CS-3002: Information Security

Serial No:

Sessional Exam-I

Total Time: 1 Hour

Total Marks: 70

Signature of Invigilator

Monday, 26th September, 2022

Course Instructors

Zainab Abaid

Ali Kamal	19I-1865	N	@ali
Student Name	Roll No.	Section	Signature

DO NOT OPEN THE QUESTION BOOK OR START UNTIL INSTRUCTED.

Instructions:

1. Attempt on question paper. Attempt all of them. Read the question carefully, understand the question, and then attempt it.
2. No additional sheet will be provided for rough work. Use the back of the last page for rough work.
3. If you need more space write on the back side of the paper and clearly mark question and part number etc.
4. After asked to commence the exam, please verify that you have **thirteen (13)** different printed pages including this title page. There is a total of 4 questions.
5. Calculator sharing is strictly prohibited.
6. Use permanent ink pens only. Any part done using soft pencil will not be marked and cannot be claimed for rechecking.

	Q-1	Q-2	Q-3	Q-4	Total
Marks Obtained	26	15	8	15	64
Total Marks	30	15	10	15	70

30

excellent !!

National University of Computer and Emerging Sciences

FAST School of Computing | Fall-2022 | Islamabad Campus

Question 1: Multiple Choice Questions [30 Marks]

Mark your answers to the MCQ's in the following answer sheet with an X in the correct box. answers not provided here will not be marked.

Sr. No	A	B	C	D	Sr. No	A	B	C	D
01		X			16	X		—	
02			X		17			X	
03				X	18			X	
04		X			19		X		
05			X		20		X		
06	—			X	21				X
07			X		22				X
08				X	23	X			
09	X				24				X
10	X				25				X
11	X				26	X			
12	—			X	27				X
13		X			28	—	X		
14		X			29		X		
15			X		30			X	

26

1. The *payload* is that part of a malware which
   a) Contains ransom paying functionality
   b) Contains the main harmful functionality of the malware
   c) Is delivered through a remote shell opened by an attacker
   d) Contains the harmless part of the malware designed to trick users into thinking it is a benign program.

2. Which of the following category of malware is most likely to perform exfiltration?
   a) Ransomware
   b) Backdoor
   c) Keylogger
   d) Zombie

3. If a piece of malware can spread itself to other files within the same computer, but you don't know if it can spread outward to other machines, what should you categorize it as?
   a) A virus only
   b) A worm only
   c) A trojan
   d) Could be a worm or a virus

4. Which of the following is the most commonly file to be infected by a macro virus?
   a) An autorun.exe file on a USB
   b) A Microsoft Office document (e.g. Word, Excel etc.)
   c) A music file on a CD
   d) A .bat file in Windows

5. A zero-day malware infection on a host within an organization may be detectable by:
   a) Using strong commercial (paid) versions of anti-virus software that are likely to have an updated databas
   b) A strong border firewall
   c) The behavioral detection component in anti-virus software
   d) A rule-base Intrusion Detection System (IDS).

6. Which of the following is an example of what a behavioral detection anti-virus should consider a cle indication of malware?
   a) Attempts to discover sandboxed or virtual environments
   b) Attempts to connect to remote servers
   c) Attempts to send emails
   d) All of the above

7. Which of the following best describes pharming?
   a) It allows attackers to target specific individuals.
   b) It specifically refers to phishing phone calls.
   c) It is phishing that does not rely on user action, but automatically redirects to a malicious site.
   d) It is the same as whaling, i.e. going after the big players in an organization.

8. The purpose of modern-day cryptography is:
   a) Ensuring confidentiality of communication
   b) Ensuring both confidentiality and availability of data
   c) Ensuring access control of data
   d) Ensuring both confidentiality and integrity of communication

9. The attacker creates an exploit in the _____ phase of the cyber kill chain

a) Weaponization
b) Delivery
c) Exploitation
d) Command and control

10. HIPAA, GDPR are laws regarding
a) Protection of electronic data privacy
b) Electronic data format for interoperability
c) Electronic data format for standardization
d) All of the above

11. Advanced Persistent Threats typically involve
a) a nation state or state-sponsored group
b) hacktivists
c) script-kiddies
d) brokers

12. Contemporary malwares include
a) Fileless malware, Cryptominers
b) Virus, Cryptominers
c) Trojan, Fileless Malware
d) None of the above

13. Which of the following statements is true?
a) As security increases functionality increases
b) As security increases convenience decreases.
c) As security increases convenience and functionality both increase.
d) All of the above

14. A user is looking for a budget management software. He finds one online that looks good, and downloads and installs it. The software, however, secretly captures the user's keystrokes, and sends exfiltrated information to a network of malicious servers; the malicious servers also periodically send updates to the software. What best describes the sort of malware that the user got infected with?
a) Virus
b) Trojan
c) Botnet
d) Worm

15. Which of the following is a possible method of detection that can work on polymorphic viruses?
a) Fingerprinting
b) Signature based detection
c) Behavioural detection
d) Both (b) and (c) are possible.

16. A malware analyst is following a string of malware infections in his organization's systems. The behaviour of the malware seems consistent across machines, but the actual malicious executable he is getting from every system is completely different in terms of API calls, function names, variable names etc. What do you think he is dealing with?

a) Advanced polymorphic malware, which is changing unpredictably in every generation.
b) Oligomorphic malware, as it has infected only a limited number of systems.
c) Metamorphic malware, as it is changing its code from one generation to the next.
d) It must be an Advanced Persistent Threat to be able to change so quickly.

17. The existence of weakness in a system or network is known as a/an
a. Attack
b. Exploit
c. Vulnerability
d. Threat

18. Which security goal is violated if a computer is no more accessible?
a) Integrity
b) Confidentiality
c) Availability
d) All of the above

19. Choose among the following techniques, which are used to hide information inside a picture.
a) Image rendering
b) Steganography
c) Rootkits
d) Bitmapping

20. Frequency analysis as a method to break encryption comes under:
a) Brute force attack
b) Cryptanalysis
c) Key guessing attack
d) None of the above.

21. Messages protected by steganography can be transmitted through:
a) Picture files
b) Music files
c) Video files
d) All the above

22. Best security practices for Windows include
a) Use only reputable applications.
b) Audit logging
c) Applying security patches in timely manner
d) All the above

23. Which of the following maybe the correct block length for AES
a) 128-bit
b) 138-bit
c) 64-bit
d) All the above

24. Which of the following is NOT a steganography technique?
a) Wax Tablet
b) Invisible Ink
c) Microdots

d) Caesar Cipher

25. Which of the following events may lead to a breach of integrity?
a) accidentally deleting files
b) entering invalid data
c) altering configurations
d) all the above

26. Which of the following is NOT a security design principle?
a) complexity
b) fail-safe defaults
c) least privilege
d) encapsulation

27. What parameters are used to ensure availability?
a) Load balancing
b) Software and data backups
c) Rollback functions
d) All the above

28. Once installed, which collection of software tools is used to gain remote access to and control over a computer or system?
a) Rootkit
b) Penetration test
c) Virus
d) Logic bomb

29. _____ is used legitimately in free versions of applications to display advertisements while a program is running but can be classified as _____ if the code records users' information or browsing habits without their consent and authorization.
a) Social engineering; malvertising
b) Adware; spyware
c) Shareware; malware
d) Adware; ransomware

30. _____ are difficult to identify as they keep on changing their type and signature.
a) Non-resident virus
b) Boot Sector Virus
c) Polymorphic Virus
d) Multipartite Virus

15

Question 2 [15 marks]

Your company has a database server that stores all of your most sensitive information, valued at $10 million based on your estimate. In the event of a breach, you estimate that at least half of your data will be exposed quickly before the attack can be contained. Thus, you will lose at least half the value of the data. You estimate that this sort of breach is very unlikely to actually occur, say about a twice-a-century occurrence. However, you still want to invest in some countermeasures. You have the following options:

1. Hire a dedicated employee to monitor the logs of the server to quickly detect breach events; at the current rate, you have to pay this employee at least $2500 per month. Since you are not investing in any additional software, this employee will only have existing tools to work with, and may not be able to instantly stop breaches. Still, you think that a dedicated worker will be able to stop the breach by the time it has affected about 25% of the database; moreover, at least some attackers will be deterred if they know that you have dedicated employees monitoring the server, so the frequency of attacks is likely to reduce further, to once in 60 years.

2. Install an intrusion prevention system that strictly monitors access to the database server and reduces the frequency of possible breaches in half. The solution you like has a one-time cost of $50,000, a yearly cost of about $40,000, plus for maximum effectiveness you should also subscribe to threat feeds from two threat intelligence companies for $10,000 and $7500 per year respectively that can integrate into the IPS.

3. Install a more complex unified threat management solution that can not reduce the frequency but will almost immediately stop any detected attacks so that no more than 5% of your data will be exposed in a breach. This solution requires you to pay $150,000 every 5 years, and also subscribe to threat feeds at a combined $20,000 per year.

Fill in the following table for each of the above countermeasures. Round decimals to the nearest integer. Compare with the base case and determine which countermeasure is the most financially viable. [13 marks]

	Base Case	Countermeasure 1	Countermeasure 2	Countermeasure 3
Asset value (AV)	10000000	10000000	10000000	10000000
Exposure Factor (EF)	0.5	0.25	0.5	0.05
Single Loss Expectancy (SLE)	5000000	2500000	5000000	500000
Annualized Rate of Occurrence (ARO)	0.02	$\frac{1}{60} = 0.016$	0.01	0.02
Annualized Loss Expectancy (ALE)	100000	41667	50000	10000
ALE Reduction for countermeasure	-	58333	50000	90000
Annualized Countermeasure Cost	-	30000	107500	50000
Annualized Net Countermeasure Value	-	28333	-57500	40000

13

Countermeasure 3 is most financially stable.

Now identify at least two simplifying assumptions you made the above risk analysis, i.e. where have you assumed something that may not necessarily be true? In other words, discuss two limitations of your analysis with respect to the above case. [2 marks]

- Salary of hired employee, in countermeasure 1 will not remain same throughout the 5 years, rather it will keep increasing.
- risk analysis does not consider one time investments, as in countermeasure 1 we are including one time cost in annualized cost.
- no way to accurately know annualized rate of occurrence.

Note: partial working does not carry marks. Your answers will be marked correct only if the final values you fill in the table are correct.

Rough work for Question 2:

$\frac{2}{100} = \frac{1}{50}$

$\frac{1}{50} \times 5000000 = 100000$

$2500 \times 12 = 30000$

$\frac{150000}{5} = 30000$

Question 3 [10 marks]

1. Suppose there is a binary key with 128- bits (128 bits-of-security). Determine how many years it would take to brute force this key using a cluster of 100 computers each of which can try out 1,000,000 combinations per second? [5 marks]
(Hint: 2^10 is approximately 10^3)

Show your working here:

Total combination: 2^{128}

Combs/sec $= 100 \times 1000000$
$= 100 \times 10^6$
$= 10^2 \times 10^6$
$= 10^8$

total time $= \frac{2^{128}}{10^8}$
$= 3.402 \times 10^{30}$ years

Final Answer: 3.402×10^{30} years i-e $3402000000 \times 10^{21}$ years !
basically infinite

2. Use the following table for a polyalphabetic cipher. Encrypt the plaintext "I AM IN FAST" using the key "ISB"
(ignore spaces). [5]
[Hint: In encrypting plaintext, the cipher letter is found at the intersection of the column headed by the plaintext letter and the row indexed by the key letter]

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

I S B I S B I S B
B I A M I N F A S T

Ciphertext: Q SN QF GIKU

Page 9 of 13

Question 4 [15 marks]

Using the information given below find the cipher text for AES. Your answers will be marked only if the values recorded in the matrices on the next page are correct. Partial working does not marks.

A hexadecimal XOR table is given on the last page for your reference. Do your rough work on the page.

47	9c	90	6f
92	b8	2f	90
eb	32	af	63
61	b6	ef	db

Plain text

45	d3	76	7f
88	dd	43	96
91	5c	6c	72
f8	4c	f7	60

Cipher Key

c1	48	29	74
02	cb	da	28
66	99	bd	46
e8	ce	ca	05

State after Round 9

5f	8b	c7	e1
b3	05	66	0b
fe	70	16	61
92	08	fe	e0

Round 10 Key

	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

S-Box

Input:

c1	48	29	74
02	cb	da	28
66	99	bd	46
e8	ce	ca	05

= Substitution through S-Box

Result of operation 1:

78	52	A5	92
77	1F	57	34
33	EE	7A	5A
9B	8B	74	6B

15

= Shift

Result of operation 2:

78	52	A5	92
1F	57	34	77
7A	5A	33	EE
6B	9B	8B	74

Add i-e result of op2 XOR round 10 k

Result of operation 3:

27	09	62	73
AC	52	52	7C
84	2A	25	8F
F9	93	75	94

Final Ciphertext:

27	09	62	73
AC	52	52	7C
84	2A	25	8F
F9	93	75	94

← This is final cipher text

Hexadecimal XOR table

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
1	1	0	3	2	5	4	7	6	9	8	B	A	D	C	F	E
2	2	3	0	1	6	7	4	5	A	B	8	9	E	F	C	D
3	3	2	1	0	7	6	5	4	B	A	9	8	F	E	D	C
4	4	5	6	7	0	1	2	3	C	D	E	F	8	9	A	B
5	5	4	7	6	1	0	3	2	D	C	F	E	9	8	B	A
6	6	7	4	5	2	3	0	1	E	F	C	D	A	B	8	9
7	7	6	5	4	3	2	1	0	F	E	D	C	B	A	9	8
8	8	9	A	B	C	D	E	F	0	1	2	3	4	5	6	7
9	9	8	B	A	D	C	F	E	1	0	3	2	5	4	7	6
A	A	B	8	9	E	F	C	D	2	3	0	1	6	7	4	5
B	B	A	9	8	F	E	D	C	3	2	1	0	7	6	5	4
C	C	D	E	F	8	9	A	B	4	5	6	7	0	1	2	3
D	D	C	F	E	9	8	B	A	5	4	7	6	1	0	3	2
E	E	F	C	D	A	B	8	9	6	7	4	5	2	3	0	1
F	F	E	D	C	B	A	9	8	7	6	5	4	3	2	1	0

How to use the table:

Example: XOR 25 and B6

First XOR 2 and B, then XOR 5 and 6. Then concatenate the two answers.

Step 1: XOR 2 and B – use the number at the intersection of the row indexed by 2 and the column header by B, i.e. 9
Step 2: XOR 5 and 6 – use the number at the intersection of the row indexed by 5 and the column headed by 6, i.e. 3
Step 3: Concatenate: Answer is 93

Rough work

A5 xor C9

= 62 => A xor C : 6

5 xor 7 : 2

concat = 62