

University of Mumbai

Examinations Commencing from 23rd December 2020 to 6th January 2021 and from 7th January 2021
to 20th January 2021

Program: **Computer Engineering**

Curriculum Scheme: 2016

Examination: BE Semester VII

Course Code: ILO7016 and Course Name: CYBER SECURITY AND LAWS

Time: 2 hour

Max. Marks: 80

Q1.	Choose the correct option for following questions. All the Questions are compulsory and carry equal marks
1.	_____ is a violent act done using the Internet, which either threatens any technology user or leads to loss of life or otherwise harms anyone in order to accomplish political gain.
Option A:	Cyber campaign
Option B:	Cyber-terrorism
Option C:	Cyber attack
Option D:	Cyber Defamation
2.	_____ means the protection of data from modification by unknown users.
Option A:	Confidentiality
Option B:	Integrity
Option C:	Authentication
Option D:	Non-repudiation
3.	_____ occurs when some one forcefully takes control of web site (by cracking Password and later changing it).
Option A:	Web jacking
Option B:	Phishing
Option C:	Data diddling
Option D:	Sniffing
4.	_____ is the information gathering phase in ethical hacking from the target user.
Option A:	Reconnaissance
Option B:	Scanning
Option C:	Gaining access
Option D:	Maintaining access
5.	_____ is a collection of internet-connected devices infected by malware that allow hackers to
Option A:	Ransom ware
Option B:	Botnet
Option C:	Spoofing
Option D:	Sniffing
6.	_____ is a path or means by which an attacker can gain access to a

	computer or to network server to deliver a payload.
Option A:	Attack Vector
Option B:	Worm
Option C:	Phishing
Option D:	Cyber Defamation
7.	Which of them is a proper measure of securing social networking account?
Option A:	Never keep your password with any relevant names
Option B:	Keep written records of your passwords
Option C:	Keep records of your password in audio format in your personal cell-phone
Option D:	Passwords are kept smaller in size to remember
8.	_____ 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
9.	When there is an excessive amount of data flow, which the system cannot handle, _____ attack takes place.
Option A:	Database crash attack
Option B:	Buffer Overflow attack
Option C:	SQL injection
Option D:	Cyber Stalking
10.	Which method of hacking will record all your keystrokes?
Option A:	Keyhijacking
Option B:	Keyhijacking
Option C:	Keylogging
Option D:	Keyboard monitoring
11.	The Law of Contract is noting but
Option A:	A child of commercial dealing
Option B:	A child of religion
Option C:	A child of day to day politics
Option D:	A child of economics
12.	A company wishes to ensure that no one else can use their logo.
Option A:	Copy rights
Option B:	Trade mark
Option C:	Patent
Option D:	Industrial designs
13.	The Indian Penal Code came into effect/existence from...
Option A:	6 October 1860
Option B:	5 October 1980

Option C:	1 May 1980
Option D:	6 December 1960
14.	What does EDI stand for?
Option A:	Electronic Data Interchange
Option B:	Electronic Document Interchange
Option C:	Electric Document Interchange
Option D:	Engineering Data Interchange
15.	What is the time limit for filing appeal against the order of Cyber appellate tribunal?
Option A:	30 days
Option B:	40 days
Option C:	60 days
Option D:	90 days
16.	Which section of IT Act deals with Child pornography
Option A:	Section 67D
Option B:	Section 67F
Option C:	Section 67C
Option D:	Section 67B
17.	Which section of IT Act 2000 deals with the punishment for cheating by impersonation by using computer resources?
Option A:	Section 66D
Option B:	Section 66C
Option C:	Section 66F
Option D:	Section 66B
18.	The GLBA Compliance provide
Option A:	Specifies best practices in information systems security and control.
Option B:	Outlines medical security and privacy rules
Option C:	Public Company account reform
Option D:	Financial service modernization
19.	The Sarbanes-Oxley Act
Option A:	Requires financial institutions to ensure the security of customer data.
Option B:	Specifies best practices in information systems security and control.
Option C:	Imposes responsibility on companies and management to safeguard the accuracy of financial information.
Option D:	Outlines medical security and privacy rules
20.	NERC compliance provide
Option A:	Made it a requirement for federal agencies to develop, document, and implement an information security and protection program
Option B:	Public Company account reform
Option C:	Financial service modernization
Option D:	Healthcare information security

Q2 (20 Marks)	Solve any Two Questions out of Three	10 marks each
A	Explain Cyber Defamation with example.	
B	Explain Security Standard HIPAA and GLBA	
C	Explain Cybercrime and criminal justice in IT act 2000.	

Q3. (20 Marks)	Solve any Two Questions out of Three	10 marks each
A	Explain cloud computing with cyber attack	
B	Explain the concept of Botnet and Attack vector	
C	Explain IPR in Cyber law.	