

More Linux distributions

Previously, you were introduced to the different distributions of Linux. This included KALI LINUX™. (KALI LINUX™ is a trademark of OffSec.) In addition to KALI LINUX™, there are multiple other Linux distributions that security analysts should be familiar with. In this reading, you'll learn about additional Linux distributions.

KALI LINUX™

KALI LINUX™ is an open-source distribution of Linux that is widely used in the security industry. This is because KALI LINUX™, which is Debian-based, is pre-installed with many useful tools for penetration testing and digital forensics. A **penetration test** is a simulated attack that helps identify vulnerabilities in systems, networks, websites, applications, and processes. **Digital forensics** is the practice of collecting and analyzing data to determine what has happened after an attack. These are key activities in the security industry.

However, KALI LINUX™ is not the only Linux distribution that is used in cybersecurity.

Ubuntu

Ubuntu is an open-source, user-friendly distribution that is widely used in security and other industries. It has both a command-line interface (CLI) and a graphical user interface (GUI). Ubuntu is also Debian-derived and includes common applications by default. Users can also download many more applications from a package manager, including security-focused tools. Because of its wide use, Ubuntu has an especially large number of community resources to support users.

Ubuntu is also widely used for cloud computing. As organizations migrate to cloud servers, cybersecurity work may more regularly involve Ubuntu derivatives.

Parrot

Parrot is an open-source distribution that is commonly used for security. Similar to KALI LINUX™, Parrot comes with pre-installed tools related to penetration testing and digital forensics. Like both KALI LINUX™ and Ubuntu, it is based on Debian.

Parrot is also considered to be a user-friendly Linux distribution. This is because it has a GUI that many find easy to navigate. This is in addition to Parrot's CLI.

Red Hat® Enterprise Linux®

Red Hat Enterprise Linux is a subscription-based distribution of Linux built for enterprise use. Red Hat is not free*, which is a major difference from the previously mentioned distributions. Because it's built and supported for enterprise use, Red Hat also offers a dedicated support team for customers to call about issues.

with my personal experience, you can use RHEL9 for personal use. also as of July of 2023, its parent company may be trying to break copyright law by limiting access to source code, and close sourcing the project. if they succeed many other distros might die or become less secure or die, like CentOS. I likely wont update this but you can google it yourself to see how that went.

CentOS

CentOS is an open-source distribution that is closely related to Red Hat. It uses source code published by Red Hat to provide a similar platform. However, CentOS does not offer the same enterprise support that Red Hat provides and is supported through the community.

p.s. CentOS may be dead because its parent company is trying to kill it at the time of posting this page, google it to see if it has died LOL

Arch Linux

Arch Linux is an open-source distribution known for its simplicity and user-focused design. It adheres to the "Keep It Simple, Stupid" (KISS) principle, offering a minimal base system that users can customize to their needs, reducing potential security risks, provides more control over the system, rolling-release model ensures up-to-date security updates.

A key feature is the Arch User Repository (AUR), a community-driven repository that lets users compile and install packages from source using the Arch package manager, pacman.

Key takeaways

KALI LINUX ™, Ubuntu, Parrot, Red Hat, and CentOS are all widely used Linux distributions. It's important for security analysts to be aware of these distributions that they might encounter in their career.