

Enrollment No.....



Faculty of Engineering
End Sem (Even) Examination May-2018
CA5EL12 Cyber Security

Programme: MCA

Branch/Specialisation: Computer Application

Duration: 3 Hrs.

Maximum Marks: 60

Note: All questions are compulsory. Internal choices, if any, are indicated. Answers of Q.1 (MCQs) should be written in full instead of only a, b, c or d.

- Q.1
- i. Unique issues in case of transaction in electronic form needed to be addressed were: **1**
(a) Uncitral Model Law (b) Cyber Model Law
(c) Universal Model Law (d) Tactical Model Law
 - ii. Intruders are the most common security threat which also referred as: **1**
(a) Hacker (b) Cracker (c) Both (a) and (b) (d) None of these
 - iii. _____ is (collection software robots) used for collection of software that run autonomously and automatically. **1**
(a) Botnet (b) Network (c) Cyber forensics (d) None of these
 - iv. _____ is an inspection of the potential points of exploit on a computer or network to identify security holes. **1**
(a) Vulnerability scanning (b) Antivirus scanning
(c) Firewall (d) Intrusion detection system
 - v. This is an attack in which multiple compromised systems attack a single target, causing users to be denied normal services. **1**
(a) Denial of Service (b) Phishing attack
(c) Spam mail (d) Spoofing
 - vi. When a person is harassed repeatedly by being followed, called or be written to he/she is a target of: **1**
(a) Bullying (b) Stalking (c) Identity theft (d) Phishing

[2]

- vii. _____ depends on evidence in the form of bits and bytes for a case analysis which resides on the storage medium of a digital device: **1**
(a) Secondary device (b) Computer forensics
(c) Information systems (d) Cyber security
- viii. Which of the following is not a type of volatile evidence? **1**
(a) Routing Tables (b) Main Memory
(c) Log files (d) Cached Data
- ix. Which section of IT Act deals with legal recognition of electronic records? **1**
(a) Section 2 (b) Section 3 (c) Section 4 (d) Section 5
- x. How many schedules are there in IT Act 2000? **1**
(a) 3 (b) 4 (c) 6 (d) 2
- Q.2 i. What are main components of cyber world? Define Cyber security. **2**
ii. Enlist different website threats. **3**
iii. Write a brief note on Network threats. What are the reasons networks become vulnerable? Mention its countermeasures. **5**
- OR iv. Explain emails threats. Explain email spoofing with example. **5**
- Q.3 i. Define cyber crime. How it is different from conventional crime. **2**
ii. Write a brief note on Hacking. What are the differences between hacking, cracking and phreaking? **8**
- OR iii. Write a brief note on planning a cyber crime. Also justify why passive attacks requires more time than active attacks. **8**
- Q.4 i. Enlist different types of computer frauds. **3**
ii. What are main steps for investigation cyber crime Describe by taking an example? **7**
- OR iii. Write a brief note on cyber crime risk management. **7**
- Q.5 i. What are the differences between computer and network forensics? **4**
ii. Describe tools used for forensic. Explain memory forensic and which tool can be used for same. **6**
- OR iii. Write a brief note on: Use of computer forensics in law enforcement. **6**

[3]

- Q.6 Attempt any two:
- i. Explain scope and objectives of IT ACT 2000 **5**
- ii. Explain in detail with cases : Section 65 and Section 66 **5**
- iii. Explain in details with cases :Section 67 and Section 68 **5**

Marking Scheme

CA5EL12 Cyber Security

Q.1	i.	Unique issues in case of transaction in electronic form needed to be addressed were: (a) Uncitral Model Law	1
	ii.	Intruders are the most common security threat which also referred as: (a) Hacker	1
	iii.	_____is (collection software robots) used for collection of software that run autonomously and automatically. (a) Botnet	1
	iv.	_____is an inspection of the potential points of exploit on a computer or network to identify security holes. (a) Vulnerability scanning	1
	v.	This is an attack in which multiple compromised systems attack a single target, causing users to be denied normal services. (a) Denial of Service	1
	vi.	When a person is harassed repeatedly by being followed, called or be written to he/she is a target of: (b) Stalking	1
	vii.	_____ depends on evidence in the form of bits and bytes for a case analysis which resides on the storage medium of a digital device: (b) Computer forensics	1
	viii.	Which of the following is not a type of volatile evidence? (c) Log files	1
	ix.	Which section of IT Act deals with legal recognition of electronic records? (b) Section 3	1
	x.	How many schedules are there in IT Act 2000? (b) 4	1
Q.2	i.	Components of cyber world Cyber security.	1 mark 1 mark
	ii.	Different website threats.	3
	iii.	Network threats. Reasons networks become vulnerable Its countermeasures.	1 mark 2 marks 2 marks

OR	iv.	Emails threats. Email spoofing with example.	2 marks 3 marks	5
Q.3	i.	Cyber crime. Difference between cyber crime & conventional crime.	1 mark 1 mark	2
	ii.	Hacking Differences between hacking, cracking and phreaking	2 marks 6 marks	8
OR	iii.	Planning a cyber crime Why passive attacks requires more time than active attacks	3 marks 5 marks	8
Q.4	i.	Different types of computer frauds.		3
	ii.	Steps for investigation cyber crime Describe by taking an example		7
OR	iii.	Cyber crime risk management.		7
Q.5	i.	Differences between computer and network forensics?		4
	ii.	Tools used for forensic. Tools for memory forensic	2 marks 4 marks	6
OR	iii.	Use of computer forensics in law enforcement.		6
Q.6		Attempt any two:		
	i.	Scope and objectives of IT ACT 2000		5
	ii.	Explanation of Section 65 Explanation of Section 66	2.5 marks 2.5 marks	5
	iii.	Explanation of Section 67 Explanation of Section 68	2.5 marks 2.5 marks	5
