LAB Manual

PART A

(PART A : TO BE REFFERED BY STUDENTS)

**Experiment No.02**

**A.1 Aim:**

To implement active and passive attacks / Threats using socket programming

**A.2 Prerequisite:**

Fundamentals of socket programming.

**A.3 Outcome:**

**After successful completion of this experiment students will be able to** 1. Learn the socket programming

2. Understand active and passive attacks /threats.

**A.4 Theory:**

**Active attacks:** An Active attack attempts to alter system resources or affect their operations. Active attacks involve some modification of the data stream or the creation of false statements. Types of active attacks are as follows:

* Masquerade
* Modification of messages
* Repudiation
* Replay
* Denial of Service

**Passive attacks:** A Passive attack attempts to learn or make use of information from the system but does not affect system resources. Passive Attacks are in the nature of eavesdropping on or monitoring transmission. The goal of the opponent is to obtain information that is being transmitted. Types of Passive attacks are as follows:

* The release of message content
* Traffic analysis

PART B

(PART B : TO BE COMPLETED BY STUDENTS)

***(Students must submit the soft copy as per following segments within two hours of the practical. The soft copy must be uploaded on the Blackboard or emailed to the concerned lab in charge faculties at the end of the practical in case the there is no Black board access available)***

|  |  |
| --- | --- |
| Roll. No. C023 | Name: Nilay Gaitonde |
| Class: B | Batch: B1 |
| Date of Experiment: 31-08-2022 | Date of Submission: 31-08-2022 |
| Grade: | |

**B.1 Software Code written by student:**

[Simple interception attack](https://github.com/NilayGaitonde/SS-Practicals/tree/master/Exp2/exp2a)

[cipher.py](https://github.com/NilayGaitonde/SS-Practicals/blob/a934026e36778819d659adf11903ce60d576fa92/Exp2/exp2a/ciphers.py)

[client.py](https://github.com/NilayGaitonde/SS-Practicals/blob/a934026e36778819d659adf11903ce60d576fa92/Exp2/exp2a/client.py)

[server.py](https://github.com/NilayGaitonde/SS-Practicals/blob/a934026e36778819d659adf11903ce60d576fa92/Exp2/exp2a/server.py)

[interceptor.py](https://github.com/NilayGaitonde/SS-Practicals/blob/a934026e36778819d659adf11903ce60d576fa92/Exp2/exp2a/interceptor.py)

[Modification attack](https://github.com/NilayGaitonde/SS-Practicals/tree/master/Exp2/exp2b)

[cipher.py](https://github.com/NilayGaitonde/SS-Practicals/blob/a934026e36778819d659adf11903ce60d576fa92/Exp2/exp2b/ciphers.py)

[client.py](https://github.com/NilayGaitonde/SS-Practicals/blob/a934026e36778819d659adf11903ce60d576fa92/Exp2/exp2b/client.py)

[server.py](https://github.com/NilayGaitonde/SS-Practicals/blob/a934026e36778819d659adf11903ce60d576fa92/Exp2/exp2b/server.py)

[interceptor.py](https://github.com/NilayGaitonde/SS-Practicals/blob/a934026e36778819d659adf11903ce60d576fa92/Exp2/exp2b/interceptor.py)

**B.2 Input and Output:**

**plaintext:** Hello world

**ciphertext:** Lsvi$pps\_p{h

**Interceptor attack**

A screenshot of a computer

Description automatically generated with medium confidence

**Modification Attack**

A screenshot of a computer

Description automatically generated with low confidence

**B.3 Observations and learning:**

***Learnt interception and modification of data***

**B.4 Conclusion:**

*Ceaser cipher is a string cipher that focuses on substitution*

*Transposition cipher is a string cipher that focuses on confusion*