In you start with mcp
https://medium.com/ai-cloud-lab/model-context-protocol-mcp-with-ollama-a-full-deep-dive-working-code-part-1-81a3bb6d16b3

Google gemini Ai Automation
https://github.com/SlanyCukr/bugbounty-mcp-server

bug bounty enviroment with mcp server
https://github.com/gokulapap/bugbounty-mcp-server

resources repo for mcp server
https://github.com/punkpeye/awesome-mcp-servers

mcp for kali liunx
https://github.com/Wh0am123/MCP-Kali-Server

pentest
https://github.com/ramkansal/pentestMCP
https://github.com/ibrahimsaleem/PentestThinkingMCP

We propose a three-part automation workflow:
(1) scrape and AI-analyze public endpoints into Google Docs for fast triage,
(2) run Droid Sentinel static scans and use AI to find exploit chains and validate impact,
(3) run a personal “Hunt” pipeline to continuously enumerate subdomains, CNAMEs, and cloud misconfigs. Combined, these reduce manual effort, prioritize high-impact findings, and create an auditable pipeline from discovery to report-ready evidence.

https://github.com/FancybearIN/hunt

https://github.com/ch3tanbug/DroidSentinel #appsec_static_Analyse

``