**Content**

[1. Ubuntu vs Debian 2](#_Toc12785670)

[1. OVA vs OVF vs ISO 2](#_Toc12785671)

[2. Linux Package Managers 2](#_Toc12785672)

[2. 3](#_Toc12785673)

[3. Kali linux 4](#_Toc12785674)

[3.1.1. Tools 4](#_Toc12785675)

1. Ubuntu vs Debian

Debian is one of the original Linux distros developed in 1993 and Ubuntu is a fork of Debian, and the first release of Ubuntu was in 2004. Every six month, Debian releases a testing branch, and Ubuntu adopts that latest packages from the Debian unstable branch.

* 1. OVA vs OVF vs ISO

An **OVA (Open Virtual Appliance)** is a tarball consisting of an **OVF XML,** a manifest file and a Virtual Disk.

The OVF XML is a specification of the hardware (just hardware, not the BIOS, as am not sure if a Virtual Machine can really have a BIOS of its own).

The Virtual Disk could be different based on the hypervisor you are building the OVA for.

For VMware vSphere, the virtual disk is VMDK.

If you are playing with VirtualBox in your homelab, it could be VDI.

An ISO on the other hand is not really linked to Virtualization. It is the format of CDs. It could be the operating system or just a bunch of files that could just be mounted.

* An ISO .. just the Operating System
* An OVF XML .. just the hardware
* An OVA .. is a virtual appliance that has an OVF and a VMDK (that is a virtual disk installed typically with an ISO)
  1. Linux Package Managers

1. DPKB – Debian Package Management System
   1. APT – Advanced Packaging Tool
   2. Aptitude Package Manager
   3. Synaptic Package Manager
2. RPM – Red Hat Package Manager
   1. YUM – Yellowdog Updater, Modified
   2. DNF – Dandified Yum
3. Pacman Package Manager – Arch Linux
4. Zypper Package Manager – openSUSE
5. Portage Package Manager – Gentoo
6. APK – Alpine Linux
   1. Alpine Linux

Alpine Linux is a Linux distribution based on **musl** and **BusyBox**, designed for security, simplicity, and resource efficiency. It uses a hardened kernel and compiles all user space binaries as position-independent executables with stack-smashing protection.

Because of its small size, it's heavily used in containers providing quick boot up times.

A fork of the distribution, postmarketOS, is designed to run on mobile devices.

**musl** is a C standard library intended for operating systems based on the Linux kernel, released under the MIT License.[3] It was developed by Rich Felker with the goal to write a clean, efficient and standards-conformant libc implementation

**BusyBox** is a software suite that provides several Unix utilities in a single executable file. It runs in a variety of POSIX environments such as Linux, Android, and **FreeBSD**, although many of the tools it provides are designed to work with interfaces provided by the Linux kernel. It was specifically created for embedded operating systems with very limited resources. The authors dubbed it "The Swiss Army knife of Embedded Linux", as the single executable replaces basic functions of more than 300 common commands. It is released as free software under the terms of the GNU General Public License, version 2.

**FreeBSD** is a free and open-source Unix-like operating system descended from the Berkeley Software Distribution **(BSD)**, which was based on Research Unix. The first version of FreeBSD was released in 1993. In 2005, FreeBSD was the most popular open-source BSD operating system, accounting for more than three-quarters of all installed BSD systems.

1. Kali linux

„the quiter you become, the more yo are able to hear“

Kali Linux[3] is a Debian-derived Linux distribution designed for digital forensics and penetration testing.[4][5][6][7] It is maintained and funded by Offensive Security Ltd. It was developed by Mati Aharoni and Devon Kearns of Offensive Security through the rewrite of BackTrack, their previous information security testing Linux distribution based on Knoppix. The third core developer, Raphaël Hertzog, joined them as a Debian expert

* + 1. Tools

Kali Linux includes security tools, such as:[13]

1. Aircrack-ng
2. Armitage
3. Burp suite
4. Cisco Global Exploiter, a hacking tool used to find and exploit vulnerabilities in Cisco Network systems
5. Ettercap
6. John the Ripper
7. Kismet
8. Maltego
9. Metasploit framework
10. Nmap
11. OWASP ZAP
12. Social engineering tools.
13. Sqlmap
14. Wireshark
15. Hydra
16. Reverse Engineering tools
17. Binwalk
18. Foremost
19. Volatility