LUXCORE.RED – Auto-Red Team Assistant

# Introduction

LUXCORE.RED is an LLM-controlled autonomous red teaming framework that blends adversarial AI, zero-click vectors, and real-time deception for advanced red team operations. The system leverages modular plug-ins to simulate highly complex and stealthy attack chains.

# Architecture Overview

LUXCORE.RED consists of the following core components:  
- Auto-Recon Module (OSINT & behavioral mapping)  
- Payload Generator (polymorphic + AI-enhanced)  
- Custom Protocol Abuse Engine  
- EDR/XDR Evasion Modules  
- Adversarial AI Injection Layer  
- Logging & TTP Playback Engine  
- Command & Control Framework (Covert C2)

# Code Snippet Example – LLM Payload Generator

Below is a Python snippet that shows how LUXCORE.RED may dynamically generate a phishing payload using OpenAI API:

import openai  
  
'  
 'def generate\_payload(prompt):  
'  
 ' response = openai.ChatCompletion.create(  
'  
 ' model="gpt-4",  
'  
 ' messages=[{"role": "system", "content": "You are a red team assistant"},  
'  
 ' {"role": "user", "content": prompt}]  
'  
 ' )  
'  
 ' return response.choices[0].message["content"]  
  
'  
 'payload = generate\_payload("Create a realistic spear-phishing email targeting CFO")  
'  
 'print(payload)

# Core Modules

1. Auto-Recon:  
Performs OSINT, analyzes targets’ online behavior, social graph, device metadata.

2. Payload Generator:  
Generates polymorphic payloads with prompt-engineered instructions via LLMs.

3. Protocol Abuse Engine:  
Simulates attacks via x-callback-urls, AirDrop, calendar injection, vCard exploits.

4. EDR/XDR Evasion:  
Encrypts payloads, randomizes syscall patterns, avoids memory signatures.

5. Adversarial Injection:  
Injects adversarial prompts or noise into LLMs, voice interfaces, and dashboards.

6. Covert C2:  
Uses DNS tunneling, EXIF steganography, Bluetooth LE beacons for low-detection persistence.

# Conclusion

LUXCORE.RED introduces a new paradigm in offensive security—where intelligent agents guide complex attack paths, simulate advanced threat actors, and automate cognitive intrusion. It empowers Red Team units with cutting-edge tools to stress-test modern environments in a controlled and repeatable way.