

Program: BE Information Technology

Curriculum Scheme: Revised 2016

Examination: Final Year Semester VII

Course Code: ITC702 and Course Name: Infrastructure Security

Time :2 Hour

Max.Marks:80

<b>Q1.</b>	<b>Choose the correct option for following questions. All the Questions are compulsory and carry equal marks (2 marks each)</b>
1.	An attempt to harm, damage or cause threat to a system or network is broadly termed as _____
Option A:	Cyber-crime
Option B:	Cyber Attack
Option C:	System hijacking
Option D:	Digital crime
2.	What does the term vulnerability mean?
Option A:	a computer that contains sensitive information
Option B:	a method of attack to exploit a target
Option C:	a weakness that makes a target susceptible to an attack
Option D:	a known target or victim machine
3.	What is the difference between a virus and a worm?
Option A:	Viruses hide in legitimate programs but worms do not.
Option B:	Worms self-replicate but viruses do not.
Option C:	Viruses self-replicate but worms do not.
Option D:	Worms require a host file but viruses do not
4.	Which of the following would fall into the category of “something a person Is”?
Option A:	Passwords
Option B:	Passphrases
Option C:	Fingerprints
Option D:	Smart cards
5.	The access to resource objects is strictly controlled by operating systems based on system administrator configured setting.
Option A:	Mandatory access organizations
Option B:	Discretionary access control
Option C:	Role based access control
Option D:	attribute based access control
6.	Which one of the following is not in a category of attack on file system
Option A:	Race condition attack
Option B:	Using ADS hide files
Option C:	Directory traversal
Option D:	Phishing
7.	_____ platforms are used for safety and protection of information in the cloud.

Option A:	Cloud workload protection platforms
Option B:	Cloud security protocols
Option C:	AWS
Option D:	One Drive
8.	A service that concentrates on hardware follows the _____ as a Service model
Option A:	IaaS
Option B:	CaaS
Option C:	PaaS
Option D:	RaaS
9.	SSH uses _____ to authenticate the remote computer.
Option A:	private-key cryptography
Option B:	any of public-key or private-key
Option C:	both public-key & private-key
Option D:	public-key cryptography
10.	Network layer firewall works as a _____
Option A:	Frame filter
Option B:	Content filter
Option C:	Packet filter
Option D:	Virus filter
11.	Which of the following is not an appropriate method of spoiling web server?
Option A:	Mail server intrusion
Option B:	Web application bugs
Option C:	Web shares misconfiguration
Option D:	Sessions hijacking
12.	A document that contains description of any event that has happened, which require further investigation is called as _____ .
Option A:	Test Summary Report
Option B:	Defect Report
Option C:	Bug Report
Option D:	Incident Report
13.	When should the Business Continuity Plan be reviewed?
Option A:	Whenever encountering a disaster
Option B:	At least annually or whenever significant changes occur
Option C:	Whenever the company gets audited
Option D:	Whenever the legal department declares it is time
14.	Linux operating systems store encrypted login password in a file called:
Option A:	/etc/passwd
Option B:	/etc/lib
Option C:	/etc/home
Option D:	/etc/ profile
15.	Data that should not be available to public is called as
Option A:	Element accuracy

Option B:	Element Integrity
Option C:	Sensitive data
Option D:	Non Sensitive data
16.	Which three aspects of security clearly relate to Database management system
Option A:	Confidentiality, Integrity and Availability
Option B:	Confidentiality, Integrity and Auditability
Option C:	Confidentiality, Identification and Integration
Option D:	Access control, Accounting and Reliability
17.	Paging, Segmentation, Relocation are techniques used by Operating System for _____
Option A:	File Protection
Option B:	Memory Protection
Option C:	Preventing Root kit Attack
Option D:	Device Protection
18.	While executing Shell Script the file needs to be given execute right using
Option A:	Chmod
Option B:	Touch
Option C:	Pwd
Option D:	Who
19.	Which HTTP method is used when the user first loads a webpage?
Option A:	GET
Option B:	POST
Option C:	PUT
Option D:	DELETE
20.	----- is the process of limiting the impact and the effect of an incident and preventing it from causing further damage
Option A:	Evidence gathering
Option B:	Containment
Option C:	Evidence handling
Option D:	Eradication

<b>Q2</b>	<b>Solve any Two Questions out of Three</b>	<b>10marks each</b>
A	Explain different types of malware in software security.	
B	Explain different types of Authentication methods.	
C	Explain different types of Email Attack.	

<b>Q3</b>	<b>Solve any Two Questions out of Three</b>	<b>10marks each</b>
A	Explain OWASP and its ten Vulnerabilities.	
B	Explain UTMS security with neat diagram.	
C	Write note on Cloud Identity and Access management.	