passwords.

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 40).
HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, chapter 4: Access Control (pages 147-151).
http://www.ietf.org/rfc/rfc4556.txt

QUESTION 235
What is one disadvantage of content-dependent protection of information?

A. It increases processing overhead.
B. It requires additional password entry.
C. It exposes the system to data locking.
D. It limits the user's individual address space.

Correct Answer: A
Explanation:
Source: TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.

QUESTION 236
In Mandatory Access Control, sensitivity labels attached to object contain what information?

A. The item's classification
B. The item's classification and category set
C. The item's category
D. The items's need to know

Correct Answer: B
Explanation:
A Sensitivity label must contain at least one classification and one category set.
Category set and Compartment set are synonyms, they mean the same thing. The sensitivity label must contain at least one Classification and at least one Category. It is common in some environments for a single item to belong to multiple categories. The list of all the categories to which an item belongs is called a compartment set or category set.

The following answers are incorrect:

The item's classification. Is incorrect because you need a category set as well. the item's category. Is incorrect because category set and classification would be both be required. The item's need to know. Is incorrect because there is no such thing. The need to know is indicated by the catergories the object belongs to. This is NOT the best answer.

Reference(s) used for this question:
OIG CBK, Access Control (pages 186 - 188)
AIO, 3rd Edition, Access Control (pages 162 - 163)
AIO, 4th Edittion, Access Control, pp 212-214.
Wikipedia - http://en.wikipedia.org/wiki/Mandatory_Access_Control

QUESTION 237
Which of the following statements pertaining to biometrics is false?

A. Increased system sensitivity can cause a higher false rejection rate
B. The crossover error rate is the point at which false rejection rate equals the false acceptance rate.
C. False acceptance rate is also known as Type II error.
D. Biometrics are based on the Type 2 authentication mechanism.

Correct Answer: D
Explanation:
Authentication is based on three factor types: type 1 is something you know, type 2 is something you have and type 3 is something you are. Biometrics are based on the Type 3 authentication mechanism.
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 37).

QUESTION 238
Which of following is not a service provided by AAA servers (Radius, TACACS and DIAMETER)?

A. Authentication
B. Administration
C. Accounting
D. Authorization

Correct Answer: B
Explanation:
Radius, TACACS and DIAMETER are classified as authentication, authorization, and accounting (AAA) servers.
Source: TIPTON, Harold F.& KRAUSE, MICKI, Information Security Management Handbook, 4th Edition, Volume 2, 2001, CRC Press, NY, Page 33.

also see:
The term "AAA" is often used, describing cornerstone concepts [of the AIC triad] Authentication, Authorization, and Accountability. Left out of the AAA acronym is Identification which is required before the three "A's" can follow. Identity is a claim, Authentication proves an identity, Authorization describes the action you can perform on a system once you have been identified and authenticated, and accountability holds users accountable for their actions.
Reference:
CISSP Study Guide, Conrad Misenar, Feldman p. 10-11, (c) 2010 Elsevier.

QUESTION 239
The type of discretionary access control (DAC) that is based on an individual's identity is also called:

A. Identity-based Access control
B. Rule-based Access control
C. Non-Discretionary Access Control
D. Lattice-based Access control

Correct Answer: A
Explanation:
An identity-based access control is a type of Discretionary Access Control (DAC) that is based on

an individual's identity.

DAC is good for low level security environment. The owner of the file decides who has access to the file.

If a user creates a file, he is the owner of that file. An identifier for this user is placed in the file header and/or in an access control matrix within the operating system.

Ownership might also be granted to a specific individual. For example, a manager for a certain department might be made the owner of the files and resources within her department. A system that uses discretionary access control (DAC) enables the owner of the resource to specify which subjects can access specific resources.

This model is called discretionary because the control of access is based on the discretion of the owner. Many times department managers, or business unit managers , are the owners of the data within their specific department. Being the owner, they can specify who should have access and who should not.

Reference(s) used for this question:
Harris, Shon (2012-10-18). CISSP All-in-One Exam Guide, 6th Edition (p. 220). McGraw- Hill . Kindle Edition.

QUESTION 240
In biometric identification systems, at the beginning, it was soon apparent that truly positive identification could only be based on :

A. sex of a person
B. physical attributes of a person
C. age of a person
D. voice of a person

Correct Answer: B
Explanation:
Today implementation of fast, accurate reliable and user-acceptable biometric identification systems is already under way.
From: TIPTON, Harold F.& KRAUSE, MICKI, Information Security Management Handbook, 4th Edition, Volume 1, Page 7.

QUESTION 241
Which of the following is used by RADIUS for communication between clients and servers?

A. TCP
B. SSL
C. UDP
D. SSH

Correct Answer: C
Explanation:
Source: TIPTON, Harold F.& KRAUSE, MICKI, Information Security Management Handbook, 4th Edition, Volume 2, 2001, CRC Press, NY, Page 33.

QUESTION 242

In discretionary access environments, which of the following entities is authorized to grant information access to other people?

A. Manager
B. Group Leader
C. Security Manager
D. Data Owner

Correct Answer: D
Explanation:
In Discretionary Access Control (DAC) environments, the user who creates a file is also considered the owner and has full control over the file including the ability to set permissions for that file.

The following answers are incorrect:

manager. Is incorrect because in Discretionary Access Control (DAC) environments it is the owner/user that is authorized to grant information access to other people.
group leader. Is incorrect because in Discretionary Access Control (DAC) environments it is the owner/user that is authorized to grant information access to other people.
security manager. Is incorrect because in Discretionary Access Control (DAC) environments it is the owner/user that is authorized to grant information access to other people.

IMPORTANT NOTE:
The term Data Owner is also used within Classifications as well. Under the subject of classification the Data Owner is a person from management who has been entrusted with a data set that belongs to the company. For example it could be the Chief Financial Officer (CFO) who is entrusted with all of the financial data for a company. As such the CFO would determine the classification of the financial data and who can access as well. The Data Owner would then tell the Data Custodian (a technical person) what the classification and need to know is on the specific set of data.

The term Data Owner under DAC simply means whoever created the file and as the creator of the file the owner has full access and can grant access to other subjects based on their identity.

QUESTION 243
Which of the following is NOT a technique used to perform a penetration test?

A. traffic padding
B. scanning and probing
C. war dialing
D. sniffing

Correct Answer: A
Explanation:
Traffic padding is a countermeasure to traffic analysis.

Even if perfect cryptographic routines are used, the attacker can gain knowledge of the amount of traffic that was generated. The attacker might not know what Alice and Bob were talking about, but can know that they were talking and how much they talked. In certain circumstances this can be very bad. Consider for example when a military is organising a secret attack against another nation: it may suffice to alert the other nation for them to know merely that there is a lot of secret activity going on.

As another example, when encrypting Voice Over IP streams that use variable bit rate encoding, the number of bits per unit of time is not obscured, and this can be exploited to guess spoken phrases.

Padding messages is a way to make it harder to do traffic analysis. Normally, a number of random bits are appended to the end of the message with an indication at the end how much this random data is. The randomness should have a minimum value of 0, a maximum number of N and an even distribution between the two extremes. Note, that increasing 0 does not help, only increasing N helps, though that also means that a lower percentage of the channel will be used to transmit real data. Also note, that since the cryptographic routine is assumed to be uncrackable (otherwise the padding length itself is crackable), it does not help to put the padding anywhere else, e.g. at the beginning, in the middle, or in a sporadic manner.

The other answers are all techniques used to do Penetration Testing.

References:
KRUTZ, Ronald L.& VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, pages 233, 238.
https://secure.wikimedia.org/wikipedia/en/wiki/Padding_%28cryptography%29#Traffic_anal ysis

QUESTION 244
A confidential number used as an authentication factor to verify a user's identity is called a:

A. PIN
B. User ID
C. Password
D. Challenge

Correct Answer: A
Explanation:
PIN Stands for Personal Identification Number, as the name states it is a combination of numbers.

The following answers are incorrect:

User ID This is incorrect because a Userid is not required to be a number and a Userid is only used to establish identity not verify it.
Password. This is incorrect because a password is not required to be a number, it could be any combination of characters.
Challenge. This is incorrect because a challenge is not defined as a number, it could be anything.

QUESTION 245
Which of the following is NOT an advantage that TACACS+ has over TACACS?

A. Event logging
B. Use of two-factor password authentication
C. User has the ability to change his password
D. Ability for security tokens to be resynchronized

Correct Answer: A
Explanation:
Although TACACS+ provides better audit trails, event logging is a service that is provided with TACACS.