

PhantomSweep

A fast, lightweight and scalable network security scanner

Thành viên nhóm

Hà Sơn Bin (23520149), Lê Quốc Khôi (23520769),
Võ Quốc Bảo (23520146), Nguyễn Đoàn Gia Khánh (23520720)

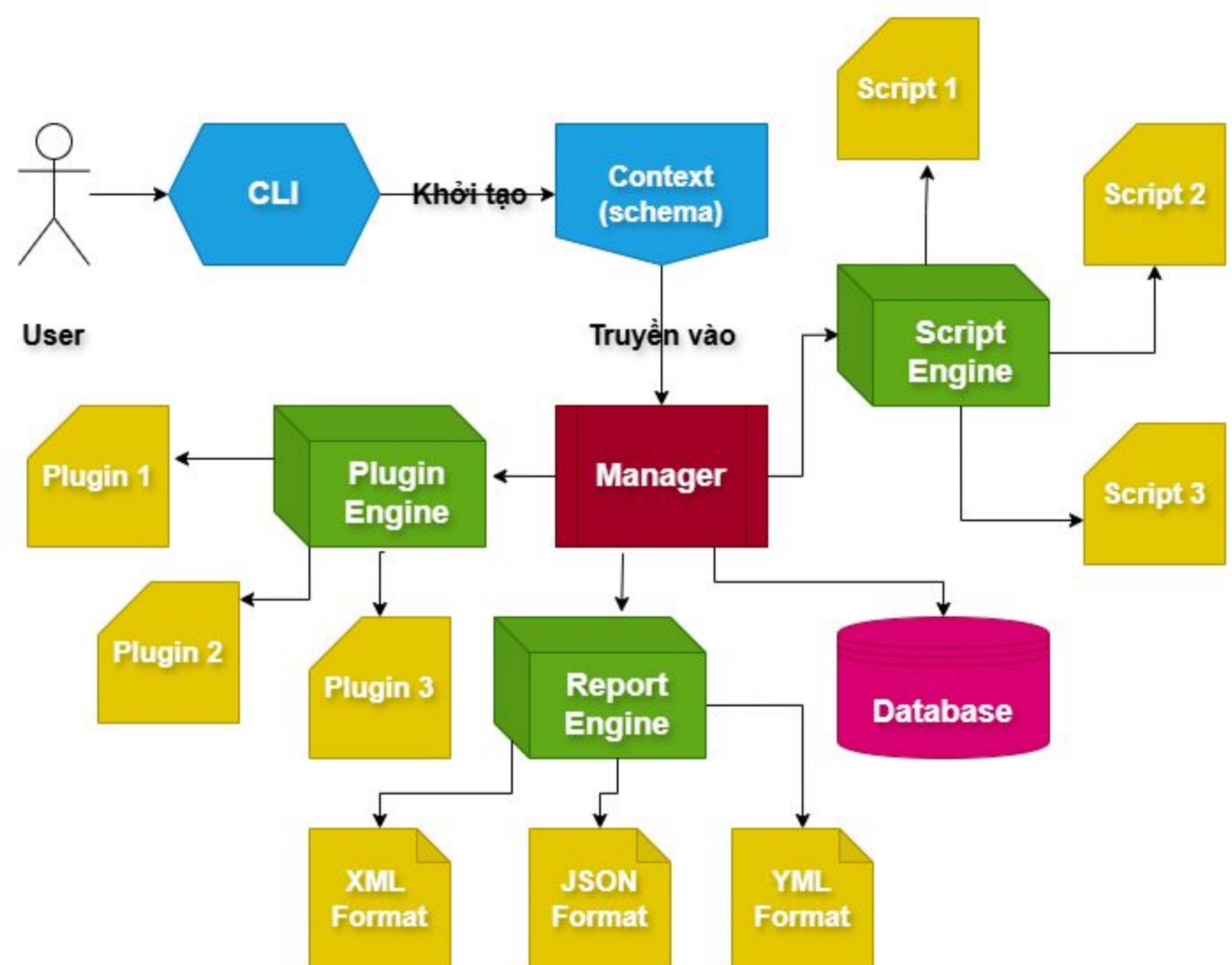
Introduction

In an era of growing service-level threats, validating network defenses is crucial. PhantomSweep is a compact port scanner that uses deterministic heuristics and a curated signature database to map exposed services. Instead of noisy brute-force sweeps, it prioritizes well-known ports with protocol fingerprints, adjusts probe timing to lower detectability, and records concise host behavior. The result: a practical, extensible tool that finds misconfigurations and generates clear, actionable reports for hardening.

Methodology

Five phase pipelines:

1. **Host discovery:** combine ARP (LAN), ICMP Echo/Timestamp, TCP SYN/ACK ping, and UDP probes
2. **Port scanning:** prefer **TCP SYN (half-open)** for speed and stealth; fall back to **TCP Connect** when raw sockets aren't available; add **UDP scan** (DNS/SNMP payloads) and **FIN scan** for SYN-filtered environments.
3. **Service & version detection:** start with banner grabbing; if uncertain, switch to **probe-and-match** against a signature set (regex + known ports/sslports + rarity) to infer service/version.
4. **OS fingerprinting:** send TCP/UDP/ICMP probes, extract TTL, window size, TCP options, DF, etc., then match against a fingerprint database
5. **Reporting:** aggregate results (host → ports → services → OS) to concise text/JSON



Experiments and Results

Environments:

- Controlled lab LAN (low noise, admin access).
- Authorized WAN targets (self-hosted VPS/VMs) with varied firewalls.

Experiment Setup:

Targets (VMs/containers):

- Linux (Ubuntu/Debian), Windows Server, FreeBSD/*BSD.
- Services enabled: SSH(22), HTTP/HTTPS(80/443), DNS(53/UDP), SNMP(161/UDP), MySQL(3306), RDP(3389), SMB(445).
- Ensure **≥1 open & ≥1 closed port** per host.

Scenarios

- S1.** Port-State Accuracy (TCP/UDP)
- S2.** Service & Version Identification
- S3.** OS Fingerprinting Robustness
- S4.** Throughput & Resource Usage
- S5.** Stealth/Detectability (IDS/IPS)
- S6.** Scalability & Stability

Conclusion

Current Limitations:

- **UDP scanning ambiguity** (open|filtered), sensitive to timeouts and ICMP rate limiting.
- **OS fingerprinting** accuracy drops with packet loss or NAT.
- **Raw-packet privileges** required for SYN/UDP/FIN on many systems; cross-platform support needs broader testing.
- **Signature DB maintenance** (new services/OS) is continuous work.

Future Work

- **Richer fingerprinting:** add HTTP/JA3/TLS, SSH-kex, DHCP/mDNS
- **Automated reporting:** export JSON/CSV and hardening templates;
- **Positioning:** stay **fast, compact, low-noise**, aimed at misconfiguration detection
- **Distributed scanning:** multi-agent + controller architecture for large ranges with centralized congestion control.
- **LLM Integration:** AI helps in automatically summarize scan result, also a Natural Language Interface Query