nonvolatile storage. Secondary storage includes disk, floppies, CD's, tape, etc. While secondary storage includes basically anything different from primary storage, virtual memory's use of secondary storage is usually confined to high-speed disk storage.

Real storage is incorrect. Real storage is another word for primary storage and distinguishes physical memory from virtual memory.

Reference(s) used for this question:

Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 17164-17171). Auerbach Publications. Kindle Edition.
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 17196-17201). Auerbach Publications. Kindle Edition.
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 17186-17187). Auerbach Publications. Kindle Edition.

QUESTION 418
An area of the Telecommunications and Network Security domain that directly affects the Information Systems Security tenet of Availability can be defined as:

A. Netware availability
B. Network availability
C. Network acceptability
D. Network accountability

Correct Answer: B
Explanation:
Network availability can be defined as an area of the Telecommunications and Network Security domain that directly affects the Information Systems Security tenet of Availability.
Source: KRUTZ, Ronald L.& VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 64.

QUESTION 419
Which of the following would best describe the difference between white-box testing and black-box testing?

A. White-box testing is performed by an independent programmer team.
B. Black-box testing uses the bottom-up approach.
C. White-box testing examines the program internal logical structure.
D. Black-box testing involves the business units

Correct Answer: C
Explanation:
Black-box testing observes the system external behavior, while white-box testing is a detailed exam of a logical path, checking the possible conditions.
Source: Information Systems Audit and Control Association, Certified Information Systems Auditor 2002 review manual, chapter 6: Business Application System Development, Acquisition, Implementation and Maintenance (page 299).

QUESTION 420
Which of the following is most concerned with personnel security?

A. Management controls
B. Operational controls
C. Technical controls
D. Human resources controls

Correct Answer: B
Explanation:
Many important issues in computer security involve human users, designers, implementers, and managers.

A broad range of security issues relates to how these individuals interact with computers and the access and authorities they need to do their jobs. Since operational controls address security methods focusing on mechanisms primarily implemented and executed by people (as opposed to systems), personnel security is considered a form of operational control.

Operational controls are put in place to improve security of a particular system (or group of systems). They often require specialized expertise and often rely upon management activities as well as technical controls. Implementing dual control and making sure that you have more than one person that can perform a task would fall into this category as well.

Management controls focus on the management of the IT security system and the management of risk for a system. They are techniques and concerns that are normally addressed by management.

Technical controls focus on security controls that the computer system executes. The controls can provide automated protection for unauthorized access of misuse, facilitate detection of security violations, and support security requirements for applications and data.

Reference use for this question:

NIST SP 800-53 Revision 4 http://dx.doi.org/10.6028/NIST.SP.800-53r4 You can get it as a word document by clicking HERE
NIST SP 800-53 Revision 4 has superseded the document below:

SWANSON, Marianne, NIST Special Publication 800-26, Security Self-Assessment Guide for Information Technology Systems, November 2001 (Page A-18).

QUESTION 421
Which of the following is BEST defined as a physical control?

A. Monitoring of system activity
B. Fencing
C. Identification and authentication methods
D. Logical access control mechanisms

Correct Answer: B
Explanation:
Physical controls are items put into place to protect facility, personnel, and resources. Examples of physical controls are security guards, locks, fencing, and lighting.

The following answers are incorrect answers:
Monitoring of system activity is considered to be administrative control.
Identification and authentication methods are considered to be a technical control.

Logical access control mechanisms is also considered to be a technical control.

Reference(s) used for this question:
Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition (Kindle Locations 1280-1282). McGraw-Hill. Kindle Edition.

QUESTION 422
Which of the following is NOT a fundamental component of an alarm in an intrusion detection system?

A. Communications
B. Enunciator
C. Sensor
D. Response

Correct Answer: D
Explanation:
Response is the correct choice. A response would essentially be the action that is taken once an alarm has been produced by an IDS, but is not a fundamental component of the alarm.

The following are incorrect answers:

Communications is the component of an alarm that delivers alerts through a variety of channels such as email, pagers, instant messages and so on.
An Enunciator is the component of an alarm that uses business logic to compose the content and format of an alert and determine the recipients of that alert.
A sensor is a fundamental component of IDS alarms. A sensor detects an event and produces an appropriate notification.
Domain: Access Control

Reference:
Official guide to the CISSP CBK. page 203.

QUESTION 423
What would be considered the biggest drawback of Host-based Intrusion Detection systems (HIDS)?

A. It can be very invasive to the host operating system
B. Monitors all processes and activities on the host system only
C. Virtually eliminates limits associated with encryption
D. They have an increased level of visibility and control compared to NIDS

Correct Answer: A
Explanation:
The biggest drawback of HIDS, and the reason many organizations resist its use, is that it can be very invasive to the host operating system. HIDS must have the capability to monitor all processes and activities on the host system and this can sometimes interfere with normal system processing.

HIDS versus NIDS
A host-based IDS (HIDS) can be installed on individual workstations and/ or servers to watch for inappropriate or anomalous activity. HIDSs are usually used to make sure users do not delete system files, reconfigure important settings, or put the system at risk in any other way.

So, whereas the NIDS understands and monitors the network traffic, a HIDS's universe is limited to the computer itself. A HIDS does not understand or review network traffic, and a NIDS does not "look in" and monitor a system's activity. Each has its own job and stays out of the other's way.

The ISC2 official study book defines an IDS as:
An intrusion detection system (IDS) is a technology that alerts organizations to adverse or unwanted activity. An IDS can be implemented as part of a network device, such as a router, switch, or firewall, or it can be a dedicated IDS device monitoring traffic as it traverses the network. When used in this way, it is referred to as a network IDS, or NIDS. IDS can also be used on individual host systems to monitor and report on file, disk, and process activity on that host. When used in this way it is referred to as a host-based IDS, or HIDS.

An IDS is informative by nature and provides real-time information when suspicious activities are identified. It is primarily a detective device and, acting in this traditional role, is not used to directly prevent the suspected attack.

What about IPS?
In contrast, an intrusion prevention system (IPS), is a technology that monitors activity like an IDS but will automatically take proactive preventative action if it detects unacceptable activity. An IPS permits a predetermined set of functions and actions to occur on a network or system; anything that is not permitted is considered unwanted activity and blocked. IPS is engineered specifically to respond in real time to an event at the system or network layer. By proactively enforcing policy, IPS can thwart not only attackers, but also authorized users attempting to perform an action that is not within policy. Fundamentally, IPS is considered an access control and policy enforcement technology, whereas IDS is considered network monitoring and audit technology.

The following answers were incorrect:
All of the other answer were advantages and not drawback of using HIDS

TIP FOR THE EXAM:
Be familiar with the differences that exists between an HIDS, NIDS, and IPS. Know that IDS's are mostly detective but IPS are preventive. IPS's are considered an access control and policy enforcement technology, whereas IDS's are considered network monitoring and audit technology.

Reference(s) used for this question:
Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition (Kindle Locations 5817-5822). McGraw-Hill. Kindle Edition.
Schneiter, Andrew (2013-04-15). Official (ISC)2 Guide to the CISSP CBK, Third Edition. Access Control ((ISC)2 Press), Domain1, Page 180-188 or on the kindle version look for Kindle Locations 3199-3203. Auerbach Publications.

QUESTION 424
Network-based Intrusion Detection systems:

A. Commonly reside on a discrete network segment and monitor the traffic on that network segment.
B. Commonly will not reside on a discrete network segment and monitor the traffic on that network segment.
C. Commonly reside on a discrete network segment and does not monitor the traffic on that network segment.
D. Commonly reside on a host and and monitor the traffic on that specific host.

Correct Answer: A

Explanation:
Network-based ID systems: Commonly reside on a discrete network segment and monitor the traffic on that network segment Usually consist of a network appliance with a Network Interface Card (NIC) that is operating in promiscuous mode and is intercepting and analyzing the network packets in real time

"A passive NIDS takes advantage of promiscuous mode access to the network, allowing it to gain visibility into every packet traversing the network segment. This allows the system to inspect packets and monitor sessions without impacting the network, performance, or the systems and applications utilizing the network."

NOTE FROM CLEMENT:
A discrete network is a synonym for a SINGLE network. Usually the sensor will monitor a single network segment, however there are IDS today that allow you to monitor multiple LAN's at the same time.

References used for this question:

KRUTZ, Ronald L.& VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 62.
Official (ISC)2 Guide to the CISSP CBK, Hal Tipton and Kevin Henry, Page 196
Additional information on IDS systems can be found here:
http://en.wikipedia.org/wiki/Intrusion_detection_system

QUESTION 425
What IDS approach relies on a database of known attacks?

A. Signature-based intrusion detection
B. Statistical anomaly-based intrusion detection
C. Behavior-based intrusion detection
D. Network-based intrusion detection

Correct Answer: A
Explanation:
A weakness of the signature-based (or knowledge-based) intrusion detection approach is that only attack signatures that are stored in a database are detected. Network-based intrusion detection can either be signature-based or statistical anomaly- based (also called behavior-based).
Source: KRUTZ, Ronald L.& VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 2: Access control systems (page 49).

QUESTION 426
Due care is not related to:

A. Good faith
B. Prudent man
C. Profit
D. Best interest

Correct Answer: C
Explanation:
Officers and directors of a company are expected to act carefully in fulfilling their tasks. A director