TNI/TCSEC MATRIX

	A1	B3	B2	B1	C2	C1
DISCRETIONARY ACCESS						
Discretionary Access Control						
Identification and Authentication						
System Integrity						
System Architecture						
Security Testing						
Security Features User's Guide Trusted Facility Manual Design Documentation Test Documentation						
CONTROLLED ACCESS						
Protect Audit Trails						
Object Reuse						
MANDATORY ACCESS CONTROL						
Labels						
Mandatory Access Control						
Process isolation in system architecture						
Design Specification & Verification						
Device labels						
Subject Sensitivity Labels						
Trusted Path						
Separation of Administrator and User functions						
Covert Channel Analysis (Only Covert Storage Channel at B2)						
Trusted Facility Management						
Configuration Management						
Trusted Recovery						
Covert Channel Analysis (Both Timing and Covert Channel analysis at B3)						
Security Administrator Role Defined						
Monitor events and notify security personnel						
Trusted Distribution						
Formal Methods						
	A1	B3	B2	B1	C2	C1

TCSEC Matric

The following are incorrect answers:

D is incorrect. D deals with minimal security.
B is incorrect. B deals with mandatory protection.
A is incorrect. A deals with verified protection.
Reference(s) used for this question:
CBK, p. 329 ?330

Shon Harris, CISSP All In One (AIO), 6th Edition , page 392-393

QUESTION 218
Who developed one of the first mathematical models of a multilevel-security computer system?

A. Diffie and Hellman.
B. Clark and Wilson.

C. Bell and LaPadula.
D. Gasser and Lipner.

Correct Answer: C
Explanation:
In 1973 Bell and LaPadula created the first mathematical model of a multi- level security system.

The following answers are incorrect:

Diffie and Hellman. This is incorrect because Diffie and Hellman was involved with cryptography.
Clark and Wilson. This is incorrect because Bell and LaPadula was the first model. The Clark-Wilson model came later, 1987.
Gasser and Lipner. This is incorrect, it is a distractor. Bell and LaPadula was the first model.

QUESTION 219
What refers to legitimate users accessing networked services that would normally be restricted to them?

A. Spoofing
B. Piggybacking
C. Eavesdropping
D. Logon abuse

Correct Answer: D
Explanation:
Unauthorized access of restricted network services by the circumvention of security access controls is known as logon abuse. This type of abuse refers to users who may be internal to the network but access resources they would not normally be allowed.
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 74).

QUESTION 220
Which TCSEC class specifies discretionary protection?

A. B2
B. B1
C. C2
D. C1

Correct Answer: D
Explanation:
C1 involves discretionary protection, C2 involves controlled access protection, B1 involves labeled security protection and B2 involves structured protection. Source: TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.

QUESTION 221
Which access control type has a central authority that determine to what objects the subjects have access to and it is based on role or on the organizational security policy?

A. Mandatory Access Control
B. Discretionary Access Control

C. Non-Discretionary Access Control
D. Rule-based Access control

Correct Answer: C
Explanation:
Non Discretionary Access Control include Role Based Access Control (RBAC) and Rule Based Access Control (RBAC or RuBAC). RABC being a subset of NDAC, it was easy to eliminate RBAC as it was covered under NDAC already.

Some people think that RBAC is synonymous with NDAC but RuBAC would also fall into this category.

Discretionary Access control is for environment with very low level of security. There is no control on the dissemination of the information. A user who has access to a file can copy the file or further share it with other users.

Rule Based Access Control is when you have ONE set of rules applied uniformly to all users. A good example would be a firewall at the edge of your network. A single rule based is applied against any packets received from the internet.

Mandatory Access Control is a very rigid type of access control. The subject must dominate the object and the subject must have a Need To Know to access the information. Objects have labels that indicate the sensitivity (classification) and there is also categories to enforce the Need To Know (NTK).

Source: KRUTZ, Ronald L.& VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 33.

QUESTION 222
Kerberos can prevent which one of the following attacks?

A. tunneling attack.
B. playback (replay) attack.
C. destructive attack.
D. process attack.

Correct Answer: B
Explanation:
Each ticket in Kerberos has a timestamp and are subject to time expiration to help prevent these types of attacks.

The following answers are incorrect:

tunneling attack. This is incorrect because a tunneling attack is an attempt to bypass security and access low-level systems. Kerberos cannot totally prevent these types of attacks.
destructive attack. This is incorrect because depending on the type of destructive attack, Kerberos cannot prevent someone from physically destroying a server.
process attack. This is incorrect because with Kerberos cannot prevent an authorzied individuals from running processes.

QUESTION 223
The primary service provided by Kerberos is which of the following?

A. non-repudiation
B. confidentiality
C. authentication
D. authorization

Correct Answer: C
Explanation:
The Correct Answer: authentication. Kerberos is an authentication service. It can use single-factor or multi-factor authentication methods.

The following answers are incorrect:

non-repudiation. Since Kerberos deals primarily with symmetric cryptography, it does not help with non-repudiation.
confidentiality. Once the client is authenticated by Kerberos and obtains its session key and ticket, it may use them to assure confidentiality of its communication with a server; however, that is not a Kerberos service as such.
authorization. Although Kerberos tickets may include some authorization information, the meaning of the authorization fields is not standardized in the Kerberos specifications, and authorization is not a primary Kerberos service.

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

ISC2 OIG,2007 p. 179-184
Shon Harris AIO v.3 152-155

QUESTION 224
What is called the verification that the user's claimed identity is valid and is usually implemented through a user password at log-on time?

A. Authentication
B. Identification
C. Integrity
D. Confidentiality

Correct Answer: A
Explanation:
Authentication is verification that the user's claimed identity is valid and is usually implemented through a user password at log-on time.
Source: KRUTZ, Ronald L.& VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 36.

QUESTION 225
Which of the following is NOT a form of detective administrative control?

A. Rotation of duties
B. Required vacations
C. Separation of duties
D. Security reviews and audits
Correct Answer: C

Explanation:
Detective administrative controls warn of administrative control violations. Rotation of duties, required vacations and security reviews and audits are forms of detective administrative controls. Separation of duties is the practice of dividing the steps in a system function among different individuals, so as to keep a single individual from subverting the process, thus a preventive control rather than a detective control.
Source: DUPUIS, Cl?ment, Access Control Systems and Methodology CISSP Open Study Guide, version 1.0 (march 2002).

QUESTION 226
Which of the following security controls might force an operator into collusion with personnel assigned organizationally within a different function in order to gain access to unauthorized data?

A. Limiting the local access of operations personnel
B. Job rotation of operations personnel
C. Management monitoring of audit logs
D. Enforcing regular password changes

Correct Answer: A
Explanation:
The questions specifically said: "within a different function" which eliminate Job Rotation as a choice.

Management monitoring of audit logs is a detective control and it would not prevent collusion.

Changing passwords regularly would not prevent such attack.

This question validates if you understand the concept of separation of duties and least privilege. By having operators that have only the minimum access level they need and only what they need to do their duties within a company, the operations personnel would be force to use collusion to defeat those security mechanism. Source: TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.

QUESTION 227
Which of the following is not a two-factor authentication mechanism?

A. Something you have and something you know.
B. Something you do and a password.
C. A smartcard and something you are.
D. Something you know and a password.

Correct Answer: D
Explanation:
Something you know and a password fits within only one of the three ways authentication could be done. A password is an example of something you know, thereby something you know and a password does not constitute a two-factor authentication as both are in the same category of factors.

A two-factor (strong) authentication relies on two different kinds of authentication factors out of a list of three possible choice:

something you know (e.g. a PIN or password),
something you have (e.g. a smart card, token, magnetic card), something you are is mostly