



NEMESIS

Continuous proof your defenses hold.

The attacker's nemesis — inevitable, inescapable.

Website
<https://nemesislabs.xyz>

Private and confidential

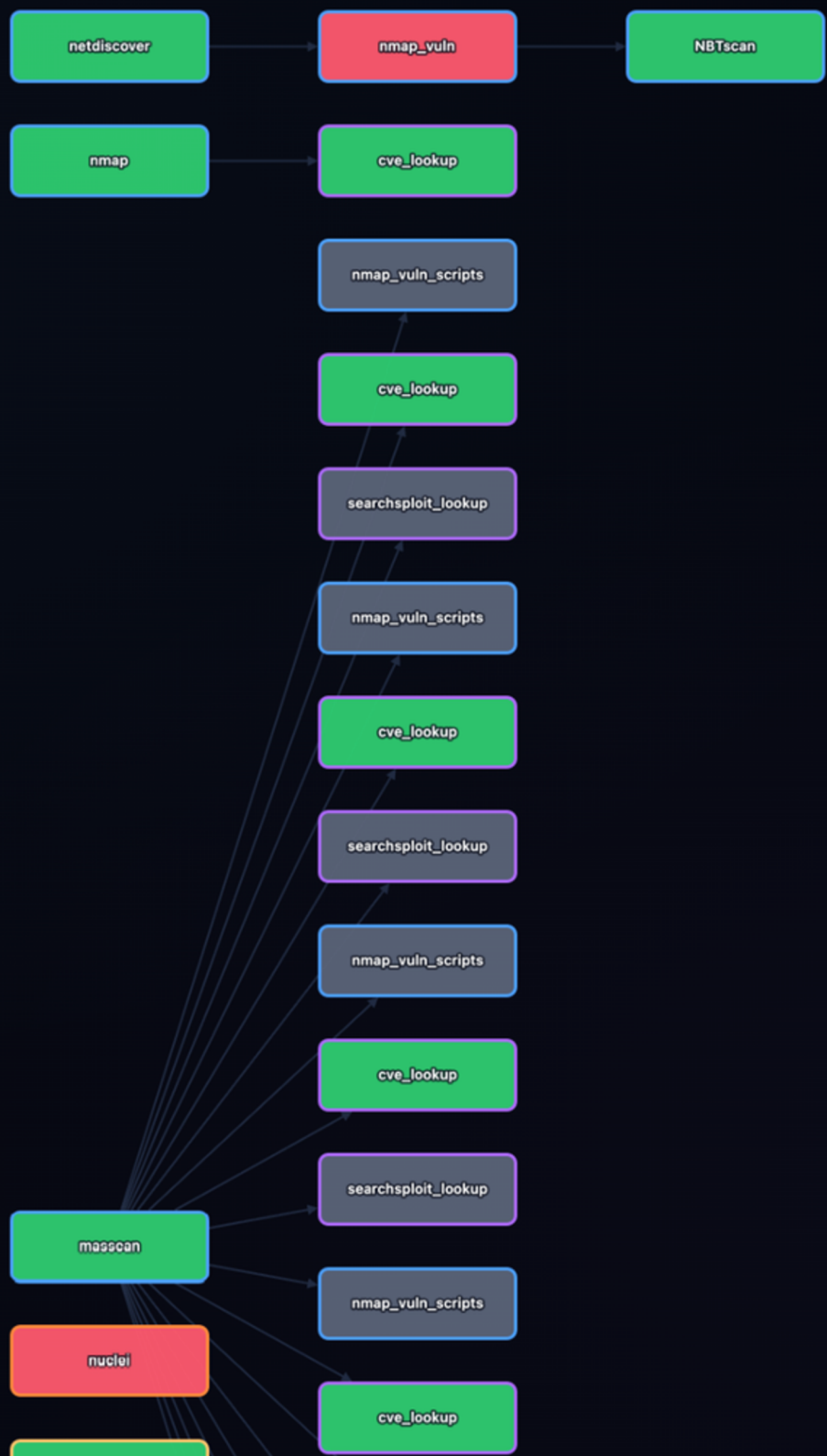
Built In
Dayton, OH · USA



network ▾ Bridged Kali (192.168.1.236) ▾ 192.168.1.0/24 Objective – e.g. "find auth by Quick Standard Thorough Exhaustive stealth:normal ▾

🚫 Evasive 🎯 llm:judge ▾ model: saved ▾ \$ 1 depth 3 cap 30 ▶ Launch ■ Stop

STOPPED 15dfaf0c · network · 192.168.1.0/24 · stopped ▾



DETAIL AGENT 138 FAILED 15

Click any node to see its command, live stdout, and findings.

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.



UNCLASSIFIED // FOR OFFICIAL USE ONLY

NEMESIS
CYBER OPERATIONS PLATFORM

v2.0

HOST 192.168.1.73
GW 192.168.1.1
Bridged Kali 192.168.1.236
21:17:47Z
Connected xyz@gmail.com

TOOLS

Search tools...

- 01 Information Gathering 40
- 02 Vulnerability Analysis 11
- 03 Web Application Analysis 27
- 04 Database Assessment 10
- 05 Password Attacks 14
- 06 Wireless Attacks 18
- 07 Reverse Engineering 35
- 08 Exploitation Tools 16
- 09 Sniffing & Spoofing 13
- 10 Post Exploitation 20
- 11 Forensics 11
- 12 Reporting Tools 7
- 13 Social Engineering Tools 7
- 14 DoS / DDoS Attacks 18
- 15 Zero-Day Discovery 0
- 16 Malware & Ransomware Libraries 0
- 17 Defender Libraries & Tools 18
- 18 Cryptography & Binary Exploitation 25
- 19 Cloud & Container Attacks 7
- 20 LLM & AI Adversarial Testing 6
- 21 Media Attacks 5

Vulnerability Assessment

Visual Pentest

Engagements

Install

QUICK LAUNCH

nmap (70)

bash (21)

amass (11)

curl (9)

recon-ng (8)

dmitry (6)

nmap [7f0f57ae] ● running 39s · last output 30s ago
exploitdb [b6f2f223] ● running 15s · last output 14s ago

```

Host is up (0.15s latency).
MAC Address: E8:38:A0:7B:55:A0 (Vizio)
Nmap scan report for 192.168.1.71
Host is up (0.25s latency).
MAC Address: C0:09:25:30:DC:46 (FN-Link Technology)
Nmap scan report for MacBookPro.lan (192.168.1.73)
Host is up (0.00029s latency).
MAC Address: 2E:87:EF:E0:AF:EB (Unknown)
Nmap scan report for 50TCLRokuTV.lan (192.168.1.122)
Host is up (0.47s latency).
MAC Address: D8:13:99:15:18:D3 (Hui Zhou Gaoshengda Technology)
Nmap scan report for 32TCLRokuTV.lan (192.168.1.147)
Host is up (0.70s latency).
MAC Address: C4:8B:66:27:00:53 (Hui Zhou Gaoshengda Technology)
Nmap scan report for 192.168.1.158
Host is up (0.15s latency).
MAC Address: 6C:99:9D:54:81:FB (Amazon Technologies)
Nmap scan report for espressif.lan (192.168.1.172)
Host is up (0.27s latency).
MAC Address: 6C:C8:40:B7:D1:74 (Espressif)
Nmap scan report for AT-T-Verge-2-5G.lan (192.168.1.203)
Host is up (0.15s latency).
MAC Address: B2:5A:01:FB:E5:24 (Unknown)
Nmap scan report for Amazon.lan (192.168.1.219)
Host is up (0.26s latency).
MAC Address: 64:B7:08:B5:6C:28 (Espressif)
Nmap scan report for iPhone-58.lan (192.168.1.234)
Host is up (0.43s latency).
MAC Address: 76:40:63:B3:D4:A1 (Unknown)
Nmap scan report for kali.lan (192.168.1.236)
Host is up.
Nmap done: 256 IP addresses (12 hosts up) scanned in 8.79 seconds
bash-5.3#
                    
```

```

searchsploit apache 2.4
-----
Exploit Title
| Path
-----
Apache + PHP < 5.3.12 / < 5.4.2 - cgi-bin Remote Code Execution
| php/remote/9290.c
Apache + PHP < 5.3.12 / < 5.4.2 - Remote Code Execution + Scanner
| php/remote/9316.py
Apache 2.2.4 - 413 Error HTTP Request Method Cross-Site Scripting
| unix/remote/30835.sh
Apache 2.4.17 - Denial of Service
| windows/dos/39037.php
Apache 2.4.17 < 2.4.38 - 'apache2ctl graceful' 'logrotate' Local Privilege Escalation
| linux/local/46676.php
Apache 2.4.23 mod_http2 - Denial of Service
| linux/dos/4909.nv
                    
```

CONNECTIONS 6

- 172.20.10.11 172.20.10.11:22
- Bridged Kali 192.168.1.236:22
- kali-host 192.168.65.2:22
- Kalivm2 127.0.0.1:2222
- kali-vm 192.168.64.5:22
- test-conn 192.168.64.5:22

+ New Connection

TARGETS 0

192.168.1.1 or example.com Add

No targets discovered yet.

LIVE INTEL 9

- ⚡ Exploit-DB
- ⚠ CVE Details
- 🕒 NVD (NIST)
- 🔴 CISA KEV
- 🔵 GitHub Advisories
- 🟡 Vulners
- 🟠 Daily Swig
- 📰 Latest Hacks
- 🗄 MITRE ATT&CK

OPERATOR'S CODE

“ The map is the attack surface. The territory is the breach. ”

— OPERATOR'S ADAGE

THREAT: LOW
● 2 sessions
exploitdb running
nmap running
ws: connected | db: ready

UNCLASSIFIED // FOR OFFICIAL USE ONLY

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.



UNCLASSIFIED // FOR OFFICIAL USE ONLY

Search tools, commands... Ctrl+K

HOST 192.168.1.73 GW 192.168.1.1

Bridged

nmap - AI Intellicense

TOOLS

Search tools...

- 01 Information Gathering 40
- 02 Vulnerability Analysis 11
- 03 Web Application Analysis 27
- 04 Database Assessment 10
- 05 Password Attacks 14
- 06 Wireless Attacks 18
- 07 Reverse Engineering 35
- 08 Exploitation Tools 16
- 09 Sniffing & Spoofing 13
- 10 Post Exploitation 20
- 11 Forensics 11
- 12 Reporting Tools 7
- 13 Social Engineering Tools 7
- 14 DoS / DDoS Attacks 18
- 15 Zero-Day Discovery 0
- 16 Malware & Ransomware Libraries 0
- 17 Defender Libraries & Tools 18
- 18 Cryptography & Binary Exploitation 25
- 19 Cloud & Container Attacks 7
- 20 LLM & AI Adversarial Testing 6
- 21 Media Attacks 5

Vulnerability Assessment

Visual Pentest

Engagements Install

QUICK LAUNCH

nmap (71)	bash (21)
amass (11)	curl (9)
recon-ng (8)	dmitry (6)

THREAT: LOW ● 1 session nmap_running

Main x Workspace 2 x +

nmap [7f0f57ae] ● running 42s · no output yet

```

Host is up (0.0080s latency).
MAC Address: 74:37:5F:FB:FA:06 (Sercomm Philippines)
Nmap scan report for 192.168.1.24
Host is up (0.15s latency).
MAC Address: E8:38:A0:7B:55:A0 (Vizio)
Nmap scan report for 192.168.1.71
Host is up (0.25s latency).
MAC Address: C0:09:25:30:DC:46 (FN-Link Technology)
Nmap scan report for MacBookPro.lan (192.168.1.73)
Host is up (0.00029s latency).
MAC Address: 2E:87:EF:E0:AF:EB (Unknown)
Nmap scan report for 50TCLRokuTV.lan (192.168.1.122)
Host is up (0.47s latency).
MAC Address: D8:13:99:15:18:D3 (Hui Zhou Gaoshengda Technology)
Nmap scan report for 32TCLRokuTV.lan (192.168.1.147)
Host is up (0.70s latency).
MAC Address: C4:8B:66:27:00:53 (Hui Zhou Gaoshengda Technology)
Nmap scan report for 192.168.1.158
Host is up (0.15s latency).
MAC Address: 6C:99:9D:54:81:FB (Amazon Technologies)
Nmap scan report for espressif.lan (192.168.1.172)
Host is up (0.27s latency).
MAC Address: 6C:C8:40:B7:D1:74 (Espressif)
Nmap scan report for AT-T-Verge-2-5G.lan (192.168.1.203)
Host is up (0.15s latency).
MAC Address: B2:5A:01:FB:E5:24 (Unknown)
Nmap scan report for Amazon.lan (192.168.1.219)
Host is up (0.26s latency).
MAC Address: 64:B7:08:B5:6C:28 (Espressif)
Nmap scan report for iPhone-58.lan (192.168.1.234)
Host is up (0.43s latency).
MAC Address: 76:40:63:B3:D4:A1 (Unknown)
Nmap scan report for kali.lan (192.168.1.236)
Host is up.
Nmap done: 256 IP addresses (12 hosts up) scanned in 8.79 seconds
bash-5.3#
                
```

> Type a command...

FOUND

Ping sweep of 192.168.1.0/24 found 12 live hosts. Most are consumer IoT — two TCL Roku TVs, two Amazon/Espressif devices, a Vizio, an iPhone, and a MacBook Pro. The interesting targets are 192.168.1.1 (Sercomm router — **osync.lan**), 192.168.1.172 (Espressif/ESP32 microcontroller — **espressif.lan**), and 192.168.1.203 (AT&T Verge 5G — likely a cellular gateway).

WHY IT MATTERS

You've got a home/SOHO network with a mix of IoT and consumer gear — 192.168.1.1 is the crown jewel (router admin panel = network pivot + credential harvest), and Espressif IoT devices are notorious for default creds, exposed debug APIs, and unencrypted firmware OTA. Severity: **high** on the router, **medium** on the IoT cluster.

NEXT STEPS (IMMEDIATE PRIORITY)

```
nmap -sV -sC -p- --min-rate 3000 -oN full_scan_router.txt 192.168.1.1
```

▶ Run

Full port + version + default script scan on the router — find admin panel, telnet, TR-069, anything Sercomm left open.

```
nmap -sV -sC -p 80,443,8080,8266,8888,23,22 --script=http-title,http-auth-finder 192.168.1.172
```

▶ Run

ESP32/ESP8266 devices commonly expose OTA update endpoints (port 8266), web config (80/8080), and serial-over-IP — grab banners and auth type before anything else.

```
nmap -sV -sC -p 80,443,22,23,8080,8443,8888 --open 192.168.1.1 192.168.1.172 192.168.1.203
```

▶ Run

Quick service sweep across the three most interesting targets simultaneously — router, IoT controller, and the 5G gateway.

Ask anything about this output...

Send

UNCLASSIFIED // FOR OFFICIAL USE ONLY



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.



Junior → senior in one tool

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



290 Kali tools

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



Stays on your network

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



UNCLASSIFIED // FOR OFFICIAL USE ONLY

← Back ×

dig

Domain Information Groper. Authoritative DNS lookup tool — query A, AAAA, MX, NS, TXT, SOA, PTR, CAA records, run zone-transfer attempts, hit arbitrary resolvers.

✨ Show AI Summary button on this tool's sessions

COMMANDS

dig {domain}
BASIC A — resolve a domain to its IPv4

dig +short {domain}
SHORT — just the IP, no headers

dig {domain} ANY
ANY — return every record type (A/AAAA/MX/TXT/NS/SOA/...)

dig {domain} TXT
TXT RECORDS — SPF, DKIM, DMARC, verification tokens

dig {domain} MX
MX RECORDS — mail infrastructure

dig {domain} NS
NS RECORDS — name server infrastructure

dig @{nameserver} {domain} AXFR
ZONE TRANSFER — try to dump the entire DNS zone

dig +trace {domain}
FULL DELEGATION TRACE — root → TLD → authoritative

dig -x {ip}
REVERSE — IP to PTR record

dig +noall +answer @{resolver} {domain}
CUSTOM RESOLVER — query a specific DNS server

for sub in \$(cat {subfile}); do dig +short \$sub | head -1; done
BULK RESOLVE — resolve a list of subdomains to IPs

▶ **NEXT STEPS**

dig finished. Read the ANSWER section for the records:
example.com. 3600 IN A 93.184.216.34 ←
the IP

UNCLASSIFIED // FOR OFFICIAL USE ONLY



The Proof

Real numbers from real runs. No marketing inflation.

24.4x

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 $W=465$, $p<0.001$.

Website
<https://nemesislabs.xyz>

Private and confidential

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.



Visual Live Pentest

— pick a completed VA run —

Bridged Kali (192.168.1.236)

safe mode

Launch Pentest

live

fd8927f7 · completed · 192.168.1.0/24

msfconsole(192.168.1.1)

online_exploit(192.168.1.1)

live_browser(http://192.168.1.1/)

hydra_db(192.168.1.73)

secretsdump(192.168.1.73)

live_browser(http://192.168.1.73:3000/#/login)

pentest run — target: 192.168.1.0/24 (safe_mode: off)

Detail Logs Browser MSF Sessions Passwords

Chain Audit Failed

Exploit attempts

(loading...)

live_browser → failed (target http://192.168.1.1/)

live_browser → failed (target http://192.168.1.73:3000/#/login)

dalfox → no_signal (target http://192.168.1.73:3000/#/search)

live_browser → no_signal (target http://192.168.1.73:3000/#/search?q=<script>alert(1)</script>)

online_exploit → failed (target 192.168.1.1)

live_browser → no_signal (target http://192.168.1.73:3000/rest/user/1)

online_exploit → failed (target 192.168.1.1)

online_exploit → failed (target 192.168.1.0/24)

online_exploit → failed (target 192.168.1.0/24)

online_exploit → failed (target http://192.168.1.1/)

live_browser → no_signal (target http://192.168.1.73:3000/#/complaint)

online_exploit → failed (target 192.168.1.0/24)

run: fd8927f7 phase: exploit events: 257 nodes: 54 findings: 0 cost: \$0.483

Download Report (PDF)



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	✓	✓	✗	✗