**DAY 16**

**Sniffing:**

Sniffing is the process of capturing and monitoring the data packets passing through the network using sniffers

Sniffing is used to perform diagnostics and typically used for observing the network traffic to troubleshoot the network issues.

**Promiscuous mode:**

Promiscuous mode is a mode where the NIC card will receive and respond to the data packets which are not intended for it.

Once the sniffing is successful the attacker can perform attacks such as:

1. Session hijacking

2. DOS attack

3. Man in The Middle attack

Information that gets captured by the attacker:

1. Usernames/Passwords

2.Credit/Debit card details

3.Chats

4.Data packets

Sniffing tools:

Like Wireshark, Ettercap(performs active sniffing)

**Types of sniffing:**

1. Passive sniffing

🡪The attacker **doesn’t** send any malicious data packets to the targeted device in order to capture the data packets

EX. Bus topology, Hub networks

2. Active sniffing

🡪The attacker sends malicious data packets to the targeted device in order to capture the data packets

EX. Switch, Router

Wireshark:

Display filters:

1.protocols (http, ftp, etc.)

2. ip.addr==192.168.10.130

In Wireshark, the protocol for https is tls (Transport layer security)

By active sniffing sniffing the attacker can perform:

1. Session hijacking

2. MITM attack

3. Capturing packets

Counter measures against active sniffing:

1. Use https

2. sftp instead of ftp

3. using advanced steganography

4. Use switch/router instead of hub

5. Use sniffing detection tools