A. Smart cards
B. Single Sign-On (SSO)
C. Symmetric Ciphers
D. Public Key Infrastructure (PKI)

Correct Answer: B
Explanation:
The advantages of SSO include having the ability to use stronger passwords, easier administration as far as changing or deleting the passwords, minimize the risks of orphan accounts, and requiring less time to access resources.
Source: KRUTZ, Ronald L.& VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 39.

QUESTION 127
Which one of the following authentication mechanisms creates a problem for mobile users?

A. Mechanisms based on IP addresses
B. Mechanism with reusable passwords
C. one-time password mechanism.
D. challenge response mechanism.

Correct Answer: A
Explanation:
Anything based on a fixed IP address would be a problem for mobile users because their location and its associated IP address can change from one time to the next. Many providers will assign a new IP every time the device would be restarted. For example an insurance adjuster using a laptop to file claims online. He goes to a different client each time and the address changes every time he connects to the ISP.

NOTE FROM CLEMENT:
The term MOBILE in this case is synonymous with Road Warriors where a user is contantly traveling and changing location. With smartphone today that may not be an issue but it would be an issue for laptops or WIFI tablets. Within a carrier network the IP will tend to be the same and would change rarely. So this question is more applicable to devices that are not cellular devices but in some cases this issue could affect cellular devices as well.

The following answers are incorrect:

mechanism with reusable password. This is incorrect because reusable password mechanism would not present a problem for mobile users. They are the least secure and change only at specific interval.

one-time password mechanism. This is incorrect because a one-time password mechanism would not present a problem for mobile users. Many are based on a clock and not on the IP address of the user.

challenge response mechanism. This is incorrect because challenge response mechanism would not present a problem for mobile users.

QUESTION 128
Which of the following is the most reliable, secure means of removing data from magnetic storage media such as a magnetic tape, or a cassette?

A. Degaussing
B. Parity Bit Manipulation
C. Zeroization
D. Buffer overflow

Correct Answer: A
Explanation:
A "Degausser (Otherwise known as a Bulk Eraser) has the main function of reducing to near zero the magnetic flux stored in the magnetized medium. Flux density is measured in Gauss or Tesla. The operation is speedier than overwriting and done in one short operation. This is achieved by subjecting the subject in bulk to a series of fields of alternating polarity and gradually decreasing strength.

The following answers are incorrect:Parity Bit Manipulation. Parity has to do with disk lerror detection, not data removal. A bit or series of bits appended to a character or block of characters to ensure that the information received is the same as the infromation that was sent.

Zeroization. Zeroization involves overwrting data to sanitize it. It is time-consuming and not foolproof. The potential of restoration of data does exist with this method. Buffer overflow. This is a detractor. Although many Operating Systems use a disk buffer to temporarily hold data read from disk, its primary purpose has no connection to data removal. An overflow goes outside the constraints defined for the buffer and is a method used by an attacker to attempt access to a system.

The following reference(s) were/was used to create this question:

Shon Harris AIO v3. pg 908
Reference: What is degaussing.

QUESTION 129
Which access control model is best suited in an environment where a high security level is required and where it is desired that only the administrator grants access control?

A. DAC
B. MAC
C. Access control matrix
D. TACACS

Correct Answer: B
Explanation:
MAC provides high security by regulating access based on the clearance of individual users and sensitivity labels for each object. Clearance levels and sensitivity levels cannot be modified by individual users -- for example, user Joe (SECRET clearance) cannot reclassify the "Presidential Doughnut Recipe" from "SECRET" to "CONFIDENTIAL" so that his friend Jane (CONFIDENTIAL clearance) can read it. The administrator is ultimately responsible for configuring this protection in accordance with security policy and directives from the Data Owner.

DAC is incorrect. In DAC, the data owner is responsible for controlling access to the object.

Access control matrix is incorrect. The access control matrix is a way of thinking about the access control needed by a population of subjects to a population of objects. This access control can be applied using rules, ACL's, capability tables, etc.

TACACS is incorrect. TACACS is a tool for performing user authentication.

References:
CBK, p. 187, Domain 2: Access Control.
AIO3, Chapter 4, Access Control.

QUESTION 130
Which security model is based on the military classification of data and people with clearances?

A. Brewer-Nash model
B. Clark-Wilson model
C. Bell-LaPadula model
D. Biba model

Correct Answer: C
Explanation:
The Bell-LaPadula model is a confidentiality model for information security based on the military classification of data, on people with clearances and data with a classification or sensitivity model.
The Biba, Clark-Wilson and Brewer-Nash models are concerned with integrity.
Source: HARE, Chris, Security Architecture and Models, Area 6 CISSP Open Study Guide, January 2002.

QUESTION 131
A network-based vulnerability assessment is a type of test also referred to as:

A. An active vulnerability assessment.
B. A routing vulnerability assessment.
C. A host-based vulnerability assessment.
D. A passive vulnerability assessment.

Correct Answer: A
Explanation:
A network-based vulnerability assessment tool/system either re-enacts system attacks, noting and recording responses to the attacks, or probes different targets to infer weaknesses from their responses.

Since the assessment is actively attacking or scanning targeted systems, network-based vulnerability assessment systems are also called active vulnerability systems.

There are mostly two main types of test:

PASSIVE: You don't send any packet or interact with the remote target. You make use of public database and other techniques to gather information about your target.

ACTIVE: You do send packets to your target, you attempt to stimulate response which will help you in gathering information about hosts that are alive, services runnings, port state, and more.

See example below of both types of attacks:
Eavesdropping and sniffing data as it passes over a network are considered passive attacks because the attacker is not affecting the protocol, algorithm, key, message, or any parts of the encryption system. Passive attacks are hard to detect, so in most cases methods are put in place to try to prevent them rather than to detect and stop them.

Altering messages , modifying system files, and masquerading as another individual are acts that are considered active attacks because the attacker is actually doing something instead of sitting back and gathering data. Passive attacks are usually used to gain information prior to carrying out an active attack.

IMPORTANT NOTE:
On the commercial vendors will sometimes use different names for different types of scans. However, the exam is product agnostic. They do not use vendor terms but general terms. Experience could trick you into selecting the wrong choice sometimes. See feedback from Jason below:

"I am a system security analyst. It is my daily duty to perform system vulnerability analysis. We use Nessus and Retina (among other tools) to perform our network based vulnerability scanning. Both commercially available tools refer to a network based vulnerability scan as a "credentialed" scan. Without credentials, the scan tool cannot login to the system being scanned, and as such will only receive a port scan to see what ports are open and exploitable"

Reference(s) used for this question:

Harris, Shon (2012-10-18). CISSP All-in-One Exam Guide, 6th Edition (p. 865). McGraw- Hill. Kindle Edition.
And DUPUIS, Clement, Access Control Systems and Methodology CISSP Open Study Guide, version 1.0, march 2002 (page 97).

QUESTION 132
Detective/Technical measures:

A. include intrusion detection systems and automatically-generated violation reports from audit trail information.
B. do not include intrusion detection systems and automatically-generated violation reports from audit trail information.
C. include intrusion detection systems but do not include automatically-generated violation reports from audit trail information.
D. include intrusion detection systems and customised-generated violation reports from audit trail information.

Correct Answer: A
Explanation:
Detective/Technical measures include intrusion detection systems and automatically-generated violation reports from audit trail information. These reports can indicate variations from "normal" operation or detect known signatures of unauthorized access episodes. In order to limit the amount of audit information flagged and reported by automated violation analysis and reporting mechanisms, clipping levels can be set.
Source: KRUTZ, Ronald L.& VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 35.

QUESTION 133
What is Kerberos?

A. A three-headed dog from the egyptian mythology.
B. A trusted third-party authentication protocol.
C. A security model.
D. A remote authentication dial in user server.

Correct Answer: B
Explanation:
Is correct because that is exactly what Kerberos is.

The following answers are incorrect:

A three-headed dog from Egyptian mythology. Is incorrect because we are dealing with Information Security and not the Egyptian mythology but the Greek Mythology.
A security model. Is incorrect because Kerberos is an authentication protocol and not just a security model.
A remote authentication dial in user server. Is incorrect because Kerberos is not a remote authentication dial in user server that would be called RADIUS.

QUESTION 134
Which of the following is NOT a system-sensing wireless proximity card?

A. magnetically striped card
B. passive device
C. field-powered device
D. transponder

Correct Answer: A
Explanation:
Source: KRUTZ, Ronald L.& VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, page 342.

QUESTION 135
Which of the following statements pertaining to the Bell-LaPadula is TRUE if you are NOT making use of the strong star property?

A. It allows "read up."
B. It addresses covert channels.
C. It addresses management of access controls.
D. It allows "write up."

Correct Answer: D
Explanation:
Bell-LaPadula Confidentiality Model10 The Bell-LaPadula model is perhaps the most well-known and significant security model, in addition to being one of the oldest models used in the creation of modern secure computing systems. Like the Trusted Computer System Evaluation Criteria (or TCSEC), it was inspired by early U.S. Department of Defense security policies and the need to prove that confidentiality could be maintained. In other words, its primary goal is to prevent disclosure as the model system moves from one state (one point in time) to another.

When the strong star property is not being used it means that both the property and the Simple Security Property rules would be applied.

The Star (*) property rule of the Bell-LaPadula model says that subjects cannot write down, this would compromise the confidentiality of the information if someone at the secret layer would write the object down to a confidential container for example.

The Simple Security Property rule states that the subject cannot read up which means that a