

# Kali Linux Tutorial For Beginners:

## What is, How to install & Use

### What Is Kali Linux?

- **Kali Linux** is a security distribution of Linux derived from Debian and specifically designed for computer forensics and advanced penetration testing.
  - **Kali Linux** contains several hundred tools that are well-designed towards various information security tasks, such as penetration testing, security research, computer forensics and reverse engineering.

### Tools In Kali Linux

Kali Linux has over 600 preinstalled penetration-testing applications to discover. Each program with its unique flexibility and use case. Kali Linux does excellent job separating these useful utilities into the following categories:

- Information Gathering
- Vulnerability Analysis
- Wireless Attacks
- Web Applications
- Exploitation Tools
- Stress Testing
- Forensics Tools
- Sniffing & Spoofing
- Password Attacks
- Maintaining Access
- Reverse Engineering
- Reporting Tools
- Hardware Hacking

### Who Uses Kali Linux & Why?

Kali Linux is truly a unique operating system, as its one of the few platforms openly used by both good guys and bad guys. Security Administrators, and Black Hat Hackers both use this operating system extensively.

# Kali Linux Tutorial For Beginners:

## What is, How to install & Use

### Professionals That Use Kali Linux

- **Security Administrators** – Security Administrators are responsible for safeguarding their institution's information and data. They use Kali Linux to review their environment(s) and ensure there are no easily discoverable vulnerabilities.
- **Network Administrators** – Network Administrators are responsible for maintaining an efficient and secure network. They use Kali Linux to audit their network. For example, Kali Linux has the ability to detect rogue access points.
- **Network Architects** – Network Architects are responsible for designing secure network environments. They utilize Kali Linux to audit their initial designs and ensure nothing was overlooked or misconfigured.
- **Pen Testers** – Pen Testers, utilize Kali Linux to audit environments and perform reconnaissance on corporate environments which they have been hired to review.
- **CISO** – CISO or Chief Information Security Officers, use Kali Linux to internally audit their environment and discover if any new applications or rogue configurations have been put in place

### Professional Users

- **Forensic Engineers** – Kali Linux possesses a "Forensic Mode", which allows a Forensic Engineer to perform data discovery and recovery in some instances.
- **White Hat Hackers** – White Hat Hackers, similar to Pen Testers use Kali Linux to audit and discover vulnerabilities which may be present in an environment.
- **Black Hat Hackers** – Black Hat Hackers, utilize Kali Linux to discover and exploit vulnerabilities. Kali Linux also has numerous social engineer applications, which can be utilized by a Black Hat Hacker to compromise an organization or individual.
- **Grey Hat Hackers** – Grey Hat Hackers, lie in between White Hat and Black Hat Hackers. They will utilize Kali Linux in the same methods as the two listed above.
- **Computer Enthusiast** – Computer Enthusiast is a pretty generic term, but anyone interested in learning more about networking or computers, in general, can use Kali Linux

### To Get Started With Kali

- The second half of the page that this link points to gives you installation instructions for Kali Linux.
- <https://www.guru99.com/kali-linux-tutorial.htm>

# Kali Linux Tutorial For Beginners: What is, How to install & Use

## Download This Version

<https://itsfoss.com/install-kali-linux-virtualbox/>

- The above link is instructions

This is the easiest version to get up and running as opposed to osi image.

- This is an OVA image

<https://www.offensive-security.com/kali-linux-vm-vmware-virtualbox-image-download/>

- The directions give you a user name and password That did not work for me. I used      Username=kali    Password=kali