National University of Computer and Emerging Sciences

FAST School of Computing **Fall-2023** **Islamabad Campus**

CS-3002: Information Security (BS-CS)

Serial No:

Sessional I
Part A
Total Time: 30 min
Total Marks: 25

Monday, 25th September, 2023

Course Instructor

Urooj Ghani, Muhammad Luqman Sumar, Sajid Hussain

_____

Signature of Invigilator

Student Name	Roll No.	Course Section	Student 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. Information Security Final Exam has two parts, make sure that you attempt both the parts (A and B). **Part B** will be given after you return **Part A**.
3. This is **Part A** of your Final Exam, estimated time to complete this part is 30 minutes.
4. No additional sheet will be provided for rough work. Use the back of the last page for rough work.
5. Your answer should only be in the space allocated for the answer.
6. After asked to commence the exam, please verify that you have seven **(7)** different printed pages including this title page. There are a total of one **(1)** questions.
7. Detach the last page **(page no 07)** which is answer page for **Part A**. You must attempt Question 1 on page no 09 and return after 30 minutes. Don't forget to write your name and roll no on the **Part A** answer sheet as well before you start.
8. Calculator sharing is strictly prohibited.
9. Use permanent ink pens only. Any part done using soft pencil will not be marked and cannot be claimed for rechecking.

	Q-1	**Total**
Marks Obtained		
Total Marks	**25**	**25**

National University of Computer and Emerging Sciences

FAST School of Computing **Fall-2023** **Islamabad Campus**

Question 1 [25 Marks]

To be answered on the last page, detach and return in 30 minutes

1. Ploutus ATM malware family detected by Symantec as
   A. Backdoor
   B. Ransomware
   C. Rootkit
   D. Adware

2. The encryption in the context of data security
   A. Storing physical documents in a highly secure vault
   B. Applying advanced mathematical algorithm to obscure data, making it inaccessible without the proper decryption key
   C. Physically securing data centers with advanced and access controls
   D. Implementing strict data retention policies and periodically purging digital records

3. What technique did Mirai botnet use to compromise IoT devices
   A. Phishing emails
   B. Password guessing and brute-force attacks
   C. Malware infected USB drives
   D. Social Engineering

4. Which of the following is an example of maintaining data integrity
   A. Implementing strong access controls
   B. Backing up data regularly
   C. Encrypting sensitive files
   D. Verifying the accuracy of data during transmission

5. What is the primary goal of access control mechanisms in information security
   A. Ensuring data availability
   B. Maintaining data confidentiality
   C. Preventing data corruption
   D. Enforcing data retention policies

6. Which of the following is a cryptographic technique used to ensure data integrity?
   A. Hashing
   B. Encryption
   C. Access control
   D. Biometric authentication

7. Which of the following is a common measure to enhance the availability of web applications
   A. Regularly changing server hardware
   B. Reducing network bandwidth
   C. Disabling SSL encryption
   D. Implementing geographically distributed servers

8. What is the primary purpose of the identification phase in the AAA security model
   Hint: Authentication, Authorization and Auditing
   A. To restrict access to authorized users only
   B. To record user activity for auditing purposes
   C. To confirm the user's identity based on provided credentials
   D. To establish secure communication channels

9. Were you sleeping in the classes?
   Hint: You can choose any option other than the option D.
   A. Yes, at times
   B. To tell you the truth, yes ma'am mostly I was sleeping
   C. No ma'am/sir, I listen to your calm soothing voice and … Zzz
   D. What kind of question this is, I will email to HoD

10. Which party is typically responsible for providing evidence of non-repudiation in a dispute involving a digital transaction?
    A. The sender
    B. The recipient
    C. A third-party mediator
    D. The legal authorities

11. How did the Heartbleed vulnerability work?
    A. It exploited a weakness in SSL/TLS protocols
    B. It allowed attackers to brute-force passwords
    C. It allowed attackers to read beyond the bounds of a buffer in server memory
    D. It caused servers to crash by overloading them with traffic

12. Which strategy relies on making critical assets appear less valuable or hiding them among less critical ones?
    A. Layering
    B. Limiting diversity
    C. Obscurity
    D. Simplicity

13. An individual hacks into a company's email server and leaks sensitive corporate emails and documents to the public. They claim to be doing it to expose corporate misconduct. What category of threat actor does this individual fall into?
    A. A script kiddie
    B. An insider threat
    C. A cybercriminal
    D. A hacktivist

14. A cybersecurity analyst notices a series of phishing emails targeting employees within their organization. Upon further investigation, they discover that the emails contained malicious attachments that, when opened, executed malware on the victims' computers. Which stage of the Cyber Kill Chain is represented by these phishing emails?
    A. Reconnaissance
    B. Delivery
    C. Execution
    D. Actions on Objectives

15. What is the primary technique used by Carbanak malware to infiltrate financial institutions?
    A. Phishing emails with malicious attachments
    B. Distributed Denial of Service (DDoS) attacks
    C. Browser vulnerabilities
    D. Social engineering through phone calls

16. A security researcher has discovered a new type of keylogger that operates in a way that evades most antivirus software. This keylogger utilizes steganography to hide its presence in image files on a computer. What type of keylogger is this most likely classified as?
    A. Memory-injecting keylogger
    B. Data-exfiltration keylogger
    C. Hardware keylogger
    D. Software keylogger

17. Did you ever checked the lectures posted on the classroom? Hint: The option d is the correct option.
    A. Wait, what… There were lectures uploaded on some classroom (whatever it is)
    B. Ma'am, the student choosing the option a, should be failed on-spot. Award me A++ grade, I have printed all of them as well
    C. If I don't check lectures, I don't feel sleepy
    D. ☺

18. A malware analyst is examining a piece of malware that spreads by attaching itself to executable files and modifying their code. What type of malware is most likely under investigation?
    A. Virus
    B. Worm
    C. Trojan
    D. Spyware

19. A security researcher discovers a new variant of the Zeus Trojan that is designed to evade antivirus detection. What term best describes this behavior?
    A. Signature-based detection
    B. Polymorphism
    C. Trojanscam
    D. Rootkit installation

20. A critical infrastructure facility was compromised by a sophisticated cyberattack. The attack leveraged vulnerabilities that were unknown to the software vendor and had not been patched. What type of vulnerabilities were exploited in this scenario?
    A. Known vulnerabilities
    B. Patched vulnerabilities
    C. Zero-day vulnerabilities
    D. Legacy vulnerabilities

21. What is the technical term for a Caesar cipher with a variable shift value that changes with each letter in the plaintext?
    A. Vigenère cipher
    B. Polyalphabetic cipher
    C. Monoalphabetic cipher
    D. Substitution cipher

22. If the keyword in a Vigenère cipher is "KEY" and the plaintext letter is 'A,' what would be the corresponding cipher text letter?
    A. K
    B. Y
    C. A
    D. E

23. You receive a message encoded with ROT13, and it reads: "Gur frperg vf zl ynfg ernq." What is the original message?
    A. "The secret is my last read."
    B. "The server is not your last date."
    C. "The cipher is my first word."
    D. "The answer is not your last word."

24. An organization needs to securely distribute encryption keys to multiple employees across different locations. Which cryptographic approach would be the most practical and secure in this situation?
    A. Symmetric cryptography
    B. Asymmetric cryptography
    C. Quantum cryptography
    D. Hybrid cryptography

25. AES-128 operates on blocks of data. What is the standard block size for data in AES encryption?
    A. 32 bits
    B. 64 bits
    C. 128 bits
    D. 256 bits

National University of Computer and Emerging Sciences

FAST School of Computing **Fall-2023** **Islamabad Campus**

CS-3002: Information Security (BS-CS) Monday, 25th September, 2023 **Course Instructor** Urooj Ghani, Muhammad Luqman Sumar, Sajid Hussain	**Final Examination** **Part A (Answer Sheet)** **Total Time: 30 min** **Total Marks: 30**

Student Name	**Roll No.**	**Section**	**Signature**

Instruction: *Please cross (X) in the full box with the correct choice, any answer not provided in the table below would not be considered. Cutting, over writing, multiple answers would be considered as incorrect. There is no negative marking.*

S. No.	**A**	**B**	**C**	**D**	**S. No.**	**A**	**B**	**C**	**D**
1.					**16.**				
2.					**17.**				
3.					**18.**				
4.					**19.**				
5.					**20.**				
6.					**21.**				
7.					**22.**				
8.					**23.**				
9.					**24.**				
10.					**25.**				
11.					**26.**				
12.					**27.**				
13.					**28.**				
14.					**29.**				
15.					**30.**				

--To be returned after first 30 minutes--