Notes of :- Information AND Network Security

* Introduction :-

→ Security is defined as "Protecting information System from unauthorized access"

→ Network Security measures are needed to Protect data during their transmission. It guarantee that data transmission are authentic.

* Security Attacks :-

Network Security attacks fall into two categories.

```
                          Attacks
            ┌───────────────────┴───────────────────┐
      Passive Attacks                          Active Attacks
      ┌──────────┴──────────┐        ┌──────┬──────┬──────────┬──────┐
 Release of        Traffic      Masquerade  Replay   Modification  Denial
 message           Analysis                           of            Service
 content                                               message
                                                       content
```

1 <u>Passive Attacks</u> :- A Passive attack attempts
— — — — — — — — to learn or make
use of information from the
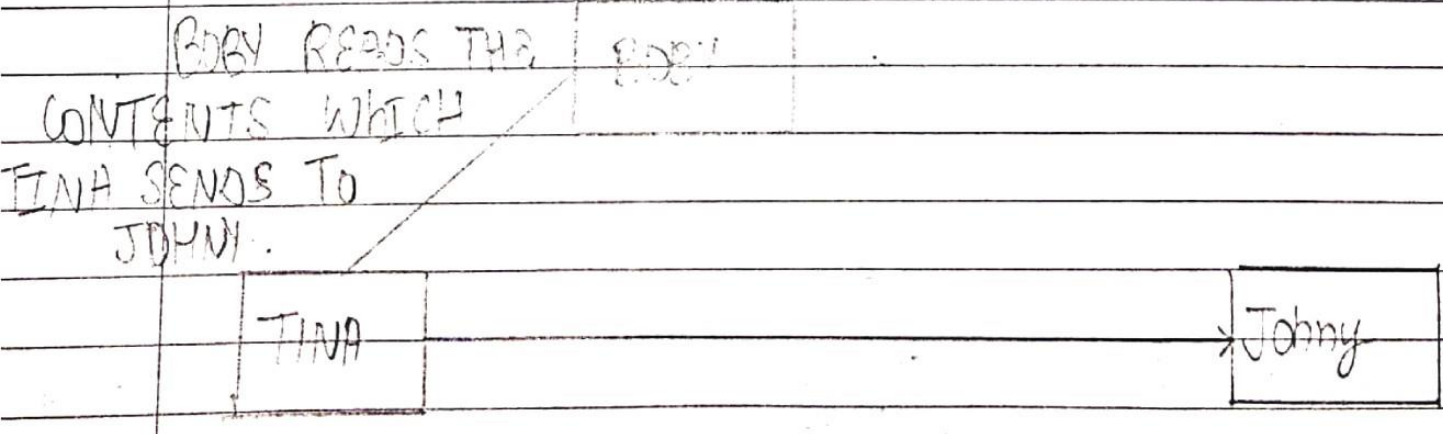system but does not affect system
resource.

Types of Passive Attacks are as following :-

(i) <u>Release of message content :-</u>

→ The attacker / Hacker will easily be able to
understand the data or information.

→ for example :- Telephonic conversation, an
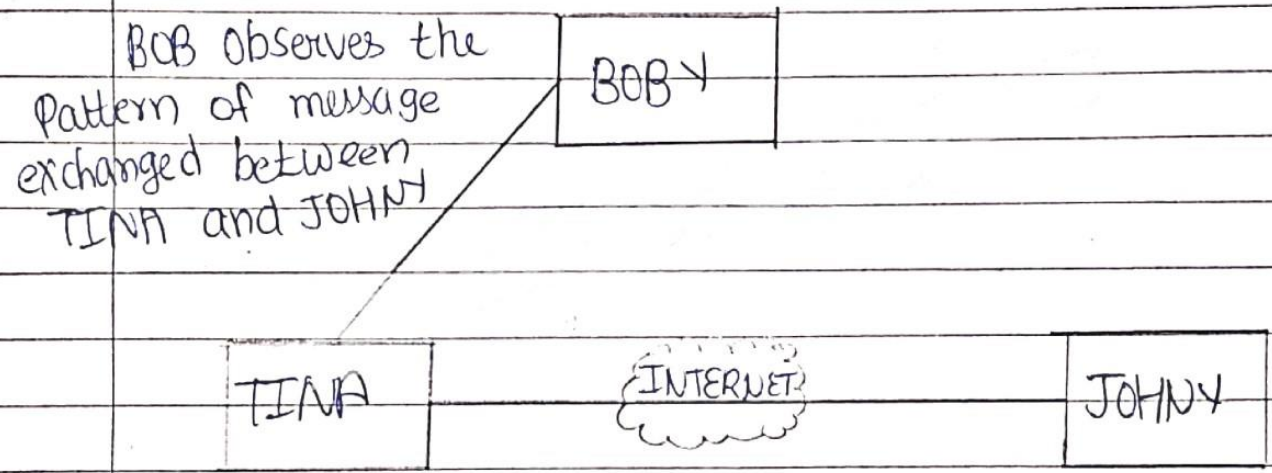email message or a transferred
file may contain senstive information.
→ we would like to prevent an
opponent from learning the contents
of these transmission.

BOBY READS THE | BOBY
CONTENTS WHICH
TINA SENDS TO
JOHN.

| TINA | →Johny |

(ii) Traffic analysis.

→ It is kind of attack done on encrypted message.

→ If we have encryption Protection, an attacke might be able to observe the Pattern of such encrypted message.

BOB observes the Pattern of message exchanged between TINA and JOHNY

```
                    ┌─────────┐
                    │  BOBY   │
                    └─────────┘
                       /
                      /
┌─────────┐        ⌒⌒⌒⌒⌒        ┌─────────┐
│  TINA   │────────(INTERNET)───────│  JOHNY  │
└─────────┘        ⌒⌒⌒⌒⌒        └─────────┘
```
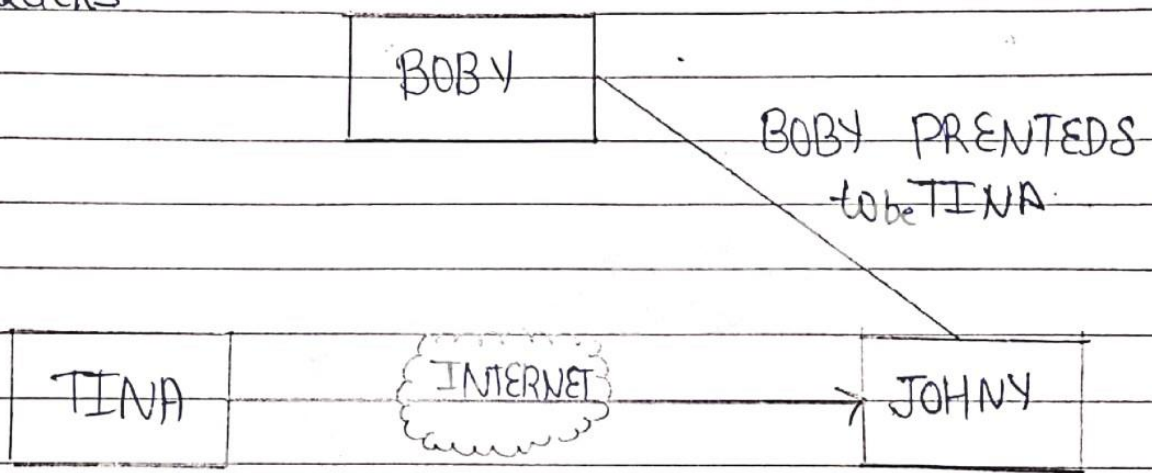
2 Active Threats (Attacks) :-

→ It involve some modification of the data stream.

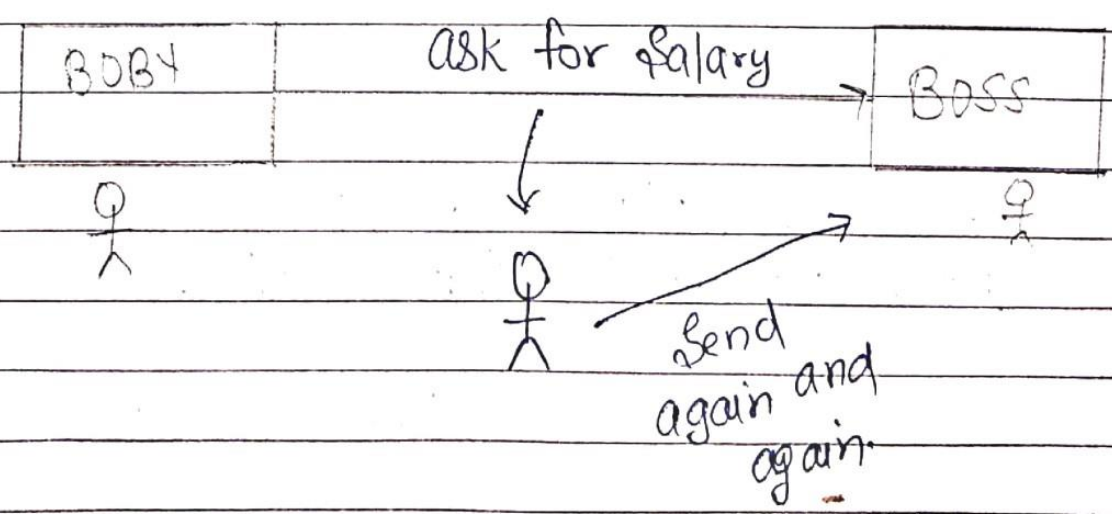→ It attempts to alter the system Resources and information.

(Types of Active Attacks are as following:

(i) **Masquerade:-** When one entity Ben Pretends to be another entity.

→ A masquerade attack usually includes one of the other forms of active attacks.

BOBY

BOBY PRENTEDS to be TINA

TINA — INTERNET → JOHNY

(ii) **Replay:-** It involves the Passive capture of a data unit and its subsequent retransmission to Produce an unauthorized effect.

BOBY   ask for Salary → BOSS

Send again and again.

(III) Modification of message :-

→ It means that some position of the message is altered, or the message is delayed or reordered, to Produce an unauthorized effect.

for example :- (i) Give 100 Rs. to JOHNY
↓
Give 500 Rs to LILY.

(II) A message meaning " ALLOW JOHNY to read file X
↓
is modified as :- "ALLOW LILY to read file Y".

(III) Denial of Service (DOS).

→ It Prevents normal use of Communication facilities.

→ This attack may have a specific target.
for example :- An entity may supress all messages directed to the Particular destination.

```
        ┌────────┐
        │ BOB'S  │ ────────┐   overload the Server
        │        │          \   by giving false
        └────────┘           \      request
┌──────┐      ⌢⌢⌢⌢        \  ┌────────┐ ┌──────┐
│ TINA │ ───( INTERNET )───────→│ JOHNY  │ │ Serve│
└──────┘      ⌣⌣⌣⌣           └────────┘ └──────┘
```

STUDYBYNOTES