ISTANBUL ALTINBAS UNIVERSITY

Name, Surname :
Number :
Lecture Code : BT/IT 530 & EBM/ECE 510
: IT/BT550 & ECE/EBM580
Lecture Name : Computer and Network Security & Advanced Computer Networks
: Bilgisayar ve Ay Güvenliği & İleri Bilgisayar Ağları
Exam Type : □ Quiiz □ Midterm ⊗ Final
Date :08.01.2019

Rules: Only 20/40 must be answerred. 2 wrong answers take one corrent answer. Duration is 30 minutes

QUESTIONS

		T	F
1	The strength of a hash function against brute-force attacks depends solely on the length of the hash code produced by the algorithm.	**T**	
2	Memory cards store and process data.		**F**
3	Computer security is protection of the integrity, availability, and confidentiality of information system resources.	**T**	
4	A logic bomb is the event or condition that determines when the payload is activated or delivered.	**T**	
5	A virus that attaches to an executable program can do anything that the program is permitted to do.	**T**	
6	Triple DES takes a plaintext block of 64 bits and a key of 56 bits to produce a ciphertext block of 64 bits.		**F**
7	A single countermeasure is sufficient for SQLi attacks.		**F**
8	An auditing function monitors and keeps a record of user accesses to system resources.	**T**	
9	The more critical a component or service, the higher the level of availability required.	**T**	
10	Identification is the means of establishing the validity of a claimed identity provided by a user.	**T**	
11	To create a relationship between two tables, the attributes that define the primary key in one table must appear as attributes in another table, where they are referred to as a foreign key.	**T**	
12	Security mechanisms typically do not involve more than one particular algorithm or protocol.		**F**
13	A user may belong to multiple groups.	**T**	
14	Keylogging is a form of host attack.		**F**
15	Many users choose a password that is too short or too easy to guess.	**T**	
16	In the context of security our concern is with the vulnerabilities of system resources.	**T**	
17	Security labels indicate which system entities are eligible to access certain resources.		**F**
18	Symmetric encryption is used primarily to provide confidentiality.	**T**	

19	Keyware captures keystrokes on a compromised system.		**F**
20	External devices such as firewalls cannot provide access control services.		**F**
21	Metamorphic code is software that can be shipped unchanged to a heterogeneous collection of platforms and execute with identical semantics.		**F**
22	Fixed server roles operate at the level of an individual database.		**F**
23	Malicious software aims to trick users into revealing sensitive personal data.	**T**	
24	The value of a primary key must be unique for each tuple of its table.	**T**	
25	Site security of the data center itself includes barriers to entry, coupled with authentication techniques for gaining physical access.		**F**
26	Assurance is the process of examining a computer product or system with respect to certain criteria.		**F**
27	A query language provides a uniform interface to the database.	**T**	
28	Depending on the details of the overall authentication system, the registration authority issues some sort of electronic credential to the subscriber.		**F**
29	A view cannot provide restricted access to a relational database so it cannot be used for security purposes.		**F**
30	An individual's signature is not unique enough to use in biometric applications.		**F**
31	The "A" in the CIA triad stands for "authenticity".		**F**
32	The authentication function determines who is trusted for a given purpose.		**F**
33	User authentication is the fundamental building block and the primary line of defense.	**T**	
34	The advantage of a stream cipher is that you can reuse keys.		**F**
35	Access control is the central element of computer security.	**T**	
36	Public-key cryptography is asymmetric.	**T**	
37	Cryptanalytic attacks try every possible key on a piece of ciphertext until an intelligible translation into plaintext is obtained.		**F**
38	Reliable input is an access control requirement.	**T**	
39	Contingency planning is a functional area that primarily requires computer security technical measures.		**F**
40	Two of the most important applications of public-key encryption are digital signatures and key management.	**T**	