**DAY 18**

Few types of attacks the hacker can perform after successful sniffing are:

1. Session hijacking

2. DOS (Denial of Service)

3. Password stealing

4. Bypass the firewall/IDS/IPS

**1. Session hijacking**

A session is an identifier for a user who is authorized from login to logout in any service where a service can be a website, a system, a server, a database

Session ID/Token: will be stored in the web browser

Session hijacking is a process where the user’s session id is taken over by the attacker.

Few reasons for session hijacking:

1. Predictable session ID

2. Session sniffing

3. Client-side attacks (XSS, trojans, malicious JS codes)

4. MITM attack

5. Man in the browser attack

1. Predictable session ID:

User1 --> session1

User2 --> session2

2. Session sniffing:

By performing network sniffing the hacker can capture and gain the valid user’s session ID and this happens if the data packets are not having encrypted data

3. Client-side attacks

4. MITM attack

5. Man in the browser attack

Session ID is stored in the cookie of the website in the user’s browser

**Bypassing the firewalls/IDS/IPS:**

The most common technique the hackers use to bypass these would by using cryptographical techniques for their exploits/malwares/payloads

Honeypots:

Honeypots are traps for hackers where the honeypots are fake replica of the internal network.

Different types of honeypots:

1. High interaction honeypots

2. Medium interaction honeypots

3. Low interaction honeypots

* gray-world.net 🡪vulnerable website
* HoneyBOT software