SNS COLLEGE OF ENGINEERING

Kurumbapalayam(Po), Coimbatore – 641 107

An Autonomous Institution

Accredited by NAAC-UGC with 'A' Grade

Approved by AICTE, Recognized by UGC & Affiliated to Anna University, Chennai

DEPARTMENT OF INFORMATION TECHNOLOGY

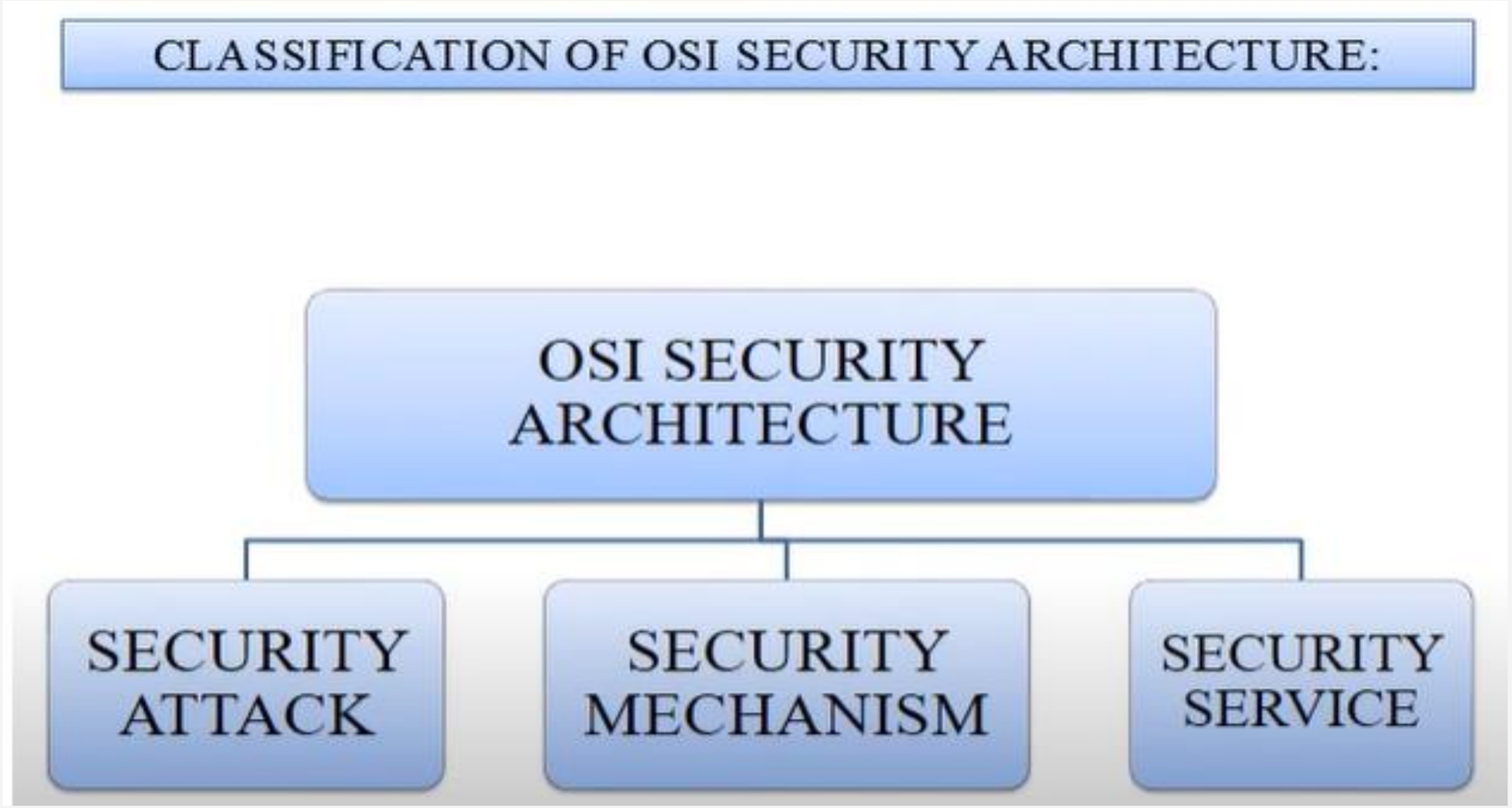
Course Code and Name : 19IT602– CRYPTOGRAPHY AND CYBER SECURITY

III YEAR / VI SEMESTER

Unit 1: INTRODUCTION TO NETWORK AND CYBER SECURITY

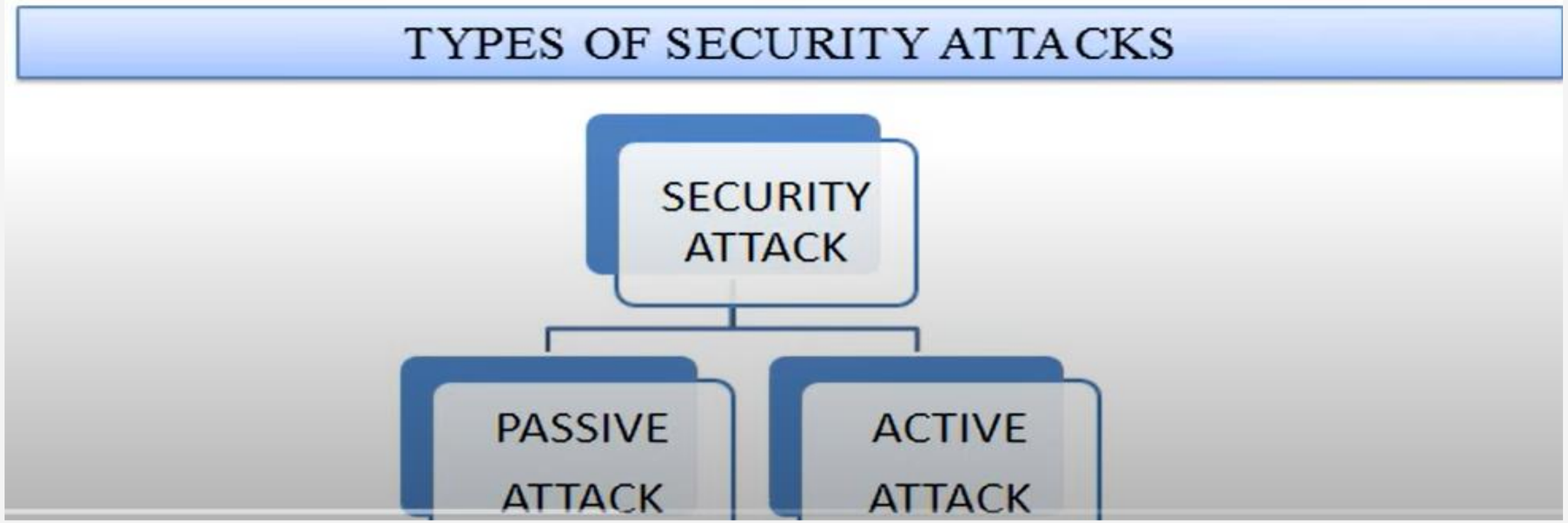
Topic 1: Security Attacks, Services and Mechanisms

Security Attacks, Services and Mechanisms



Security Attacks

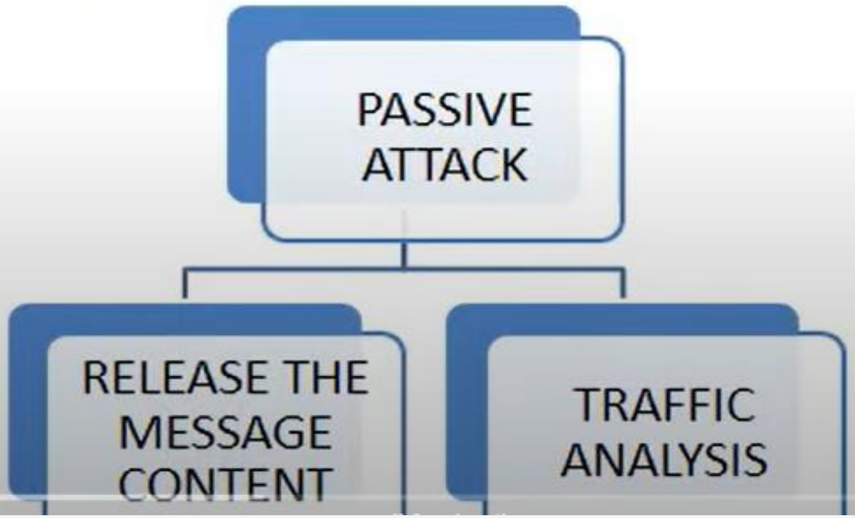
- SECURITY ATTACK IS A PROCESS OF GAINING AN ACCESS OF DATA BY UNAUTHORIZED USER
  i. ACCESSING THE DATA
  ii. MODIFYING THE DATA
  iii. DESTROYING THE DATA



- IN PASSIVE ATTACK NO DATA MODIFICATION WILL BE DONE

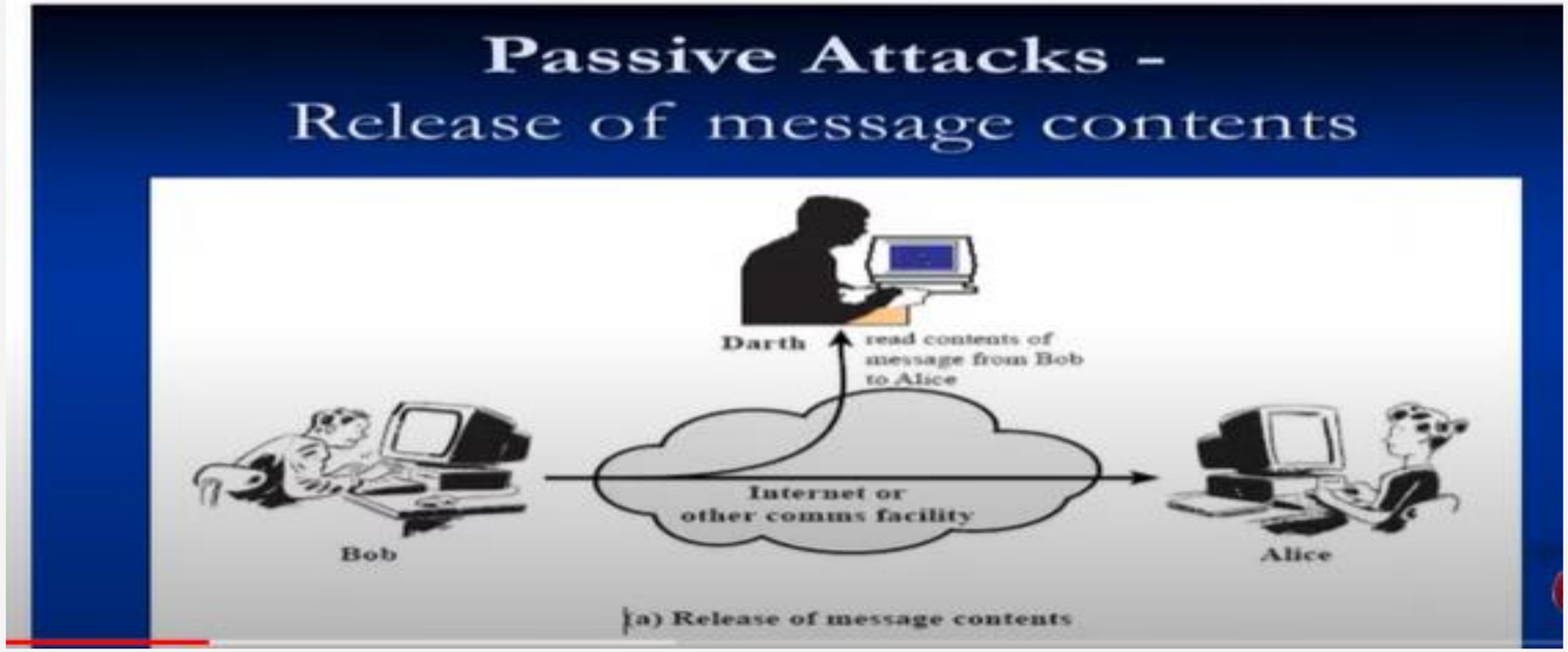
TYPES OF PASSIVE ATTACK

a. RELEASE THE MESSAGE CONTENT
b. TRAFFIC ANALYSIS



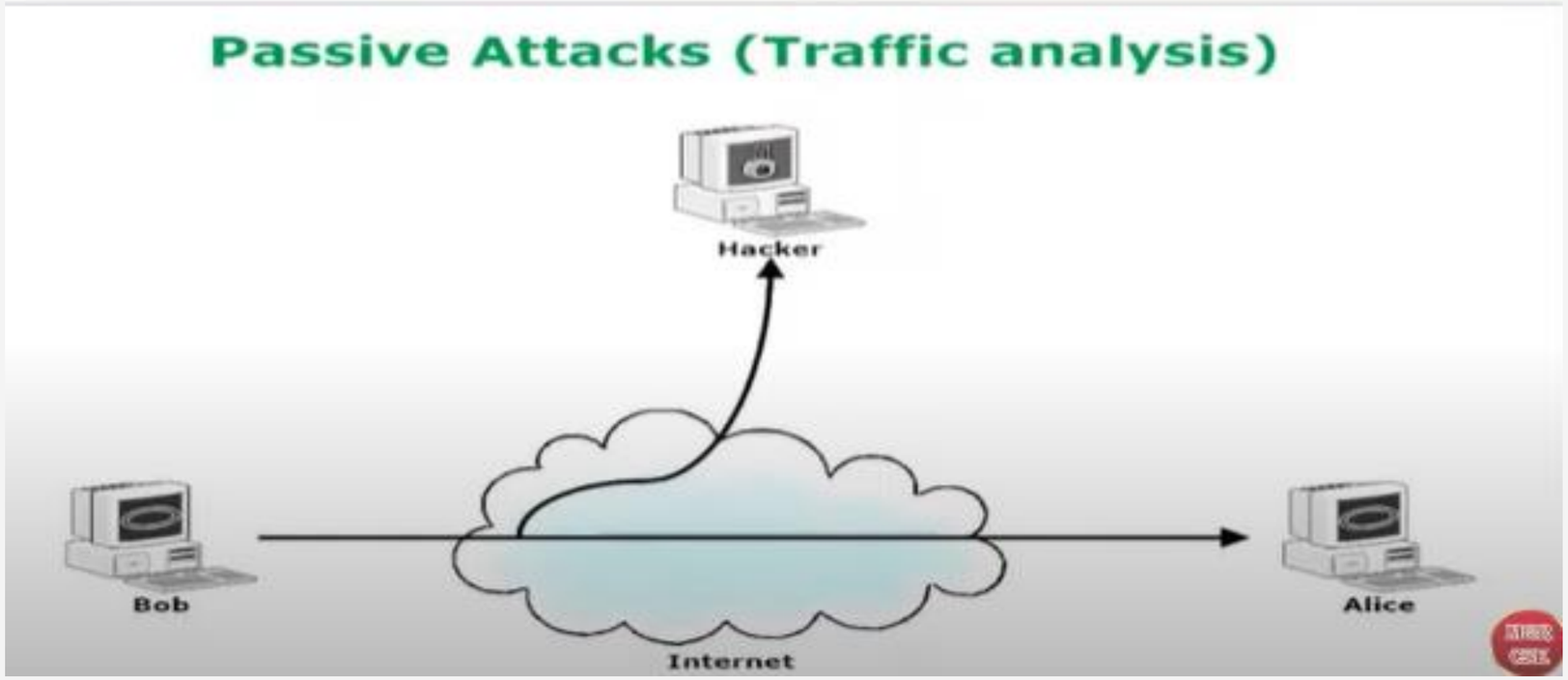
a. RELEASE THE MESSAGE CONTENT

- THIRD PARTY ONLY ACCESS THE DATA



b) TRAFFIC ANALYSIS

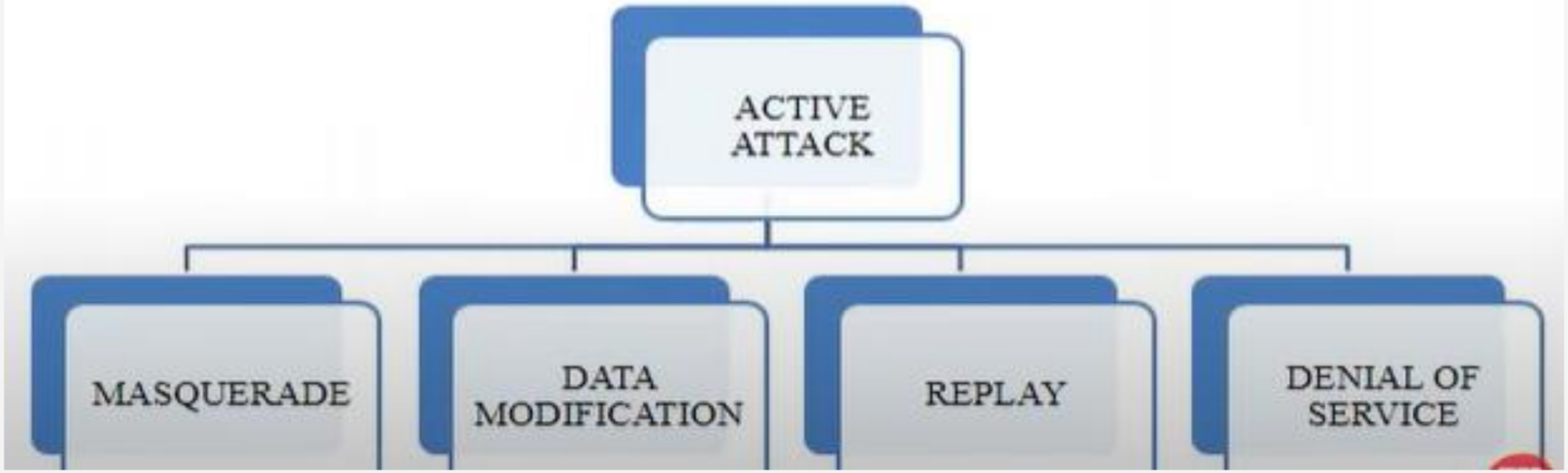
- ANALYSIS THE TRAFFIC & MODIFIES THE DATA THAT HAS TO BE USED



B) ACTIVE ATTACK

- IN ACTIVE ATTACK,DATA MODIFICATION WILL BE DONE

TYPES OF ACTIVE ATTACK

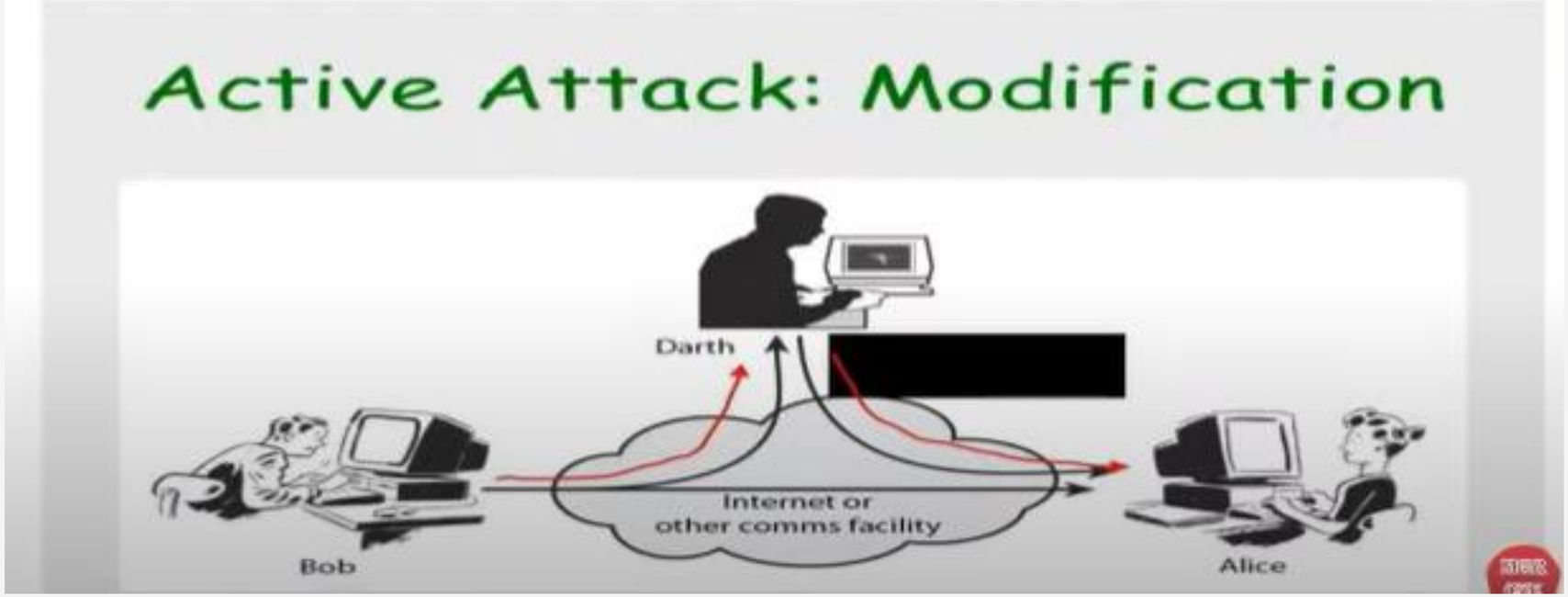


a. MASQUERADE

- SENDER SENDS THE MESSAGE TO THE RECEIVER,BUT THE THIRD PARTY(UNAUTHORIZED USER) ACCESS THE DATA & MODIFIES THE DATA AND SENDS TO THE RECEIVER IN THE NAME OF THE SENDER

b) DATA MODIFICATION

- THIRD PARTY ACCESS THE DATA THAT IS SENT BY THE SENDER TO THE RECEIVER,THIRD PARTY MODIFIES THAT DATA & SENDS TO THE RECEIVER

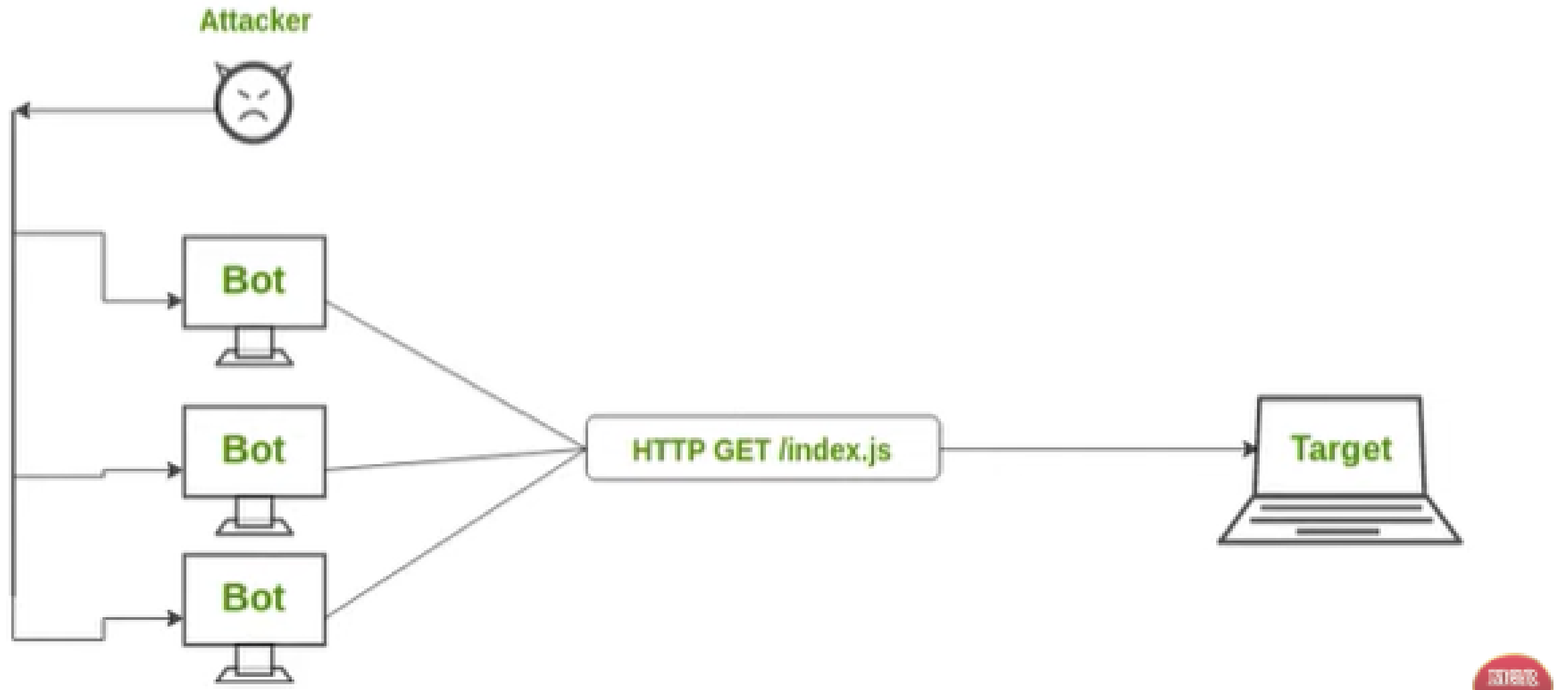


c) REPLAY

- RECEIVER RECEIVES THE DATA TWICE
- SENDER SENDS THE MESSAGE TO THE RECEIVER AS WELL AS THE THIRD PARTY WILL ACCESS THE MESSAGE AND MODIFICATION WILL BE DONE THEN THE THIRD PARTY SENDS TO THE RECEIVER.
- HOWEVER THE RECEIVER DOESN'T KNOW THE ORIGINAL MESSAGE

d) DENIAL OF SERVICE

➢ THIRD PARTY INTERUPTS THE SERVICE THAT IS SENT BY THE SERVER



References

- William Stallings, Cryptography and Network Security: Principles and Practice, PHI 3rd Edition, 2006.
- Behrouz A. Foruzan, Cryptography and Network Security, Tata McGraw Hill 2007.