Gemini-Powered OSINT Recon Bot

# One-liner

An AI-powered reconnaissance tool that automates open-source intelligence gathering and summarizes threat data using Google Gemini.

# Core Features

• Domain & IP Recon: Pulls data from crt.sh, whois, Shodan, VirusTotal, and Hunter.io.

• AI Summary: Uses Gemini Pro or Gemini 1.5 to analyze and summarize reconnaissance results.

• Visual Intelligence: Gemini Vision analyzes screenshots, leaked pages, or logos for brand spoofing.

• Report Generation: Creates a structured threat intel PDF or DOCX report.

• Chat Interface: Chatbot frontend using Gemini API for interactive querying.

• Entity Extraction: Extracts IOCs, email IDs, server info, and organization names from unstructured input.

# Tech Stack

• APIs: Gemini 1.5 Pro + Gemini Vision via Google AI Studio

• Data Sources: crt.sh, whois, Shodan, Hunter.io, Archive.org, etc.

• LLM: Gemini API via Vertex AI or Google AI Studio

• Backend: Python (FastAPI/Flask) or Node.js

• Frontend: React/Next.js + Tailwind

• Report: WeasyPrint / PDFKit / Pandoc for export

• DB (Optional): SQLite or Firebase for storing reports

# OSINT Recon Modules

• SSL Certificate Info: crt.sh, Censys

• Email Discovery: Hunter.io, Google dorking

• Subdomain Enum: crt.sh, Sublist3r

• Shodan Lookup: Shodan API

• Whois + GeoIP: WhoisXML API, IPinfo

• Archive Analysis: Archive.org snapshots

• AI Insight: Gemini summarizes each module’s output

# Example Use Case Flow

🎯 Target: example.com

1. User inputs target domain or IP

2. Bot fetches data from OSINT sources

3. Gemini summarizes: Infrastructure, exposure, leaked data, indicators

4. Optional: Upload phishing screenshot for Gemini Vision analysis

5. Generate a full PDF report

6. User interacts with chatbot (e.g., 'What ports were found open on the host?')

# Bonus Add-ons

• Scheduled Scans (daily/weekly)

• Telegram/Slack bot notifications

• CVE Matching via NVD + Gemini summary

• “Explain this IOC” feature

• Gemini translation for global content

# Real-World Value

• Cybersecurity Firms: Automates recon and report writing

• Bug Bounty Hunters: Saves time during target recon

• Threat Intel Analysts: Quick visual + text summary

• SOC Teams: Faster triage of potential threats

# Example Prompt for Gemini

You are a cybersecurity analyst. Analyze the following OSINT data and summarize:  
  
1. Risky domains or subdomains  
  
2. Possible leaked emails or credentials  
  
3. Any misconfigured services or ports  
  
4. Suggested next steps  
  
[PASTE RAW OSINT JSON HERE]

# How to Present It (for Job Hunting)

• Deploy it live on Firebase or Vercel

• Record a 2-min demo video showing real-world use

• Write a blog: 'How I Built an OSINT Bot with Gemini & Google AI'

• Open-source with README, screenshots, and clear instructions