SNS COLLEGE OF ENGINEERING

Kurumbapalayam (Po), Coimbatore – 641 107

An Autonomous Institution

Accredited by NBA – AICTE and Accredited by NAAC – UGC with 'A' Grade
Approved by AICTE, New Delhi & Affiliated to Anna University, Chennai

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING-IOT Including CS&BCT

COURSE NAME : 19SB402 NETWORKING AND CYBERSECURITY

II YEAR / IV SEMESTER

Unit III- Network Threats

Topic : Active and Passive Network Threats

Network Security

- Network security is the **deployment and monitoring** of **cyber security** solutions to protect organization's IT systems from attacks.

- It also **covers** policies surrounding the handling of **sensitive information**.

Network security involves the following solutions:

- Network segmentation
- Data loss prevention (DLP)
- Firewalls
- Intrusion prevention systems (IPS)

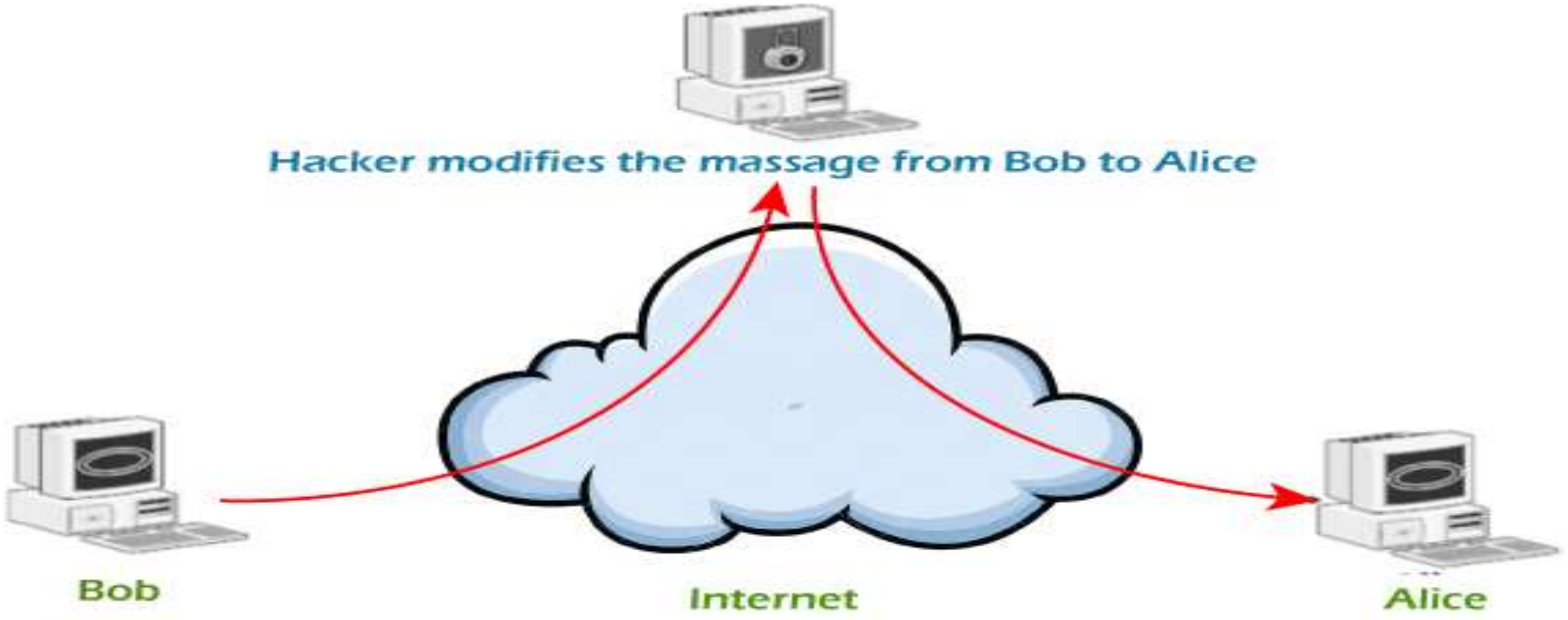
ACTIVE AND PASSIVE NETWORK THREATS

ACTIVE NETWORK THREATS

- An active attack is a **danger to the integrity(original data)** and **availability of the data**.
- Data integrity is the assurance that **digital information is uncorrupted** and can only be accessed or modified by those authorized to do so.
- The purpose behind active attacks is to **harm the system** or the organization.
- An **active attack** is a type of security attack in which the attacker **intercepts** the network connection and tries to alter the content of the message.
- Active attacks may change the system resources.

- The common actions involved in an active attack are masquerade, denial of service, change of the message's content, repudiation, replay, etc.
- They are harmful for both system and its resources.
- Note that, in case of active attacks, **the victim is notified about the attack.**
- There are some techniques that we can practice to prevent the active attacks such as use one−time password (OTP), generation of random session key, etc.

EXAMPLE OF ACTIVE NETWORK THREATS

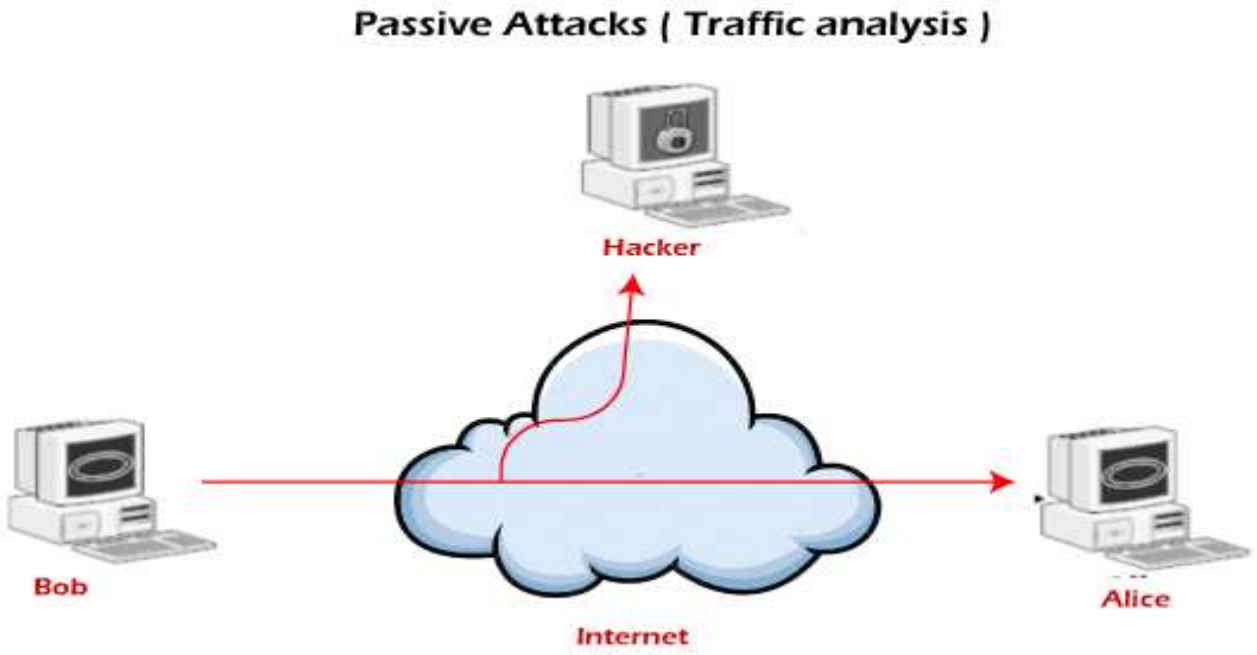


Active Attacks (Modifications of messages)

PASSIVE NETWORK THREATS

- Passive attack is a **danger to the confidentiality** of the data.
- Passive attacks **aim to learn about the system or the organization.**
- In passive attacks, the attacker **observes the messages**, then **copy and save** them and can use it for malicious purposes.
- The attacker does not try to change the information or content he/she gathered.
- Passive attacks do not harm the system, they can be a danger for the confidentiality of the message.

EXAMPLE OF PASSIVE NETWORK THREATS



- Unlike active attacks, in passive attacks, **victims do not get informed about the attack.**

- It is **difficult to detect** as there is **no alteration in the message**.

- Passive attacks can be **prevented by using some encryption techniques**.

We can try the below-listed measures to prevent these attacks

- We should avoid posting sensitive information or personal information online. Attackers can use this information to hack your network.

- We should use the encryption method for the messages and make the messages unreadable for any unintended intruder.

DIFFERENCE BETWEEN ACTIVE AND PASSIVE ATTACK

Key	Active Attack	Passive Attack
Modification	In Active Attack, information is modified.	In Passive Attack, information remain unchanged.
Dangerous For	Active Attack is dangerous for Integrity as well as Availability.	Passive Attack is dangerous for Confidentiality.
Attention	Attention is to be paid on detection.	Attention is to be paid on prevention.

DIFFERENCE BETWEEN ACTIVE AND PASIVE ATTACK

Key	Active Attack	Passive Attack
Impact on System	An Active Attack can damage the system.	A Passive Attack does not have any impact on the regular functioning of a system.
Victim	The victim gets informed in an active attack.	The victim does not get informed in a passive attack.
System Resources	System Resources can be changed in active attack.	System Resources are not changed in passive attack.

Any Query????

Thank you……