SE-007

NED UNIVERSITY OF ENGINEERING & TECHNOLOGY

FINAL YEAR FALL SEMESTER (SOFTWARE ENGINEERING)
EXAMINATIONS 2018
BATCH 2015-2016

Time: 3 Hours

Dated:14-02-2019
Max.Marks:60

Network & Information Security - CT-460

Instructions:

- **Attempt ALL questions.**
- **Make neat and clean diagrams where necessary.**
- **Questions can be attempted in any order but all parts of a question must be attempted together.**

Q1			
	(a)	**EXPLAIN** the fundamental Security Design Principles. **[CLO-1]**	[4]
	(b)	**DESCRIBE** Anomaly Detection Approach and its classification of IDS (Intrusion Detection System). **[CLO-1]**	[4]
	(c)	**EXPLAIN** why it is impossible to design a perfectly secure Network & Information System. **[CLO-1]**	[4]
Q2			
	(a)	**DESCRIBE** how Public Key Cryptosystem can be used to achieve both Authentication and Secrecy. Draw the diagram as well **[CLO-1]**	[4]
	(b)	With the help of diagram **EXPLAIN** the Round function **"F"** of DES Algorithm. **[CLO-1]**	[4]
	(c)	Consider the following threats to Web security and **EXPLAIN** how each is countered by a particular feature of SSL/TLS. **[CLO-1]** a. Man-in-the-middle attack: An attacker interposes during key exchange, acting as the client to the server and as the server to the client. b. Password sniffing: Passwords in HTTP or other application traffic are eaves-dropped.	[4]
Q3			
	(a)	You are Cloud Service Provider (CSP) providing Web Hosting Services to different customers. A Customer wants to host his site **www.mysite.com** in a secure manner. **DETERMINE** how you will secure this site using PKI and HTTPS. **[CLO-2]**	[6]
	(b)	**DETERMINE** the following Denial of Service Attacks with the help of example **[CLO-2]** • TCP SYN Flooding Attacks • ICMP Flooding • Reflection Attacks	[6]
Q4			
	(a)	An organization decides to secure their network using Firewall. As security consultant you have been assigned the task to develop and implement Access Policy for the organization. The organization has different network devices (Routers, Switches etc.), Servers like Web, Email, DNS etc. and end-users. Organization requires that its Web and Email Services will be available to outside world. Internal users of organization can access the internet accept Facebook and Twitter. Assume that internal organization network consists of 10.10.0.0/16 subnet. **EXAMINE** this situation and write Access Policy as a pseudo code. Also draw the diagram of your proposed solution indicating **DMZ** and **Distributed Firewall** location. **[CLO-2]**	[6]

Q1 Q5 Q4 Q2 Q3
4 + 4 + 3 + 12 + 10 + 7 + 9

(b) You have been assigned the task for protecting an organization from different DDoS attacks. The organization has different network devices (Routers, Switches etc.), Servers like Web, Email, DNS etc. and end-users. **CONSTRUCT** defense mechanism for DDoS attacks on this organization. **[CLO-2]** [6]

Q5 (a) **APPLY** the following AES operation on the given Matrix. **[CLO-2]** [4]

i) "Byte Substitution" and then

ii) "Shift Row".

EA	04	65	85
83	45	5D	96
5C	33	98	B0
F0	2D	AD	C5

	y															
	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
B	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
E	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

Table for Q5(a)

(b) Alice wants to send message "3" to Bob using RSA Algorithm. Given, **p=5, q=7.** **CALCULATE** the Public, Private Key, Cipher Text, and Decrypt the Cipher Text to recover the original message i.e. "3". **[CLO-2]** [4]

(c) Following Table shows a sample of a packet filter firewall ruleset for an imaginary network of IP address that range from 192.168.1.0 to 192.168.1.254. **DETERMINE** the effect of each rule **[CLO-2]** [4]

Rule #	Source Address	Source Port	Dest Address	Dest Port	Action
1	Any	Any	192.168.1.0	>1023	Allow
2	192.168.1.1	Any	Any	Any	Deny
3	Any	Any	192.168.1.1	Any	Deny
4	Any	Any	192.168.1.3	HTTP	Allow

Table for Q5(c)