CYBERSECURITY TRAINING
(WEEK 2 - Day3)

1.1 Introduction to **DoS and DDoS Attacks**

- What is DoS Attack?

  A **Denial of Service (DoS)** attack is a **malicious attempt** to disrupt the normal functioning of a server, service, or network by **overwhelming it with a flood of internet traffic**. The goal is to **make the system unavailable** to legitimate users.

- What is a DDoS Attack?

  A **Distributed Denial of Service (DDoS)** attack is a **type of DoS attack** where the **traffic comes from**

multiple sources, often thousands of infected computers (called a **botnet**). This makes the attack **harder to block** and more damaging.

- Key Difference:

  DoS = one system attacking
  DDoS = many systems attacking simultaneously

1.2 Common DoS Attack techniques

ICMP Flood (Ping Flood)

- Sends large numbers of **ICMP** Echo Request (ping) packets to the target system.

- **Goal**: Exhaust the network bandwidth and processing resources.

- **Impact**: System becomes too busy responding to pings, unable to serve real users.

- **Tools used**: `ping -f` (Linux), or custom scripts.

SYN Flood

- Exploits the TCP three-way handshake process.
- Impact: Server’s connection table gets full → no new legitimate connections.

- Defense: SYN cookies, increasing backlog queue, firewalls.