



- Expert Verified, Online, **Free**.



CERTIFICATION TEST

- CertificationTest.net - Cheap & Quality Resources With Best Support

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.

Suggested Answer: C

🗨️ **Conkerzin** 1 year, 1 month ago

Is content of this page enough to pass GCFA exam?
upvoted 1 times

🗨️ **senjouahara** 5 months, 2 weeks ago

there are pbl less than 20 questions that are relevant to current GCFA exam, it gets refreshed frequently so don't get your hopes up.
upvoted 1 times

🗨️ **Genesis777** 1 year, 1 month ago

No its not enough to pass, the questions can support you if you study well. BUT Learn the concepts (hands-on labs) very well to pass the cyber live part of the exam. Even if you have 80% to 90% of the multiple choice questions right and don't complete any of the virtual labs or even pass at least 80% of the labs (8 to 10 out of 11 labs) in the exam. You will fail.
upvoted 1 times

🗨️ **PrismWalker** 1 year, 7 months ago

The command that Adam has run is intended to wipe the contents of the hard disk. Here's what it does:

- `dd if=/dev/random of=/dev/hda`: This part of the command writes random data to the hard disk (`/dev/hda`). The `dd` command is used for low-level copying from one location (if, or input file) to another (of, or output file). In this case, it's copying from `/dev/random`, which generates random data, to `/dev/hda`, which represents the hard disk.
 - `dd if=/dev/zero of=/dev/hda`: This part of the command writes zeros to the hard disk, effectively overwriting the random data from the previous command.
 - `for ((i = 0;i<11;i++)); do ... done`: This is a loop that runs the `dd` commands 11 times. This is likely done to make sure that the data is thoroughly overwritten and cannot be recovered.
- upvoted 1 times

🗨️ **PrismWalker** 1 year, 7 months ago

i think it's C
upvoted 1 times

🗨️ **boyladdudeman** 4 years, 2 months ago

C is correct
upvoted 1 times

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

Suggested Answer: A

  **PrismWalker** 1 year, 1 month ago

Trademark law protects the use of words, symbols, or logos that identify and distinguish the source of goods or services. In this case, the employee's use of a nearly identical trademark is likely to confuse consumers into believing that the employee's garments are affiliated with the company.

- Cyber law is a broad term that encompasses a wide range of laws and regulations related to computers and the Internet. It is not directly applicable to this case.
- Copyright law protects original works of authorship, including literary, dramatic, musical, and artistic works. It is not directly applicable to this case because the garment designs are not considered to be original works of authorship.
- Espionage law is the law that deals with the theft of trade secrets or other confidential information. It is not directly applicable to this case because the employee did not steal trade secrets.

upvoted 1 times

  **PrismWalker** 1 year, 1 month ago

A is correct

upvoted 1 times

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

Suggested Answer: *B*

Community vote distribution

B (100%)

  **gnnggnngnng** 7 months ago

Selected Answer: B

Windows 98 stores registry tools in the Windows directory.

upvoted 1 times

  **PrismWalker** 1 year, 1 month ago

It's B for me

upvoted 2 times

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

Suggested Answer: D

Community vote distribution

D (100%)

  **gnnggnngngng** 7 months ago

Selected Answer: D

Cain can perform password cracking, Windows enumeration, and VoIP sniffing.

upvoted 1 times

  **PrismWalker** 1 year, 1 month ago

D is correct

upvoted 2 times

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

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

Suggested Answer: C

Community vote distribution

C (100%)

  **gnnggnngnng** 7 months ago

Selected Answer: C

HFS is a macOS file system and is not supported by the Linux kernel by default.

upvoted 1 times

  **Mohandakkhli** 10 months, 1 week ago

Selected Answer: C

HFS is not supported

FAT32 Is fully supported for usb storage and memory card

upvoted 2 times

  **PrismWalker** 1 year, 1 month ago

The Linux kernel has support for NTFS. Starting from Linux kernel 5.15, it includes Paragon Software's NTFS3 kernel driver, which provides improved support for NTFS.

But stating back to the old days. I think it's B

upvoted 1 times

  **twirlerrose** 1 year, 2 months ago

It definitely supports Fat32. I read an article that starting in 2022 it started supporting NTFS so maybe it's just an old question?

upvoted 1 times

  **twirlerrose** 1 year, 2 months ago

Vfat and HFS are supported.

upvoted 1 times

  **ShH0lm3s** 1 year, 9 months ago

Where does this come from? Linux doesn't support APFS and probably ReFS, but FAT32 is universal.

https://en.wikipedia.org/wiki/FAT_filesystem_and_Linux

upvoted 1 times

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

Suggested Answer: A

Community vote distribution

A (100%)

  **gnnggnngnng** 7 months ago

Selected Answer: A

BSD layer in OS X (XNU) provides the system call interface.

upvoted 1 times

  **PrismWalker** 1 year, 1 month ago

The BSD subsystem is responsible for many user-level functionalities and system interfaces but is not the primary system program interface provided by the kernel.

So it's A

upvoted 2 times

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

Suggested Answer: *B*

Community vote distribution

B (100%)

  **gnnggnngnng** 7 months ago

Selected Answer: B

B is Correct. FAT32 is supported by both Windows Me and XP, making it suitable for dual boot.

upvoted 1 times

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

Suggested Answer: D

Community vote distribution

D (100%)

  **gnngngngngng** 7 months ago

Selected Answer: D

This type of email is classic chain letter behavior, intended to proliferate widely under false pretenses.

upvoted 1 times

  **PrismWalker** 1 year, 1 month ago

Spambots are automated programs that send out large amounts of spam, which is unsolicited or bulk email that is sent to multiple recipients without their permission. Spambots are often used to advertise products or services, but they can also be used to spread malware or phishing scams.



Chain letters are a type of email that asks the recipient to forward it to a certain number of other people. The chain letter may promise good luck or fortune to those who forward it, but it may also contain threats or warnings. Chain letters are often used to spread misinformation or to collect email addresses.

upvoted 1 times

  **PrismWalker** 1 year, 1 month ago

Chain letters for sure

upvoted 1 times

  **twirlerrose** 1 year, 2 months ago

Spambot. Chain letters usually tell you to forward to X-number of people or bad luck will happen.

upvoted 1 times

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

Suggested Answer: D

Community vote distribution

D (100%)

  **gnnggnngnng** 7 months ago

Selected Answer: D

The Electronic Communications Privacy Act allows the FBI to issue National Security Letters.
upvoted 1 times

  **PrismWalker** 1 year, 1 month ago

The Electronic Communications Privacy Act of 1986 (ECPA) allows the FBI to issue National Security Letters (NSLs) to ISPs ordering them to disclose records about their customers. NSLs are a type of administrative subpoena that can be used to obtain a wide range of information, including phone records, email records, and IP addresses.
upvoted 1 times

  **PrismWalker** 1 year, 1 month ago

It's D
upvoted 1 times

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

Suggested Answer: D

Community vote distribution

D (100%)

🗳️ 👤 **gnnggnngnng** 7 months ago

Selected Answer: D

Windows responds with RST to any unexpected FIN, making it identifiable via FIN scanning.

upvoted 1 times

🗳️ 👤 **PrismWalker** 1 year, 1 month ago

D is correct

upvoted 1 times

Which of the following encryption methods uses AES technology?


- A. Dynamic WEP
- B. Static WEP
- C. TKIP
- D. CCMP

Suggested Answer: *D*

  **PrismWalker** 1 year, 1 month ago

CCMP, or Counter Mode with Cipher Block Chaining Message Authentication Code Protocol, is a security protocol used in Wi-Fi networks. It uses AES technology to encrypt data and provide authentication.

upvoted 1 times

  **PrismWalker** 1 year, 1 month ago

It's D

upvoted 1 times

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

Suggested Answer: A

Community vote distribution

A (100%)

🗲️ 👤 **gnnggnngnng** 7 months ago

Selected Answer: A

Electronic surveillance is used to monitor ongoing computer crime.

upvoted 1 times

🗲️ 👤 **Jonesq** 7 months, 3 weeks ago

Selected Answer: A

I think A

upvoted 1 times

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

Suggested Answer: C

Community vote distribution

C (100%)

🗨️ 👤 **gnnggnnggnng** 7 months ago

Selected Answer: C

Brain was the first virus to infect the DOS FAT boot sector.

upvoted 1 times

🗨️ 👤 **Lokmane14** 1 year, 1 month ago

Selected Answer: C

Brain virus is correct. It was written in 1986 and it targeted IBM PC-compatible computers.

upvoted 1 times



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

Suggested Answer: C

Community vote distribution

C (100%)

  **Jonesq** 7 months, 3 weeks ago

Selected Answer: C

C is right

upvoted 1 times

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

Suggested Answer: A

Community vote distribution

A (100%)

🗨️ 👤 **1913a4b** 3 months, 4 weeks ago

Selected Answer: A

A is correct

upvoted 1 times

🗨️ 👤 **Jonesq** 7 months, 3 weeks ago

Selected Answer: A

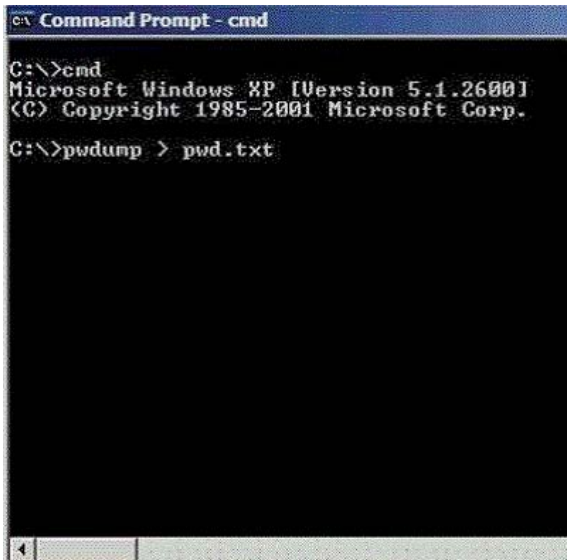
I think A

upvoted 2 times

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 check on 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:



```
Command Prompt - cmd
C:\>cmd
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\>pwdump > pwd.txt
```

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.

Suggested Answer: C

Currently there are no comments in this discussion, be the first to comment!

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

Suggested Answer: BC

Community vote distribution



gnnggnngnng 7 months ago

Selected Answer: BC

Boot sector virus - Directly infects the MBR or boot sector of storage devices.

Multipartite virus- Infects both the boot sector and system files (.EXE, .COM).

upvoted 1 times

sasa2323123 7 months ago

Selected Answer: A

I think it's A

upvoted 1 times

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

Suggested Answer: ABD

Currently there are no comments in this discussion, be the first to comment!

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

Suggested Answer: C

Community vote distribution

C (100%)

  **gnnggnngngng** 7 months ago

Selected Answer: C

The Secure Authentication for EnCase (SAFE) server is used for secure network acquisition within the EnCase forensic environment. It authenticates users, controls access to network devices, and uses encryption to secure communications.

upvoted 1 times

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.

Suggested Answer: A

Community vote distribution

A (100%)

 **gnnggnngnng** 7 months ago

Selected Answer: A

Preserving the email server and its logs maintains the chain of custody.
upvoted 1 times

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

Suggested Answer: B

Community vote distribution

B (100%)

  **gnnggnngnng** 7 months ago

Selected Answer: B

Step Component Purpose

1 NTLDR Loads boot loader and reads BOOT.INI



2 BOOT.INI Specifies installed OS paths

3 NTDETECT.COM Collects and passes hardware info

4 HAL.DLL Abstracts hardware differences

5 NTOSKRNL.EXE Boots the Windows kernel and initiates OS load

upvoted 1 times

  **Jonesq** 7 months, 3 weeks ago

Selected Answer: B

B is right!

upvoted 2 times

SIMULATION -

Fill in the blank with the appropriate name.

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

Suggested Answer: *RFC 3227*

Currently there are no comments in this discussion, be the first to comment!

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

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

Suggested Answer: *D*

Community vote distribution

D (100%)

  **gnnggnngngng** 7 months ago

Selected Answer: D

NTFS supports file-level security.

upvoted 1 times

  **Jonesq** 7 months, 3 weeks ago

Selected Answer: D

D is right!

upvoted 2 times

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

Suggested Answer: D

Community vote distribution

D (100%)

🗨️ 👤 **gnnggnngngng** 7 months ago

Selected Answer: D

Adam is isolating the network and preparing imaging, which is part of containment.

upvoted 1 times

🗨️ 👤 **Jonesq** 7 months, 3 weeks ago

Selected Answer: D

Is right!

upvoted 2 times

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

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

Suggested Answer: A

Currently there are no comments in this discussion, be the first to comment!

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

Suggested Answer: B

Community vote distribution

B (100%)

  **gnnggnngnng** 7 months ago

Selected Answer: B

Bluesnarfing allows unauthorized access to a Bluetooth-enabled device.

upvoted 1 times

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.

Suggested Answer: *E*

Currently there are no comments in this discussion, be the first to comment!

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

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

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

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

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.

Suggested Answer: ABD

Currently there are no comments in this discussion, be the first to comment!

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.

Suggested Answer: ABD

Currently there are no comments in this discussion, be the first to comment!

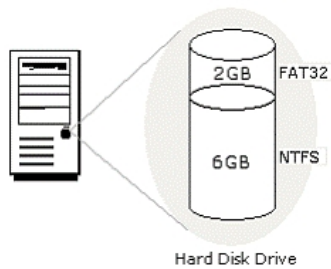
An organization monitors the hard disks of its employees' computers from time to time. Which policy does this pertain to?

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

Suggested Answer: C

Currently there are no comments in this discussion, be the first to comment!

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.

Suggested Answer: C

Currently there are no comments in this discussion, be the first to comment!

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

Suggested Answer: ABD

Currently there are no comments in this discussion, be the first to comment!

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

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

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

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

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)

Suggested Answer: *CD*

Currently there are no comments in this discussion, be the first to comment!

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

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

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

Suggested Answer: AB

Community vote distribution

BC (100%)

🗲️ 👤 **1913a4b** 4 months ago

Selected Answer: BC

Answer should be B and C
upvoted 1 times

🗲️ 👤 **gnnggnnggnng** 7 months ago

Selected Answer: BC

EFS uses public key cryptography, specifically RSA.
upvoted 1 times

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

Suggested Answer: A

Currently there are no comments in this discussion, be the first to comment!

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

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

Suggested Answer: *D*

  **ruslanira** 1 year, 1 month ago

/k - Copies files and retains the read-only attribute on destination files if present on the source files. By default, xcopy removes the read-only attribute.
upvoted 4 times

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

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

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

Suggested Answer: *ABD*

Currently there are no comments in this discussion, be the first to comment!

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

Suggested Answer: C

Currently there are no comments in this discussion, be the first to comment!

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.

Suggested Answer: A

Currently there are no comments in this discussion, be the first to comment!

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

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

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

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

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

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

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

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

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

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

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

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

- A. NTFS
- B. CIFS
- C. ext2
- D. ZFS

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

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

Suggested Answer: *ABC*

  **ruslanira** 1 year, 1 month ago

The backup utility can store backups either locally on the SecurePlatform machine hard drive or to an FTP server, TFTP server or SCP server.
upvoted 2 times

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

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

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.

Select and Place:

Correct steps	Choose from here
	Footprinting
	Session hijacking
	Placing backdoors
	Identifying the active system
	Web server hacking
	Enumerating the system

Suggested Answer:

Correct steps	Choose from here
Footprinting	Session hijacking
Identifying the active system	Placing backdoors
Enumerating the system	Web server hacking

Currently there are no comments in this discussion, be the first to comment!

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.

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

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

Suggested Answer: *BCD*

Currently there are no comments in this discussion, be the first to comment!

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

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

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.

Suggested Answer: *ABC*

Currently there are no comments in this discussion, be the first to comment!

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

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

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)

Suggested Answer: B

Currently there are no comments in this discussion, be the first to comment!

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

Suggested Answer: A

Currently there are no comments in this discussion, be the first to comment!

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

Suggested Answer: ABC

🗨️ 👤 **kamau5** 1 year, 4 months ago

Sam Spade is also a graphical tool which allows you to do DNS interrogation and many other things. The features which make Sam Spade a key security tool are:

Advanced DNS - DIG tool requests all the DNS records for a host or domain

Zone Transfer - ask a DNS server for all it knows about a domain

SMTP Relay Check - check whether a mail server allows third party relaying

Scan Addresses - scan a range of IP addresses looking for open ports

Crawl Web site - search a Web site, looking for email addresses, offsite links, download a Web site

Search IP block - finds the IP block for an organization

Sam Spade also does whois, traceroute, finger and dns lookup.

upvoted 1 times

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.

Suggested Answer: AB

Currently there are no comments in this discussion, be the first to comment!

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

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

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.

Suggested Answer: *BC*

Currently there are no comments in this discussion, be the first to comment!

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@wetpaintmail.com>
X-YahooFilteredBulk: 216.168.54.25
X-MailISG: IIOjRIWLDzhqPeX9g5WgzYv2Hbqcg/v47u8ekfvp65bE42euHuhU2OU9QtaJk9tnI3dhriCmF.cmkU96g9e8ggD
X-Originating-IP: [216.168.54.25]
Authentication-Results: mta251.mail.re3.yahoo.com from=vetpaintmail.com; domainkey=pass (ok)
Received: from 216.168.54.25 (EHLO mail.wetpaintmail.com) (216.168.54.25) by mta251.mail.re3.yahoo.com with SMTP
Received: from wetpaintmail.com ([172.16.10.90]) by mail.wetpaintmail.com (StrongMail Enterprise 4.1.1.1(4.1.1-448:
X-VirtualServer: Digest
X-VirtualServerGroup: Digest
X-MailingID: 1181167079:164600:11249857716:19100:11133:11133
X-SMHeaderMap: mid="X-MailingID"
X-Mailers: StrongMail Enterprise 4.1.1.1(4.1.1-44827)
X-Destination-ID: itzme_adee@yahoo.com
X-SMFBID: aXR6bWVhYWRIZU85YWwhby5jb20=
DomainKey-Signature: a=rsa-sha1; c=noenv; s=customer; d=wetpaintmail.com; q=dns; b=Yv6LHRzb+8Jaik8frikFeO2WPnpkJM5J1F
Content-Transfer-Encoding: 7bit
Content-Type: multipart/alternative; boundary="-----=_NextPart_0F9_1F0B_2109CDA4.577F5A4D"
Reply-To: <no-reply@wetpaintmail.com>
MIME-Version: 1.0
Message-ID: <1181167079.1133@wetpaintmail.com>
Subject: The Ethical Hacking Weekly Digest
Date: Mon, 10 Aug 2009 07:57:02 -0700
To: itzme_adee@yahoo.com
From:  The Ethical Hacking <info@wetpaintmail.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

Suggested Answer: C

Currently there are no comments in this discussion, be the first to comment!

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.

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

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

Suggested Answer: D

Community vote distribution

B (100%)

🗳️ 👤 **1913a4b** 3 months, 4 weeks ago

Selected Answer: B

Answer should be B if can only select one. Otherwise D can be considered
upvoted 1 times

🗳️ 👤 **Analyst2023** 1 year, 3 months ago

Answer should be B.

Distribution, and production of child pornography is a federal crime under the "Child Pornography Prevention Act of 1996" (CPPA) and the "Protect Act of 2003" (PROTECT Act), both of which were passed to strengthen existing laws related to child sexual exploitation.D
upvoted 3 times

🗳️ 👤 **ruslanira** 1 year, 7 months ago

H.R.3494 - Protection of Children From Sexual Predators Act of 1998

- Title II: Protection of Children From Child Pornography - Provides for the prosecution of individuals for the production of child pornography if the visual depiction was produced with materials that have been mailed, shipped, or transported in interstate or foreign commerce, including by computer.
upvoted 1 times


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

Suggested Answer: *D*

Community vote distribution

A (100%)

  **1913a4b** 3 months, 4 weeks ago

Selected Answer: A

Correct answer should be A, answer is wrong

upvoted 1 times

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

Suggested Answer: ABCD

Community vote distribution

ABC (100%)

  **1913a4b** 3 months, 4 weeks ago

Selected Answer: ABC

Answer should be ABC, D is more of a compliance rather than a response enhancement
upvoted 1 times

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

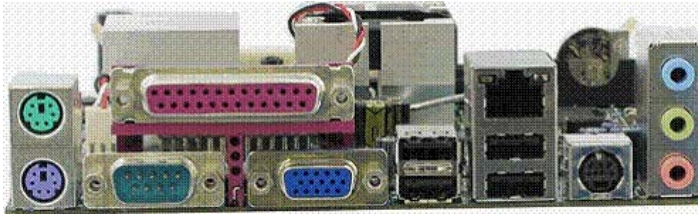
Suggested Answer: A

Currently there are no comments in this discussion, be the first to comment!

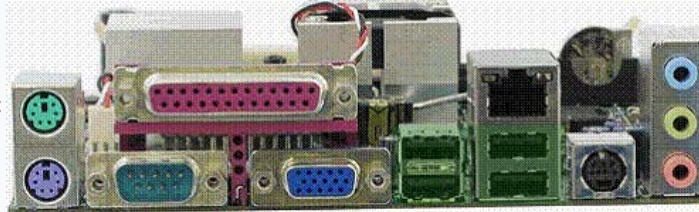
HOTSPOT -

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?

Hot Area:



Suggested Answer:



 Analyst2023 1 year, 3 months ago

should be USB because there are up to 127 devices connected to USB.

upvoted 1 times

 ruslanira 1 year, 7 months ago

It has to be RJ-45 port

upvoted 1 times

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.

Suggested Answer: AD

Currently there are no comments in this discussion, be the first to comment!

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

Suggested Answer: *BD*

Currently there are no comments in this discussion, be the first to comment!

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

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

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.

Suggested Answer: *AB*

Currently there are no comments in this discussion, be the first to comment!

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

Suggested Answer: *ABCD*

Currently there are no comments in this discussion, be the first to comment!

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

Suggested Answer: A

Currently there are no comments in this discussion, be the first to comment!

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.

Suggested Answer: *AB*

Currently there are no comments in this discussion, be the first to comment!

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

Suggested Answer: *ABD*

Currently there are no comments in this discussion, be the first to comment!

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

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

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

Suggested Answer: *D*

  **ruslanira** 1 year, 1 month ago

Fport is a portable command line utility that will report all open TCP and UDP ports to the user. The port analyzer maps each open port to an application which distinguishes it from the netstat -an command in Windows which otherwise provides the same level of detail and information.
upvoted 2 times

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

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

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

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

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)

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

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 MASter
- B. ImageMASter 4002i
- C. ImageMASter Solo-3
- D. FireWire DriveDock

Suggested Answer: C

Currently there are no comments in this discussion, be the first to comment!

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.

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Which of the following prevents malicious programs from attacking a system?

- A. Anti-virus program
- B. Smart cards
- C. Biometric devices
- D. Firewall

Suggested Answer: A

Currently there are no comments in this discussion, be the first to comment!

Which of the following terms refers to a mechanism which proves that the sender really sent a particular message?

- A. Confidentiality
- B. Authentication
- C. Non-repudiation
- D. Integrity

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Adam works as a professional Computer Hacking Forensic Investigator. A project has been assigned to him by the chief security officer of a cloth manufacturing company who suspects that one of the employees is selling the design of the clothes outside the company. The security officer asked Adam to investigate the iPhone of the employee, as he suspects that there might be some sensitive information stored in his iPhone. On investigation Adam found out that the employee tries to destroy the evidence on his iPhone. He presses and holds the Home and Power buttons until the device is forced into recovery mode. Which of the following actions occurred when iPhone is set into recovery mode?

- A. iPhone will be prevented from booting temporarily.
- B. The file system will be destroyed.
- C. Nothing will happen.
- D. Data will be destroyed.

Suggested Answer: A

Currently there are no comments in this discussion, be the first to comment!

Which of the following is a file management tool?

- A. Defrag
- B. MSCONFIG
- C. Device Manager
- D. Windows Explorer

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Which of the following is a correct sequence of different layers of Open System Interconnection (OSI) model?

- A. Physical layer, data link layer, network layer, transport layer, presentation layer, session layer, and application layer
- B. application layer, presentation layer, network layer, transport layer, session layer, data link layer, and physical layer
- C. Physical layer, data link layer, network layer, transport layer, session layer, presentation layer, and application layer
- D. Physical layer, network layer, transport layer, data link layer, session layer, presentation layer, and application layer

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

John works as a professional Ethical Hacker. He is assigned a project to test the security of www.weare-secure.com. He is working on the Linux operating system.

He wants to sniff the we-are-secure network and intercept a conversation between two employees of the company through session hijacking. Which of the following tools will John use to accomplish the task?

- A. Ethercap
- B. Tripwire
- C. Hunt
- D. IPChains

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

You are the Network Administrator and your company has recently implemented encryption for all emails. You want to check to make sure that the email packages are being encrypted. What tool would you use to accomplish this?

- A. Password cracker
- B. Packet sniffer
- C. Performance Monitor
- D. Vulnerability analyzer

Suggested Answer: *B*

  **ruslanira** 1 year, 1 month ago

Packet sniffer will show if emails were sent across the network encrypted or clear-text.

upvoted 2 times

Which of the following file systems contains hardware settings of a Linux computer?

- A. /var
- B. /etc
- C. /proc
- D. /home

Suggested Answer: C

  **PrismWalker** 1 year, 1 month ago

The /proc file system in Linux contains information about the system's hardware settings and the status of running processes. It's a virtual file system that provides a mechanism for kernel to send information to processes.

upvoted 1 times

Which of the following is a set of exclusive rights granted by a state to an inventor or his assignee for a fixed period of time in exchange for the disclosure of an invention?

- A. Snooping
- B. Copyright
- C. Utility model
- D. Patent

Suggested Answer: *D*

  **PrismWalker** 1 year, 1 month ago

A patent is a set of exclusive rights granted by a state to an inventor or his assignee for a fixed period of time in exchange for the disclosure of an invention. This allows the inventor to prevent others from using, making, or selling the invention without their permission for a certain period of time.

upvoted 1 times

Which of the following tools can be used to perform a whois query?

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

- A. Sam Spade
- B. SuperScan
- C. Traceroute
- D. WsPingPro

Suggested Answer: *ABD*

Currently there are no comments in this discussion, be the first to comment!

Adam works as a professional Computer Hacking Forensic Investigator. A project has been assigned to him to investigate the main server of SecureEnet Inc. The server runs on Debian Linux operating system. Adam wants to investigate and review the GRUB configuration file of the server system.

Which of the following files will Adam investigate to accomplish the task?

- A. /boot/grub/menu.lst
- B. /boot/grub/grub.conf
- C. /boot/boot.conf
- D. /grub/grub.com

Suggested Answer: A

Community vote distribution

A (100%)

🗨️ 👤 **1913a4b** 4 months ago

Selected Answer: A

On legacy Debian, it should be A is correct

upvoted 1 times

🗨️ 👤 **ruslanira** 1 year, 1 month ago

B should be correct. It's where the GRUB configuration file is located.

upvoted 1 times

You are the Security Consultant and have been contacted by a client regarding their encryption and hashing algorithms. Their in-house network administrator tells you that their current hashing algorithm is an older one with known weaknesses and is not collision resistant. Which algorithm are they most likely using for hashing?

- A. SHA
- B. MD5
- C. PKI
- D. Kerberos

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

You work as a Network Administrator for a bank. For securing the bank's network, you configure a firewall and an IDS. In spite of these security measures, intruders are able to attack the network. After a close investigation, you find that your IDS is not configured properly and hence is unable to generate alarms when needed. What type of response is the IDS giving?

- A. False Positive
- B. True Negative
- C. True Positive
- D. False Negative

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

John works as a Network Administrator for Perfect Solutions Inc. The company has a Linux-based network. John is working as a root user on the Linux operating system. Which of the following commands will John use to display information about all mounted file systems?

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

- A. du
- B. ls
- C. df
- D. df -m

Suggested Answer: *CD*

Currently there are no comments in this discussion, be the first to comment!

Which of the following statements about registry is true?

Each correct answer represents a complete solution. Choose three.

- A. It is divided in many areas known as hives.
- B. It was first introduced with Windows 95 operating system.
- C. It is a centralized configuration database that stores information related to a Windows computer.
- D. It can be edited using SCANREG utility.

Suggested Answer: ABC

Currently there are no comments in this discussion, be the first to comment!

Which of the following diagnostic codes sent by POST to the internal port h80 refers to the system board error?

- A. 200 to 299
- B. 100 to 199
- C. 400 to 499
- D. 300 to 399

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Victor works as a professional Ethical Hacker for SecureNet Inc. He wants to use Steganographic file system method to encrypt and hide some secret information.

Which of the following disk spaces will he use to store this secret information?

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

- A. Hidden partition
- B. Slack space
- C. Dumb space
- D. Unused Sectors

Suggested Answer: *ABD*

Currently there are no comments in this discussion, be the first to comment!

Which of the following is the Windows feature on which the file management can be performed by a PC user?

- A. Activity Monitor
- B. Task Manager
- C. Windows Explorer
- D. Finder

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

You are responsible for maintaining and troubleshooting PC's at your company. The receptionist reports her screen has gone blue. When you get there you notice the 'blue screen of death' with an error message NTFS_FILE_SYSTEM. What is the most likely cause of this error?

- A. The hard disk is corrupt
- B. A virus
- C. Windows was installed improperly.
- D. Get the latest patch for Windows.

Suggested Answer: A

Currently there are no comments in this discussion, be the first to comment!

Which of the following types of firewall functions at the Session layer of OSI model?

- A. Application-level firewall
- B. Switch-level firewall
- C. Packet filtering firewall
- D. Circuit-level firewall

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Joseph works as a Web Designer for WebTech Inc. He creates a Web site and wants to protect it from lawsuits. Which of the following steps will he take to accomplish the task?

Each correct answer represents a part of the solution. Choose all that apply.

- A. Restrict the access to the site.
- B. Restrict shipping in certain areas.
- C. Restrict the transfer of information.
- D. Restrict customers according to their locations.

Suggested Answer: *ABD*

Currently there are no comments in this discussion, be the first to comment!

Trinity wants to send an email to her friend. She uses the MD5 generator to calculate cryptographic hash of her email to ensure the security and integrity of the email. MD5 generator, which Trinity is using operates in two steps:

- ⇒ Creates check file
- ⇒ Verifies the check file

Which of the following MD5 generators is Trinity using?

- A. MD5 Checksum Verifier
- B. Mat-MD5
- C. Chaos MD5
- D. Secure Hash Signature Generator



Suggested Answer: A

Currently there are no comments in this discussion, be the first to comment!

Which utility enables you to access files from a Windows .CAB file?

- A. ACCESS.EXE
- B. WINZIP.EXE
- C. XCOPY.EXE
- D. EXTRACT.EXE

Suggested Answer: *D*

  **twirlerrose** 1 year, 2 months ago

Winzip will open CAB files

upvoted 1 times

Adam works as a professional Computer Hacking Forensic Investigator. He has been assigned with a project to investigate a computer in the network of

SecureEnet Inc. The compromised system runs on Windows operating system. Adam decides to use Helix Live for Windows to gather data and electronic evidences starting with retrieving volatile data and transferring it to server component via TCP/IP. Which of the following application software in Helix Windows

Live will he use to retrieve volatile data and transfer it to the server component via TCP/IP?

- A. FSP
- B. Drive Manager
- C. FTK imager
- D. FAU

Suggested Answer: A

Currently there are no comments in this discussion, be the first to comment!

Adam works as a professional Computer Hacking Forensic Investigator. A project has been assigned to him to investigate a compromised system of a cyber criminal, who hides some information in his computer. This computer runs on Linux operating system. Adam wants to extract the data units of a file, which is specified by its meta-data address. He is using the Sleuth Kit for this purpose. Which of the following commands in the Sleuth kit will he use to accomplish the task?

- A. dcat
- B. ifind
- C. icat
- D. istat

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Which of the following graphical tools is used to navigate through directory structures?

- A. Disk Cleanup
- B. System Information
- C. Disk Management
- D. Windows Explorer

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

John is a black hat hacker. FBI arrested him while performing some email scams. Under which of the following US laws will john be charged?

- A. 18 U.S.C. 2701
- B. 18 U.S.C. 1030
- C. 18 U.S.C. 1362
- D. 18 U.S.C. 2510

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Mark has been hired by a company to work as a Network Assistant. He is assigned the task to configure a dial-up connection. He is configuring a laptop. Which of the following protocols should he disable to ensure that the password is encrypted during remote access?

- A. MSCHAP
- B. SPAP
- C. MSCHAP V2
- D. PAP

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Which of the following anti-child pornography organizations helps local communities to create programs and develop strategies to investigate child exploitation?

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

Suggested Answer: B

Community vote distribution

D (100%)

🗳️ 👤 **1913a4b** 3 months, 4 weeks ago

Selected Answer: D

Answer should be D, it is catered to local communities
upvoted 1 times

Which of the following statements about the HKEY_LOCAL_MACHINE registry hive is true?

- A. It contains the user profile for the user who is currently logged on to the computer.
- B. It contains information about the local computer system, including hardware and operating system data, such as bus type, system memory, device drivers, and startup control parameters.
- C. It contains configuration data for the current hardware profile.
- D. It contains data that associates file types with programs and configuration data for COM objects, Visual Basic programs, or other automation.

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Adam works as a professional Computer Hacking Forensic Investigator. A project has been assigned to him to investigate and examine drive image of a compromised system, which is suspected to be used in cyber crime. Adam uses Forensic Sorter to sort the contents of hard drive in different categories. Which of the following type of image formats is NOT supported by Forensic Sorter?

- A. PFR image file
- B. iso image file
- C. RAW image file
- D. EnCase image file

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

In the United States, Title VII of the 1964 Civil Rights Act was formulated to protect an employee from discrimination on the basis of religion, color, race, national origin, and sex. This law makes discrimination in employment illegal. Which of the following was the original emphasis of the Act?

- A. Protect fundamental rights of an employee
- B. Equal position to all employees
- C. Protect woman in the workplace
- D. Prevent child pornography

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Your network has a Windows 2000 Server computer with FAT file system, shared by several users.

This system stores sensitive data. You decide to encrypt this data to protect it from unauthorized access. You want to accomplish the following goals:

- ☞ Data should be secure and encrypted.
- ☞ Administrative efforts should be minimum.
- ☞ You should have the ability to recover encrypted files in case the file owner leaves the company.
- ☞ Other permissions on encrypted files should be unaffected.
- ☞ File-level security is required on the disk where data is stored.
- ☞ Encrypting or decrypting of files should not be the responsibility of the file owner.

You take the following steps to accomplish these goals :

- ☞ Convert the FAT file system to Windows 2000 NTFS file system.
- ☞ Use Encrypting File System (EFS) to encrypt data.

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


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

- A. File-level security is available on the disk where data is stored.
- B. You have the ability to recover encrypted files in case the file owner leaves the company.
- C. Encrypting or decrypting of files is no longer the responsibility of the file owner.
- D. Data are secured and encrypted.
- E. Administrative efforts are minimum.
- F. Other permissions on encrypted files are unaffected.

Suggested Answer: ABCDEF

Community vote distribution

ABDF (100%)

 **1913a4b** 3 months, 4 weeks ago

Selected Answer: ABDF

Answer should be ABDF, CE is not correct

upvoted 1 times

Which of the following statements are true about Compact Disc (CD) and Digital Versatile Disk (DVD)?

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

- A. CDs and DVDs are affected by EMP from nuclear detonations.
- B. Data is encoded in the form of tiny pits on the surface of the CD and DVD.
- C. CDs and DVDs are not affected by X-rays, and other sources of electromagnetic radiation.
- D. It takes a small amount of energy to affect the data that written on CD and DVD.

Suggested Answer: *BD*

Community vote distribution

AB (100%)

🗨️ 👤 **1913a4b** 3 months, 4 weeks ago

Selected Answer: AB

only A and B is correct

upvoted 1 times

🗨️ 👤 **ruslanira** 1 year, 1 month ago

BC should be correct here

upvoted 3 times

Sandra wants to create a full system state backup of her computer, which is running on Microsoft Windows XP operating system. Which of the following is saved in full state system backup?



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

- A. file system information
- B. Registry
- C. Windows boot files
- D. Active Directory (NTDS)

Suggested Answer: BCD

Community vote distribution

ABC (100%)

  **1913a4b** 3 months, 4 weeks ago

Selected Answer: ABC

Answer should be ABC, D only applies if it is a domain controller
upvoted 1 times

Which of the following U.S. Federal laws addresses computer crime activities in communication lines, stations, or systems?

- A. 18 U.S.C. 1030
- B. 18 U.S.C. 1362
- C. 18 U.S.C. 2701
- D. 18 U.S.C. 2510
- E. 18 U.S.C. 1029

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

This type of virus infects programs that can execute and load into memory to perform predefined steps for infecting systems. It infects files with the extensions .EXE, .COM, .BIN, and .SYS. As it can replicate or destroy these types of files, the operating system becomes corrupted and needs reinstallation. This type of virus is known as _____.

- A. Polymorphic virus
- B. Stealth virus
- C. Boot sector virus
- D. File virus
- E. Multipartite virus

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Which of the following is a documentation of guidelines that computer forensics experts use to handle evidences?

- A. Chain of evidence
- B. Chain of custody
- C. Incident response policy
- D. Evidence access policy

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

John works as a professional Ethical Hacker. He has been assigned the project of testing the security of www.we-are-secure.com. He traceroutes the We-are-secure server and gets the following result:

```
traceroute to IP_address (IP_address): 1-30 hops, 38 byte packets
1 SF-rt5-fe9-0.geo.net (166.90.6.1) 0.48 ms 0.440 ms 0.378 ms
2 SF-core1-h1.geo.net (166.90.1.17) 0.618 ms 0.571 ms 0.521 ms
3 SF-rt2-f0.geo.net (166.90.5.7) 1.19 ms 1.94 ms 1.13 ms
4 * * *
5 * * *
```

Considering the above traceroute result, which of the following statements can be true?

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

- A. While tracerouting, John's network connection has become slow.
- B. Some router along the path is down.
- C. The We-are-secure server is using a packet filtering firewall.
- D. The IP address of the We-are-secure server is not valid.

Suggested Answer: ABC

Community vote distribution

C (100%)

🗨️ 👤 1913a4b 3 months, 4 weeks ago

Selected Answer: C

Answer should be C only

upvoted 1 times

Which of the following directories contains administrative commands and daemon processes in the Linux operating system?

- A. /etc
- B. /dev
- C. /usr
- D. /sbin

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

You work as the Network Administrator for McNeil Inc. The company has a Unix-based network. You want to query an image root device and RAM disk size.

Which of the following Unix commands can you use to accomplish the task?

- A. rdev
- B. mount
- C. setfdprm
- D. rdump

Suggested Answer: A

Currently there are no comments in this discussion, be the first to comment!

Which of the following is used to authenticate asymmetric keys?

- A. Password
- B. Digital signature
- C. MAC Address
- D. Demilitarized zone (DMZ)

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Sarah has created a site on which she publishes a copyrighted material. She is ignorant that she is infringing copyright. Is she guilty under copyright laws?

A. Yes

B. No

Suggested Answer: A

Currently there are no comments in this discussion, be the first to comment!

Which of the following describes software technologies that improve portability, manageability, and compatibility of applications by encapsulating them from the underlying operating system on which they are executed?

- A. Group Policy
- B. System registry
- C. System control
- D. Application virtualization

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

You work as a Network Administrator for Tech Perfect Inc. The company has a TCP/IP-based network. You are configuring a wireless LAN on the network. You experience interference on your network. Through investigation, you come to know that three foreign WAPs are within the range of your LAN. Although they have different SSIDs than yours, they are working on the same channel as yours.

Which of the following steps will you take to reduce the interference?

- A. Configure the same SSID as of the foreign networks.
- B. Install a router on your network.
- C. Change your WAP's channel.
- D. Install an external antenna.

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

John works as a professional Ethical Hacker. He has been assigned the project of testing the security of www.we-are-secure.com. He has successfully completed the following pre-attack phases while testing the security of the server:

- ☞ Footprinting
- ☞ Scanning

Now he wants to conduct the enumeration phase. Which of the following tools can John use to conduct it?

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

- A. WinSSLMiM
- B. PsPasswd
- C. PsFile
- D. UserInfo

Suggested Answer: *BCD*

Currently there are no comments in this discussion, be the first to comment!

In 2001, the Council of Europe passed a convention on cybercrime. It was the first international treaty seeking to address computer crime and Internet crimes by harmonizing national laws, improving investigative techniques, and increasing cooperation among nations. On 1 March 2006, the Additional Protocol to the Convention on Cybercrime came into force. Which of the following statements clearly describes this protocol?

- A. The convention of cybercrime is only applied within Europe.
- B. It requires participating states to criminalize the dissemination of racist and xenophobic material through computer systems.
- C. The convention of cybercrime should immediately be put on hold until there is an inclusion of a new or amended article.
- D. English speaking states in Europe such as Ireland and the United Kingdom should sign the convention.

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Which of the following are the benefits of information classification for an organization?

Each correct answer represents a complete solution. Choose two.

- A. It ensures that modifications are not made to data by unauthorized personnel or processes.
- B. It helps identify which information is the most sensitive or vital to an organization.
- C. It helps reduce the Total Cost of Ownership (TCO).
- D. It helps identify which protections apply to which information.

Suggested Answer: *BD*

Currently there are no comments in this discussion, be the first to comment!

You work as a Network Administrator for Net World International. You want to configure a Windows 2000 computer to dual boot with Windows 98. The hard disk drive of the computer will be configured as a single partition drive. Which of the following file systems will you use to accomplish this?

- A. NTFS
- B. HPFS
- C. FAT16
- D. FAT32

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Which of the following registry hives stores configuration information specific to a particular user who is currently logged on to the computer?

- A. HKEY_USERS
- B. HKEY_CURRENT_USER
- C. HKEY_LOCAL_MACHINE
- D. HKEY_CLASSES_ROOT

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Which of the following enables an inventor to legally enforce his right to exclude others from using his invention?

- A. Artistic license
- B. Phishing
- C. Spam
- D. Patent

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

John works as a professional Ethical Hacker. He has been assigned a project to test the security of www.we-are-secure.com. He wants to test the effect of a virus on the We-are-secure server. He injects the virus on the server and, as a result, the server becomes infected with the virus even though an established antivirus program is installed on the server. Which of the following do you think are the reasons why the antivirus installed on the server did not detect the virus injected by

John?

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

- A. The mutation engine of the virus is generating a new encrypted code.
- B. The virus, used by John, is not in the database of the antivirus program installed on the server.
- C. John has created a new virus.
- D. John has changed the signature of the virus.

Suggested Answer: *ABCD*

Currently there are no comments in this discussion, be the first to comment!

Which of the following command line tools are available in Helix Live acquisition tool on Windows?

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

- A. .cab extractors
- B. ipconfig
- C. netstat
- D. whois

Suggested Answer: ABC

Community vote distribution

BCD (100%)

🗨️ 👤 **1913a4b** 3 months, 4 weeks ago

Selected Answer: BCD

Answer should be BCD, A is not typically included
upvoted 1 times

Adam works as a Computer Hacking Forensic Investigator. He has been assigned a project to investigate child pornography. As the first step, Adam found that the accused is using a Peer-to-peer application to network different computers together over the internet and sharing pornographic materials of children with others. Which of the following are Peer-to-Peer applications?

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

- A. Gnutella
- B. Kismet
- C. Hamachi
- D. Freenet

Suggested Answer: *ACD*

Currently there are no comments in this discussion, be the first to comment!

You are a professional Computer Hacking forensic investigator. You have been called to collect the evidences of Buffer Overflows or Cookie snooping attack.

Which of the following logs will you review to accomplish the task?

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

- A. System logs
- B. Event logs
- C. Web server logs
- D. Program logs

Suggested Answer: *ABD*

Currently there are no comments in this discussion, be the first to comment!



Which of the following tools is used to extract human understandable interpretation from the computer binary files?

- A. FTK Imager
- B. Word Extractor
- C. FAU
- D. Galleta

Suggested Answer: *B*

Community vote distribution

C (100%)

  **1913a4b** 3 months, 3 weeks ago

Selected Answer: C

FAU is the correct answer

upvoted 1 times

John works as a professional Ethical Hacker. He has been assigned the task of testing the security of www.we-are-secure.com. He has performed the footprinting step and now he has enough information to begin scanning in order to detect active computers. He sends a ping request to a computer using ICMP type 13. What kind of ICMP message is John using to send the ICMP ping request message?

- A. Address mask request
- B. Echo request
- C. Information request (obsolete)
- D. Timestamp request (obsolete)

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Which of the following statements are true about routers?

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

- A. Routers organize addresses into classes, which are used to determine how to move packets from one network to another.
- B. Routers are responsible for making decisions about which of several paths network (or Internet) traffic will follow.
- C. Routers do not limit physical broadcast traffic.
- D. Routers act as protocol translators and bind dissimilar networks.

Suggested Answer: ABD

Community vote distribution

B (100%)

🗨️ 👤 **1913a4b** 3 months, 4 weeks ago

Selected Answer: B

Answer should be B only

upvoted 1 times

John, a novice web user, makes a new E-mail account and keeps his password as "apple", his favorite fruit. John's password is vulnerable to which of the following password cracking attacks?

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

- A. Rule based attack
- B. Brute Force attack
- C. Dictionary attack
- D. Hybrid attack

Suggested Answer: *BCD*

Currently there are no comments in this discussion, be the first to comment!

Which of the following tools is used to modify registry permissions in Windows?

- A. POLEDIT
- B. REGEDIT
- C. REGEDT32
- D. SECEDIT

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Which of the following file systems provides integrated security?

- A. CDFS
- B. EFS
- C. HPFS
- D. FAT32

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Convention on Cybercrime, created by the Council of Europe, is the treaty seeking to address Computer crime and Internet crimes by harmonizing national laws, improving investigative techniques, and increasing cooperation among nations. Which of the following chapters of Convention of Cybercrime contains the provisions for mutual assistances and extradition rules related to cybercrimes?

- A. Chapter II
- B. Chapter IV
- C. Chapter III
- D. Chapter I

Suggested Answer: C

Currently there are no comments in this discussion, be the first to comment!

Adam works as a Security Analyst for Umbrella Inc. He suspects that a virus exists in the network of the company. He scanned the client system with latest signature-based anti-virus, but no productive results have been obtained. Adam suspects that a polymorphic virus exists in the network. Which of the following statements are true about the polymorphic virus?

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

- A. When the user runs the infected file in the disk, it loads virus into the RAM.
- B. The mutation engine of polymorphic virus generates a new encrypted code, this changes the signature of the virus.
- C. It has the ability to mutate and can change its known viral signature and hide from signature based antivirus programs.
- D. The new virus resides in the main memory of the computer and does not infect other files of the operating system.

Suggested Answer: *ABC*

Currently there are no comments in this discussion, be the first to comment!

Which of the following laws or acts, formed in Australia, enforces prohibition against cyber stalking?

- A. Stalking by Electronic Communications Act (2001)
- B. Malicious Communications Act (1998)
- C. Anti-Cyber-Stalking law (1999)
- D. Stalking Amendment Act (1999)

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

In which of the following files does the Linux operating system store passwords?

- A. Password
- B. Passwd
- C. Shadow
- D. SAM

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

What is the name of the group of blocks which contains information used by the operating system in Linux system?

- A. logblock
- B. Systemblock
- C. Bootblock
- D. Superblock

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Which of the following wireless network standards operates on the 5 GHz band and transfers data at a rate of 54 Mbps?

- A. 802.11a
- B. 802.11u
- C. 802.11g
- D. 802.11b

Suggested Answer: A

Currently there are no comments in this discussion, be the first to comment!

Which of the following tools is a wireless sniffer and analyzer that works on the Windows operating system?

- A. Kismet
- B. Aircrack-ng
- C. Wireshark
- D. Airodump-ng

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Which of the following is a password-cracking program?

- A. Netcat
- B. L0phtcrack
- C. SubSeven
- D. NetSphere

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Which of the following is used for remote file access by UNIX/Linux systems?

- A. NetWare Core Protocol (NCP)
- B. Common Internet File System (CIFS)
- C. Server Message Block (SMB)
- D. Network File System (NFS)

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Which of the following file systems is used by both CD and DVD?

- A. Network File System (NFS)
- B. New Technology File System (NTFS)
- C. Compact Disk File System (CDFS)
- D. Universal Disk Format (UDF)

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Which of the following firewalls depends on the three-way handshake of the TCP protocol?

- A. Proxy-based firewall
- B. Stateful firewall
- C. Packet filter firewall
- D. Endian firewall

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!