Install Guide for Kali Linux – Bare Metal Deployments

Welcome to BeeHive! We're a group of CyberSecurity experts with one goal in mind – arming the world with the proper advice and tools needed to continue to protect it. In this document, you'll find instructions on how to proceed with a Bare Metal install of Kali Linux. Kali Linux is a build of the Linux Operating System targeted towards IT Professionals, CyberSecurity Enthusiasts, and Professional Penetration Testers and includes multiple packages and programs designed for use in professional scenarios, as well as internal tweaks and changes to make Kali Linux in theory a more bulletproof operating system than say, Ubuntu or Linux Mint.

Before we continue, the information that makes our lawyers happy. First, by following these instructions you are following the instructions that work for 90% of Kali Linux installations and deployments. HOWEVER, your machine may be unique in specific and unaccounted for ways that could impede your install, and those may not be documented here. Factually, you need to recognize that venturing into “alternate” operating systems is NOT a tested-and-true process, and bugs are to be EXPECTED and PREDICTED, never should a bug surprise you. Additionally, Linux does not support officially every single driver and module that Microsoft Windows does. By using a Linux deployment, you lose native support for many driver installs and thus, not everything may work as expected, intended, or described. By proceeding to acknowledge this warning and follow these instructions, you accept that these are **GENERALIZED INSTALLATION AND DEPLOYMENT DIRECTIONS**, and that failure to understand exactly what you're trying to do in the install can result in corrupted data, wiped bootloaders, and whole lots of other non-sense.

Second, an open warning. CyberSecurity involves zero guarantees as to safety and security, especially if you're the one researching it. While Kali Linux is, in professional usage, a fantastic tool...it has a high probability of mis-use, or use against targets and organizations that have not authorized it. While we don't condone “rogue” and mis-aligned hacktivism, we accept and support its existence. Thus, we issue this warning. **By proceeding with this installation guide, you understand the implications of committing unauthorized operations against targets. Depending on your target, you may face anything from absolutely nothing, to criminal charges, to government-ordered court appearances in exchange for actions against these targets. You may also face malicious counter-operations against you, or your family, should you not properly protect yourself. By continuing this install, in summary, you indicate complete understanding and awareness of the dangers of participation in CyberSecurity, and you lift us of any fault attributable. You're on your own on this one, chief.**

You'll need the following to follow our suggested installation protocol.

If moving from Windows: 2x USB Drive (8GB+)
If installing on brand new machine: 1x USB Drive (8GB+)
BalenaEtcher
Kali Linux NetInstaller Image

You can find copies of referenced software attached to the GitHub,
https://github.com/BeeHiveCyberSecurity

*****Getting Started*****

We'll begin the installation flow as if you're preparing to install alongside an active Windows deployment.

1. Create a Windows 10 Recovery Media.
   You need a way to un-fuck your machine if you screw it up during the install. You'll need to have a recovery ISO for Windows 10 on one of the two drives. First, you'll want to use the "MediaCreationTool.exe" included on our GitHub to turn a USB Drive into a Rescue Drive. This is a fairly straightforward, GUI-guided process. Plug the USB drive into your system, launch MediaCreationTool.exe, and follow the instructions to create a Windows 10 recovery drive. After its done, close MediaCreationTool.exe, eject and remove the Windows 10 USB from your computer, mark it so you won't mix it up, and place it to the side.

2. Download the Kali Linux NetInstaller ISO.
   We've included a copy of this on the GitHub as well for you.

3. Download balenaEtcher.
   You'll need this software to "etch" a bootable copy of the ISO onto your USB Drive. Dragging the ISO onto the drive is not the proper way to create a bootable USB drive. Things will not work unless you perform this step. Seriously.

4. Etch the NetInstaller ISO.
   Depending on your drive and system performance, this may take a short bit. Feel free to grab a snack. Also, ensure that you have file verification enabled in balenaEtcher. It should be enabled by default but, we all click things on accident. Once etched, eject the USB, unplug, and shut your computer down.

5. Disable BIOS Security Features
   This is again, very important step. If you miss something here, shit won't work. Make sure that before you try to boot to the USB, that you've **DISABLED** Secure Boot, **ENABLED** Legacy Boot (if available) and that you've disabled your machine's CSM (Compatibility Support Module), as this will ALSO cause errors. Once you've disabled much of this, then you're ready to boot to the USB.

6. Boot to the USB
   Shut your computer back down after adjusting your BIOS's security features. Insert USB. Boot machine and spam your “Boot Select” keyboard key. Every BIOS seems to have a different key they prefer to use, but give F-11 a shot. If that doesn't work, try DEL. If that doesn't work...consult your motherboard's instructions manual, honestly. We left the help desk behind for a reason, nothing personal.

7. Install Kali
   The Kali Linux installation is offered in both guided, and unguided flavors. Once the machine is powered up, you will be prompted to select your preferred installation mode in the GRUB menu. Select graphical install and continue. Next couple of screens will ask you to select locale information such as your preferred **language**, your country, and keyboard layout. Once through the local information, the loader will automatically install some additional components and configure your network related settings. Then the installer will prompt for a **hostname** and **domain** for this installation. Provide appropriate information for the environment and continue installing. Set a password for your Kali Linux machine and hit continue. **DO NOT FORGET THIS PASSWORD**. After the password is set, the installer will prompt you to set the **time zone** and then pauses at the disk partitioning. The installer will now provide you four choices about the partitions of the disk. The easiest option for you is to use **‘Guided – Use Entire Disk’**. Experienced users can use the “Manual” partitioning method for more granular configuration options. Select the partitioning disk (the recommended option is all files in one partition for new users) & then hit on continue. Confirm all changes to be made to the disk on the host machine. Be aware that if you continue it will **ERASE DATA ON THE DISK**. Once you confirm the partition changes, the installer will run through the process of installing the files. Let it install the system automatically, this may take a while…Next you will be asked to install the GRUB boot loader. Select ‘Yes’ and pick the device to write the necessary boot loader information to the hard drive which is required to boot Kali. Once the installer finishes installing **GRUB** to the disk, click on continue to finish the installation, it will install some final stage files.

Note: If you've installed Kali alongside Windows 10, you may need to manually change your boot “option” to switch inbetween operating systems. In our BIOS, kali created a boot option simply labeled “kali”. HOWEVER, not all BIOS's operate the same and your experience may very.

NOW - A couple #pro #tips

1. Install the KDE Plasma 5 desktop environment over the XFCE one. You'll thank us later.
2. Install the “large” package selection.
3. Choose a VPN service that has a native Linux client, or supports OpenVPN manual credentials.