FC0-U51^{Q&As}

CompTIA IT Fundamentals+ Certification Exam

Pass CompTIA FC0-U51 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass4itsure.com/fc0-u51.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by CompTIA Official Exam Center

Instant Download After Purchase

100% Money Back Guarantee

365 Days Free Update

800,000+ Satisfied Customers

SATISFACTION GUARANTEED
100%
SATISFACTION GUARANTEED

QUESTION 1

Which of the following computer components are used to store data? (Select TWO).

A. GPU

B. HDD

C. RAM

D. NIC

E. CPU

Correct Answer: BC

QUESTION 2

Which of the following technologies is used to detect unauthorized attempts to access and manipulate computer systems locally or through the Internet or an intranet?

A. Demilitarized zone (DMZ)

B. Firewall

C. Intrusion detection system (IDS)

D. Packet filtering

Correct Answer: C

An Intrusion detection system (IDS) is used to detect unauthorized attempts to access and manipulate computer systems locally or through the Internet or an intranet. It can detect several types of attacks and malicious behaviors that can compromise the security of a network and computers. This includes network attacks against vulnerable services, unauthorized logins and access to sensitive data, and malware (e.g. viruses, worms, etc.). An IDS also detects attacks that originate from within a system. In most cases, an IDS has three main components: Sensors, Console, and Engine. Sensors generate security events. A console is used to alert and control sensors and to monitor events. An engine is used to record events and to generate security alerts based on received security events. In many IDS implementations, these three components are combined into a single device. Basically, following two types of IDS are used : Network-based IDS Host-based IDS Answer option D is incorrect. Packet filtering is a method that allows or restricts the flow of specific types of packets to provide security. It analyzes the incoming and outgoing packets and lets them pass or stops them at a network interface based on the source and destination addresses, ports, or protocols. Packet filtering provides a way to define precisely which type of IP traffic is allowed to cross the firewall of an intranet. IP packet filtering is important when users from private intranets connect to public networks, such as the Internet. Answer option B is incorrect. A firewall is a tool 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. Answer option A is incorrect. Demilitarized zone (DMZ) or perimeter network is a small network that lies in between the Internet and a private network. It is the boundary between the Internet and an internal network, usually a combination of firewalls and bastion hosts that are gateways between inside networks and outside networks. DMZ provides a large enterprise network or corporate network the ability to use the Internet while still maintaining its security. Reference: "http://en.wikipedia.org/wiki/Intrusion-detection_system"

QUESTION 3

Which of the following devices does SCSI support?

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

A. Tape drive

B. Sound card

C. CD drive

D. Modem

E. Hard disk drive

Correct Answer: AC

Small Computer System Interface (SCSI) supports CD drive, tape drive, and hard disk drive.

What is SCSI? Hide

Small Computer System Interface (SCSI) is the second most popular drive interface in use today after the Integrated Drive

Electronics (IDE) interface. SCSI is faster than IDE and supports more devices. SCSI devices, such as hard disk drive and CD-ROM drive, are better suited in a network environment in which many users access shared drives simultaneously.

SCSI has three standards: SCSI-1, SCSI-2, and SCSI-3.

Reference: TechNet, Contents: "Storage Management Operations Guide"

QUESTION 4

Which of the following actions can a technician take to reduce the chances of static charges being built up? Each correct answer represents a complete solution. Choose three.

A. Wear silken clothes.

B. Do not wear wrist strap.

C. Remove carpets from computer rooms.

D. Wear cotton clothes.

E. Increase humidity level.

Correct Answer: CDE

In order to reduce the chances of static charges being built up, users or technicians will have to take the following steps:

Wear cotton clothes. This will reduce the chance of building up of static charges. Do not cover the computer room\\'s floor with carpets. This stops neutralizing of static charges.

Increase humidity level. Humidity helps dissipate static charges.

What is ESD?

ESD stands for Electrostatic discharge. The static electricity that we generate everyday creates ESD. If you walk across a carpet and touch someone, you experience a mild shock. Electrostatic discharge occurs when the electrostatic charge

is transferred from one charged entity to another entity sensitive to that charge. To minimize Electrostatic discharge (ESD) problems, consider wearing a wrist strap when you are working with computer components. A wrist strap is a wire with

a watchband-style strap at one end and a plug or clip on the other end. The wrist strap plug or clip is connected to the ground or to the piece of equipment being worked on. Answer option A is incorrect. A technician should not wear silken

clothes during computer servicing, as silken clothes are more likely to generate static charges than cotton clothes. Answer option B is incorrect. Wearing wrist strap will keep a technician grounded. Hence, static charges cannot build up.

Reference: "http://en.wikipedia.org/wiki/Electrostatic_discharge"

QUESTION 5

A technician needs to troubleshoot a user\\'s computer. The user leaves personal credentials written on a piece of paper for the technician. Which of the following principles has the user violated?

A. Password confidentiality

B. Password complexity

C. Password reuse

D. Password expiration

Correct Answer: A