Automatic Pentesting Framework Workflow

Complete Process Flow from Initialization to Reporting **START** User Input (Target, Options, Mode) Configuration Check (API Keys, Tools, Paths) Mode Selection? Manual **Autonomous** Legend: Chatbot Traditional CLI Pentesting PentestGPT Natural Language Al-Driven Autonomous Testing Start/End **User Input** Decision Reconnaissance Scanning
PHASE 1: RECONNAISSANCE Exploitation AI/ML Target Classification (Web, Network, Mixed) Reporting Process OSINT Gathering (theHarvester) Port Scanning (Nmap, SYN) **DNS Enumeration Shodan Search** (Amass, DNS) (Passive Recon) Service Analysis (Identify Running Services) **Workflow Notes:** • Autonomous mode uses AI for decision-making • All phases can be run independently • Self-healing recovers from errors Custom Checks (Scripts) Continuous learning improves love itime (Templates) Nikto (Web Server) SQLMap (SQL Injection) API Testing (REST/GraphQL) Exploit Prioritization (CVSS, Impact Analysis) Exploitable Vulns Found? No Document Findings (No Critical Vulns) Payload Generation (Metasploit, Custom) PHASE 3: EXPLOITATION & PAYLOAD GENERATION Reverse Shells Exploitation Attempt (Safe Mode) **Post-Exploitation** (Evidence Collection) AI/ML ENHANCEMENT (Optional) Continuous **Self-Healing** Pattern Threat **Prediction** Learning System Recognition PHASE 4: REPORTING & DOCUMENTATION Report Generation (HTML, MD, JSON, PDF) Evidence Files Executive Summary Technical Details Remediation Steps Risk Assessment