Domains of Computer Security, 2001, John Wiley & Sons, Page 37. Also: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, chapter 4: Access Control (pages 136-137).

QUESTION 16
What is a common problem when using vibration detection devices for perimeter control?

A. They are vulnerable to non-adversarial disturbances.
B. They can be defeated by electronic means.
C. Signal amplitude is affected by weather conditions.
D. They must be buried below the frost line.

Correct Answer: A
Explanation:
Vibration sensors are similar and are also implemented to detect forced entry. Financial institutions may choose to implement these types of sensors on exterior walls, where bank robbers may attempt to drive a vehicle through. They are also commonly used around the ceiling and flooring of vaults to detect someone trying to make an unauthorized bank withdrawal.

Such sensors are proned to false positive. If there is a large truck with heavy equipment driving by it may trigger the sensor. The same with a storm with thunder and lighting, it may trigger the alarm even thou there are no adversarial threat or disturbance.

The following are incorrect answers:

All of the other choices are incorrect.

Reference used for this question:
Harris, Shon (2012-10-18). CISSP All-in-One Exam Guide, 6th Edition (pp. 495-496). McGraw-Hill . Kindle Edition.

QUESTION 17
What is the difference between Access Control Lists (ACLs) and Capability Tables?

A. Access control lists are related/attached to a subject whereas capability tables are related/attached to an object.
B. Access control lists are related/attached to an object whereas capability tables are related/attached to a subject.
C. Capability tables are used for objects whereas access control lists are used for users.
D. They are basically the same.

Correct Answer: B
Explanation:
Capability tables are used to track, manage and apply controls based on the object and rights, or capabilities of a subject. For example, a table identifies the object, specifies access rights allowed for a subject, and permits access based on the user's posession of a capability (or ticket) for the object. It is a row within the matrix.

To put it another way, A capabiltiy table is different from an ACL because the subject is bound to the capability table, whereas the object is bound to the ACL.

CLEMENT NOTE:

If we wish to express this very simply:

Capabilities are attached to a subject and it describe what access the subject has to each of the objects on the row that matches with the subject within the matrix. It is a row within the matrix. ACL's are attached to objects, it describe who has access to the object and what type of access they have. It is a column within the matrix.

The following are incorrect answers:

"Access control lists are subject-based whereas capability tables are object-based" is incorrect.
"Capability tables are used for objects whereas access control lists are used for users" is incorrect.
"They are basically the same" is incorrect.

References used for this question:

CBK, pp. 191 - 192
AIO3 p. 169

QUESTION 18
What is considered the most important type of error to avoid for a biometric access control system?

A. Type I Error
B. Type II Error
C. Combined Error Rate
D. Crossover Error Rate

Correct Answer: B
Explanation:
When a biometric system is used for access control, the most important error is the false accept or false acceptance rate, or Type II error, where the system would accept an impostor.

A Type I error is known as the false reject or false rejection rate and is not as important in the security context as a type II error rate. A type one is when a valid company employee is rejected by the system and he cannot get access even thou it is a valid user.

The Crossover Error Rate (CER) is the point at which the false rejection rate equals the false acceptance rate if your would create a graph of Type I and Type II errors. The lower the CER the better the device would be.

The Combined Error Rate is a distracter and does not exist.
Source: TIPTON, Harold F.& KRAUSE, Micki, Information Security Management Handbook, 4th edition (volume 1), 2000, CRC Press, Chapter 1, Biometric Identification (page 10).

QUESTION 19
In biometric identification systems, at the beginning, it was soon apparent that truly positive identification could only be based on physical attributes of a person. This raised the necessity of answering 2 questions :

A. what was the sex of a person and his age
B. what part of body to be used and how to accomplish identification that is viable
C. what was the age of a person and his income level

D. what was the tone of the voice of a person and his habits

Correct Answer: B
Explanation:
Today implementation of fast, accurate reliable and user-acceptable biometric identification systems is already taking place. Unique physical attributes or behavior of a person are used for that purpose.

From: TIPTON, Harold F.& KRAUSE, MICKI, Information Security Management Handbook, 4th Edition, Volume 1, Page 7.

QUESTION 20
Which of the following can be defined as a framework that supports multiple, optional authentication mechanisms for PPP, including cleartext passwords, challenge-response, and arbitrary dialog sequences?

A. Extensible Authentication Protocol
B. Challenge Handshake Authentication Protocol
C. Remote Authentication Dial-In User Service
D. Multilevel Authentication Protocol.

Correct Answer: A
Explanation:
RFC 2828 (Internet Security Glossary) defines the Extensible Authentication Protocol as a framework that supports multiple, optional authentication mechanisms for PPP, including cleartext passwords, challenge-response, and arbitrary dialog sequences. It is intended for use primarily by a host or router that connects to a PPP network server via switched circuits or dial-up lines. The Remote Authentication Dial-In User Service (RADIUS) is defined as an Internet protocol for carrying dial-in user's authentication information and configuration information between a shared, centralized authentication server and a network access server that needs to authenticate the users of its network access ports. The other option is a distracter.
Source: SHIREY, Robert W., RFC2828: Internet Security Glossary, may 2000.

QUESTION 21
Which of the following is implemented through scripts or smart agents that replays the users multiple log-ins against authentication servers to verify a user's identity which permit access to system services?

A. Single Sign-On
B. Dynamic Sign-On
C. Smart cards
D. Kerberos

Correct Answer: A
Explanation:
SSO can be implemented by using scripts that replay the users multiple log- ins against authentication servers to verify a user's identity and to permit access to system services.

Single Sign on was the best answer in this case because it would include Kerberos.

When you have two good answers within the 4 choices presented you must select the BEST one. The high level choice is always the best. When one choice would include the other one that would be the best as well.

Reference(s) 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 40.

QUESTION 22
Which of the following biometric characteristics cannot be used to uniquely authenticate an individual's identity?

A. Retina scans
B. Iris scans
C. Palm scans
D. Skin scans

Correct Answer: D
Explanation:
The following are typical biometric characteristics that are used to uniquely authenticate an individual's identity:

Fingerprints
Retina scans
Iris scans
Facial scans
Palm scans
Hand geometry
Voice
Handwritten signature dynamics

Source: KRUTZ, Ronald L.& VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 39. And: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, chapter 4: Access Control (pages 127-131).

QUESTION 23
Which of the following statements relating to the Bell-LaPadula security model is FALSE (assuming the Strong Star property is not being used) ?

A. A subject is not allowed to read up.
B. The property restriction can be escaped by temporarily downgrading a high level subject.
C. A subject is not allowed to read down.
D. It is restricted to confidentiality.

Correct Answer: C
Explanation:
It is not a property of Bell LaPadula model.

The other answers are incorrect because:

A subject is not allowed to read up is a property of the 'simple security rule' of Bell LaPadula model.
The property restriction can be escaped by temporarily downgrading a high level subject can be escaped by temporarily downgrading a high level subject or by identifying a set of trusted objects which are permitted to violate the property as long as it is not in the middle of an operation.

It is restricted to confidentiality as it is a state machine model that enforces the confidentiality aspects of access control.

Reference:
Shon Harris AIO v3 , Chapter-5 : Security Models and Architecture , Page:279-282

QUESTION 24
Which of the following can best eliminate dial-up access through a Remote Access Server as a hacking vector?

A. Using a TACACS+ server.
B. Installing the Remote Access Server outside the firewall and forcing legitimate users to authenticate to the firewall.
C. Setting modem ring count to at least 5.
D. Only attaching modems to non-networked hosts.

Correct Answer: B
Explanation:
Containing the dial-up problem is conceptually easy: by installing the Remote Access Server outside the firewall and forcing legitimate users to authenticate to the firewall, any access to internal resources through the RAS can be filtered as would any other connection coming from the Internet.

The use of a TACACS+ Server by itself cannot eliminate hacking.

Setting a modem ring count to 5 may help in defeating war-dialing hackers who look for modem by dialing long series of numbers.

Attaching modems only to non-networked hosts is not practical and would not prevent these hosts from being hacked.

Source: STREBE, Matthew and PERKINS, Charles, Firewalls 24seven, Sybex 2000, Chapter 2: Hackers.

QUESTION 25
Which type of attack involves impersonating a user or a system?

A. Smurfing attack
B. Spoofing attack
C. Spamming attack
D. Sniffing attack

Correct Answer: B
Explanation:
A spoofing attack is when an attempt is made to gain access to a computer system by posing as an authorized user or system. Spamming refers to sending out or posting junk advertising and unsolicited mail. A smurf attack is a type of denial-of-service attack using PING and a spoofed address. Sniffing refers to observing packets passing on a network.
Source: KRUTZ, Ronald L.& VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 3: Telecommunications and Network Security (page 77).