Linux is a highly customizable operating system with various distributions (distros) that cater to different needs. These distros differ in the tools, programs, and interfaces they offer, making it essential for security analysts to understand which distribution they are using to know what resources are available.

**Key Points:**

1. **Linux Distributions (Distros)**:
   * Distributions are different versions of Linux built on the same kernel but customized with unique tools and features.
   * Some popular examples include **Debian**, **Ubuntu**, and **Kali Linux**.
2. **Analogy**:
   * **Kernel as the engine**: Just like an engine powers different vehicles, the Linux kernel is the foundation of every distro.
   * **Distributions as different vehicles**: Like vehicles designed for different purposes (e.g., trucks, buses, cars), distros serve various roles. For example, **Kali Linux** is used for penetration testing, while **Ubuntu** is suitable for general-purpose tasks.
3. **Customizability**:
   * Linux's open-source nature allows users to modify and create custom distros.
   * Distros are built from parent distributions, such as **Red Hat** being the parent of **CentOS** or **Ubuntu** derived from **Debian**.

**Why Understanding Distributions Is Important for Security Analysts:**

* Each distribution offers a different set of tools and configurations.
* Knowing the distribution helps analysts determine which security tools, package management systems, and interfaces are available for performing security tasks.

**KALI LINUX™ Overview:**

**KALI LINUX™** is a Debian-based, open-source Linux distribution specifically designed for **penetration testing** and **digital forensics**. It is widely used in security by professionals due to its vast array of pre-installed tools, which assist in identifying system vulnerabilities and conducting forensic analysis.

**Key Points:**

1. **Purpose**:
   * Kali Linux is tailored for penetration testing, vulnerability assessment, and digital forensics. It includes tools specifically built to test the security of systems, networks, websites, applications, and more.
2. **Virtual Machine Use**:
   * It's recommended to run Kali Linux on a **virtual machine**. This prevents system damage and allows users to revert to a previous state if something goes wrong, offering a safer testing environment.
3. **Penetration Testing Tools**:
   * **Metasploit**: Identifies and exploits vulnerabilities on machines.
   * **Burp Suite**: Tests for vulnerabilities in web applications.
   * **John the Ripper**: A password-cracking tool.
4. **Digital Forensics Tools**:
   * **tcpdump**: A command-line tool to capture and analyze network traffic.
   * **Wireshark**: A graphical tool for analyzing live or captured network traffic.
   * **Autopsy**: A forensic tool used for analyzing hard drives and smartphones, important in digital investigations.

**Why It’s Important for Security Analysts:**

* Kali Linux is indispensable for those involved in **penetration testing** or **digital forensics**, providing a comprehensive suite of tools that streamline and enhance security investigations.
* It allows analysts to simulate cyberattacks, uncover vulnerabilities, and perform thorough investigations into network activities and digital evidence following attacks.

**Other 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.

## AlmaLinux

**AlmaLinux** is a community-driven Linux distribution that was created as a stable replacement for CentOS. CentOS was an open-source distribution that is closely related to Red Hat, and its final stable release, CentOS 8, was in December 2021. CentOS used source code published by Red Hat to provide a similar platform. AlmaLinux is designed to be a drop-in replacement for CentOS 8. This ensures that applications and configurations that worked on CentOS will continue to function on AlmaLinux.

## 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.