ITExams

Exam code or name...

CompTIA IT Fundamentals v6.0 (FC0-U51)

Page: 46 / 58
Total 286 questions

10 questions per page

Question 226 (Topic 3)

Which of the following are touch screen technologies?
Each correct answer represents a complete solution. Choose all that apply.

A. Surface Wave
B. Resistive
C. Transitive
D. Capacitive

Expose Correct Answer

Answer : **A,B,D**

Explanation: Touch screen is a computer display screen that is sensitive to human touch. It allows a user to interact with a computer by touching the icons or graphical buttons on the monitor screen. It is a system that is designed to help users who have difficulty in using mouse or keyboard and is used with information kiosks, computer-based training devices etc. A touch screen panel is attached externally to the monitor that is connected to a serial or Universal Serial Bus (USB) port on a computer. Nowadays, monitors are also available with built-in touch screen technology. There are three types of touch screen technologies: 1.Resistive 2.Capacitive 3.Surface Wave Answer option C is incorrect. There is no such touch screen technology as Transitive. Reference: "http://en.wikipedia.org/wiki/Touchscreen"

Next Question

Question 227 (Topic 3)

Which of the following types of attacks entices a user to disclose personal information such as social security number, bank account details, or credit card number?

A. Password guessing attack
B. Spoofing
C. Phishing
D. Replay attack

Expose Correct Answer

Answer : **C**

Explanation: Phishing is a type of scam that entice a user to disclose personal information such as social security number, bank account details, or credit card number. An example of phishing attack is a fraudulent e-mail that appears to come from a user's bank asking to change his online banking password. When the user clicks the link available on the e-mail, it directs him to a phishing site which replicates the original bank site. The phishing site lures the user to provide his personal information. Answer option B is incorrect. Spoofing is a technique that makes a transmission appear to have come from an authentic source by forging the IP address, email address, caller ID, etc. In IP spoofing, a hacker modifies packet headers by using someone else's IP address to his identity. However, spoofing cannot be used while surfing the Internet, chatting on- line, etc. because forging the source IP address causes the responses to be misdirected. Answer option D is incorrect. Replay attack is a type of attack in which attackers capture packets containing passwords or digital signatures whenever packets pass between two hosts on a network. In an attempt to obtain an authenticated connection, the attackers then resend the captured packet to the system. Answer option A is incorrect. A password guessing attack occurs when an unauthorized user tries to log on repeatedly to a computer or network by guessing usernames and passwords. Many password guessing programs that attempt to break passwords are available on the Internet. Following are the types of password guessing attacks: Brute force attack Dictionary attack Reference: "http://en.wikipedia.org/wiki/Phishing"

Next Question

Question 228 (Topic 3)

Which of the following firewalls inspects the actual contents of packets?

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

Expose Correct Answer

Answer : **B**

Explanation: The application level firewall inspects the contents of packets, rather than the source/destination or connection between the two. An Application level firewall operates at the application layer of the OSI model. Answer option C is incorrect. The circuit-level firewall regulates traffic based on whether or not a trusted connection has been established. It operates at the session layer of the OSI model. Answer option A is incorrect. The packet filtering firewall filters traffic based on the headers. It operates at the network layer of the OSI model. Answer option D is incorrect. The stateful inspection firewall assures the connection between the two parties is valid and inspects packets from this connection to assure the packets are not malicious. Reference: "http://en.wikipedia.org/wiki/Firewall_(networking)#Third_generation_- _application_layer"

Next Question

Question 229 (Topic 3)

Which of the following are used by FireWire 800 devices?

A. 6-pin connectors
B. 10-pin connectors
C. 9-pin connectors
D. 4-pin connectors

Expose Correct Answer

primarily for video transfer from digital movie cameras. Answer options D and A are incorrect. FireWire 400 devices use 4-pin or 6-pin connectors. Reference: "http://en.wikipedia.org/wiki/FireWire "

Next Question

Question 230 (Topic 3)

You are responsible for purchasing computer hardware for a school district. You have been looking at various sales brochures advocating various types of memory. What would be one advantage to buying dual-channel memory?

A. It will reduce memory bottlenecks.
B. It will be twice as fast as single channel memory.
C. It has no advantage over single channel memory.
D. It will have more memory capacity than single channel memory.

Expose Correct Answer

Answer : **A**

Explanation: Dual Channel memory offers two channels for data to move through it. This may reduce bottle necks. Answer options B and D are correct. The dual or single channel issue is unrelated to memory speed or capacity. Answer option C is incorrect. It will have an advantage over single channel, though the advantages are slight. Reference: http://www.pcextreme.net/reviews/ram/dual-channel-vs-single-memory- configuration/

Next Question

Page: 46 / 58
Total 286 questions

10 questions per page

Facebook

Twitter

Youtube

contact@itexams.com