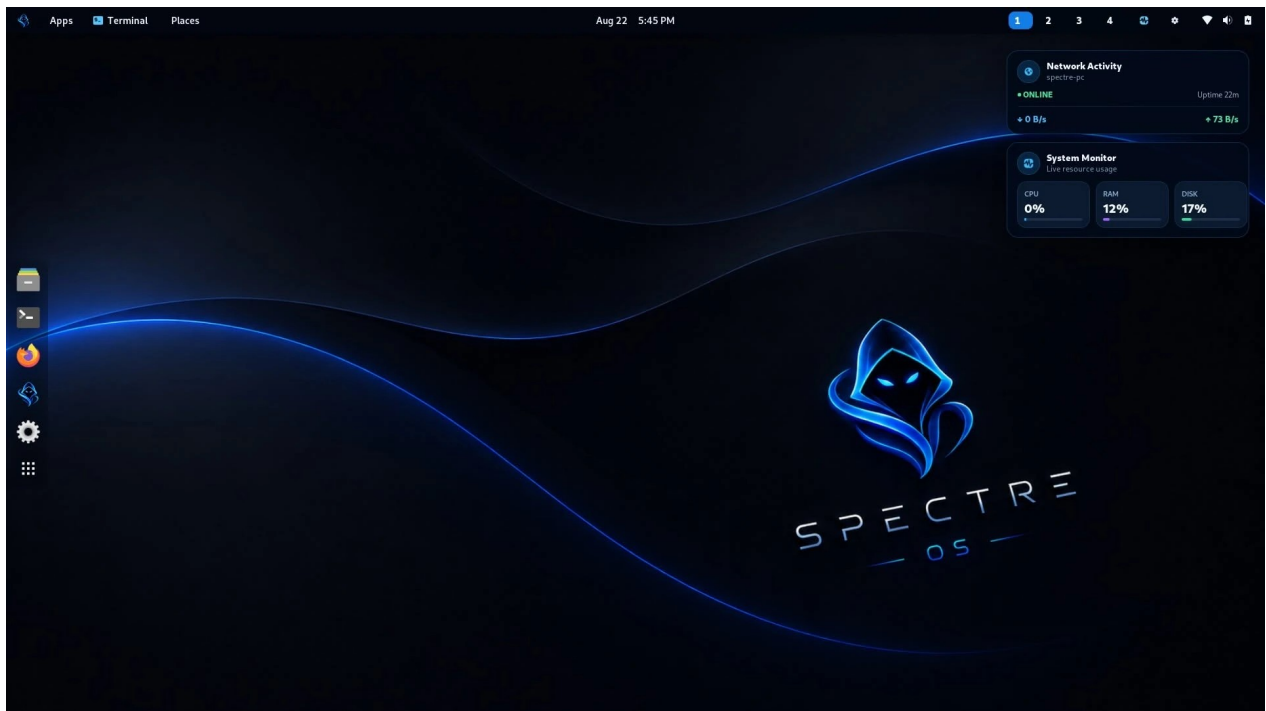


SPECTRE / 1.0

Discover Linux Spectre

A practical everyday Linux desktop with an optional cybersecurity toolbox.

Edition	Linux Spectre / Spectre OS 1.0
Document	PUBLIC EDITION • 11 October 2026



Actual project screenshot. Display and application availability depend on installed hardware and configuration.

Prepared from the project's source packages, website materials, recorded installation/acceptance logs, and upstream documentation.

Welcome to Linux Spectre

Linux Spectre, also known as Spectre OS 1.0, is an independent Linux desktop project built around a simple idea: a computer should be useful for everyday work, while still giving interested users a convenient path to learn and practice authorized cybersecurity skills.

Rather than asking every user to make a penetration-testing distribution their main daily operating system, Linux Spectre keeps the familiar GNOME desktop as the primary workspace and offers an optional Kali-based toolbox when security utilities are needed.

In one sentence. Linux Spectre is a general-purpose Linux desktop with Spectre ToolHub, a native interface for selecting Kali security-tool packages in a separate container.

Why I created Linux Spectre

Creator statement, edited from the project origin story for clarity.

“I created Linux Spectre because I wanted one operating system for both daily computing and cybersecurity learning. Kali Linux inspired me through its powerful tools for penetration testing and ethical hacking, but it is designed primarily for security professionals rather than as a typical everyday desktop. I wanted a different balance: a practical daily system with security tools available when I actually need them.”

“I was drawn to the Debian ecosystem because of its history, wide package ecosystem and reputation for stability-focused releases. I also took inspiration for the name Spectre from the Windows debloating project commonly known as Ghost Spectre. I wanted to create my own Linux project with its own purpose and identity.”

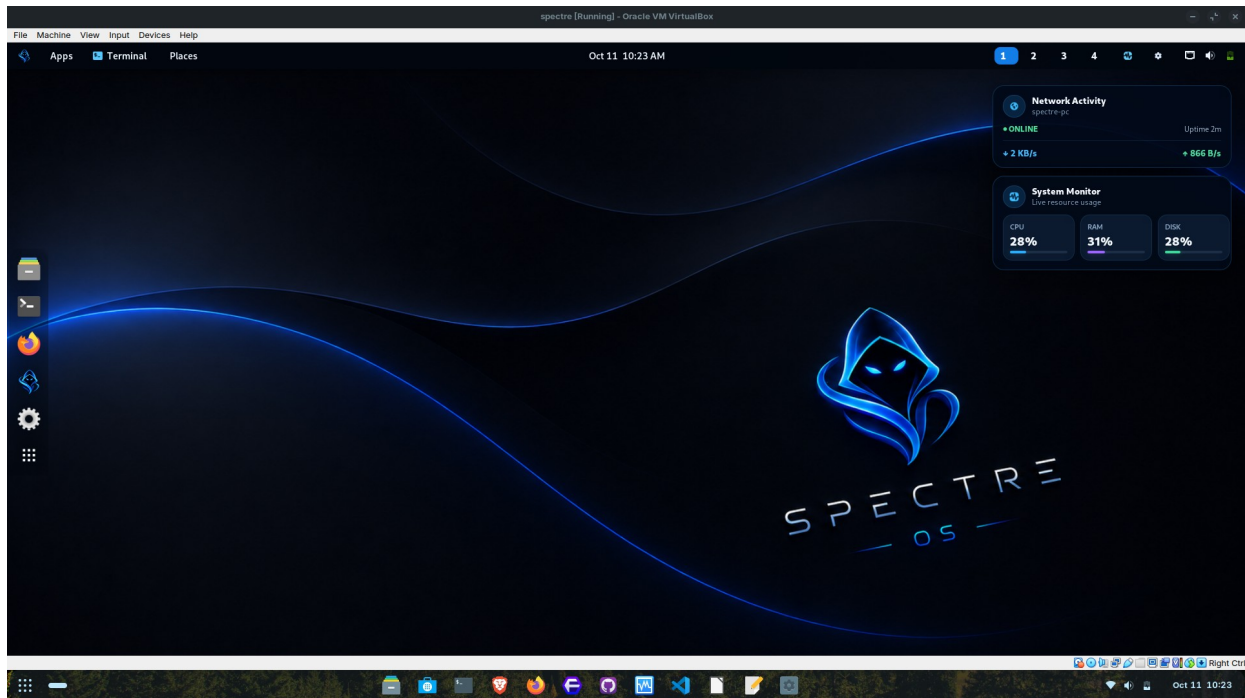
— Project creator, CodeDev by Edward

These statements describe the creator’s inspiration, not a claim that Kali is unusable for ordinary tasks, that Debian created every Linux distribution, or that Linux Spectre is affiliated with Kali, Debian, Ghost Spectre or Microsoft.

The design philosophy

- A comfortable daily desktop comes first.
- Security utilities are optional and installed selectively, not forced into the base system.
- Use the Debian-family Linux ecosystem for conventional applications and system maintenance.
- Keep Kali package management inside the toolbox rather than mixing its repositories into the host.
- Make security learning accessible while encouraging authorized and responsible usage.

Meet the desktop

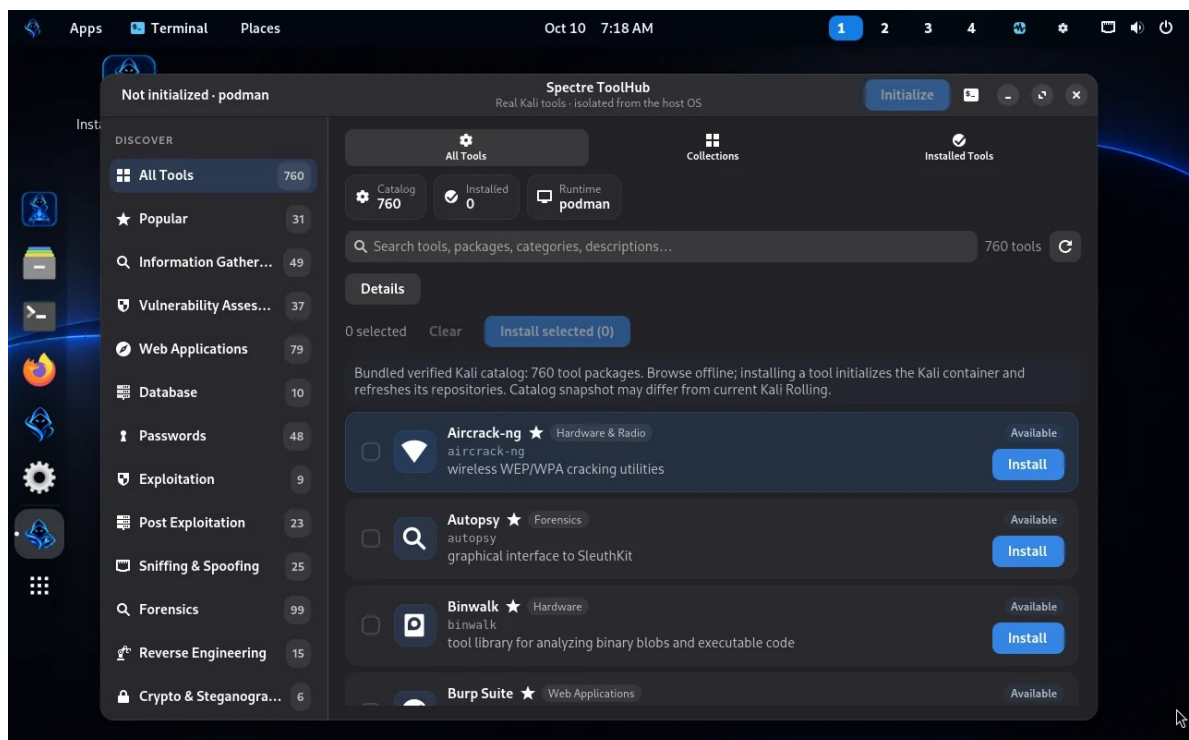


Actual screenshot of an installed Linux Spectre desktop running in VirtualBox.

Linux Spectre provides a GNOME graphical desktop with a branded visual design. The familiar app launcher, file workflow, terminal and desktop settings make it suitable for general-purpose activities such as browsing, document work, development and learning Linux.

A custom kernel identifies itself as 7.1.8-spectre in the verified 1.0 build. The installer supports an x86_64 test environment; a fresh VirtualBox installation and full-window desktop display have been demonstrated. Application availability and hardware compatibility vary by installation.

Spectre ToolHub: the signature feature



Spectre ToolHub, shown in a project capture; its interface helps discover and install selected Kali tool packages.

Spectre ToolHub is a desktop application built with GTK4/libadwaita. It presents a curated, searchable snapshot of 760 Kali-related tool-package entries, including package descriptions and categories. After initialization, it can refresh information from Kali's live package metadata.

760 ≠ preinstalled. The 760 number describes catalog entries visible for discovery. Installing all 760 programs is neither automatic nor required, and some package names or dependencies can change over time.

What can you do with ToolHub?

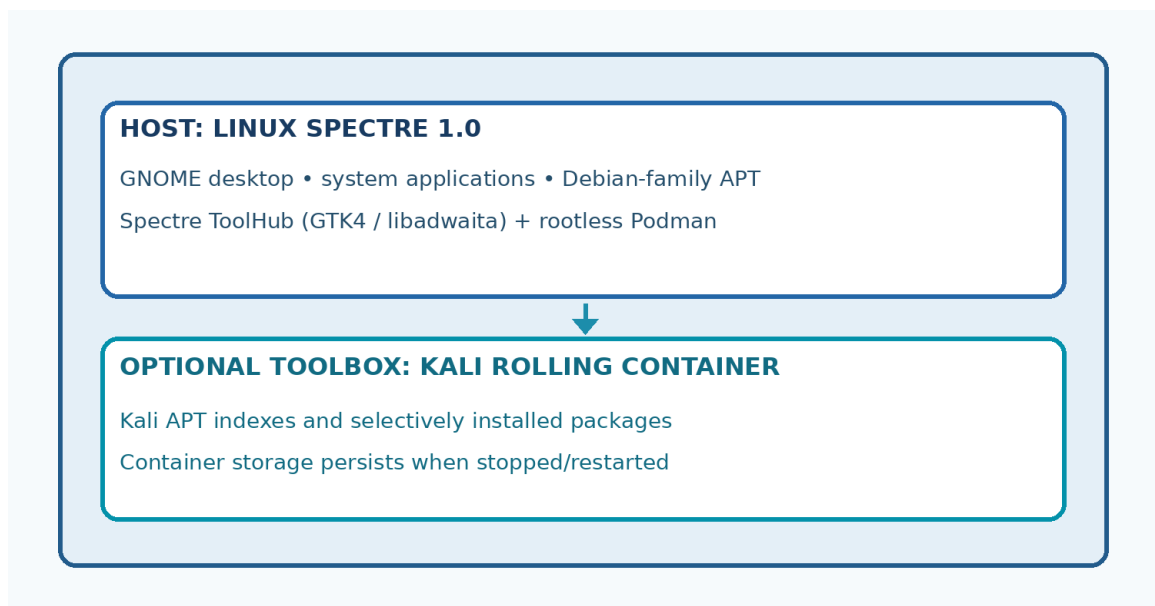
- Explore package choices before downloading a Kali container.
- Select useful packages for authorized network assessment, security study or laboratory exercises.
- Install a package or a small batch and see real installation progress.
- Check what is installed, remove unneeded packages and update the Kali package indexes.
- Keep the selected tools in the same container so they remain available after the container is stopped and later restarted.

Why is that useful?

If you need a security utility occasionally, you do not have to maintain a full penetration-testing distribution as your primary desktop. The ordinary host environment stays focused on daily use, while Kali's tooling resides in a managed, separate workspace. This can reduce package-repository conflicts and makes it easier to understand where tools are installed.

ToolHub is not an exploit automation service, and it does not grant permission to test third-party computers. Users remain responsible for knowing the purpose of tools and using them lawfully.

How the Kali toolbox works



Two environments: everyday Linux Spectre host and optional Kali Rolling container.

- 1. Browse: ToolHub shows the bundled catalog even before Kali is downloaded.
- 2. Initialize: ToolHub pulls the official Kali Rolling container image when internet is available.
- 3. Install: selected packages are installed with APT inside the Kali container, not into the desktop host.
- 4. Reuse: return to the same toolbox later, start it if stopped, and use previously installed packages.

The verified example is Nmap 7.99: the developer installed it inside spectre-kali-toolbox, rebooted the VM, restarted the container, and ran Nmap again without reinstalling it. That confirms persistence for the tested environment and package.

What Linux Spectre is—and what it is not

Linux Spectre is	Linux Spectre is not
A Linux desktop with a separate on-demand Kali toolbox	A rebranded Kali Linux ISO
Designed for everyday computing plus occasional authorized security work	A guarantee that every Kali tool works in every environment
A Debian-family system according to the project's build description	Proof that it tracks Debian Stable updates identically to stock Debian
An independent project inspired by several Linux and desktop projects	Affiliated with or endorsed by Kali, Debian or Ghost Spectre
A project with developer-tested VirtualBox functionality	Certified for all laptops, Wi-Fi adapters and GPUs

Kali's own documentation explains that it is optimized for penetration-testing specialists and not recommended as a typical general-purpose desktop for many users. Debian is one of the most influential Linux distribution families, but not literally the ancestor of every Linux distribution.

Who is Linux Spectre for?

Audience	What they may appreciate
Students and Linux newcomers	A daily desktop to learn terminal basics and system concepts
Developers and IT technicians	A Linux workspace with optional diagnostics and security-learning utilities
Cybersecurity learners	An organized way to choose tools for authorized lab work
Security professionals	A daily-use machine with a separate Kali tooling environment, within known container limits

Linux Spectre does not promise automatic safety. Ethical hacking means having permission, a defined scope and respect for privacy. This project is intended for learning, personal labs and legitimate professional assessment.

Getting started

Important before installing. Back up your files. OS installation may overwrite a selected disk. Start with a VM if you are unfamiliar with Linux installations.

1. Download the official ISO only when the maintainer publishes a verified distribution link.
2. Compare the image SHA-256 to the trusted checksum below.
3. Boot a new VirtualBox VM or prepared installer media. A tested VM profile used Debian 64-bit, 4 GB RAM, two vCPUs and a 40 GB disk; this is not a published minimum requirement.
4. Follow the graphical installation prompts, confirm the target disk, and create your user account.

- After login, use the desktop normally. Open Spectre ToolHub when you want to explore the Kali package catalog.

Release-named ISO: Spectre-OS-1.0-x86_64.iso

SHA-256: a49d7602a772c2db1dfb72411e47574ec908c5337d05131cb10433119f689d76

If you are evaluating the OS before a public binary release URL is posted, use the website for screenshots and product information; do not assume any third-party mirror is authentic.

Common questions

Is Linux Spectre the same as Kali Linux?

No. Linux Spectre is an independent GNOME desktop project that starts an optional official Kali Rolling container for selected tool packages.

Are 760 penetration-testing tools already installed?

No. ToolHub has a 760-entry catalog snapshot. Actual packages are installed individually or in controlled batches when selected.

Can I use it for browsing, development and everyday work?

That is the design goal. Exact applications and hardware support depend on the installed build and user requirements.

Does ToolHub work without internet?

You can browse the bundled catalog offline. A first-time Kali image pull, repository refresh and new package downloads require internet.

Will my installed tools disappear after reboot?

The verified Kali container retained Nmap after reboot and restart. Deleting/recreating the container can remove packages unless separate storage or backups have been arranged.

Can every Wi-Fi or USB penetration-testing device work inside the container?

No. The current unprivileged default container is not intended for direct monitor-mode Wi-Fi or privileged USB hardware access.

Is it secure by default?

Rootless Podman and host/container package separation provide useful boundaries, but do not establish formal security certification. Apply updates and use tools responsibly.

Why “Spectre”?

The creator admired the name associated with a debloated Windows project and decided to use it for a distinct Linux concept. The projects are not affiliated.

Is the project already downloadable?

The installation image has passed functional testing in the documented VirtualBox environment. Public distribution still depends on the project owner’s publication and applicable license compliance.

What has been tested?

Component	Developer-observed outcome
Fresh VM installation	Booted into installed GNOME desktop
Kernel	7.1.8-spectre reported by uname

VirtualBox display	Guest service and clients active; full-window display demonstrated
Rootless Podman	Rootless=true; account provisioner successful
ToolHub/Kali package	Nmap 7.99 executed inside Kali container
Persistence	Existing container restarted after reboot; Nmap still installed
Source/legal release review	Not asserted complete

Open technology, independence and responsibility

Linux Spectre builds on software developed by the wider Linux ecosystem. Debian, Kali Linux, GNOME, Podman, VirtualBox and other names belong to their respective communities or trademark owners. Linux Spectre is an independent project; inspiration does not mean sponsorship or endorsement.

Before public ISO distribution, the maintainer must complete the license, notice and corresponding-source review for included third-party components, including the specific VirtualBox Guest Additions payload. The public website and documentation can be available separately from the OS binary.

The objective of this project is an approachable desktop and responsible cybersecurity learning environment, not an offensive toolkit for unauthorized activity.

Where to learn more

Project website: <https://linux-spectre.myportfoliohub.online/>

Debian releases: <https://www.debian.org/releases/>

Debian derivatives: <https://www.debian.org/derivatives/>

Kali intended audience: <https://www.kali.org/docs/introduction/should-i-use-kali-linux/>

Kali official containers: <https://www.kali.org/docs/containers/official-kalilinux-docker-images/>

Podman rootless: <https://docs.podman.io/en/latest/markdown/podman.1.html>

Document version: 1.0 (public guide), 11 October 2026. Product version and documentation version are distinct. The accompanying Technical Handbook records deeper implementation and maintenance information.