Project: LUXCORE.RED

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 Codebase for GIDEON Framework

## main.py

import os  
from gideon.modules.recon import start\_recon  
from gideon.modules.exploit import trigger\_exploit  
from gideon.modules.deception import initiate\_deception  
  
def main():  
 print("[+] Initiating GIDEON Offensive Framework")  
 start\_recon()  
 trigger\_exploit()  
 initiate\_deception()  
  
if \_\_name\_\_ == '\_\_main\_\_':  
 main()

## recon.py

def start\_recon():  
 print("[\*] Starting Reconnaissance Phase")  
 # Insert OSINT, port scanning, subdomain enumeration logic here  
 return True

## exploit.py

def trigger\_exploit():  
 print("[\*] Executing Exploitation Chain")  
 # Example: CVE chaining, custom payload generation  
 return True

## deception.py

def initiate\_deception():  
 print("[\*] Deploying AI-Driven Deception Layer")  
 # AI impersonation, false flags, telemetry manipulation  
 return True