NEMESIS
by Autogon Inc.

NEMESIS

Continuous proof your defenses hold.

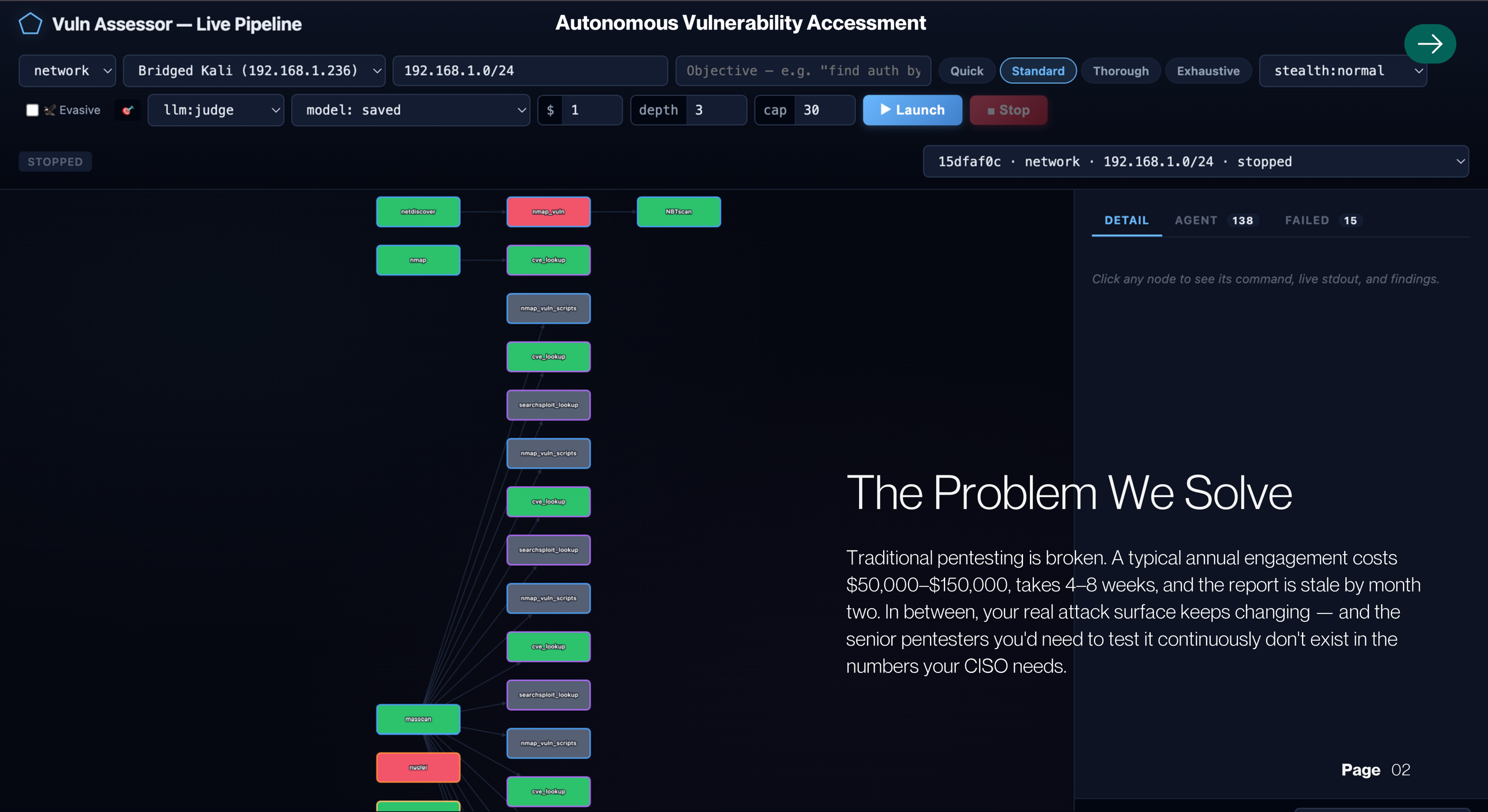
The attacker's nemesis — inevitable, inescapable.

Website
https://nemesislabs.xyz

Private and confidential

Built In

Dayton, OH · USA



The Problem We Solve

Traditional pentesting is broken. A typical annual engagement costs $50,000–$150,000, takes 4–8 weeks, and the report is stale by month two. In between, your real attack surface keeps changing — and the senior pentesters you'd need to test it continuously don't exist in the numbers your CISO needs.

What's Broken in Today's Market

01.

Annual Pentests Go Stale

A pentest report is a photograph of one moment. By month two, deployments, configs, and dependencies have shifted enough that the findings no longer describe your real risk.

02.

You Can't Hire Enough Seniors

ISC² puts the global cybersecurity workforce shortage at 3.4M. Senior pentesters cost $200K+ loaded and are usually already booked. Continuous testing with humans is a non-starter.

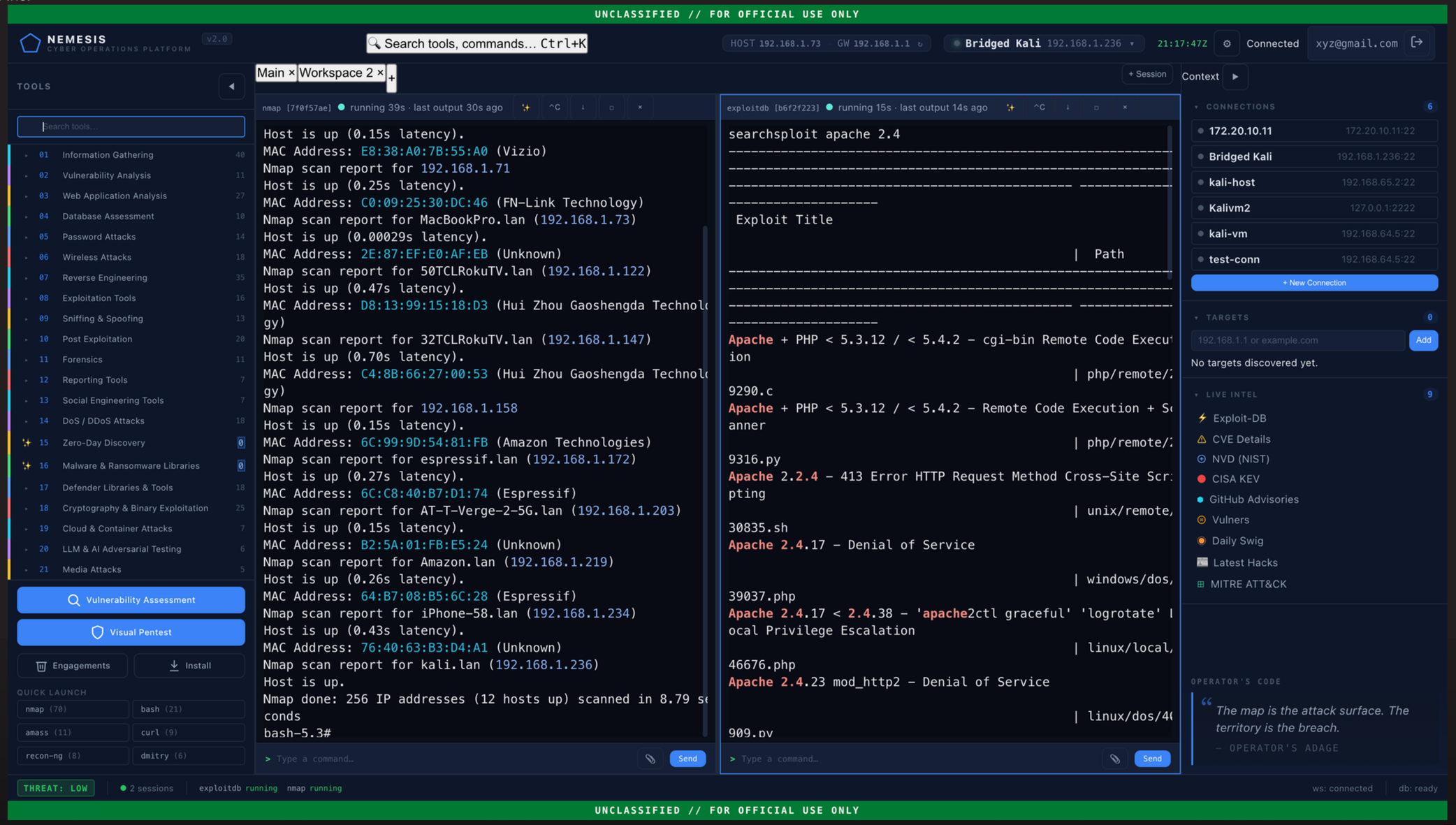
03.

Scanners Miss Chained Findings

Industry data: ~73% of breach chains require connecting evidence across more than two tools. Fixed-script scanners produce noise; they can't reason across the chain a real attacker would walk.

NEMESIS
by Autogon Inc.

290 Kali tools. Multi-tile terminals. One dashboard.



Our Solution, Reimagined

Closed-loop autonomy

Nemesis plans, executes, and replans across 290 real Kali tools through one reasoning loop — recon to report, with every step's output feeding the next decision.

Two modes from one engine

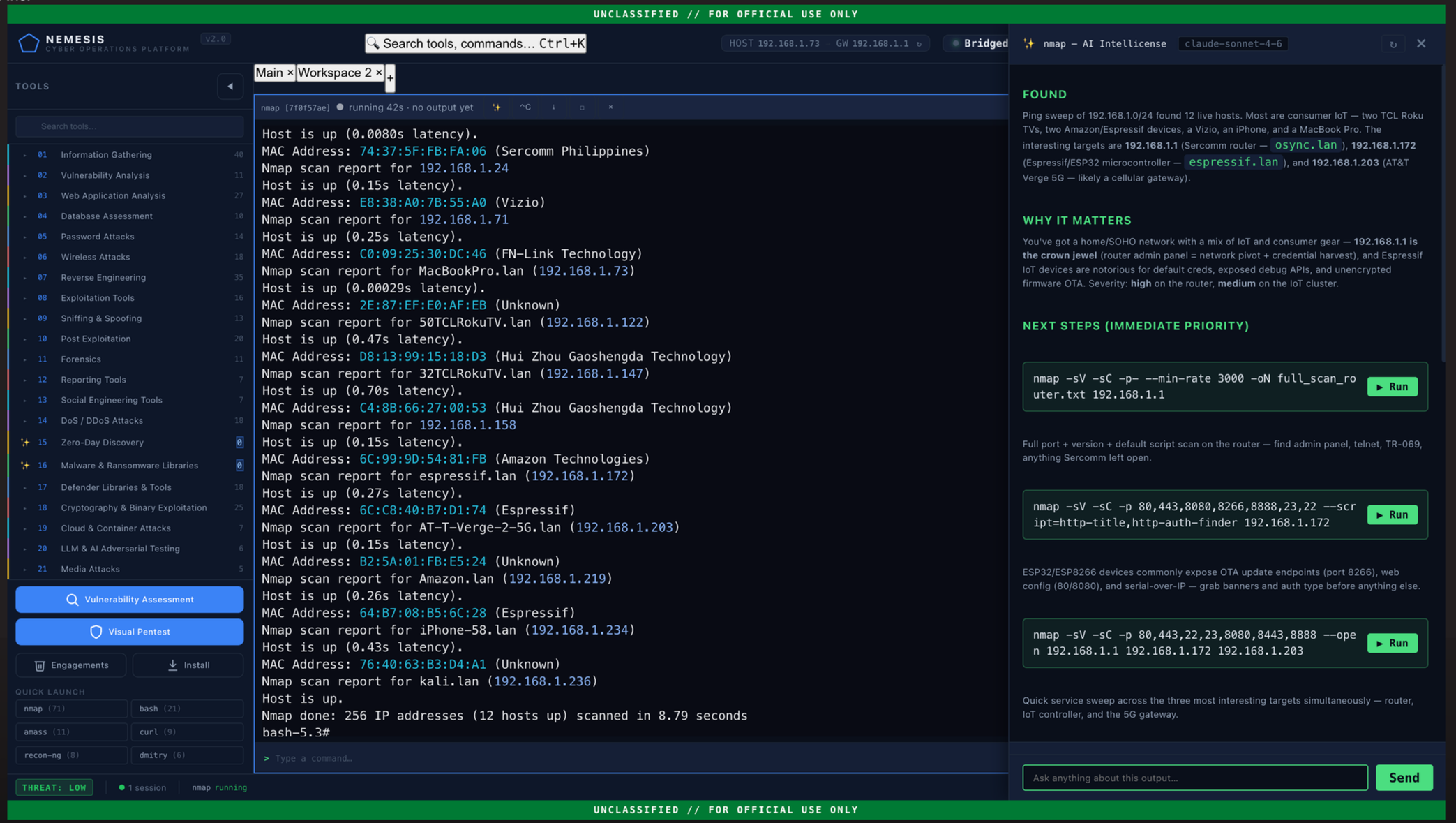
Auto Mode runs the whole engagement end-to-end. Co-Pilot Mode has a human operator drive, while the LLM hands them the next three commands with the target pre-filled.

Self-hosted. BYOK.

Nemesis runs on your infrastructure. Each pentester brings their own LLM key (Anthropic / OpenAI / Gemini). No data leaves your network. Hash chained audit log built in.

NEMESIS
by Autogon Inc.

Co-Pilot — Intellicense next-steps



NEMESIS
by Autogon Inc.

Key Benefits

Nemesis replaces three things at once: the annual pentest, the noisy continuous scanner, and the senior pentester you can't hire. Self-hosted, BYOK, auditable.

24.4× more findings

Closed-loop replanning, peer-reviewed against fixed-script scanners. p<0.001 over 120 controlled-study runs.

290 Kali tools

Cataloged across 17 active offensive categories. The LLM picks the right one per phase per target type.

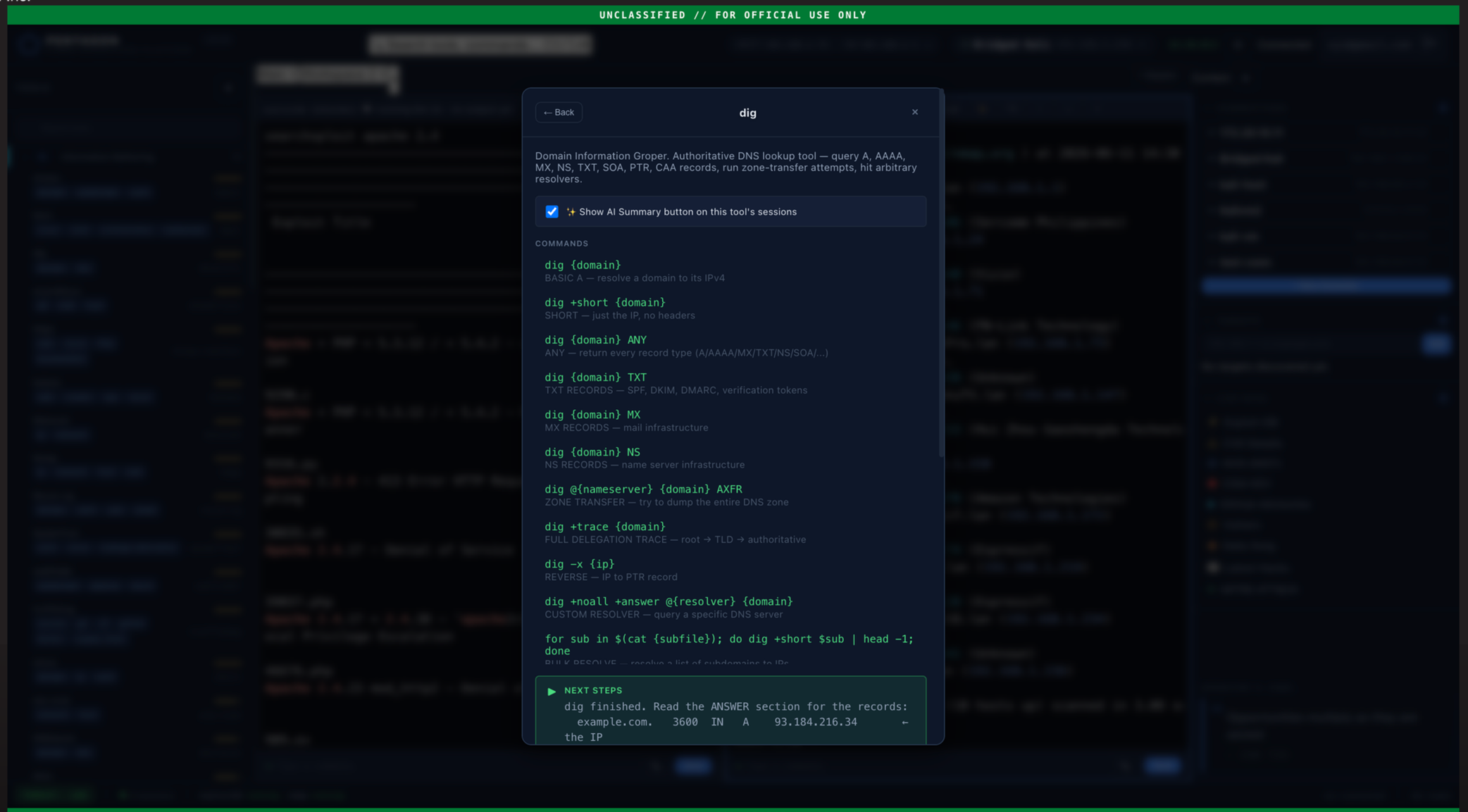
Junior → senior in one tool

Co-Pilot reads tool output, names the target, hands the operator the next three commands.

Stays on your network

Nemesis, the Kali host, the audit log — all yours. BYOK for each pentester. No SaaS upcharge.

Every tool ships with multiple attacker flavored commands



NEMESIS
by Autogon Inc.

The Proof

Real numbers from real runs. No marketing inflation.

24.4×

more findings than fixed-script automation

Controlled ablation study. 30 OWASP-class targets. 120 runs across full / no-replan / no-fusion / random-order conditions. Wilcoxon W=465, p<0.001.

DURING THE STUDY

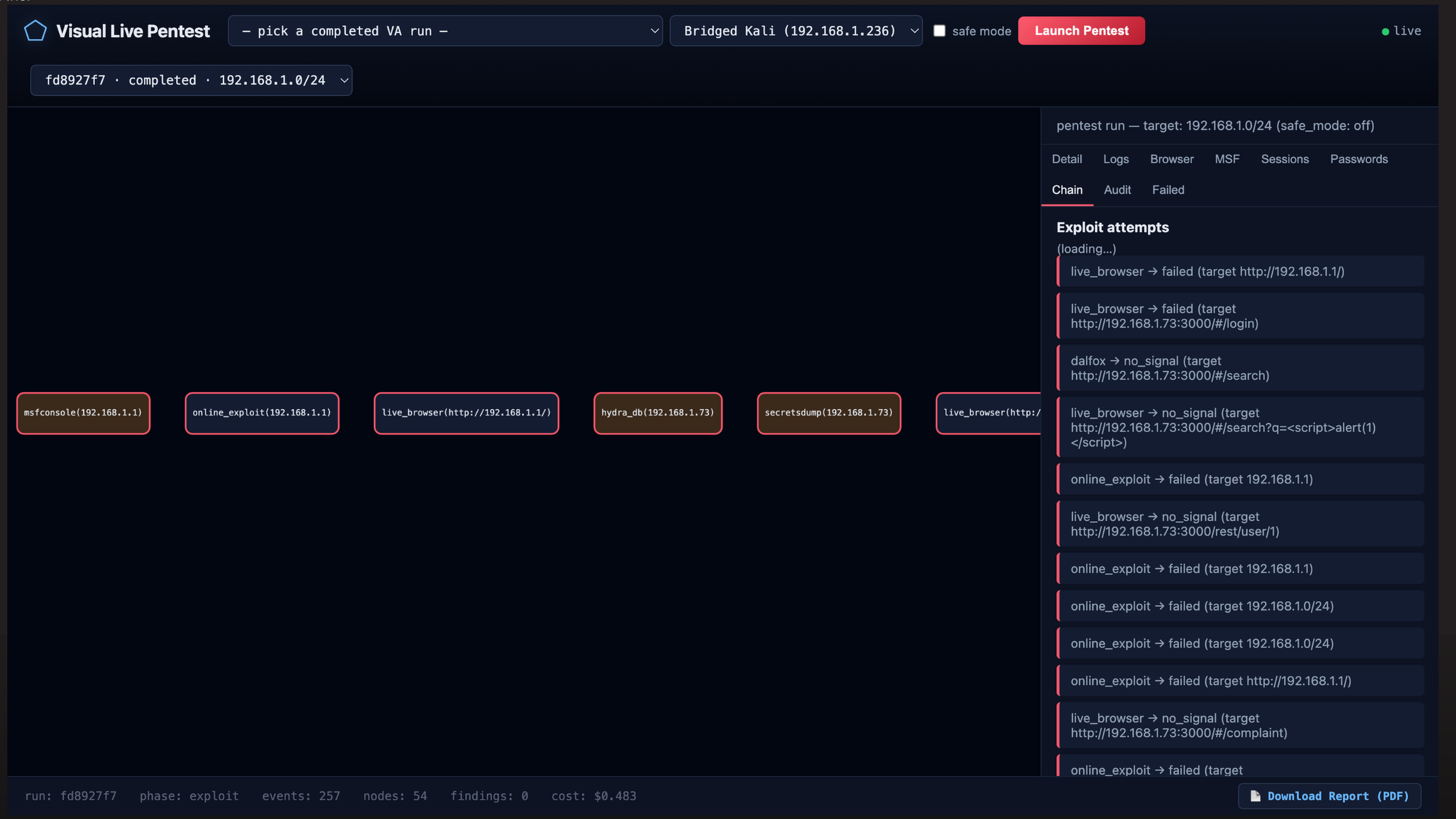
3 CVSS 9.8 CVEs

autonomously discovered

CVE-2024-38476 · Apache mod_rewrite SSRF
CVE-2024-38474 · Apache mod_rewrite substitution
CVE-2023-25690 · HTTP request smuggling

Surfaced by Nemesis's NSE invocations — no human steering.

Autonomous Pentest



NEMESIS
by Autogon Inc.

COMPETITION

Capability	NEMESIS	Nessus / Qualys	Pentera / Horizon3	PentestGPT-style
Closed-loop LLM reasoning	✓	✗	partial	✗
Executes (not just suggests)	✓	✓	✓	✗
Cross-tool intelligence fusion	✓	✗	✓	✗
290 Kali tools cataloged	✓	~80	varies	✗
Co-Pilot for human operators	✓	✗	✗	partial
Self-hosted, on-prem	✓	✓	✗	varies
BYOK per pentester	✓	✗	✗	varies
Hash-chained audit log	✓	✗	✗	✗
Cost transparency per engagement	✓	✓	✗	✗