APJ ABDUL KALAM TECHNOLOGICAL UNIVERSITY

Scheme for Valuation/Answer Key

Scheme of evaluation (marks in brackets) and answers of problems/key

EIGHTH SEMESTER B.TECH DEGREE EXAMINATION, MAY 2019

Course Code: CS472

Course Name: PRINCIPLES OF INFORMATION SECURITY

Max. Marks: 100 Duration: 3 Hours

PART A

Answer all questions, each carries 4 marks.

		Marks
1	Brute force attack	(4)
2	Attacks on confidentiality,integrity, availability or Attacks- malicious code, brute force, Timing attack, sniffers	(4)
3	Integrity policies	(4)
4	Phishing is the process of luring a victim to a fake website by clicking on a link. (2mark) any example (2mark)	(4)
5	Any two differences (2 each).	(4)
6	• If Cookies Are Used: ▫ Scope as strict as possible ▫ Set 'secure' flag ▫ Set 'HttpOnly' flag On the client, consider disabling JavaScript (if possible) or use something like the No Script Firefox extension.	(4)
7	Frame spoofing - 2 marks Diagram - 2 marks	(4)
8	Signalling messages in UMTS are individually authenticated and integrity protected 2)Supports mutual authentication 3)Data and signalling messages are encrypted 4)Messages on all the wireless links are encrypted 5)provides "network domain security"-protecting signalling and other data between nodes in the provider domain Write any four. Each carries one mark	(4)
9	Definition- 2 mark Example using HTTP request and response- 1 mark each	(4)
10	Information leakage, Data Corruption, Violation of user privacy, Spoofed tags	(4)

PART B

Answer any two full questions, each carries 9 marks.

11	a)	Role based access control	(2)
		Example	(2)
	b)	1 difference	(2)
	c)	Mandatory access control	(3)
12	a)	Chinese wall model	(3)
		Diagram	(2)
	b)	Confidentiality, availability, integrity,authentication	(4)
13	a)	Star property	(4)
	b)	Windows Access Control Algorithm- 5 marks (If some points based on mandatory access control is written give 3 marks)	(5)

PART C

Answer any two full questions, each carries 9 marks.

14	a)	BOF-when a space allocated to a variable is not efficient to accomodate the variable in memory-stack related preliminaries two exploitations- Use of shell code - Return into Lib-C	(5)
	b)	A website has Cross site scripting if it includes malicious scripts crafted by an attacker in pages returned by it. Malicious code-javascript-examples	(4)
15	a)	Assumptions-2 equations- 1mark * 2 limitations- 1 (If any other worm propagation model is explained give 3 marks.)	(5)
	b)	Two types- E-mail worms(2 marks) P2P worms 2 marks	(4)
16	a)	Server builds an sql query based on input from user- entering part of an sql command as an input parameter- changing semantics of original query –4 marks Prevention methods -1 mark	(5)
	b)	Any one worm- 1 mark Characteristics- 3 marks eg CodeRed , Slammer etc	(4)

PART D

Answer any two full questions, each carries 12 marks.

17	a)	Link level security –Diagrams that shows creation and use of the link key - 2 marks. Computing the link key – 2 marks Using the link key-1	(6)

mark Hacking the link key-1mark(If general description about Bluetooth is given give 2 marks)

b) Step1 :Authorization request from cellphone -1 mark (6)
Step2: Creation and transmission of Authentication vectors -2 mark
Step3: Cellphone Response -1 mark
Step4:Computation/Receipt of encryption key -1 mark
Diagram-1 mark

18 a) Working of online card based payment system with steps- 8 marks (8)

b) Any 2 concerns with examples- 2 marks each (4)

19 a) Diagram – 3 marks (6)
Mac generation and encryption in CCMP Explanation – 3 marks
Or
Any answer related to 802.11i should also be given marks.

b) Any 2 technologies- XML or SOAP or WSDL(3 marks each). If any other technologies not mentioned in the syllabus is described it can also be given marks. (6)

****