# Lateralus Pentester v2.0

Engine rewrite, four new modules, developer edition

Lateralus Language

bad-antics · April 2026 · Lateralus Offensive Security

**ABSTRACT** Lateralus Pentester v2.0 is a ground-up rewrite of the scan orchestration engine, a capability-scoped sandbox for every running module, and the addition of four new module families: **Active Directory / Kerberos**, **Web Application**, **Container & Kubernetes**, and the **Report Templating** subsystem. The total module count rises from 9 to 13. This document summarizes what changed, what broke, and how existing v1 playbooks should be migrated. It also announces the **Developer Edition**, a free tier for proven contributors.

## 1. Engine Rewrite

The v1 engine dispatched modules through a thread pool with a shared SQLite database. This model topped out at roughly 1,200 concurrent targets on commodity hardware. v2.0 replaces that engine with an async/await core built on std.async.v2 (Lateralus v0.6.0) that reliably drives **10,000 concurrent targets** per operator workstation in our test lab.

```
v1  engine:  1,200 concurrent targets,  2.1 GB RSS peak
v2  engine: 10,000 concurrent targets,  1.8 GB RSS peak
          (8.3x throughput, 14% lower memory)
```

The new engine is single-writer for the result store and uses a lock-free MPSC channel for module output. Every module runs in a capability-scoped sandbox: a module tagged Net.Connect cannot touch the filesystem without an explicit Fs.* capability, even if compromised.

## 2. New Modules

### 2.1 Active Directory / Kerberos

Kerberoasting, AS-REP roasting, ACL abuse graph generation (BloodHound-compatible export), DCSync simulation, and unconstrained-delegation enumeration. Integrates with the existing credential vault.

### 2.2 Web Application

HTTP/2 and HTTP/3 aware crawler; detection for OWASP Top 10 (2021); template-injection taxonomy covering Jinja, Twig, ERB, Velocity, Smarty. Authenticated scanning via recorded HAR replay.

### 2.3 Container & Kubernetes

Container image inspection (CVE matching against distro and language ecosystems), K8s RBAC auditor, pod-escape dry-run harness (safe-only; no live exploitation by default), and a kubeconfig drift detector.

### 2.4 Report Templating

Reports are now generated from Markdown templates with a typed context object. Built-in templates: executive summary, technical findings, remediation tracker, retest report. Custom templates can import partials and inherit from base layouts.

## 3. Operator-Visible Changes

- New TUI built on the std.term v2 rendering stack; keyboard-only operation; multi-pane layout.
- Scan definitions move from TOML to a DSL embedded in Lateralus; type-checked; autocomplete in the editor.

- Scan state is crash-tolerant: kill the process and resume from the last completed target.
- Plugin API v2; v1 plugins require a shim (provided) or a port.

## 4. Developer Edition

Pentester v2.0 introduces a **free Developer Edition** for contributors who have demonstrated sustained open-source work on Lateralus or the broader offensive-security ecosystem. It includes every feature of the paid tier, with the single restriction that scan results are watermarked "Developer Edition" and are not suitable for client deliverables.

Eligibility is reviewed by the GRUG team. Applicants submit a short handle, links to public portfolios, and a description of the work they would like to do with the tool. Applications go to wizard@lateralus.dev and are reviewed within seven days.

## 5. Migration from v1

- Run pentester migrate v1-playbook.toml to translate an existing playbook to the DSL.
- The credential vault format is compatible; no migration is required.
- Custom report templates written for v1's Handlebars engine must be ported; a porting guide ships with v2.
- Plugins exposing the v1 ModuleHost trait should be re-linked against ModuleHost2; most require only the interface change.

## 6. Availability

Pentester v2.0 ships on **April 2026**. Paid licenses (Operator and Team tiers) are available from lateralus.dev/pentester. Developer Edition is granted on request; see Section 4.

This document is versioned with the v2.0 release and will be updated for point releases (v2.0.x) with cumulative changelog entries.