LUXCORE.RED – Auto-Red Team Assistant

Codename: GIDEON – Guided Interactive Deception and Offensive Networker  
Type: LLM-Autonomous Red Team Assistant (Live-Agent Simulative System)  
Domain: Cyber Offense Automation | Recon | Exploitation | Payload Delivery | AI-Driven Deception

# Core Architecture Overview

A modular framework leveraging LLM for decision making across seven offensive phases:

|  |  |  |
| --- | --- | --- |
| Module | Description | LLM Role |
| Phase 1: Target Intelligence Collection | Harvest assets, subdomains, emails, breaches | Guide footprinting logic, generate dorks, pivot queries |
| Phase 2: Recon & Enumeration Engine | Map ports, services, and hosts | Analyze results, recommend priority targets |
| Phase 3: Exploitation Decision Tree | Match exploits from CVE/ExploitDB | Select tools, build payloads dynamically |
| Phase 4: Payload Customization | Auto-generate shellcode, bypasses | Obfuscate payloads, adjust for AV/EDR evasion |
| Phase 5: Initial Access Simulation | Phishing, zero-click, misconfigs | Draft spearphishing emails, create impersonation scripts |
| Phase 6: Post-Exploitation Automation | Lateral movement, data exfil | Suggest persistence, identify privilege paths |
| Phase 7: Reporting/Logging | Generate Red Team report in PDF/HTML | Summarize TTPs, link MITRE ATT&CK steps |