Vendor: GIAC

Exam Code: GCFA

Exam Name: GIAC Certified Forensics Analyst

Version: Demo

QUESTION NO: 1

Adam, a malicious hacker has successfully gained unauthorized access to the Linux system of

Umbrella Inc. Web server of the company runs on Apache. He has downloaded sensitive documents and database files from the computer. After performing these malicious tasks, Adam finally runs the following command on the Linux command box before disconnecting. for ((i = 0;i<11;i++)); do

dd if=/dev/random of=/dev/hda && dd if=/dev/zero of=/dev/hda done

Which of the following actions does Adam want to perform by the above command?

A. Making a bit stream copy of the entire hard disk for later download.
B. Deleting all log files present on the system.
C. Wiping the contents of the hard disk with zeros.
D. Infecting the hard disk with polymorphic virus strings.

Answer: C

QUESTION NO: 2

Adam works as a Computer Hacking Forensic Investigator for a garment company in the United States. A project has been assigned to him to investigate a case of a disloyal employee who is suspected of stealing design of the garments, which belongs to the company and selling those garments of the same design under different brand name. Adam investigated that the company does not have any policy related to the copy of design of the garments. He also investigated that the trademark under which the employee is selling the garments is almost identical to the original trademark of the company. On the grounds of which of the following laws can the employee be prosecuted?

A. Trademark law
B. Cyber law
C. Copyright law
D. Espionage law

Answer: A

QUESTION NO: 3

You work as a Network Administrator for Perfect Solutions Inc. You install Windows 98 on a computer. By default, which of the following folders does Windows 98 setup use to keep the

registry tools?

A. $SYSTEMROOT$REGISTRY
B. $SYSTEMROOT$WINDOWS
C. $SYSTEMROOT$WINDOWSREGISTRY
D. $SYSTEMROOT$WINDOWSSYSTEM32

Answer: B

QUESTION NO: 4

Which of the following tools can be used to perform tasks such as Windows password cracking, Windows enumeration, and VoIP session sniffing?

A. John the Ripper
B. L0phtcrack
C. Obiwan
D. Cain

Answer: D

QUESTION NO: 5

Which of the following type of file systems is not supported by Linux kernel?

A. vFAT
B. NTFS
C. HFS
D. FAT32

Answer: D

QUESTION NO: 6

Which of the following modules of OS X kernel (XNU) provides the primary system program interface?

A. BSD

B. LIBKERN
C. I/O Toolkit
D. Mach

Answer: A

QUESTION NO: 7

You work as a Network Administrator for Blue Bell Inc. You want to install Windows XP Professional on your computer, which already has Windows Me installed. You want to configure your computer to dual boot between Windows Me and Windows XP Professional. You have a single 40GB hard disk.

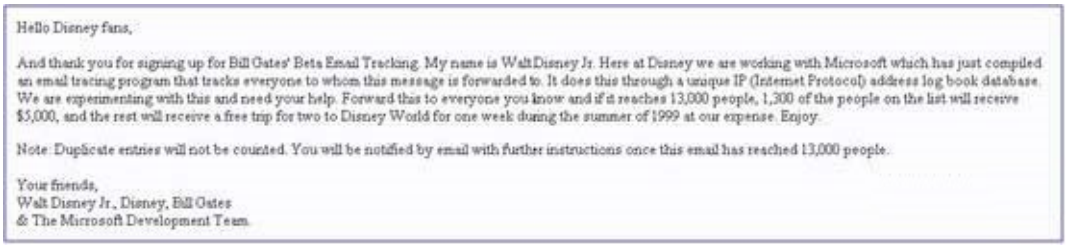
Which of the following file systems will you choose to dual-boot between the two operating systems?

A. NTFS
B. FAT32
C. CDFS
D. FAT

Answer: B

QUESTION NO: 8

John works as a professional Ethical Hacker. He has been assigned the project of testing the security of www.we-are-secure.com. He receives the following e-mail:



Hello Disney fans,

And thank you for signing up for Bill Gates' Beta Email Tracking. My name is Walt Disney Jr. Here at Disney we are working with Microsoft which has just compiled an email tracing program that tracks everyone to whom this message is forwarded to. It does this through a unique IP (Internet Protocol) address log book database. We are experimenting with this and need your help. Forward this to everyone you know and if it reaches 13,000 people, 1,300 of the people on the list will receive $5,000, and the rest will receive a free trip for two to Disney World for one week during the summer of 1999 at our expense. Enjoy.

Note: Duplicate entries will not be counted. You will be notified by email with further instructions once this email has reached 13,000 people.

Your friends,
Walt Disney Jr., Disney, Bill Gates
& The Microsoft Development Team.

The e-mail that John has received is an example of _____.

A. Virus hoaxes
B. Spambots
C. Social engineering attacks
D. Chain letters

Answer: D

QUESTION NO: 9

Which of the following Acts enacted in United States allows the FBI to issue National Security Letters (NSLs) to Internet service providers (ISPs) ordering them to disclose records about their customers?

A. Wiretap Act
B. Computer Fraud and Abuse Act
C. Economic Espionage Act of 1996
D. Electronic Communications Privacy Act of 1986

Answer: D

QUESTION NO: 10

TCP FIN scanning is a type of stealth scanning through which the attacker sends a FIN packet to the target port. If the port is closed, the victim assumes that this packet was sent mistakenly by the attacker and sends the RST packet to the attacker. If the port is open, the FIN packet will be ignored and the port will drop the packet. Which of the following operating systems can be easily identified with the help of TCP FIN scanning?

A. Solaris
B. Red Hat
C. Knoppix
D. Windows

Answer: D

QUESTION NO: 11

Which of the following encryption methods uses AES technology?

A. Dynamic WEP
B. Static WEP

C. TKIP
D. CCMP

Answer: D

QUESTION NO: 12

Mark works as a security manager for SofTech Inc. He is using a technique for monitoring what the employees are doing with corporate resources. Which of the following techniques is being used by Mark to gather evidence of an ongoing computer crime if a member of the staff is e-mailing company's secrets to an opponent?

A. Electronic surveillance
B. Civil investigation
C. Physical surveillance
D. Criminal investigation

Answer: A

QUESTION NO: 13

Which of the following is the first computer virus that was used to infect the boot sector of storage media formatted with the DOS File Allocation Table (FAT) file system?

A. Melissa
B. Tequila
C. Brain
D. I love you

Answer: C

QUESTION NO: 14

Which of the following attacks saturates network resources and disrupts services to a specific computer?

A. Teardrop attack
B. Polymorphic shell code attack

C. Denial-of-Service (DoS) attack
D. Replay attack

Answer: C

QUESTION NO: 15

Peter works as a Technical Representative in a CSIRT for SecureEnet Inc. His team is called to investigate the computer of an employee, who is suspected for classified data theft. Suspect's computer runs on Windows operating system. Peter wants to collect data and evidences for further analysis. He knows that in Windows operating system, the data is searched in pre-defined steps for proper and efficient analysis. Which of the following is the correct order for searching data on a Windows based system?

A. Volatile data, file slack, registry, memory dumps, file system, system state backup, internet traces
B. Volatile data, file slack, registry, system state backup, internet traces, file system, memory dumps
C. Volatile data, file slack, internet traces, registry, memory dumps, system state backup, file system
D. Volatile data, file slack, file system, registry, memory dumps, system state backup, internet traces

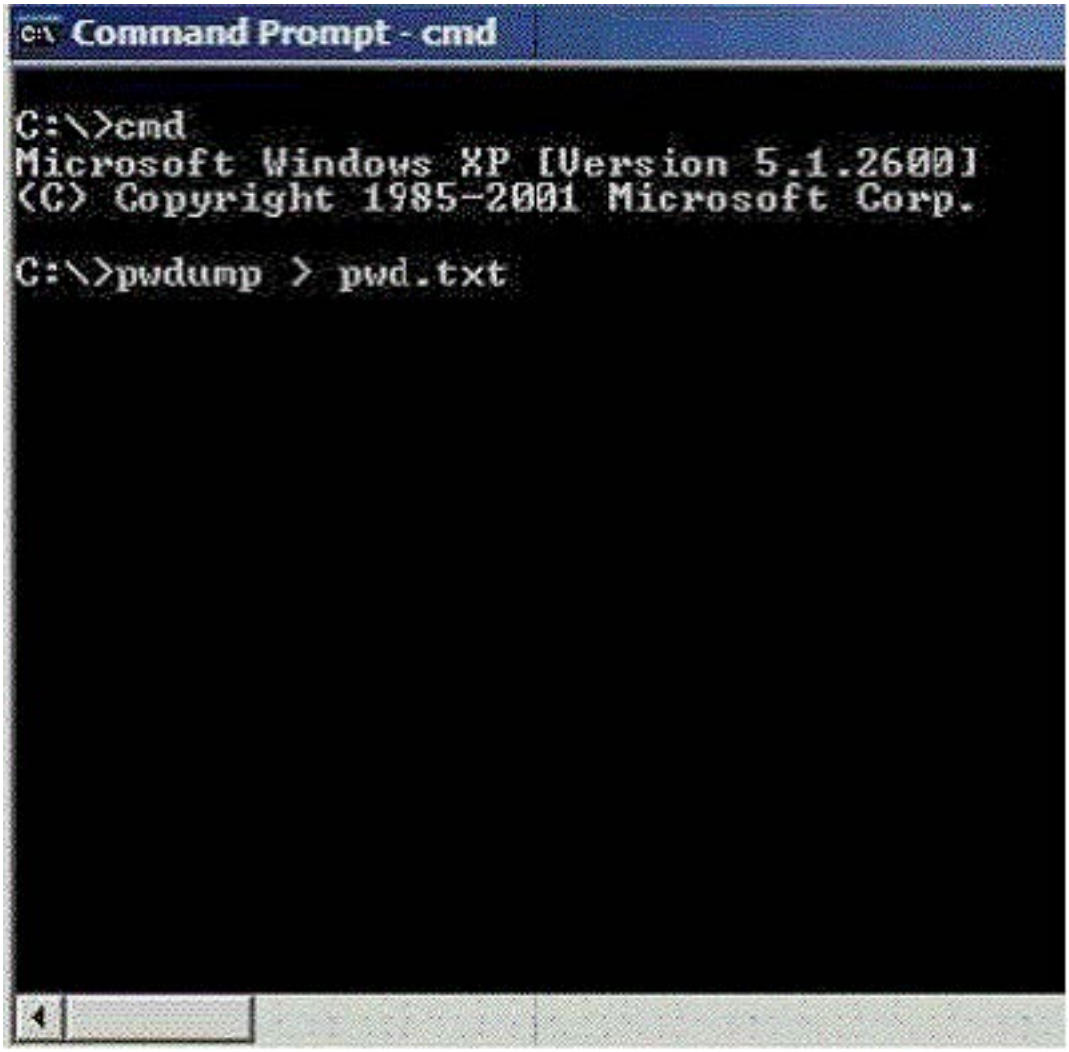
Answer: D

QUESTION NO: 16

Adam works as a Security Administrator for Umbrella Inc. He is responsible for securing all 15 servers of the company. To successfully accomplish the task, he enables the hardware and software firewalls and disables all unnecessary services on all the servers. Sales manager of the company asks Adam to run emulation software on one of the servers that requires the telnet service to function properly. Adam is concerned about the security of the server, as telnet can be a very large security risk in an organization. Adam decides to perform some footprinting, scanning, and penetration testing on the server to checkon the server to check the security. Adam telnets into the server and writes the following command:

HEAD / HTTP/1.0

After pressing enter twice, Adam gets the following results:



Which of the following tasks has Adam just accomplished?

A. Poisoned the local DNS cache of the server.
B. Submitted a remote command to crash the server.
C. Grabbed the banner.
D. Downloaded a file to his local computer.

Answer: C

QUESTION NO: 17

The MBR of a hard disk is a collection of boot records that contain disk information such as disk architecture, cluster size, and so on. The main work of the MBR is to locate and run necessary operating system files that are required to run a hard disk. In the context of the operating system, MBR is also known as the boot loader. Which of the following viruses can infect the MBR of a hard disk?

Each correct answer represents a complete solution. Choose two.

A. Stealth
B. Boot sector
C. Multipartite
D. File

Answer: B,C

QUESTION NO: 18

You work as a professional Computer Hacking Forensic Investigator for DataEnet Inc. You want to investigate e-mail information of an employee of the company. The suspected employee is using an online e-mail system such as Hotmail or Yahoo. Which of the following folders on the local computer will you review to accomplish the task?

Each correct answer represents a complete solution. Choose all that apply.

A. History folder
B. Temporary Internet Folder
C. Download folder
D. Cookies folder

Answer: A,B,D

QUESTION NO: 19

Which of the following methods is used by forensic investigators to acquire an image over the network in a secure manner?

A. DOS boot disk
B. Linux Live CD
C. Secure Authentication for EnCase (SAFE)
D. EnCase with a hardware write blocker

Answer: C

QUESTION NO: 20

You company suspects an employee of sending unauthorized emails to competitors. These emails are alleged to contain confidential company data. Which of the following is the most important step

for you to take in preserving the chain of custody?

A. Preserve the email server including all logs.
B. Make copies of that employee's email.
C. Seize the employee's PC.
D. Place spyware on the employee's PC to confirm these activities.

Answer: A

QUESTION NO: 21

Which of the following is the correct order of loading system files into the main memory of the system, when the computer is running on Microsoft's Windows XP operating system?

A. NTLDR, BOOT.ini, HAL.dll, NTDETECT.com, NTOSKRNL.exe
B. NTLDR, BOOT.ini, NTDETECT.com, HAL.dll, NTOSKRNL.exe
C. NTLDR, BOOT.ini, HAL.dll, NTDETECT.com, NTOSKRNL.exe
D. BOOT.ini, HAL.dll, NTDETECT.com, NTLDR, NTOSKRNL.exe

Answer: B

QUESTION NO: 22

Fill in the blank with the appropriate name.

_____is a list, which specifies the order of volatility of data in a Windows based system.

A. RFC 3227

Answer: A

QUESTION NO: 23

Which of the following file systems provides file-level security?

A. CDFS
B. FAT
C. FAT32

D. NTFS

Answer: D

QUESTION NO: 24

Adam works as an Incident Handler for Umbrella Inc. He is informed by the senior authorities that the server of the marketing department has been affected by a malicious hacking attack. Supervisors are also claiming that some sensitive data are also stolen. Adam immediately arrived to the server room of the marketing department and identified the event as an incident. He isolated the infected network from the remaining part of the network and started preparing to image the entire system. He captures volatile data, such as running process, ram, and network connections.

Which of the following steps of the incident handling process is being performed by Adam?

A. Recovery
B. Eradication
C. Identification
D. Containment

Answer: D

QUESTION NO: 25

Which of the following is the process of overwriting all addressable locations on a disk?

A. Drive wiping
B. Spoofing
C. Sanitization
D. Authentication

Answer: A

QUESTION NO: 26

An executive in your company reports odd behavior on her PDA. After investigation you discover that a trusted device is actually copying data off the PDA. The executive tells you that the behavior started shortly after accepting an e-business card from an unknown person. What type of attack is this?

A. Session Hijacking
B. Bluesnarfing
C. PDA Hijacking
D. Privilege Escalation

Answer: B

QUESTION NO: 27

You work as a Network Administrator for Net Perfect Inc. The company has a Windows Server 2008 network environment. The network is configured as a Windows Active Directory-based single forest single domain network. The network is configured on IP version 6 protocol. All the computers on the network are connected to a switch device. One day, users complain that they are unable to connect to a file server. You try to ping the client computers from the server, but the pinging fails. You try to ping the server's own loopback address, but it fails to ping. You restart the server, but the problem persists.

What is the most likely cause?

A. The cable that connects the server to the switch is broken.
B. Automatic IP addressing is not working.
C. The switch device is not working.
D. The server is configured with unspecified IP address.
E. The server's NIC is not working.

Answer: E

QUESTION NO: 28

You want to upgrade a partition in your computer's hard disk drive from FAT to NTFS. Which of the following DOS commands will you use to accomplish this?

A. FORMAT C: /s
B. CONVERT C: /fs:ntfs
C. SYS C:
D. FDISK /mbr

Answer: B

QUESTION NO: 29

A firewall is a combination of hardware and software, used to provide security to a network. It is used to protect an internal network or intranet against unauthorized access from the Internet or other outside networks. It restricts inbound and outbound access and can analyze all traffic between an internal network and the Internet. Users can configure a firewall to pass or block packets from specific IP addresses and ports. Which of the following tools works as a firewall for the Linux 2.4 kernel?

A. OpenSSH
B. IPTables
C. IPChains
D. Stunnel

Answer: B

QUESTION NO: 30

You work as a Web developer for ABC Inc. You want to investigate the Cross-Site Scripting attack on your company's Web site. Which of the following methods of investigation can you use to accomplish the task?

Each correct answer represents a complete solution. Choose all that apply.

A. Review the source of any HTML-formatted e-mail messages for embedded scripts or links in the URL to the company's site.
B. Look at the Web server's logs and normal traffic logging.
C. Use Wireshark to capture traffic going to the server and then searching for the requests going to the input page, which may give log of the malicious traffic and the IP address of the source.
D. Use a Web proxy to view the Web server transactions in real time and investigate any communication with outside servers.

Answer: A,B,D

QUESTION NO: 31

Adam works as a professional Penetration tester. A project has been assigned to him to employ penetration testing on the network of Umbrella Inc. He is running the test from home and had downloaded every security scanner from the Internet. Despite knowing the IP range of all of the systems, and the exact network configuration, Adam is unable to get any useful results.

Which of the following is the most like cause of this problem?

Each correct answer represents a complete solution. Choose all that apply.

A. Security scanners are only as smart as their database and cannot find unpublished vulnerabilities.
B. Security scanners cannot perform vulnerability linkage.
C. Security scanners are smart as their database and can find unpublished vulnerabilities.
D. Security scanners are not designed to do testing through a firewall.

Answer: A,B,D

QUESTION NO: 32

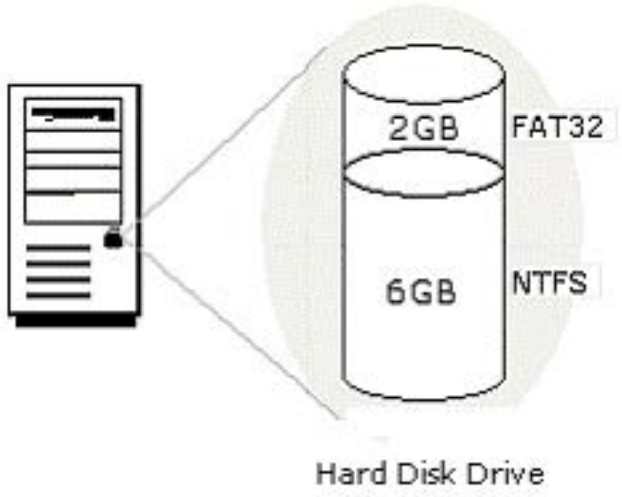
An organization monitors the hard disks of its employees' computers from time to time. Which policy does this pertain to?

A. Network security policy
B. User password policy
C. Privacy policy
D. Backup policy

Answer: C

QUESTION NO: 33

You work as a Network Administrator for Net World International. You have configured the hard disk drive of your computer as shown in the image below:



The computer is configured to dual-boot with Windows 2000 Server and Windows 98. While

working on Windows 2000 Server, you save a file on the 6GB partition. You are unable to find the file while working on Windows 98. You are not even able to access the partition on which the file is saved. What is the most likely cause?

A. The file is corrupt.
B. The 6GB partition is corrupt.
C. Windows 98 does not support the NTFS file system.
D. Files saved in Windows 98 are not supported by Windows 2000.

Answer: C

QUESTION NO: 34

Peter works as a Computer Hacking Forensic Investigator. He has been called by an organization to conduct a seminar to give necessary information related to sexual harassment within the work place. Peter started with the definition and types of sexual harassment. He then wants to convey that it is important that records of the sexual harassment incidents should be maintained, which helps in further legal prosecution. Which of the following data should be recorded in this documentation?

Each correct answer represents a complete solution. Choose all that apply.

A. Names of the victims
B. Date and time of incident
C. Nature of harassment
D. Location of each incident

Answer: A,B,D

QUESTION NO: 35

Which of the following types of computers is used for attracting potential intruders?

A. Bastion host
B. Data pot
C. Files pot
D. Honey pot

Answer: D

QUESTION NO: 36

Which of the following standard file formats is used by Apple's iPod to store contact information?

A. HFS+
B. hCard
C. vCard
D. FAT32

Answer: C

QUESTION NO: 37

Which of the following file systems cannot be used to install an operating system on the hard disk drive?

Each correct answer represents a complete solution. Choose two.

A. Windows NT file system (NTFS)
B. High Performance File System (HPFS)
C. Log-structured file system (LFS)
D. Compact Disc File System (CDFS)
E. Novell Storage Services (NSS)

Answer: C,D

QUESTION NO: 38

Which of the following types of evidence proves or disproves a specific act through oral testimony based on information gathered through the witness's five senses?

A. Conclusive evidence
B. Best evidence
C. Hearsay evidence
D. Direct evidence

Answer: D

QUESTION NO: 39

Which of the following two cryptography methods are used by NTFS Encrypting File System (EFS) to encrypt the data stored on a disk on a file-by-file basis?

A. Digital certificates
B. Public key
C. RSA
D. Twofish

Answer: A,B

QUESTION NO: 40

Which of the following sections of an investigative report covers the background and summary of the report including the outcome of the case and the list of allegations?

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

Answer: A

QUESTION NO: 41

Which of the following switches of the XCOPY command copies attributes while copying files?

A. /o
B. /p
C. /k
D. /s

Answer: D

QUESTION NO: 42

Which of the following directories in Linux operating system contains device files, which refers to physical devices?

A. /boot
B. /etc
C. /dev
D. /bin

Answer: C

QUESTION NO: 43

Which of the following directories cannot be placed out of the root filesystem?

Each correct answer represents a complete solution. Choose all that apply.

A. /sbin
B. /etc
C. /var
D. /lib

Answer: A,B,D

QUESTION NO: 44

On which of the following locations does the Windows NT/2000 operating system contain the SAM, SAM.LOG, SECURITY.LOG, APPLICATION.LOG, and EVENT.LOG files?

A. \%Systemroot%system32
B. \%Systemroot%profiles
C. \%Systemroot%system32config
D. \%Systemroot%help

Answer: C

QUESTION NO: 45

You are handling technical support calls for an insurance company. A user calls you complaining that he cannot open a file, and that the file name appears in green while opening in Windows Explorer.

What does this mean?

A. The file is encrypted.
B. The file belongs to another user.
C. The file is infected with virus.
D. The file is compressed.

Answer: A

QUESTION NO: 46

Which of the following is a name, symbol, or slogan with which a product is identified?

A. Trade secret
B. Patent
C. Copyright
D. Trademark

Answer: D

QUESTION NO: 47

Which of the following file systems supports the hot fixing feature?

A. FAT16
B. exFAT
C. FAT32
D. NTFS

Answer: D

QUESTION NO: 48

John works as a professional Ethical Hacker. He has been assigned a project for testing the security of www.we-are-secure.com. He wants to corrupt an IDS signature database so that performing attacks on the server is made easy and he can observe the flaws in the We-are-secure server. To perform his task, he first of all sends a virus that continuously changes its signature to avoid detection from IDS. Since the new signature of the virus does not match the old signature, which is entered in the IDS signature database, IDS becomes unable to point out the malicious virus. Which of the following IDS evasion attacks is John performing?

A. Evasion attack
B. Session splicing attack
C. Insertion attack
D. Polymorphic shell code attack

Answer: D

QUESTION NO: 49

You work as the Network Administrator for McNeil Inc. The company has a Unix-based network. You want to fix partitions on a hard drive. Which of the following Unix commands can you use to accomplish the task?

A. fdformat
B. exportfs
C. fsck
D. fdisk

Answer: D

QUESTION NO: 50

Which of the following is a type of intruder detection that involves logging network events to a file for an administrator to review later?

A. Packet detection
B. Passive detection
C. Active detection
D. Event detection

Answer: B

QUESTION NO: 51

Which of the following file systems is designed by Sun Microsystems?

A. NTFS
B. CIFS

C. ext2
D. ZFS

Answer: D

QUESTION NO: 52

Mark works as a Network Administrator for Net Perfect Inc. The company has a Linux-based network. Mark installs a Checkpoint Firewall NGX on a SecurePlatform device. He performs a scheduled backup of his system settings and products configuration. Where are these backup files stored?

Each correct answer represents a complete solution. Choose all that apply.

A. SCP
B. TFTP
C. Locally on the SecurePlatform machine hard drive
D. On a PC in a file named userC

Answer: A,B,C

QUESTION NO: 53

Which of the following evidences are the collection of facts that, when considered together, can be used to infer a conclusion about the malicious activity/person?

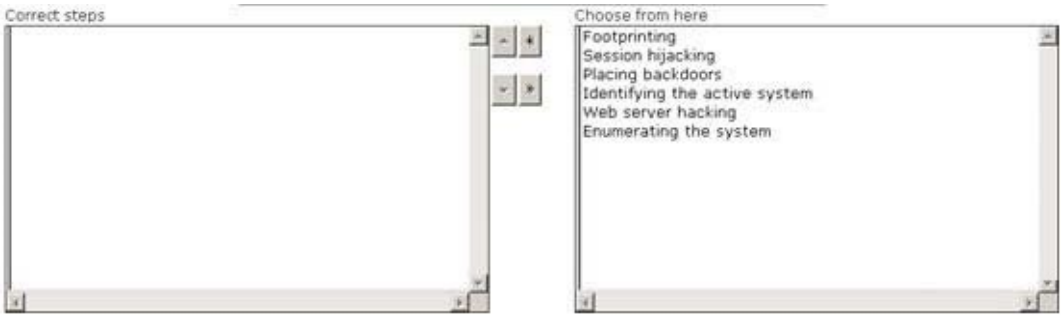
A. Corroborating
B. Circumstantial
C. Incontrovertible
D. Direct

Answer: B

QUESTION NO: 54

Maria works as a professional Ethical Hacker. She recently got a project to test the security of www.we-are-secure.com. Arrange the three pre-test phases of the attack to test the security of weare-secure.

Answer:



QUESTION NO: 55

You are working with a team that will be bringing in new computers to a sales department at a company. The sales team would like to keep not only their old files, but system settings as well on the new PC's. What should you do?

A. Use the Disk Management tool to move everything to the new computer.
B. Copy the files and the Windows Registry to a removable media then copy it onto the new machines.
C. Do a system backup (complete) on each old machine, then restore it onto the new machines
D. Use the User State Migration tool to move the system settings and files to the new machines.

Answer: D

QUESTION NO: 56

By gaining full control of router, hackers often acquire full control of the network. Which of the following methods are commonly used to attack Routers?

Each correct answer represents a complete solution. Choose all that apply.

A. By launching Social Engineering attack
B. By launching Max Age attack
C. Route table poisoning
D. By launching Sequence++ attack

Answer: B,C,D

QUESTION NO: 57

Which of the following is the process of comparing cryptographic hash functions of system executables and configuration files?

A. Spoofing
B. File integrity auditing
C. Reconnaissance
D. Shoulder surfing

Answer: B

QUESTION NO: 58

Which of the following are the primary goals of the incident handling team?

Each correct answer represents a complete solution. Choose all that apply.

A. Prevent any further damage.
B. Freeze the scene.
C. Repair any damage caused by an incident.
D. Inform higher authorities.

Answer: A,B,C

QUESTION NO: 59

Which of the following is the correct order of digital investigations Standard Operating Procedure (SOP)?

A. Initial analysis, request for service, data collection, data analysis, data reporting
B. Initial analysis, request for service, data collection, data reporting, data analysis
C. Request for service, initial analysis, data collection, data reporting, data analysis
D. Request for service, initial analysis, data collection, data analysis, data reporting

Answer: D

QUESTION NO: 60

Which of the following is the initiative of United States Department of Justice, which provides state and local law enforcement agencies the tools to prevent Internet crimes against children, and catches the distributors of child pornography on the Internet?

A. Innocent Images National Initiative (IINI)
B. Internet Crimes Against Children (ICAC)
C. Project Safe Childhood (PSC)
D. Anti-Child Porn.org (ACPO)

Answer: B

QUESTION NO: 61

Mark is the Administrator of a Linux computer. He wants to check the status of failed Telnet-based login attempts on the Linux computer. Which of the following shell commands will he use to accomplish the task?

A. GREP
B. CP
C. FSCK
D. CAT

Answer: A

QUESTION NO: 62

Which of the following tools are used for footprinting?

Each correct answer represents a complete solution. Choose all that apply.

A. Sam spade
B. Traceroute
C. Whois
D. Brutus

Answer: A,B,C

QUESTION NO: 63

You work as a Network Administrator for Peach Tree Inc. The company currently has a FAT-based Windows NT network. All client computers run Windows 98. The management wants all client computers to be able to boot in Windows XP Professional. You want to accomplish the following goals:

The file system should support file compression and file level security.

All the existing data and files can be used by the new file system.

Users should be able to dual-boot their computers.

You take the following steps to accomplish these goals:

Convert the FAT file system to NTFS using the CONVERT utility.

Install Windows XP and choose to upgrade the existing operating system during setup.

Which of the following goals will you be able to accomplish?

Each correct answer represents a complete solution. Choose all that apply.

A. The file system supports file compression and file level security.
B. All the existing data and files can be used by the new file system.
C. Users are able to dual-boot their computers.
D. None of the goals are accomplished.

Answer: A,B

QUESTION NO: 64

You work as the Network Administrator for McNeil Inc. The company has a Unix-based network. You want to allow direct access to the filesystems data structure. Which of the following Unix commands can you use to accomplish the task?

A. du
B. debugfs
C. df
D. dosfsck

Answer: B

QUESTION NO: 65

You work as a Network Administrator for Web World Inc. You want to host an e-commerce Web site on your network. You want to ensure that storage of credit card information is secure. Which of the following conditions should be met to accomplish this?

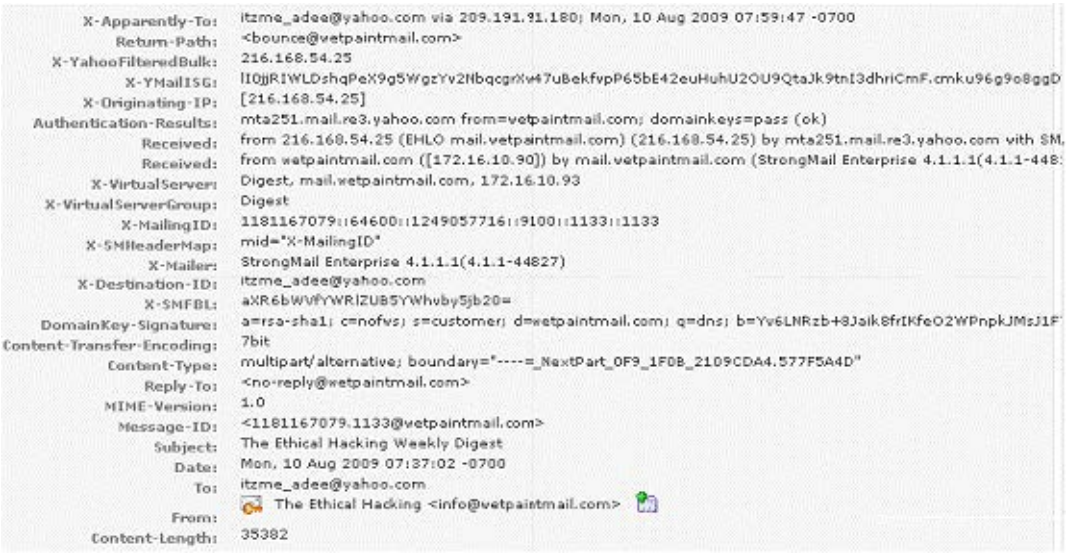
Each correct answer represents a complete solution. Choose all that apply.

A. NT authentication should be required for all customers before they provide their credit card numbers.
B. Strong encryption software should be used to store credit card information.
C. Only authorized access should be allowed to credit card information.
D. The NTFS file system should be implemented on a client computer.

Answer: B,C

QUESTION NO: 66

You work as a Network Security Analyzer. You got a suspicious email while working on a forensic project. Now, you want to know the IP address of the sender so that you can analyze various information such as the actual location, domain information, operating system being used, contact information, etc. of the email sender with the help of various tools and resources. You also want to check whether this email is fake or real. You know that analysis of email headers is a good starting point in such cases. The email header of the suspicious email is given below:



X-Apparently-To:	itzme_adee@yahoo.com via 209.191.91.180; Mon, 10 Aug 2009 07:59:47 -0700
Return-Path:	<bounce@vetpaintmail.com>
X-YahooFilteredBulk:	216.168.54.25
X-YMailISG:	lI0jjRIWLDshqPeX9g5WgzYv2NbqcgrXw47uBekfvpP65bE42euHuhU2OU9QtaJk9tnI3dhriCmF.cmku96g9o8ggD
X-Originating-IP:	[216.168.54.25]
Authentication-Results:	mta251.mail.re3.yahoo.com from=vetpaintmail.com; domainkeys=pass (ok)
Received:	from 216.168.54.25 (EHLO mail.vetpaintmail.com) (216.168.54.25) by mta251.mail.re3.yahoo.com with SM
Received:	from vetpaintmail.com ([172.16.10.90]) by mail.vetpaintmail.com (StrongMail Enterprise 4.1.1.1(4.1.1-448
X-VirtualServer:	Digest, mail.vetpaintmail.com, 172.16.10.93
X-VirtualServerGroup:	Digest
X-MailingID:	1181167079::64600::1249057716::9100::1133::1133
X-SMHeaderMap:	mid="X-MailingID"
X-Mailer:	StrongMail Enterprise 4.1.1.1(4.1.1-44827)
X-Destination-ID:	itzme_adee@yahoo.com
X-SMFBL:	aXR6bWVfYWRlZUB5YWhvby5jb20=
DomainKey-Signature:	a=rsa-sha1; c=nofws; s=customer; d=vetpaintmail.com; q=dns; b=Yv6LNRzb+8Jaik8frIKfeO2WPnpkJMsJ1F
Content-Transfer-Encoding:	7bit
Content-Type:	multipart/alternative; boundary="----=_NextPart_0F9_1F0B_2109CDA4.577F5A4D"
Reply-To:	<no-reply@vetpaintmail.com>
MIME-Version:	1.0
Message-ID:	<1181167079.1133@vetpaintmail.com>
Subject:	The Ethical Hacking Weekly Digest
Date:	Mon, 10 Aug 2009 07:37:02 -0700
To:	itzme_adee@yahoo.com
From:	The Ethical Hacking <info@vetpaintmail.com>
Content-Length:	35382

What is the IP address of the sender of this email?

A. 172.16.10.90
B. 209.191.91.180

C. 216.168.54.25
D. 141.1.1.1

Answer: C

QUESTION NO: 67

You work as a Network Administrator for uCertify Inc. You want to edit the MSDOS.SYS file, in your computer, from the DOS prompt. You are unable to find the file. What is the most likely cause?

A. It is a read-only file.
B. It is a built-in command in the COMMAND.COM file.
C. Someone has deleted the file.
D. It is a hidden file.

Answer: D

QUESTION NO: 68

John works for an Internet Service Provider (ISP) in the United States. He discovered child

pornography material on a Web site hosted by the ISP. John immediately informed law enforcement authorities about this issue. Under which of the following Acts is John bound to take such an action?

A. Civil Rights Act of 1991
B. PROTECT Act
C. Civil Rights Act of 1964
D. Sexual Predators Act

Answer: D

QUESTION NO: 69

Adam works as a professional Computer Hacking Forensic Investigator with the local police of his area. A project has been assigned to him to investigate a PDA seized from a local drug dealer. It is expected that many valuable and important information are stored in this PDA. Adam follows investigative methods, which are required to perform in a pre-defined sequential manner for the

successful forensic investigation of the PDA. Which of the following is the correct order to perform forensic investigation of PDA?

A. Identification, Collection, Examination, Documentation
B. Examination, Collection, Identification, Documentation
C. Documentation, Examination, Identification, Collection
D. Examination, Identification, Collection, Documentation

Answer: D

QUESTION NO: 70

The incident response team has turned the evidence over to the forensic team. Now, it is the time to begin looking for the ways to improve the incident response process for next time. What are the typical areas for improvement?

Each correct answer represents a complete solution. Choose all that apply.

A. Information dissemination policy
B. Additional personnel security controls
C. Incident response plan
D. Electronic monitoring statement

Answer: A,B,C,D

QUESTION NO: 71

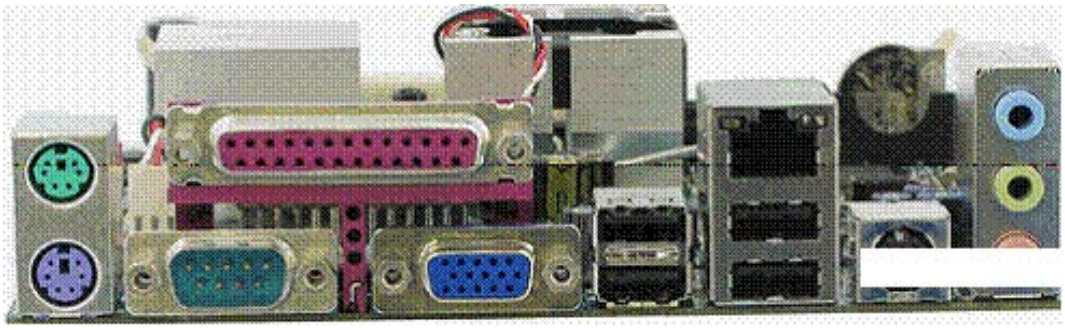
Adam works as a professional Computer Hacking Forensic Investigator. He has been assigned with the project of investigating an iPod, which is suspected to contain some explicit material. Adam wants to connect the compromised iPod to his system, which is running on Windows XP (SP2) operating system. He doubts that connecting the iPod with his computer may change some evidences and settings in the iPod. He wants to set the iPod to read-only mode. This can be done by changing the registry key within the Windows XP (SP2) operating system. Which of the following registry keys will Adam change to accomplish the task?

A. HKEY_LOCAL_MACHINE\System\CurrentControlset\Control\StorageDevicePolicies
B. HKEY_LOCAL_MACHINE\CurrentControlset\Control\StorageDevicePolicies
C. HKEY_LOCAL_MACHINE\System\CurrentControlset\StorageDevicePolicies
D. HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion

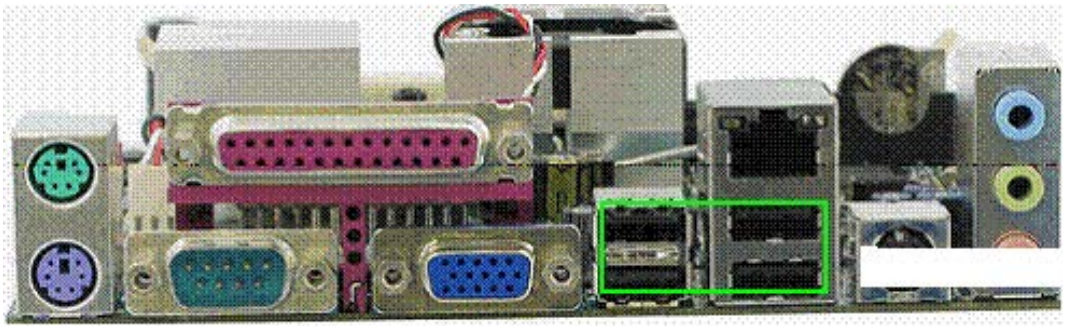
Answer: A

QUESTION NO: 72 HOTSPOT

Identify the port in the image given below, which can be connected to the hub to extend the number of ports, and up to 127 devices can be connected to it?



Answer:



QUESTION NO: 73

Nathan works as a Computer Hacking Forensic Investigator for SecureEnet Inc. He uses Visual TimeAnalyzer software to track all computer usage by logging into individual users account or specific projects and compile detailed accounts of time spent within each program. Which of the following functions are NOT performed by Visual TimeAnalyzer?

Each correct answer represents a complete solution. Choose all that apply.

A. It monitors all user data such as passwords and personal documents.
B. It gives parents control over their children's use of the personal computer.
C. It tracks work time, pauses, projects, costs, software, and internet usage.
D. It records specific keystrokes and run screen captures as a background process.

Answer: A,D

QUESTION NO: 74

Which of the following IP addresses are private addresses?

Each correct answer represents a complete solution. Choose all that apply.

A. 19.3.22.17
B. 192.168.15.2
C. 192.166.54.32
D. 10.0.0.3

Answer: B,D

QUESTION NO: 75

Sandra, a novice computer user, works on Windows environment. She experiences some problem regarding bad sectors formed in a hard disk of her computer. She wants to run CHKDSK command to check the hard disk for bad sectors and to fix the errors, if any, occurred. Which of the following switches will she use with CHKDSK command to accomplish the task?

A. CHKDSK /I
B. CHKDSK /C /L
C. CHKDSK /V /X
D. CHKDSK /R /F

Answer: D

QUESTION NO: 76

Which of the following statements about an extended partition are true?

Each correct answer represents a complete solution. Choose two.

A. It can be sub-divided into logical drives.
B. It cannot be formatted or assigned a drive letter.
C. A maximum of four extended partitions can exist on a single basic disk.
D. It cannot contain more than one logical drive.

Answer: A,B

QUESTION NO: 77

You are reviewing a Service Level Agreement between your company and a Web development vendor.

Which of the following are security requirements you should look for in this SLA?

Each correct answer represents a complete solution. Choose all that apply.

A. Time to respond to bug reports
B. Encryption standards
C. Security Monitoring
D. Guarantees on known security flaws

Answer: A,B,C,D

QUESTION NO: 78

Which of the following is used to detect the bad sectors in a hard disk under Linux environment?

A. Badblocks
B. CheckDisk
C. ScanDisk
D. CHKDSK

Answer: A

QUESTION NO: 79

Which of the following statements are NOT true about volume boot record or Master Boot Record?

Each correct answer represents a complete solution. Choose all that apply.

A. The end of MBR marker is h55CC.
B. The actual program can be 512 bytes long.
C. Volume boot sector is present at cylinder 0, head 0, and sector 1 of the default boot drive.
D. Four 16 bytes master partition records are present in MBR.

Answer: A,B

QUESTION NO: 80

Which of the following tools can be used by a user to hide his identity?

Each correct answer represents a complete solution. Choose all that apply.

A. Proxy server
B. Anonymizer
C. Rootkit
D. IPchains
E. War dialer

Answer: A,B,D

QUESTION NO: 81

Normally, RAM is used for temporary storage of data. But sometimes RAM data is stored in the hard disk, what is this method called?

A. Cache memory
B. Static memory
C. Virtual memory
D. Volatile memory

Answer: C

QUESTION NO: 82

Nathan works as a professional Ethical Hacker. He wants to see all open TCP/IP and UDP ports of his computer. Nathan uses the netstat command for this purpose but he is still unable to map open ports to the running process with PID, process name, and path. Which of the following commands will Nathan use to accomplish the task?

A. ping

B. Psloggedon
C. Pslist
D. fport

Answer: D

QUESTION NO: 83

Adam works as a professional Computer Hacking Forensic Investigator. He works with the local police. A project has been assigned to him to investigate an iPod, which was seized from a student of the high school. It is suspected that the explicit child pornography contents are stored in the iPod. Adam wants to investigate the iPod extensively. Which of the following operating systems will Adam use to carry out his investigations in more extensive and elaborate manner?

A. Linux
B. MINIX 3
C. Windows XP
D. Mac OS

Answer: D

QUESTION NO: 84

Which of the following parameters is NOT used for calculating the capacity of the hard disk?

A. Bytes per sector
B. Number of heads
C. Total number of sectors
D. Number of platters

Answer: D

QUESTION NO: 85

In which of the following access control models can a user not grant permissions to other users to see a copy of an object marked as secret that he has received, unless they have the appropriate permissions?

A. Discretionary Access Control (DAC)
B. Access Control List (ACL)
C. Mandatory Access Control (MAC)
D. Role Based Access Control (RBAC)

Answer: C

QUESTION NO: 86

Adam works as a professional Computer Hacking Forensic Investigator. He has been called by the FBI to examine data of the hard disk, which is seized from the house of a suspected terrorist. Adam decided to acquire an image of the suspected hard drive. He uses a forensic hardware tool, which is capable of capturing data from IDE, Serial ATA, SCSI devices, and flash cards. This tool can also produce MD5 and CRC32 hash while capturing the data. Which of the following tools is Adam using?

A. Wipe MASSter
B. ImageMASSter 4002i
C. ImageMASSter Solo-3
D. FireWire DriveDock

Answer: C

QUESTION NO: 87

Adam works as a professional Computer Hacking Forensic Investigator. A project has been assigned to him to investigate the BlackBerry, which is suspected to be used to hide some important information. Which of the following is the first step taken to preserve the information in forensic investigation of the BlackBerry?

A. Keep BlackBerry in 'ON' state.
B. Remove the storage media.
C. Eliminate the ability of the device to receive the push data.
D. Turn off the BlackBerry.

Answer: C

QUESTION NO: 88
Which of the following prevents malicious programs from attacking a system?

Trying our product !

★ **100%** Guaranteed Success

★ **100%** Money Back Guarantee

★ **365 Days** Free Update

★ **Instant Download** After Purchase

★ **24x7** Customer Support

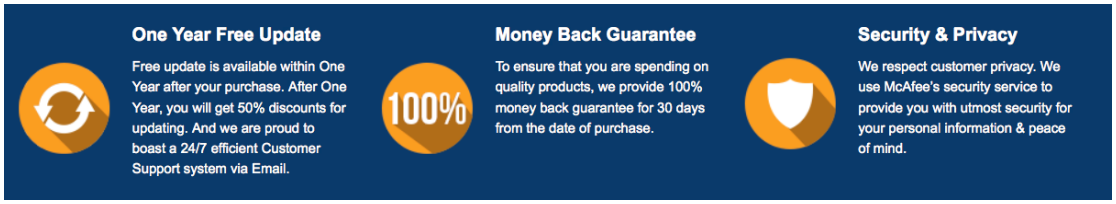
★ Average **99.9%** Success Rate

★ More than **69,000** Satisfied Customers Worldwide

★ Multi-Platform capabilities - **Windows, Mac, Android, iPhone, iPod, iPad, Kindle**

Need Help

Please provide as much detail as possible so we can best assist you.
To update a previously submitted ticket:



Guarantee & Policy | Privacy & Policy | Terms & Conditions