Program: BE Information Technology Engineering

Curriculum Scheme: Revised 2012

Examination: Third Year Semester VI

Course Code: TEITC603 and Course Name: SYSTEM AND WEB SECURITY

Time: 1hour Max. Marks: 50

==========

==========

Note to the students:- All the Questions are compulsory and carry equal marks .

Q1.	_____ is a weakness that can be exploited by attackers
Option A:	System with Virus
Option B:	System without firewall
Option C:	System with vulnerabilities
Option D:	System with a strong password
Q2.	_____ type of exploit requires accessing to any vulnerable system for enhancing privilege for an attacker to run the exploit.
Option A:	Local exploits
Option B:	Remote exploits
Option C:	System exploits
Option D:	Network exploits
Q3.	The full form of Malware is _____
Option A:	Malfunctioned Software
Option B:	Multipurpose Software
Option C:	Malicious Software
Option D:	Malfunctioning of Security
Q4.	_____ is a code injecting method used for attacking the database of a system / website
Option A:	HTML injection
Option B:	SQL Injection
Option C:	Malicious code injection
Option D:	XML Injection
Q5.	What type of attack uses a fraudulent server with a relay address?
Option A:	NTLM
Option B:	MITM
Option C:	NetBIOS
Option D:	SMB

Q6.	Wireshark is a _____ tool.
Option A:	Network protocol analysis
Option B:	Network connection security
Option C:	Connection analysis
Option D:	Defending malicious packet-filtering
Q7.	What protocol is the Active Directory database based on?
Option A:	LDAP
Option B:	TCP
Option C:	SQL
Option D:	HTTP
Q8.	In public key cryptosystem which is kept as public?
Option A:	Encryption keys
Option B:	Decryption keys
Option C:	Encryption & Decryption keys
Option D:	Keys
Q9.	Private key algorithm is used for _____ encryption and public key algorithm is used for _____ encryption.
Option A:	Messages, Session key
Option B:	Session key, Messages
Option C:	Session
Option D:	Keys
Q10.	Secure Hash function or algorithm developed by:
Option A:	NIST
Option B:	IEEE
Option C:	ANSI
Option D:	CSI
Q11.	Decryption algorithm:
Option A:	Encrypts input data
Option B:	Decrypts the Encrypted data
Option C:	Plaintext
Option D:	Ciphertext
Q12.	Cryptography can be divided into _____ types.
Option A:	5
Option B:	4
Option C:	3
Option D:	2
Q13.	Data which is easily readable & understandable without any special algorithm or method is called _____

Option A:	Cipher-text
Option B:	Plain text
Option C:	Raw text
Option D:	Encrypted text
Q14.	Which of the following is not the primary objective of cryptography?
Option A:	Confidentiality
Option B:	Data Integrity
Option C:	Data Redundancy
Option D:	Authentication
Q15.	_____ takes the plain text and the key as input for creating cipher-text.
Option A:	Decryption Algorithm
Option B:	Hashing Algorithm
Option C:	Tuning Algorithm
Option D:	Encryption Algorithm
Q16.	In _____ same keys are implemented for encrypting as well as decrypting the information.
Option A:	Symmetric Key Encryption
Option B:	Asymmetric Key Encryption
Option C:	Asymmetric Key Decryption
Option D:	Hash-based Key Encryption
Q17.	Botnets are managed by _____
Option A:	Bot-holders
Option B:	Bot-herders
Option C:	Bot-trainers
Option D:	Bot-creators
Q18.	_____ are implemented to carry out distributed DDoS attacks, steal data, send spam messages & permits the hacker to access various devices & its connection.
Option A:	Trojan
Option B:	Virus
Option C:	Botnet
Option D:	Worms
Q19.	Infected computers and other systems within the botnet are called _____
Option A:	Killers
Option B:	Vampires
Option C:	Zombies

Option D:	Gargoyles
Q20.	The bot program allows the bot-herders to perform all operations from a _____ location.
Option A:	Corporate
Option B:	Open
Option C:	Local
Option D:	Remote
Q21.	The _____ method provides a one-time session key for two parties.
Option A:	Diffie-Hellman
Option B:	RSA
Option C:	DES
Option D:	AES
Q22.	What is the term used for the secret key for symmetric encryption that is generated for use for a short period of time?
Option A:	Stream Key
Option B:	Session Key
Option C:	Strategic Key
Option D:	Sequence Key
Q23.	Authentication applied to all of the packet except for the IP header is _____ .
Option A:	Security Mode
Option B:	Tunnel Mode
Option C:	Transport Mode
Option D:	Cipher Mode
Q24.	Insertion of messages into the network from a fraudulent source is a _____ attack.
Option A:	Masquerade
Option B:	Source Repudiation
Option C:	Sequence Modification
Option D:	Spoofing
Q25.	MAC is used to ensure
Option A:	Authentication
Option B:	Confidentiality
Option C:	Authentication and integrity
Option D:	Authentication and confidentiality