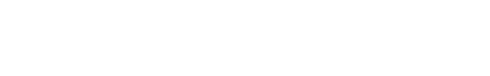
|  |  |  |  |
| --- | --- | --- | --- |
|  | |  |  | | --- | --- | | **Department of Computer Science**  **Bahria University** | **CSC-407: Information Security**  **Semester 08 (Fall 2023)** | |

**ASSIGNMENT 01**



Marks: 05

**NAME AYESHA SHAHZAD**

**CLASS: BS-CS 8th Semester**

**ENROLL#: 02-134201-083**

**Marks Obtained: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Instructions.**

* The deadline for this assignment is before or on 25/Oct/2023.
* This will be handwritten assignment, on every page you should write your name and the enrollment number
* You have to answer and submit in SOFTCOPY(pdf) and HARDCOPY of the given draft on your LMS.
* WARNING:
  + This is an individual assignment; you must solve it by yourself. Any form of plagiarism will result in receiving a zero in the assignment.
  + Late submissions will not be accepted. Any assignment submitted after the deadline will receive zero.

1

**QUESTION (5 Marks)**

**(CLO1, PLO2, C2)**

1. **Explain** how we can distinguish between the Masquerade and the Replay attacks? Give an example to elaborate your answer.

|  |  |
| --- | --- |
| Masquerade | Replay |
| In a masquerade attack, an attacker impersonates a legitimate user or entity to gain unauthorized access to a system, application, or network. | In a replay attack, an attacker intercepts and then retransmits data that was previously recorded or captured during a legitimate transaction. The attacker doesn't alter the data but simply plays it back at a later time. |
| The attacker typically steals or forges credentials, such as usernames and passwords, to appear as someone they are not. | The attacker captures data packets, messages, or authentication tokens and replays them, often to trick a system into performing an action it shouldn't. |
| Masquerade involves impersonation. | Replay focuses on reusing captured data. |
| Masquerade attacks may involve altering data | Replay attacks don't modify data; they simply repeat it. |
| **Example**  Suppose you have a company’s intranet portal that allows employees to access sensitive company data. An attacker gains access to an employee’s login credentials (e.g., username and password) through techniques like phishing. They then use these stolen credentials to log in to the portal as the legitimate employee, giving them unauthorized access to company resources. | **Example**  Consider a scenario where a user logs into their online banking account. During the login process, the system generates a unique authentication token, which is sent to the user's device. An attacker intercepts this token while in transit. Later, the attacker replays this token to the bank's server to gain access to the user's account without having the actual login credentials**.** |

You need to **convert** your name (i.e., plain-text) into a cipher-text with the following ciphers:

