Total No. of Questions: 6 *Total No. of Printed Pages:3*

Enrollment No.....

Faculty of Engineering

End Sem (Odd) Examination Dec-2019

OE00059 Cyber Security

Programme: B.Tech. Branch/Specialisation: All

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. What is the purpose of a Denial of Service attack? **1**

(a) Exploit a weakness in the TCP/IP stack
(b) To execute a Trojan on a system
(c) To overload a system so it is no longer operational
(d) To shutdown services by turning them off

ii. How is IP address spoofing detected? **1**

(a) Installing and configuring a IDS that can read the IP header
(b) Comparing the TTL values of the actual and spoofed addresses
(c) Implementing a firewall to the network
(d) Identify all TCP sessions that are initiated but does not complete successfully

iii. Phishing is a form of _____. **1**

(a) Spamming (b) Identify Theft
(c) Impersonation (d) Scanning

iv. Sniffing is used to perform _____ fingerprinting. **1**

(a) Passive stack (b) Active stack
(c) Passive banner grabbing (d) Scanned

v. In Message Integrity, SHA-l hash algorithms create an N-bit message digest out of a message of **1**

(a) 512 Bit Blocks. (b) 1001 Bit Blocks.
(c) 1510 Bit Blocks. (d) 2020 Bit Blocks.

vi. What is the hash function used in the division method? **1**

(a) h(k) = k/m (b) h(k) = k mod m
(c) h(k) = m/k (d) h(k) = m mod k

P.T.O.

vii. Network layer firewall has two sub-categories as **1**
(a) State full firewall and stateless firewall
(b) Bit oriented firewall and byte oriented firewall
(c) Frame firewall and packet firewall
(d) None of these

viii. A session symmetric key between two parties is used **1**
(a) Depends on situation (b) Only once
(c) Twice (d) Multiple times

ix. Performance, reliability, and security are criteria of **1**
(a) Efficient network (b) Intranet
(c) Protocols (d) None of these

x. _____ forensics is the systematic tracking of incoming and outgaining traffic on the network. **1**
(a) Server (b) Computer (c) Criminal (d) Network

Q.2 i. Explain Keyloggers and Spywares. **2**
ii. Differentiate torjan horses and backdoors. **3**
iii. Discuss the classification of cyber crime with suitable examples. **5**
OR iv. Explain existing preventive measures to protect society from the cyber crime. **5**

Q.3 i. Explain DoS and DDoS attack. **2**
ii. Describe the need of cyber security policy. **3**
iii. Discuss the internet governance in terms of challenges and constraints. **5**
OR iv. Explain Security aspects of HTTP application and services and SOAP Services. **5**

Q.4 i. Describe access control in cyber security. **3**
ii. What are biometrics and list different usage of biometrics data in the society. **7**
OR iii. Write drawbacks of unprotected broadband communications, poor cyber security awareness and weak authentication. **7**

Q.5 i. Differentiate between digital signature and digital certificate. **4**
ii. Explain the Diffe-Hellman key exchange protocol with suitable example. **6**
OR iii. Explain hash function with example. **6**

Q.6 Attempt any two:
i. What are the roles of International law in cyberspaces? **5**
ii. State the objectives of National Cyber Security Policy. **5**
iii. Illustrate any five different types of cyber attacks. **5**

******

Marking Scheme
OE00059 Cyber Security

Q.1	i.	What is the purpose of a Denial of Service attack? (c) To overload a system so it is no longer operational		**1**
	ii.	How is IP address spoofing detected? (b) Comparing the TTL values of the actual and spoofed addresses		**1**
	iii.	Phishing is a form of _____. (c) Impersonation		**1**
	iv.	Sniffing is used to perform _____ fingerprinting. (a) Passive stack		**1**
	v.	In Message Integrity, SHA-l hash algorithms create an N-bit message digest out of a message of (a) 512 Bit Blocks.		**1**
	vi.	What is the hash function used in the division method? (b) h(k) = k mod m		**1**
	vii.	Network layer firewall has two sub-categories as (a) State full firewall and stateless firewall		**1**
	viii.	A session symmetric key between two parties is used (b) Only once		**1**
	ix.	Performance, reliability, and security are criteria of (a) Efficient network		**1**
	x.	_____ forensics is the systematic tracking of incoming and outgaining traffic on the network. (d) Network		**1**
Q.2	i.	Keyloggers Spywares	1 mark 1 mark	**2**
	ii.	Difference torjan horses and backdoors 1 mark for each difference	 (1 mark * 3)	**3**
	iii.	Classification of cyber crime Examples	3 marks 2 marks	**5**
OR	iv.	Preventive measures to protect society from the cyber crime.		**5**
Q.3	i.	DoS DDoS attack	1 mark 1 mark	**2**
	ii.	Need of cyber security policy.		**3**
	iii.	Challenges Constraints	2 marks 3 marks	**5**
OR	iv.	Security aspects of HTTP application Services SOAP Services.	3 marks 1 mark 1 mark	**5**
Q.4	i.	Access control in cyber security 1 mark for each	 (1 mark * 3)	**3**
	ii.	Biometrics List different usage of biometrics data	2 marks 5 marks	**7**
OR	iii.	Drawbacks of Unprotected broadband communications Poor cyber security awareness Weak authentication	 2 marks 2 marks 3 marks	**7**
Q.5	i.	Digital signature Digital certificate	2 marks 2 marks	**4**
	ii.	Diffe-Hellman key exchange protocol Example	3 marks 3 marks	**6**
OR	iii.	Hash function Example	3 marks 3 marks	**6**
Q.6		Attempt any two:		
	i.	Roles of International law in cyberspaces 1 mark for each role	 (1 mark * 5)	**5**
	ii.	Objectives of National Cyber Security Policy 1 mark for each objective	 (1 mark * 5)	**5**
	iii.	Any five different types of cyber attacks 1 mark for each attack	 (1 mark * 5)	**5**

******