kali 简介

Kali Linux 是基于 Debian 的 Linux 发行版，设计用于数字取证和渗透测试。由 Offensive Security Ltd 维护和资助。最先由 Offensive Security 的 Mati Aharoni 和 Devon Kearns 通过重写 BackTrack 来完成，BackTrack 是他们之前写的用于取证的 Linux 发行版 。

Kali Linux 预装了许多渗透测试软件，包括 nmap (端口扫描器)、Wireshark (数据包分析器)、John the Ripper (密码破解器),以及 Aircrack-ng (一应用于对无线局域网进行渗透测试的软件).[2] 用户可通过硬盘、live CD 或 live USB 运行 Kali Linux。Metasploit 的 Metasploit Framework 支持 Kali Linux，Metasploit 一套针对远程主机进行开发和执行 Exploit 代码的工具。

Kali Linux 既有 32 位和 64 位的镜像。可用于 x86 指令集。同时还有基于 ARM 架构的镜像，可用于树莓派和三星的 ARM Chromebook

软件名称：Kali Linux

开发商：Offensive Security

软件版本： Kali Linux 2.0

更新时间：2015 年 8 月 11 日

软件大小：3.0G

软件授权：开源软件

Kali linuxKali Linux 特性

Kali 是 BackTrack Linux 完全遵循 Debian 开发标准的完整重建.全新的目录框架、复查并打包所有工具、还为 VCS 建立了 Git 树.

· 超过 300 个渗透测试工具: 复查了 BackTrack 里的每一个工具之后,去掉了一部分已经无效或功能重复的工具.

· 永久免费: Kali Linux 一如既往的免费.你永远无需为 Kali Linux 付费.

· 开源 Git 树: 是开源软件忠实的拥护者,那些想调整或重建包的人可以浏览开发树得到所有源代码.

· 遵循 FHS: Kali 的开发遵循 Linux 目录结构标准,用户可以方便的找到命令文件、帮助文件、库文件等..

· 支持大量无线设备: 尽可能的使 Kali Linux 支持更多的无线设备,能正常运行在各种各样的硬件上,能兼容大量 USB 和其它无线设备.

· 集成注入补丁的内核: 作为渗透测试者或开发团队经常需要做无线安全评估.所以的内核包含了最新的注入补丁.

· 安全的开发环境: Kali Linux 开发团队由一群可信任的人组成,他们只能在使用多种安全协议的时候提交包或管理源.

· 包和源有 GPG 签名: 每个开发者都会在编译和提交 Kali 的包时对它进行签名,并且源也会对它进行签名.

· 多语言: 虽然渗透工具趋向于用英语,但确保 Kali 有多语言支持,可以让用户使用本国语言找到他们工作时需要的工具.

· 完全的可定制: 完全理解,不是每个人都赞同的设计决定,所以让更多有创新精神的用户定制 Kali Linux(甚至定制内核)成他们喜欢的样子变得尽可能的容易.

· ARMEL 和 ARMHF 支持: 自从基于 ARM 的设备变得越来越普遍和廉价,就知道该竭尽全力的做好 Kali 的 ARM 支持.因此有了的 ARMEL 和 ARMHF 架构的系统.Kali Linux 有完整的主线发行版的 ARM 源,所以 ARM 版的工具将会和别的版本同时更新.Kali 可以运行在如下的 ARM 设备:

◦ rk3306 mk/ss808

◦ Raspberry Pi

◦ ODROID U2/X2

◦ MK802/MK802 II

◦ Samsung Chromebook

Kali linuxKali Linux 与 Debian 的区别

Kali Linux 面向专业的渗透测试和安全审计.因此,Kali Linux 已经进行了如下的多处核心的修改:

单用户,设计成 root 权限登录:由于安全审计的本质，Kali Linux 被设计成使用”单用户,root 权限“方案.

默认禁用网络服务:Kali Linux 包含了默认禁用网络服务的 sysvinit hooks.它们允许用户在 Kali Linux 安装各种的服务,允许用户安装各种包,同时仍然确保我们默认的发行版安全.附加的服务，例如蓝牙也会被默认列入黑名单.

定制的内核:Kali Linux 使用打过无线注入补丁的上游内核.

Kali linux 软件支持

给用户提供了大量的安全工具软件。

Kali Linux 还支持 Live CD 和 Live USB 启动方式，用户可以直接从移动介质启动该系统而不用将系统安装在硬盘上。

Kali Linux 集成了以下安全软件:

Metasploit

RFMON

Aircrack-NG

Gerix Wifi Cracker

Kismet

Nmap

Ophcrack

Ethercap

Wireshark (formerly known as Ethereal)

BeEF (Browser Exploitation Framework)

Hydra

OWASP Mantra Security Framework （一套基于 FireFox 的工具、插件和脚本）

Cisco OCS Mass Scanner （通过 telnet 以及默认密码扫描思科路由器）

exploit 程序比如 浏览器

BackTrack 工具软件分成 12 大类:

Information Gathering（信息收集）

Vulnerability Assessment（漏洞评定工具）

Exploitation Tools（攻击工具）

Privilege Escalation（用户提权）

Maintaining Access（维护登录）

Reverse Engineering（逆向工程）

RFID Tools（RFID 工具）

Stress testing（压力测试）

Forensics（取证）

Reporting Tools（报告工具）

Services（服务）

Miscellaneous（杂项）

Kali linux 版本更新

2014 年 5 月 27 日 1.0.7 发布

2014 年 7 月 22 日 1.0.8 发布支持 EFI BOOT

2014 年 8 月 25 日 1.0.9 发布

2015 年 8 月 11 日 2.0 发布

2016 年 1 月 21 日首个滚动更新版本 Kali-Rolling (2016.1) 发布

。