Day 150

Topic: DoS & DDoS Attacks

Objective: To understand Denial of Service attacks and stress testing.

Theoretical Concepts:
We defined DoS (one attacker, one target) vs DDoS (Distributed attackers). We discussed Volume-based attacks (UDP floods), Protocol attacks (SYN floods), and Application Layer attacks (HTTP floods).

Practical Work:
We used **hping3** to simulate a SYN Flood attack on our lab test server. Command: *hping3 -S --flood -V -p 80 [Target IP]*. We observed the CPU usage on the target server spike to 100% and the web service become unresponsive. We also discussed mitigation strategies like rate limiting and Blackholing.

Tools Used: hping3, Metasploit.

Outcome: Understood the mechanics of flooding attacks and the impact on service availability.