 195
- (Exam Topic 4)
Recently, an Internal web app that a government agency utilizes has become unresponsive, Betty, a network engineer for the government agency, has been tasked to determine the cause of the web application's unresponsiveness. Betty launches Wlreshark and begins capturing the traffic on the local network. While analyzing the results, Betty noticed that a syn flood attack was underway. How did Betty know a syn flood attack was occurring?

A. Wireshark capture shows multiple ACK requests and SYN responses from single/multiple IP address(es)
B. Wireshark capture does not show anything unusual and the issue is related to the web application
C. Wireshark capture shows multiple SYN requests and RST responses from single/multiple IP address(es)
D. Wireshark capture shows multiple SYN requests and ACK responses from single/multiple IP address(es)

Answer: C

NEW QUESTION 200
- (Exam Topic 4)
"In exceptional circumstances, where a person finds it necessary to access original data held on a computer or on storage media, that person must be competent to do so and be able to explain his/her actions and the impact of those actions on the evidence, in the court." Which ACPO principle states this?

A. Principle 1
B. Principle 3
C. Principle 4
D. Principle 2

Answer: D

NEW QUESTION 205
- (Exam Topic 4)
Place the following In order of volatility from most volatile to the least volatile.

A. Registers and cache, routing tables, temporary file systems, disk storage, archival media
B. Register and cache, temporary file systems, routing tables, disk storage, archival media
C. Registers and cache, routing tables, temporary file systems, archival media, disk storage
D. Archival media, temporary file systems, disk storage, archival media, register and cache

Answer: B

NEW QUESTION 209
- (Exam Topic 4)
A computer forensics Investigator or forensic analyst Is a specially trained professional who works with law enforcement as well as private businesses to retrieve Information from computers and other types of data storage devices. For this, the analyst should have an excellent working knowledge of all aspects of the computer. Which of the following is not a duty of the analyst during a criminal investigation?

A. To create an investigation report
B. To fill the chain of custody
C. To recover data from suspect devices
D. To enforce the security of all devices and software in the scene

Answer: D

NEW QUESTION 210
- (Exam Topic 4)
Debbie has obtained a warrant to search a known pedophiles house. Debbie went to the house and executed the search warrant to seize digital devices that have been recorded as being used for downloading Illicit Images. She seized all digital devices except a digital camera. Why did she not collect the digital camera?

A. The digital camera was not listed as one of the digital devices in the warrant
B. The vehicle Debbie was using to transport the evidence was already full and could not carry more items
C. Debbie overlooked the digital camera because it is not a computer system
D. The digital camera was ol
E. had a cracked screen, and did not have batterie
F. Therefore, it could not have been used in a crime.

Answer: A

NEW QUESTION 214
- (Exam Topic 4)
In forensics. are used lo view stored or deleted data from both files and disk sectors.

A. Hash algorithms
B. SI EM tools
C. Host interfaces
D. Hex editors

Answer: D

NEW QUESTION 218
- (Exam Topic 4)
Choose the layer in iOS architecture that provides frameworks for iOS app development?

A. Media services
B. Cocoa Touch
C. Core services
D. Core OS

Answer: C

NEW QUESTION 220
- (Exam Topic 4)
Data density of a disk drive is calculated by using

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

Answer: D

NEW QUESTION 223
- (Exam Topic 3)

Which of the following Android libraries are used to render 2D (SGL) or 3D (OpenGL/ES) graphics content to the screen?

A. OpenGL/ES and SGL
B. Surface Manager
C. Media framework
D. WebKit

Answer: A

NEW QUESTION 225
- (Exam Topic 3)
You are assigned a task to examine the log files pertaining to MyISAM storage engine. While examining, you are asked to perform a recovery operation on a MyISAM log file. Which among the following MySQL Utilities allow you to do so?

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

Answer: C

NEW QUESTION 226
- (Exam Topic 3)
Which list contains the most recent actions performed by a Windows User?

A. MRU
B. Activity
C. Recents
D. Windows Error Log

Answer: A

NEW QUESTION 227
- (Exam Topic 3)
Which cloud model allows an investigator to acquire the instance of a virtual machine and initiate the forensics examination process?

A. PaaS model
B. IaaS model
C. SaaS model
D. SecaaS model

Answer: B

NEW QUESTION 229
- (Exam Topic 3)
Which of the following file system uses Master File Table (MFT) database to store information about every file and directory on a volume?

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

Answer: D

NEW QUESTION 230
- (Exam Topic 3)
What do you call the process of studying the changes that have taken place across a system or a machine after a series of actions or incidents?

A. Windows Services Monitoring
B. System Baselining
C. Start-up Programs Monitoring
D. Host integrity Monitoring

Answer: D

NEW QUESTION 231
- (Exam Topic 3)
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. Administrative Investigation
B. Criminal Investigation
C. Both Criminal and Administrative Investigation
D. Civil Investigation

Answer: B

NEW QUESTION 234
- (Exam Topic 3)
Hard disk data addressing is a method of allotting addresses to each of data on a hard disk.

A. Physical block
B. Operating system block
C. Hard disk block
D. Logical block

Answer: A

NEW QUESTION 239
- (Exam Topic 3)
Which of these Windows utility help you to repair logical file system errors?

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

Answer: D

NEW QUESTION 244
- (Exam Topic 3)
Amber, a black hat hacker, has embedded malware into a small enticing advertisement and posted it on a popular ad-network that displays across various websites. What is she doing?

A. Malvertising
B. Compromising a legitimate site
C. Click-jacking
D. Spearphishing

Answer: A

NEW QUESTION 249
- (Exam Topic 3)
Which forensic investigation methodology believes that criminals commit crimes solely to benefit their criminal enterprises?

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

Answer: C

NEW QUESTION 254
- (Exam Topic 3)
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. Non-Disclosure Agreement
D. Service Level Agreement

Answer: B

NEW QUESTION 258
- (Exam Topic 3)
Andie, a network administrator, suspects unusual network services running on a windows system. Which of the following commands should he use to verify unusual network services started on a Windows system?

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

Answer: D

NEW QUESTION 261
- (Exam Topic 3)
Which of the following is a non-zero data that an application allocates on a hard disk cluster in systems running on Windows OS?

A. Sparse File
B. Master File Table
C. Meta Block Group

D. Slack Space

Answer: B

NEW QUESTION 265
- (Exam Topic 3)
%3cscript%3ealert(”XXXXXXXX”)%3c/script%3e is a script obtained from a Cross-Site Scripting attack.
What type of encoding has the attacker employed?

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

Answer: B

NEW QUESTION 267
- (Exam Topic 3)
What is an investigator looking for in the rp.log file stored in a system running on Windows 10 operating system?

A. Restore point interval
B. Automatically created restore points
C. System CheckPoints required for restoring
D. Restore point functions

Answer: C

NEW QUESTION 269
- (Exam Topic 3)
In which registry does the system store the Microsoft security IDs?

A. HKEY_CLASSES_ROOT (HKCR)
B. HKEY_CURRENT_CONFIG (HKCC)
C. HKEY_CURRENT_USER (HKCU)
D. HKEY_LOCAL_MACHINE (HKLM)

Answer: D

NEW QUESTION 274
- (Exam Topic 3)
An investigator enters the command sqlcmd -S WIN-CQQMK62867E -e -s"," -E as part of collecting the primary data file and logs from a database. What does the "WIN-CQQMK62867E” represent?

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

Answer: B

NEW QUESTION 278
- (Exam Topic 3)
Which of the following ISO standard defines file systems and protocol for exchanging data between optical disks?

A. ISO 9660
B. ISO/IEC 13940
C. ISO 9060
D. IEC 3490

Answer: A

NEW QUESTION 280
- (Exam Topic 3)
When a user deletes a file, the system creates a $I file to store its details. What detail does the $I file not contain?

A. File Size
B. File origin and modification
C. Time and date of deletion
D. File Name

Answer: B

NEW QUESTION 285
- (Exam Topic 3)
Steve, a forensic investigator, was asked to investigate an email incident in his organization. The organization has Microsoft Exchange Server deployed for email

communications. Which among the following files will Steve check to analyze message headers, message text, and standard attachments?

A. PUB.EDB
B. PRIV.EDB
C. PUB.STM
D. PRIV.STM

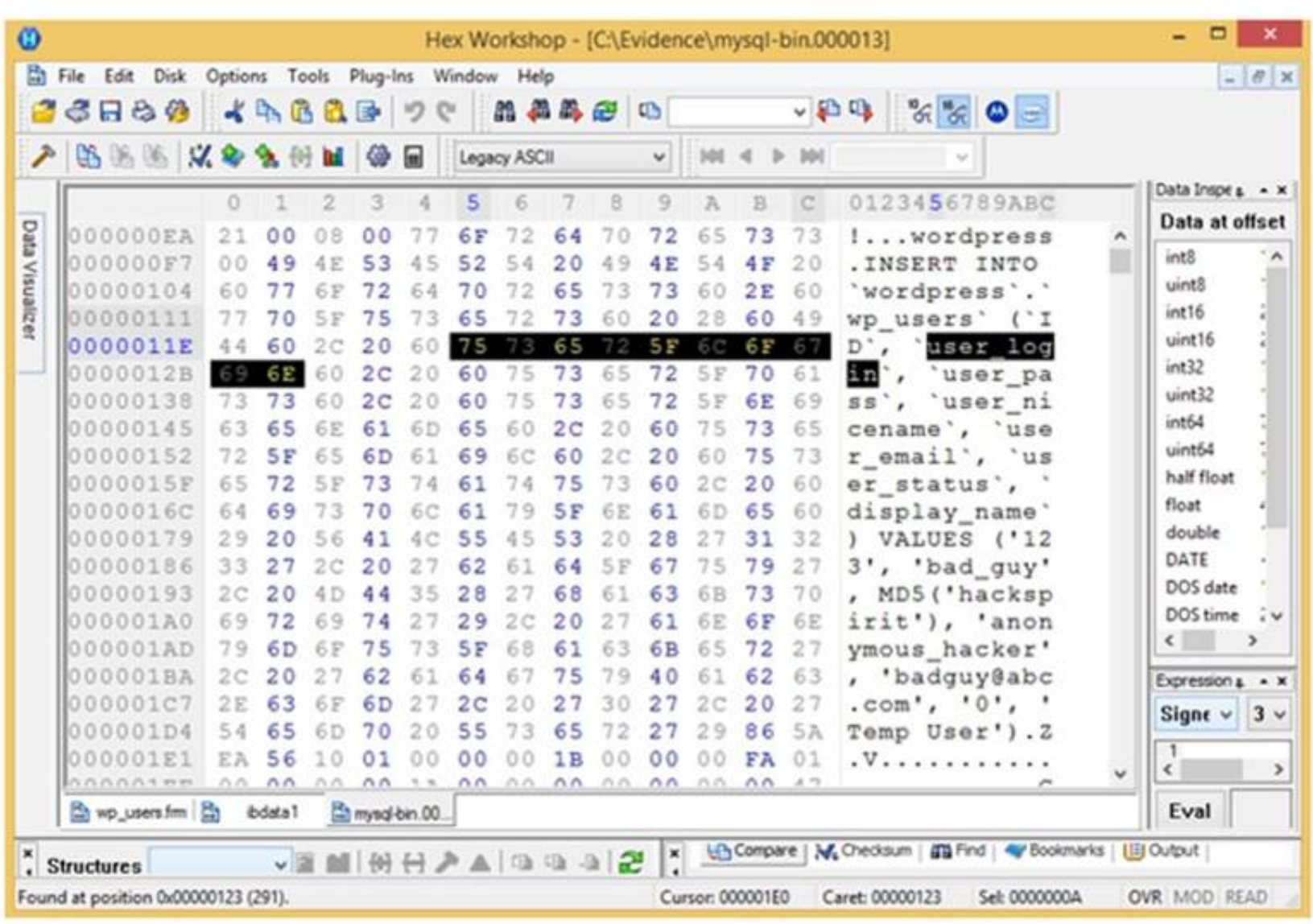
Answer: B

NEW QUESTION 287
- (Exam Topic 3)
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. .cbl
B. .log
C. .ibl
D. .txt

Answer: C

NEW QUESTION 288
- (Exam Topic 3)
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

Answer: D

NEW QUESTION 293
- (Exam Topic 3)
What is the framework used for application development for iOS-based mobile devices?

A. Cocoa Touch
B. Dalvik
C. Zygote
D. AirPlay

Answer: A

NEW QUESTION 296
- (Exam Topic 3)

Which among the following web application threats is resulted when developers expose various internal implementation objects, such as files, directories, database records, or key-through references?

A. Remote File Inclusion
B. Cross Site Scripting
C. Insecure Direct Object References
D. Cross Site Request Forgery

Answer: C

NEW QUESTION 297
- (Exam Topic 3)
What value of the "Boot Record Signature" is used to indicate that the boot-loader exists?

A. AA55
B. 00AA
C. AA00
D. A100

Answer: A

NEW QUESTION 298
- (Exam Topic 3)
When analyzing logs, it is important that the clocks of all the network devices are synchronized. Which protocol will help in synchronizing these clocks?

A. UTC
B. PTP
C. Time Protocol
D. NTP

Answer: D

NEW QUESTION 299
- (Exam Topic 3)
Which among the following tools can help a forensic investigator to access the registry files during postmortem analysis?

A. RegistryChangesView
B. RegDIIView
C. RegRipper
D. ProDiscover

Answer: C

NEW QUESTION 304
- (Exam Topic 3)
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

Answer: B

NEW QUESTION 307
- (Exam Topic 3)
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: B

NEW QUESTION 311
- (Exam Topic 3)
Which of the following is a federal law enacted in the US to control the ways that financial institutions deal with the private information of individuals?

A. SOX
B. HIPAA 1996
C. GLBA
D. PCI DSS

Answer: C

NEW QUESTION 314
- (Exam Topic 3)
Which of the following is NOT an anti-forensics technique?

A. Data Deduplication
B. Password Protection
C. Encryption
D. Steganography

Answer: A

NEW QUESTION 319
- (Exam Topic 3)
While analyzing a hard disk, the investigator finds that the file system does not use UEFI-based interface. Which of the following operating systems is present on the hard disk?

A. Windows 10

B. Windows 8
C. Windows 7
D. Windows 8.1

Answer: C

NEW QUESTION 324
- (Exam Topic 3)
Lynne receives the following email:
Dear lynne@gmail.com! We are sorry to inform you that your ID has been temporarily frozen due to incorrect or missing information saved at 2016/11/10 20:40:24
You have 24 hours to fix this problem or risk to be closed permanently! To proceed Please Connect >> My Apple ID
Thank You The link to My Apple ID shows http://byggarbetsplatsen.se/backup/signon/ What type of attack is this?

A. Mail Bombing
B. Phishing
C. Email Spamming
D. Email Spoofing

Answer: B

NEW QUESTION 327
- (Exam Topic 3)
To reach a bank web site, the traffic from workstations must pass through a firewall. You have been asked to review the firewall configuration to ensure that workstations in network 10.10.10.0/24 can only reach the bank web site 10.20.20.1 using https. Which of the following firewall rules meets this requirement?

A. if (source matches 10.10.10.0/24 and destination matches 10.20.20.1 and port matches 443) then permit
B. if (source matches 10.10.10.0/24 and destination matches 10.20.20.1 and port matches 80 or 443) then permit
C. if (source matches 10.10.10.0 and destination matches 10.20.20.1 and port matches 443) then permit

Answer: A

NEW QUESTION 328
- (Exam Topic 3)
Examination of a computer by a technically unauthorized person will almost always result in:

A. Rendering any evidence found inadmissible in a court of law
B. Completely accurate results of the examination
C. The chain of custody being fully maintained
D. Rendering any evidence found admissible in a court of law

Answer: A

NEW QUESTION 331
- (Exam Topic 3)
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. http://victim.com/scripts/..%c0%af../..%c0%af../..%c0%af../..%c0%af../..%c0%af../..%c0%af../..%c0%af../..%c0%af../winnt/system32/cmd.exe?/c+dir+C:\Winnt\system32\Logfiles\W3SVC1
B. [Wed Oct 11 14:32:52 2000] [error] [client 127.0.0.1] client denied by server configuration:/export/home/live/ap/htdocs/test
C. 127.0.0.1 - frank [10/Oct/2000:13:55:36 -0700]"GET /apache_pb.gif HTTP/1.0" 200 2326
D. 127.0.0.1 - - [10/Apr/2007:10:39:11 +0300]] [error] "GET /apache_pb.gif HTTP/1.0" 200 2326

Answer: B

NEW QUESTION 334
- (Exam Topic 3)
Select the tool appropriate for finding the dynamically linked lists of an application or malware.

A. SysAnalyzer
B. ResourcesExtract
C. PEiD
D. Dependency Walker

Answer: D

NEW QUESTION 338
- (Exam Topic 3)
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. Identifying file obfuscation
C. Static analysis
D. Dynamic analysis

Answer: A

NEW QUESTION 340
- (Exam Topic 3)
Which of the following is NOT a physical evidence?

A. Removable media
B. Cables
C. Image file on a hard disk
D. Publications

Answer: C

NEW QUESTION 345
- (Exam Topic 3)
An attacker successfully gained access to a remote Windows system and plans to install persistent backdoors on it. Before that, to avoid getting detected in future, he wants to cover his tracks by disabling the
last-accessed timestamps of the machine. What would he do to achieve this?

A. Set the registry value of HKLM\SYSTEM\CurrentControlSet\Control\FileSystem\NtfsDisableLastAccessUpdate to 0
B. Run the command fsutil behavior set disablelastaccess 0
C. Set the registry value of HKLM\SYSTEM\CurrentControlSet\Control\FileSystem\NtfsDisableLastAccessUpdate to 1
D. Run the command fsutil behavior set enablelastaccess 0

Answer: C

NEW QUESTION 349
- (Exam Topic 3)
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. Encrypted FEK
B. Checksum
C. EFS Certificate Hash
D. Container Name

Answer: B

NEW QUESTION 353
- (Exam Topic 2)
Which password cracking technique uses every possible combination of character sets?

A. Rainbow table attack
B. Brute force attack
C. Rule-based attack
D. Dictionary attack

Answer: B

NEW QUESTION 355
- (Exam Topic 2)
Smith, a forensic examiner, was analyzing a hard disk image to find and acquire deleted sensitive files. He stumbled upon a $Recycle.Bin folder in the root directory of the disk. Identify the operating system in use.

A. Windows 98
B. Linux
C. Windows 8.1
D. Windows XP

Answer: D

NEW QUESTION 359
- (Exam Topic 2)
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: $Recycled.Bin
B. C: \$Recycle.Bin
C. C:\RECYCLER
D. C:\$RECYCLER

Answer: B

NEW QUESTION 363
- (Exam Topic 2)
What must an investigator do before disconnecting an iPod from any type of computer?

A. Unmount the iPod
B. Mount the iPod

C. Disjoin the iPod
D. Join the iPod

Answer: A

NEW QUESTION 365
- (Exam Topic 2)
In the following email header, where did the email first originate from?

```
Microsoft Mail Internet Headers Version 2.0
Received: from smtp1.somedomain.com ([199.190.129.133]) by somedomain.com
with Microsoft SMTPSVC(6.0.3790.1830);
         Fri, 1 Jun 2007 09:43:08 -0500
Received: from david1.state.us.gov.us (david1.state.ok.gov [172.16.28.115])
        by smtp1.somedomain.com (8.13.1/8.12.11) with ESMTP id l51EfCEh032241
        for <someone@somedomain.com>; Fri, 1 Jun 2007 09:41:13 -0500
Received: from simon1.state.ok.gov.us ([172.18.0.199]) by
david1.state.ok.gov.us with Microsoft SMTPSVC(6.0.3790.1830);
         Fri, 1 Jun 2007 09:41:13 -0500
X-Ninja-PIM: Scanned by Ninja
X-Ninja-AttachmentFiltering: (no action)
X-MimeOLE: Produced By Microsoft Exchange V6.5.7235.2
Content-class: urn:content-classes:message
Return-Receipt-To: "Johnson, Jimmy" <jimmy@somewherelese.com>
MIME-Version: 1.0
```

A. Somedomain.com
B. Smtp1.somedomain.com
C. Simon1.state.ok.gov.us
D. David1.state.ok.gov.us

Answer: C

NEW QUESTION 369
- (Exam Topic 2)
What type of analysis helps to identify the time and sequence of events in an investigation?

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

Answer: D

NEW QUESTION 372
- (Exam Topic 2)
When a router receives an update for its routing table, what is the metric value change to that path?

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

Answer: C

NEW QUESTION 373
- (Exam Topic 2)
Using Internet logging software to investigate a case of malicious use of computers, the investigator comes across some entries that appear odd.

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

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

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

Answer: A

NEW QUESTION 376
- (Exam Topic 2)
The investigator wants to examine changes made to the system's registry by the suspect program. Which of the following tool can help the investigator?

A. TRIPWIRE
B. RAM Capturer
C. Regshot
D. What's Running

Answer: C

NEW QUESTION 378
- (Exam Topic 2)
After attending a CEH security seminar, you make a list of changes you would like to perform on your network to increase its security. One of the first things you change is to switch the RestrictAnonymous setting from 0 to 1 on your servers. This, as you were told, would prevent anonymous users from establishing a null session on the server. Using Userinfo tool mentioned at the seminar, you succeed in establishing a null session with one of the servers. Why is that?

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

Answer: C

NEW QUESTION 382
- (Exam Topic 2)
Charles has accidentally deleted an important file while working on his Mac computer. He wants to recover the deleted file as it contains some of his crucial business secrets. Which of the following tool will help Charles?

A. Xplico
B. Colasoft's Capsa
C. FileSalvage
D. DriveSpy

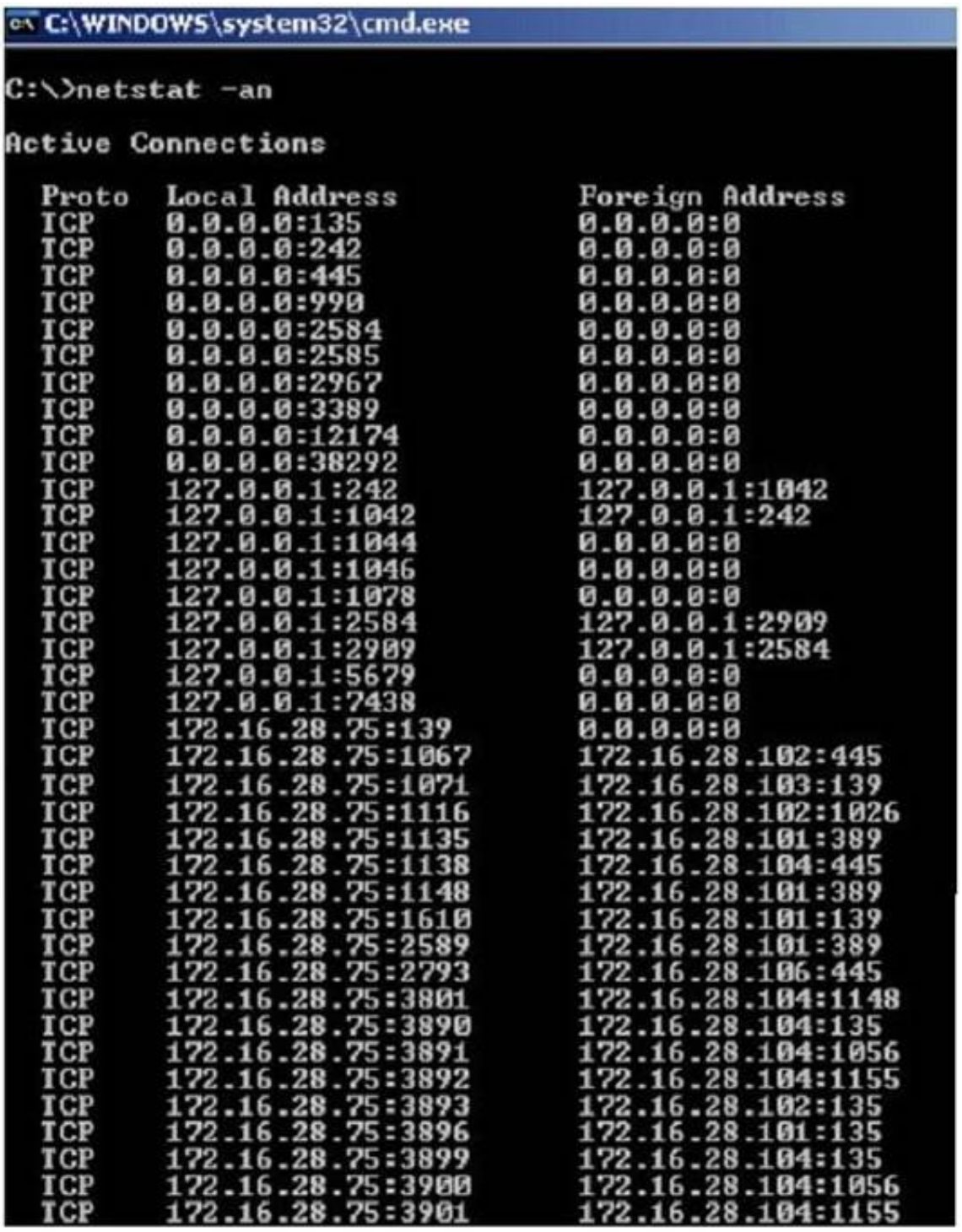
Answer: C

NEW QUESTION 386
- (Exam Topic 2)
Which program is the bootloader when Windows XP starts up?

A. KERNEL.EXE
B. NTLDR
C. LOADER
D. LILO

Answer: B

NEW QUESTION 390
- (Exam Topic 2)
Jack Smith is a forensics investigator who works for Mason Computer Investigation Services. He is investigating a computer that was infected by Ramen Virus.



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

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

Answer: B

NEW QUESTION 395
- (Exam Topic 2)

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

Answer: B

NEW QUESTION 398
- (Exam Topic 2)
NTFS has reduced slack space than FAT, thus having lesser potential to hide data in the slack space. This is because:

A. FAT does not index files
B. NTFS is a journaling file system
C. NTFS has lower cluster size space
D. FAT is an older and inefficient file system

Answer: C

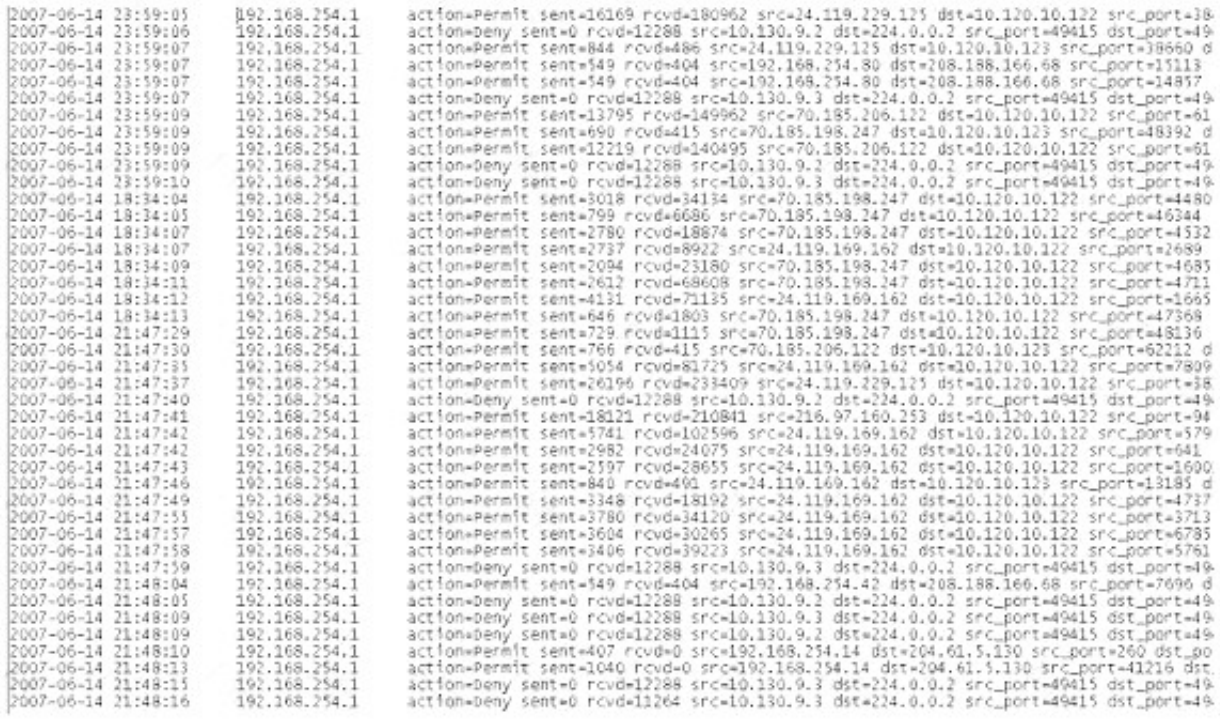
NEW QUESTION 401
- (Exam Topic 2)
Which of the following tool can the investigator use to analyze the network to detect Trojan activities?

A. Regshot
B. TRIPWIRE

C. RAM Computer
D. Capsa

Answer: D

NEW QUESTION 406
- (Exam Topic 2)
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. A smurf attack has been attempted
B. A denial of service has been attempted
C. Network intrusion has occurred
D. Buffer overflow attempt on the firewall.

Answer: C

NEW QUESTION 410
- (Exam Topic 2)
What is the primary function of the tool CHKDSK in Windows that authenticates the file system reliability of a volume?

A. Repairs logical file system errors
B. Check the disk for hardware errors
C. Check the disk for connectivity errors
D. Check the disk for Slack Space

Answer: A

NEW QUESTION 413
- (Exam Topic 2)
When investigating a wireless attack, what information can be obtained from the DHCP logs?

A. The operating system of the attacker and victim computers
B. IP traffic between the attacker and the victim
C. MAC address of the attacker
D. If any computers on the network are running in promiscuous mode

Answer: C

NEW QUESTION 416
- (Exam Topic 2)
When needing to search for a website that is no longer present on the Internet today but was online few years back, what site can be used to view the website collection of pages?

A. Proxify.net
B. Dnsstuff.com
C. Samspade.org
D. Archive.org

Answer: D

NEW QUESTION 417
- (Exam Topic 2)
Your company's network just finished going through a SAS 70 audit. This audit reported that overall, your network is secure, but there are some areas that needs improvement. The major area was SNMP security. The audit company recommended turning off SNMP, but that is not an option since you have so many remote nodes to keep track of. What step could you take to help secure SNMP on your network?

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

Answer: D

NEW QUESTION 418
- (Exam Topic 2)
You have been given the task to investigate web attacks on a Windows-based server. Which of the following commands will you use to look at the sessions the machine has opened with other systems?

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

Answer: D

NEW QUESTION 422
- (Exam Topic 2)
Ivanovich, a forensics investigator, is trying to extract complete information about running processes from a system. Where should he look apart from the RAM and virtual memory?

A. Swap space
B. Application data
C. Files and documents
D. Slack space

Answer: A

NEW QUESTION 424
- (Exam Topic 2)
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. Destination IP address
B. Source IP address
C. Login IP address
D. None of the above

Answer: A

NEW QUESTION 425
- (Exam Topic 2)
Sectors are pie-shaped regions on a hard disk that store data. Which of the following parts of a hard disk do not contribute in determining the addresses of data?

A. Sectors
B. Interface
C. Cylinder
D. Heads

Answer: B

NEW QUESTION 428
- (Exam Topic 2)
Why would a company issue a dongle with the software they sell?

A. To provide source code protection
B. To provide wireless functionality with the software
C. To provide copyright protection
D. To ensure that keyloggers cannot be used

Answer: C

NEW QUESTION 432
- (Exam Topic 2)
Who is responsible for the following tasks?

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

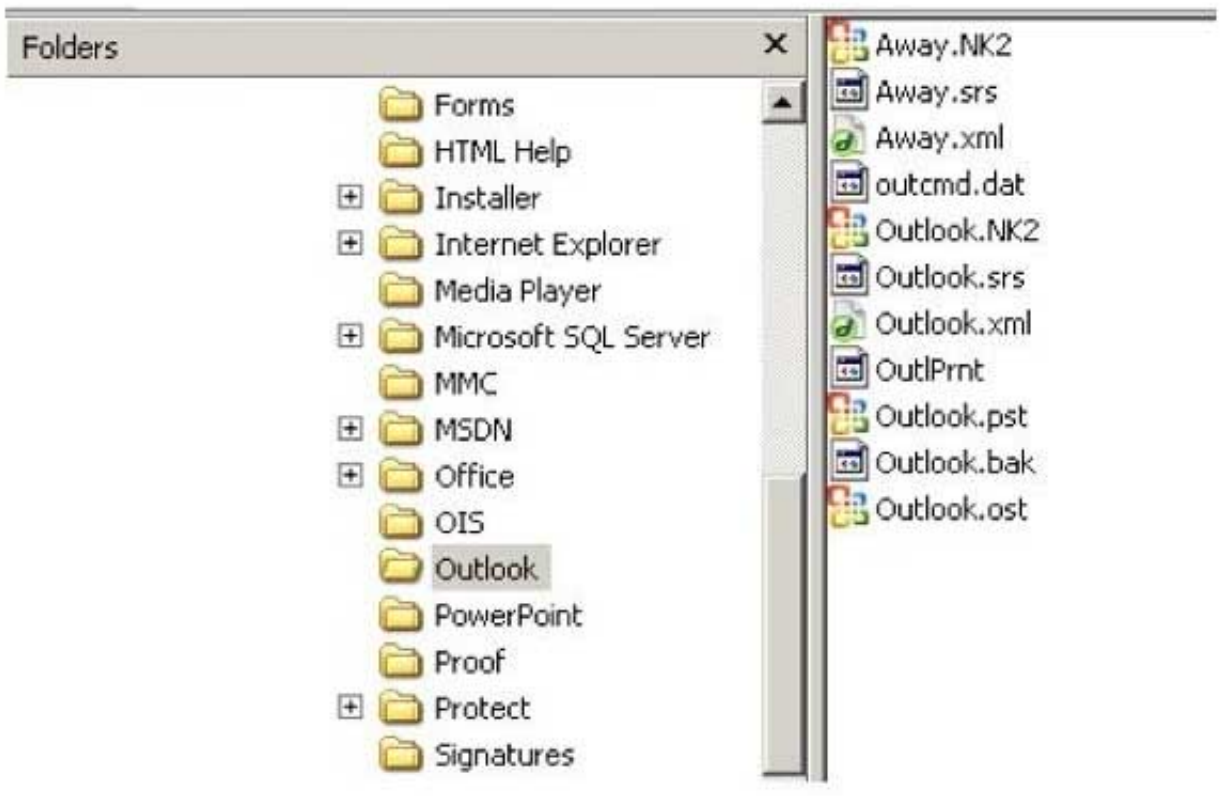
Answer: A

NEW QUESTION 435
- (Exam Topic 2)
Which among the following files provides email header information in the Microsoft Exchange server?

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

Answer: B

NEW QUESTION 439
- (Exam Topic 2)
In the following directory listing,



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

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

Answer: D

NEW QUESTION 442
- (Exam Topic 2)
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. Man-in-the-Middle Attack
B. Sniffer Attack
C. Buffer Overflow
D. DDoS

Answer: D

NEW QUESTION 446
- (Exam Topic 2)
In Steganalysis, which of the following describes a Known-stego attack?

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

Answer: C

NEW QUESTION 451
- (Exam Topic 2)
Why should you never power on a computer that you need to acquire digital evidence from?

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

Answer: A

NEW QUESTION 455
- (Exam Topic 2)
Which of the following stages in a Linux boot process involve initialization of the system's hardware?

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

Answer: A

NEW QUESTION 459
- (Exam Topic 2)
Wireless access control attacks aim to penetrate a network by evading WLAN access control measures such as AP MAC filters and Wi-Fi port access controls. Which of the following wireless access control attacks allow the attacker to set up a rogue access point outside the corporate perimeter and then lure the employees of the organization to connect to it?

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

Answer: B

NEW QUESTION 463
- (Exam Topic 2)
What file is processed at the end of a Windows XP boot to initialize the logon dialog box?

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

Answer: A

NEW QUESTION 468
- (Exam Topic 2)
Which MySQL log file contains information on server start and stop?

A. Slow query log file
B. General query log file
C. Binary log
D. Error log file

Answer: D

NEW QUESTION 469
- (Exam Topic 2)
What must be obtained before an investigation is carried out at a location?

A. Search warrant
B. Subpoena
C. Habeas corpus
D. Modus operandi

Answer: A

NEW QUESTION 473
- (Exam Topic 2)
While presenting his case to the court, Simon calls many witnesses to the stand to testify. Simon decides to call Hillary Taft, a lay witness, to the stand. Since Hillary is a lay witness, what field would she be considered an expert in?

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

Answer: B

NEW QUESTION 474
- (Exam Topic 2)
What is the location of the binary files required for the functioning of the OS in a Linux system?

A. /run
B. /bin
C. /root
D. /sbin

Answer: B

NEW QUESTION 478
- (Exam Topic 2)
Madison is on trial for allegedly breaking into her university internal network. The police raided her dorm room and seized all of her computer equipment. Madison lawyer is trying to convince the judge that the
seizure was unfounded and baseless. Under which US Amendment is Madison lawyer trying to prove the police violated?

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

Answer: D

NEW QUESTION 481
- (Exam Topic 2)
When marking evidence that has been collected with the “aaa/ddmmyy/nnnn/zz” format, what does the “nnnn” denote?

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

Answer: D

NEW QUESTION 485
- (Exam Topic 2)
Richard is extracting volatile data from a system and uses the command doskey/history. What is he trying to extract?

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

Answer: B

NEW QUESTION 488
- (Exam Topic 2)
In Windows Security Event Log, what does an event id of 530 imply?

A. Logon Failure – Unknown user name or bad password
B. Logon Failure – User not allowed to logon at this computer
C. Logon Failure – Account logon time restriction violation
D. Logon Failure – Account currently disabled

Answer: C

NEW QUESTION 489
- (Exam Topic 2)
Files stored in the Recycle Bin in its physical location are renamed as Dxy.ext, where “x” represents the
_____.

A. Drive name
B. Original file name’s extension
C. Sequential number
D. Original file name

Answer: A

NEW QUESTION 493
- (Exam Topic 2)
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. HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management
B. HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\System Management
C. HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Device Management
D. HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management\PrefetchParameters

Answer: A

NEW QUESTION 498
- (Exam Topic 2)
Madison is on trial for allegedly breaking into her university's internal network. The police raided her dorm room and seized all of her computer equipment. Madison's lawyer is trying to convince the judge that the seizure was unfounded and baseless. Under which US Amendment is Madison's lawyer trying to prove the police violated?

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

Answer: A

NEW QUESTION 500
- (Exam Topic 2)
If a PDA is seized in an investigation while the device is turned on, what would be the proper procedure?

A. Keep the device powered on
B. Turn off the device immediately
C. Remove the battery immediately
D. Remove any memory cards immediately

Answer: A

NEW QUESTION 504
- (Exam Topic 2)
Before performing a logical or physical search of a drive in Encase, what must be added to the program?

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

Answer: B

NEW QUESTION 509
- (Exam Topic 2)
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

NEW QUESTION 512
- (Exam Topic 2)
What is the smallest physical storage unit on a hard drive?

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

Answer: C

NEW QUESTION 515
- (Exam Topic 2)
Using Linux to carry out a forensics investigation, what would the following command accomplish? dd if=/usr/home/partition.image of=/dev/sdb2 bs=4096 conv=notrunc,noerror

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

Answer: D

NEW QUESTION 519
.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

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

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

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

Money Back Guarantee

312-49v10 Practice Exam Features:

* 312-49v10 Questions and Answers Updated Frequently

* 312-49v10 Practice Questions Verified by Expert Senior Certified Staff

* 312-49v10 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* 312-49v10 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year