📌 Team Jailbreak Capability Breakdown

This document summarizes the strategic strengths of each member of the infrastructure jailbreak team based on their assigned papers and mapped attack surfaces. Despite assigning papers based on length, the resulting distribution turned out to be highly effective, forming a complete attack triangle across system, behavioral, and application-level exploits.

☑ Team Papers and Attack Types

Person	Papers	Covered Tactic
You	Paper 4, 17, 19	✅ Prompt-level control (persuasion, triggers) + behavioral drift
Simo	Paper 6, 8, 18	✅ Multi-turn escalation (GOAT, Crescendo) + sleeper backdoors
Leo	Paper 1, 5, 20	✅ Prompt injection (HOUYI), multilingual filter evasion, data poisoning

🧠 Tactical Breakdown

• You: Perfect for anything that touches system prompts or alignment leaks.

• Simo: Perfect for gradual behavior corruption, refusal suppression, or stealth override.

• Leo: Perfect for web-style prompt injection, app-layer hacks, and language-based evasion.

Together you form:

- • One **system breaker** (you)
- • One **mind bender** (Simo)
- • One **API infiltrator** (Leo)