Information Security

Tuesday January 11, 2022

Course Instructor

Dr. Danish Shehzad, Dr. Irfan ul Haq,
Dr. Umer Aftab

Serial No:

Final Term Exam

Total Time:45 Min

Total Marks: 40

_____
Signature of Invigilator

Roll No	Section	Signature
_____	_____	_____

DO NOT OPEN THE QUESTION BOOK OR START UNTIL INSTRUCTED.

Instructions:

1. Verify at the start of the exam that you have a total of forty (40) MCQ's printed on seven (07) pages including this title page.
2. Attempt all questions on the question-book and in the given order.
3. The exam is closed books, closed notes. Please see that the area in your threshold is free of any material classified as 'useful in the paper' or else there may a charge of cheating.
4. Read the questions carefully for clarity of context and understanding of meaning and make assumptions wherever required, for neither the invigilator will address your queries, nor the teacher/examiner will come to the examination hall for any assistance.
5. Fit in all your answers in the provided space. You may use extra space on the last page if required. If you do so, clearly mark question/part number on that page to avoid confusion.
6. Use only your own stationery and calculator. If you do not have your own calculator, use manual calculations.
7. Use only permanent ink-pens. Only the questions attempted with permanent ink-pens will be considered. Any part of paper done in lead pencil cannot be claimed for checking/rechecking.

	Q-1	Total
Total Marks	40	**40**
Marks Obtained		

Vetted By: _____Vetter Signature: _____

University Answer Sheet Required: **No** ☐ **Yes** ☐

Question 1 **Marks: 40**

Choose the correct option.
Overwriting, cutting, erasing is not allowed in this Question.
Mark answers on the last sheet otherwise your paper will not be checked.

1. **A cipher that scrambles letters into different positions is referred to as what?**
   A. Substitution
   B. Stream
   C. Running key
   D. Transposition
2. **Attack which forces a user (end user) to execute unwanted actions on a web application in which he/she is currently authenticated…**
   A. Cross-site scoring scripting
   B. Cross-site request forgery
   C. Cross-site scripting
   D. Two-factor authentication
3. **The goal of cryptanalysis is to…?**
   A. unfold coded signals that will be accepted as authentic.
   B. ensure that the key has no repeating segments.
   C. reduce the system overhead for cryptographic functions.
   D. determine the number of encryption permutations required.
4. **What type of malware is self-contained and it does not need to be part of another computer program to propagate?**
   A. Computer virus
   B. Trojan house
   C. Computer worm
   D. Polymorphic virus
5. **Cryptography does not concern itself with:**
   A. Availability
   B. Authenticity
   C. Integrity
   D. Confidentiality
6. **Which of the following is not an appropriate method for web application hacking?**
   A. CSRF
   B. XSS

C. Brute-Force
D. SQL Injection

7. **The cross-site scripting (XSS) in which malicious code come from current HTTP requests**
   A. Stored XSS
   B. DOM based XSS
   C. Reflected XSS
   D. Deflected XSS
8. **Web server will log which part of a GET request?**
   A. Hidden tags
   B. Query strings
   C. Header
   D. Cookies
9. **What is the common cause of buffer over flows, cross-site scripting, SQL injection and format string attacks?**
   A. Unvalidated input
   B. Lack of authentication
   C. Improper error handing
   D. Insecure configuration management
10. **Cross Site Scripting is an attack against.**
    A. Client (Browser)
    B. Database
    C. Web Server
    D. None
11. **Which of the following describes the first step in establishing an encrypted session using a Data Encryption Standard (DES) key?**
    A. Key clustering
    B. Key compression
    C. Key signing
    D. Key exchange
12. **A _____ is a sequential segment of the memory location that is allocated for containing some data such as a character string or an array of integers.**
    A. Stack
    B. Queue
    C. External storage
    D. Buffer
13. **In what way does the RSA algorithm differs from the Data Encryption Standard (DES)?**
    A. It cannot produce a digital signature
    B. It eliminates the need for a key-distribution center
    C. It is based on a symmetric algorithm
    D. It uses a public key for encryption

14. How many types of buffer-overflow attack are there?

A. 4
B. 2
C. 5
D. 3

15. Let suppose a search box of an application can take at most 200 words, and you've inserted more than that and pressed the search button; the system crashes. Usually this is because of limited _____

A. Buffer
B. External storage
C. Processing power
D. Local storage

16. A system security engineer is evaluation methods to store user passwords in an information system, so what may be the best method to store user passwords and meeting the confidentiality security objective?

A. Password-protected file
B. File restricted to one individual
C. One-way encrypted file
D. Two-way encrypted file

17. In a _____ attack, the extra data that holds some specific instructions in the memory for actions is projected by a cyber-criminal or penetration tester to crack the system.

A. Phishing
B. MiTM
C. Buffer-overflow
D. Clickjacking

18. Which of the following characteristics is not of a good stream cipher?

A. Long periods of no repeating patterns.
B. Statistically predictable.
C. Keystream is not linearly related to the key.
D. Statistically unbiased keystream.

19. Which of the followings is an example of simple substitution algorithm?

A. Rivest, Shamir, Adleman (RSA)
B. Data Encryption Standard (DES)
C. Caesar cipher
D. Blowfish

20. Applications developed by programming languages like ____ and _____ have this common buffer-overflow error.

A. C, Ruby
B. Python, Ruby
C. C, C++
D. Tcl, C#

21. Old operating systems like _____ and NT-based systems have buffer-overflow attack a common vulnerability.

A. Windows 7

B. Chrome
C. IOS12
D. UNIX

22. What is a good format specifier to store large numbers in a format string attack?

A. %s
B. %d
C. %ll
D. %hn

23. Number of bytes written so far in printf function can be saved into a variable by using which format specifier.

A. %s
B. %d
C. %x
D. %n

24. Format string is the_____argument of printf function.

A. First
B. Second
C. Third
D. Fourth

25. The DES Algorithm Cipher System consists of _____rounds (iterations) each with a round key.

A. 12
B. 18
C. 9
D. 16

26. The Countermeasure of XSS attack is?

A. Content Security Policy
B. Turning Code into data
C. Treat code only as data
D. All of them

27. The countermeasure of SQL injection that separate code and data and pass both through separate channel to avoid code inject is called?

A. Prepared Statement
B. Query Statement
C. Proper statement
D. Structural Statement

28. Point out the correct statement.

A. Parameterized data cannot be manipulated by a skilled and determined attacker
B. Procedure that constructs SQL statements should be reviewed for injection vulnerabilities
C. The primary form of SQL injection consists of indirect insertion of code

D. None of the mentioned

29. Which type of cookies attached only with same-site request?

A. Simple Cookie
B. Lax Cookie
C. Strict Cookie
D. None of them

30. _____ is an attack method for decoding user credentials. Using this technique attacker can log on as user & gain access to authorized data.

A. Cookie Snooping
B. Cache Snooping
C. Cookie Jacking
D. Cache Compromising

31. Which of the following language is used for injecting executable malicious code for web application hacking?

A. Tag-Script
B. JavaScript
C. Frame-Script
D. Engine Script

32. The code that can generate its source code as output is called?

A. Coin Code
B. Quine Code
C. Low level Language code
D. HTML Code

33. The Diffie-Hellman algorithm is primarily used to provide which of the following?

A. Confidentiality
B. Integrity
C. Non-repudiation
D. Key exchange

34. How many bits make up the effective Data Encryption Standard (DES) key?

A. 60 B. 56
C. 32 D. 16

35. Which type of XSS attack is not stored on server or database?

A. 1 Persistent XSS
B. Persistent XSS
C. 0 Persistent XSS
D. Non-Persistent XSS

36. The main risk to a web application in a cross-site scripting attack is …?

A. Loss of data integrity
B. Compromise of users
C. Destruction of data
D. None of the above

37. Which of the following asymmetric encryption algorithm is based on the difficulty of factoring large numbers?

A. AES
B. RSA
C. Elliptic Curve Cryptosystems (ECCs)
D. El Gamal

38. Computation of the discrete logarithm is the basis of the cryptographic system

A. symmetric cryptography
B. asymmetric cryptography
C. deffie-hellman key exchange
D. secret key cryptography

39. This function is part of a program that is running on a 32-bit x86 system; the compiler does not change the order of variables on the stack.

```
void function(char *input)
{   int i = 1;   char buffer[8];   int j = 2;
strcpy(buffer,input);
printf("%x %x %s\n",i,j,buffer);
}
```

What is the minimum length of a string – passed to the function through the input parameter – that can crash the application?

A. 9
B. 10
C. 11
D. 12

40. Which of the following is TRUE about the type of SQL Injection attack?

A. Install malicious program
B. Export valuable data
C. Get user login detail
D. All of the above

Mark answers on the last sheet otherwise your paper will not be checked.

S#	MCQs				S#	MCQs			
1	A	B	C	D	21	A	B	C	D
2	A	B	C	D	22	A	B	C	D

3	A	B	C	D	**23**	A	B	C	D
4	A	B	C	D	**24**	A	B	C	D
5	A	B	C	D	**25**	A	B	C	D
6	A	B	C	D	**26**	A	B	C	D
7	A	B	C	D	**27**	A	B	C	D
8	A	B	C	D	**28**	A	B	C	D
9	A	B	C	D	**29**	A	B	C	D
10	A	B	C	D	**30**	A	B	C	D
11	A	B	C	D	**31**	A	B	C	D
12	A	B	C	D	**32**	A	B	C	D
13	A	B	C	D	**33**	A	B	C	D
14	A	B	C	D	**34**	A	B	C	D
15	A	B	C	D	**35**	A	B	C	D
16	A	B	C	D	**36**	A	B	C	D
17	A	B	C	D	**37**	A	B	C	D
18	A	B	C	D	**38**	A	B	C	D
19	A	B	C	D	**39**	A	B	C	D
20	A	B	C	D	**40**	A	B	C	D