

**University of Mumbai**  
**Online Examination 2020**

**Program: BE Engineering**  
**Curriculum Scheme: R-2016**  
**Examination: Final Year Semester VII**  
**Course Code: ILOC 7016      Course Name: Cyber Security & Laws**  
**Time: 1 hour      Max. Marks: 50**

1		The crossing of cyber boundaries into other people's computer systems into spaces where rights of ownership or title have already been established and causing damage is called _____
	a	Cyber violence
	b	Cyber deceptions
	c	Cyber trespass
	d	Cyber threat
2		Following is not a integrity related cyber crime:
	a	Phreaking/Chipping
	b	Cracking/Hacking
	c	Online grooming
	d	Denial of service
3		_____ is a potential carrier for worms and other malware
	a	General applications
	b	Internet-based application
	c	Operating system
	d	Messages
4		A group of computers that is networked together and used by hackers to steal information is called a ...
	a	Internet
	b	Intranet
	c	Botnet

	d	Rootkit
5		Jason receives notices that he has unauthorized charges on his credit card account. What type of attack is Jason a victim of?
	a	Social engineering
	b	Phishing
	c	Identity theft
	d	Bad luck
6		A _____ is a small malicious program that runs hidden on infected system.
	a	Virus
	b	Trojan
	c	Shareware
	d	Adware
7		_____ gets propagated through networks and technologies like SMS, Bluetooth, wireless medium, USBs and infrared to affect mobile phones.
	a	Worms
	b	Antivirus
	c	Malware
	d	Adware
8		Which one of the following responses is not a recommended way to avoid being victimized by malicious Trojans targeting Symbian-based devices?
	a	Ensure users upgrade their devices every 12 months.
	b	Keep firmware and OS versions up to date.
	c	Use mobile antispyware and antivirus software.
	d	Install only Symbian-signed programs or programs from a trusted source.
9		_____ is an activity that takes place when cyber-criminals infiltrates any data source and takes away or alters sensitive information.
	a	Data-hack
	b	Data-stealing
	c	Database altering
	d	Data breach

10		_____ is type of Buffer Overflow?
	a	Heap Buffer Overflow
	b	HIT Overflow
	c	Hope Overflow
	d	Hide Overflow
11		What is the name of the viruses that fool a user into downloading and/or executing them by pretending to be useful applications?
	a	Worm
	b	Cracker
	c	Keylogger
	d	Trojan horses
12		Application layer DoS attack is also known as _____
	a	Layer4 DoS attack
	b	Layer5 DoS attack
	c	Layer6 DoS attack
	d	Layer7 DoS attack
13		Following is not a DoS attack:
	a	Volume Based Attacks
	b	Ping of Death,
	c	Hacking
	d	Smurf DDoS
14		What is the process of evaluating IT assets, their importance to the organization, and their susceptibility to threats, to measure the risk exposure of these assets?
	a	Security
	b	Risk management
	c	Risk assessment
	d	Firewall

15		When a software is pirated, it harmes.....
	a	Software Developers
	b	Management
	c	Operator
	d	People
16		_____ is a conceptual electronic space unbounded by distance or other physical limitations
	a	E-commerce
	b	Cyberspace
	c	Information technology
	d	internet
17		Property Rights (IPR) protect the use of information and ideas that are of -----
	a	Ethical value
	b	Moral value
	c	Social value
	d	Commercial value
18		From mobile shopping to online payment encryption and beyond, ecommerce encompasses a wide variety of ----, ----, and ---- for both online buyers and sellers.
	a	data, sales, and tools
	b	data, systems, and tools
	c	data, systems, and sales
	d	data, sales, and tools
19		Which section of IT Act 2000 deals with the punishment for cheating by impersonation by using computer resources?
	a	Section 66D
	b	Section 66C
	c	Section 67F
	d	Section 67D
20		What is the punishment for identity theft in IT Act?

	a	Two year imprisonment or 1 lakh rupees penalty or both
	b	Three year imprisonment or 1 lakh rupees penalty or both
	c	Three year imprisonment or 2 lakh rupees penalty or both
	d	One year imprisonment
21		The ---- section deals with power to issue directions for blocking for public access of any information through any computer resource
	a	68
	b	69A
	c	69B
	d	72
22		The section --- defines punishment for dishonestly receiving stolen computer resource or communication device.
	a	66A
	b	66B
	c	66D
	d	66E
23		Under the GLBA, each manager or service-person is only allowed to___
	a	Manage one type of financial product/instrument
	b	Manage two type of financial product/instrument
	c	Manage three type of financial product/instrument
	d	Manage four type of financial product/instrument
24		National Institute of Standards and Technology (NIST) is responsible for
	a	Maintaining and updating the compliance documents as directed by GLBA
	b	Maintaining and updating the compliance documents as directed by HIPPA
	c	Maintaining and updating the compliance documents as directed by ISO
	d	Maintaining and updating the compliance documents as directed by FISMA
25		The ----- is a set of security standards formed in 2004 by Visa, MasterCard, Discover Financial Services, JCB International and American Express.

	a	Payment Card Industry Data Security Standard (PCI DSS)
	b	Payment Card Institute Data Security Standard (PCI DSS)
	c	Payment Card Information & Data Security Standard (PCI DSS)
	d	Payment Card Industry Double Security Standard (PCI DSS)