DATE: 7 JULY 2025 **DAY: MONDAY**

DAY 12 — Timing Side-Channel Attack Theory

LEARNING OBJECTIVES:-

- Study timing side-channel concepts.
- Learn how attackers measure computation delays.

Overview:-

Day 12 introduced the theoretical concept of timing attacks. The session explained how attackers exploit response time variations in password comparison functions.

Activites:-

- Reviewed research on early-exit string comparisons.
- Analyzed ESP32 login logic for timing weaknesses.

Insights:-

- Learned how tiny delays leak sensitive information.
- Understood how insecure code reveals password patterns.