Kali Linux 渗透测试实战 1.1 Kali Linux 简介

如果您之前使用过或者了解 BackTrack 系列 Linux 的话，那么我只需要简单的说，Kali 是 BackTrack 的升级换代产品，从 Kali 开始，BackTrack 将成为历史。如果您没接触过 BackTrack 也没关系 ,我们从头开始了解 Kali Linux。按照官方网站的定义，Kali Linux 是一个高级渗透测试和安全审计 Linux 发行版。作为使用者，我简单的把它理解为，一个特殊的 Linux 发行版，集成了精心挑选的渗透测试和安全审计的工具，供渗透测试和安全设计人员使用。也可称之为平台或者框架。

1.1 Kali Linux 简介

目录

信息搜集

漏洞分析

Web 程序

密码攻击

无线攻击

漏洞利用工具集

嗅探欺骗

权限维持

逆向工程

压力测试

硬件 Hacking

数字取证

报告工具集

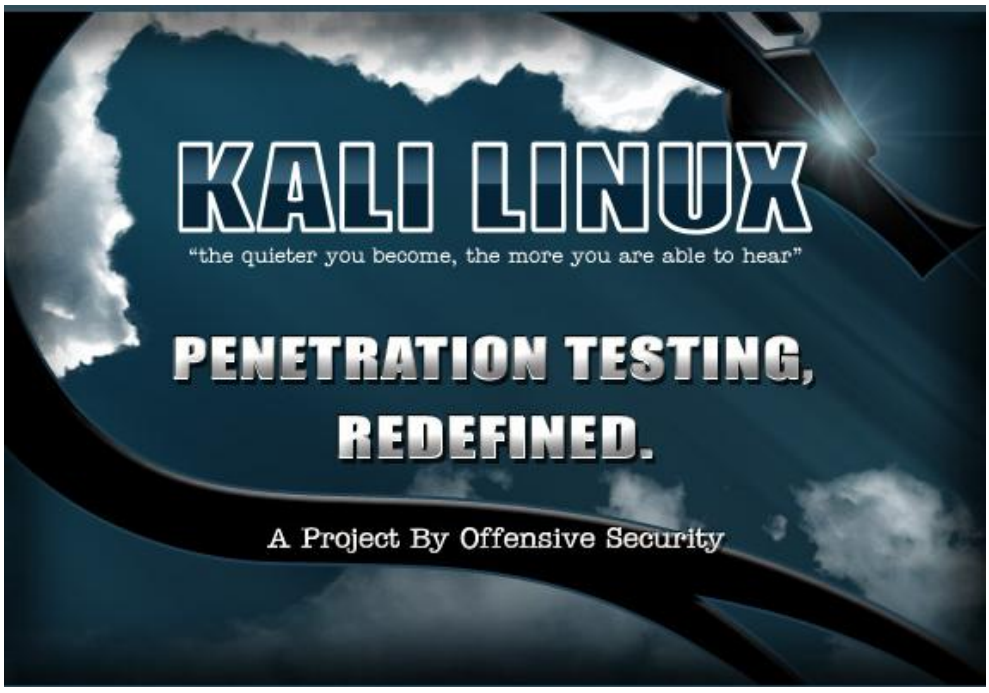
系统服务

小结

如果您之前使用过或者了解 BackTrack 系列 Linux 的话，那么我只需要简单的说，Kali 是 BackTrack 的升级换代产品，从 Kali 开始，BackTrack 将成为历史。

如果您没接触过 BackTrack 也没关系，我们从头开始了解 Kali Linux。

按照官方网站的定义，Kali Linux 是一个高级渗透测试和安全审计 Linux 发行版。作为使用者，我简单的把它理解为，一个特殊的 Linux 发行版，集成了精心挑选的渗透测试和安全审计的工具，供渗透测试和安全设计人员使用。也可称之为平台或者框架。



Kali Linux

作为 Linux 发行版，Kali Linux 是在 BackTrack Linux 的基础上，遵循 Debian 开发标准，进行了完全重建。并且设计成单用户登录，root 权限，默认禁用网络服务。

关于系统特性，定制，在不同设备上的安装，请在 Kali Linux 官网上查阅，http://www.kali.org/。官网上还有一份中文版的说明文档，但是我总觉得要么是自动翻译的，要么是外国人自行翻译的，读起来非常不通顺，但是仍然可作为参考，见 http://cn.docs.kali.org/。

中文文档

因为本书的核心内容是渗透测试，Kali Linux 只是平台，更多的关于系统本身的内容不会详细介绍。下面我们来看看 Kali 自带的工具集，介绍完这些工具，相信你也就了解了 Kali Linux 的功能。

上图是安装完 Kali Linux（在下一节，会简单介绍虚拟机下 Kali Linux 的安装和配置）系统自带的工具集。最顶层是十佳安全工具，这些工具都被包含在下面的工具分类中。

Kali Linux 将所带的工具集划分为十四个大类，这些大类中，很多工具是重复出现的，因为这些工具同时具有多种功能，比如 nmap 既 能作为信息搜集工具也能作为漏洞探测工具。其中大部分工具的使用，都会在之后的章节中做介绍和实例演示。另外，这里介绍的工具都是系统默认推荐的工具，我 们也可以自

行添加新的工具源，丰富工具集。根据笔者的经验，绝大多数情况下，系统推荐的工具已经足够使用了。一些专用工具，会在特定的测试场景下被引入， 在后续章节中会详细说明。

1.信息搜集

信息搜集工具集又分为 DNS 分析、IDS/IPS 识别、SMB 分析、SMTP 分析、SNMP 分析、SSL 分析、VoIP 分析、VPN 分析、存活主机识别、电话分析、服务指纹识别、流浪分析、路由分析、情报分析、系统指纹识别共 15 个小分类。

信息搜集工具分类

DNS 分析包含 dnsdict6、dnsenum 等 12 个工具，如下图。

Dns 分析工具

IDS/IPS 识别包含 fragrout、fragrouter、ftest、lbd、wafwOOf 四个工具。

IDS/IPS 识别工具

扩展---IDS/IPS

IDS(intrusion detection system),即入侵检测系统。是一种对网络传输进行即时监视 ,在发现可疑传输时发出警报或者采取主动反应措施的网络安全设备。它与其他网络安全设备的不同之处便在于 ,IDS 是一种积极主动的安全防护技术。

IPS（Intrusion Prevention System）即入侵防御系统。IPS 位于防火墙和网络的设备之间。这样，如果检测到攻击，IPS 会在这种攻击扩散到网络的其它地方之前阻止这个恶意的通信。

二者的区别：

入侵检测系统注重的是网络安全状况的监管。入侵防御系统关注的是对入侵行为的控制。

入侵检测系统需要部署在网络内部的中心点，需要能够观察到所有网络数据。入侵防御系统需要部署在网络的边界。

入侵检测系统的核心价值在于通过对全网信息的分析，了解信息系统的安全状况，进而指导信息系统安全建设目标以及安全策略的确立和调整，而入侵防御系统的核心价值在于安全策略的实施—对黑客行为的阻击;入侵检测系统需要部署在网络内部，监控范围可以覆盖整个子网，包括来自外部的数据以及内部终端之间传输的数据，入侵防御系统则必须部署在网络边界，抵御来自外部的入侵，对内部攻击行为无能为力。

参考：

http://security.zdnet.com.cn/security_zone/2009/0412/1362627.shtml

smb 分析包含如下工具：

smb 分析工具

扩展---smb 协议

MB 简介 SMB 是 Server Message Block 的简写 ,这个协议用于共享文件，共享打印机，共享串口等用途。我们之所以能够在 windows 的网络邻居下访问一个域内的其他机器，就是通过这个协议实现的。SMB 协议是一个很重要的协议，目前绝大多数的 PC 上都在运行这一协议，windows 系统都充当着 SMB 协议的客户端和服务器，所以 SMB 是一个遵循客户机服/务器模式的协议。SMB 服务器负责通过网络提供可用的共享资源给 SMB 客户机，服务器和客户机之间通过 TCP/IP 协议、或者 IPX 协议、或者是 NetBEUI 进行连接。

参考：http://msdn.microsoft.com/en-us/library/cc246231.aspx

smtp 分析包含如下工具:

smtp 分析工具

snmp 分析报告如下工具：

snmp 分析工具

SSL 分析包含如下工具：

ssl 分析工具

VoIP 分析包含如下工具：

VoIP 分析工具

扩展—VoIP 简介

VoIP 是 Voice over Internet Protocol 的缩写，指的是将模拟的声音讯号经过压缩与封包之后，以数据封包的形式在 IP 网络的环境进行语音讯号的传输，通俗来说也就是互联网电话、网络电话或者简称 IP 电话的意思。

参考资料：

https://www.cisco.com/application/pdf/en/us/guest/tech/tk587/c1506/ccmigration_09186a008012dd36.pdf

VPN 分析只包含一个工具：ike-scan

vpn 分析工具

存活主机识别包含的工具：

存活主机识别工具

服务器指纹识别包含如下工具：

服务器指纹识别工具

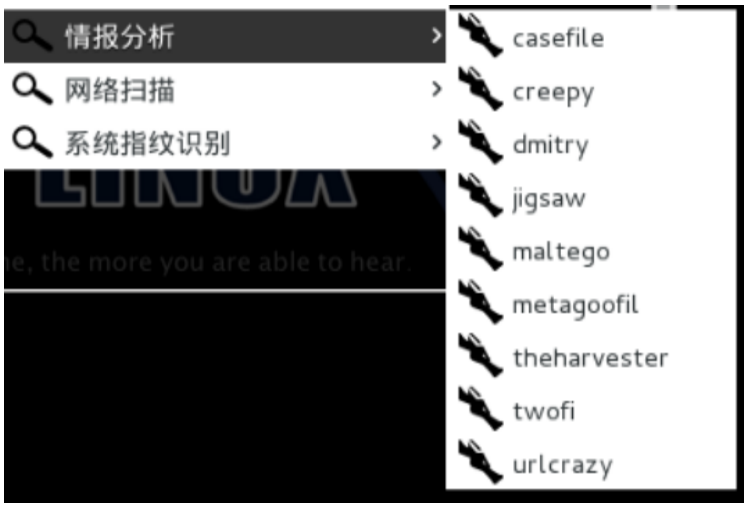
流量分析包含如下工具：

流量分析工具

路由分析包含如下工具：

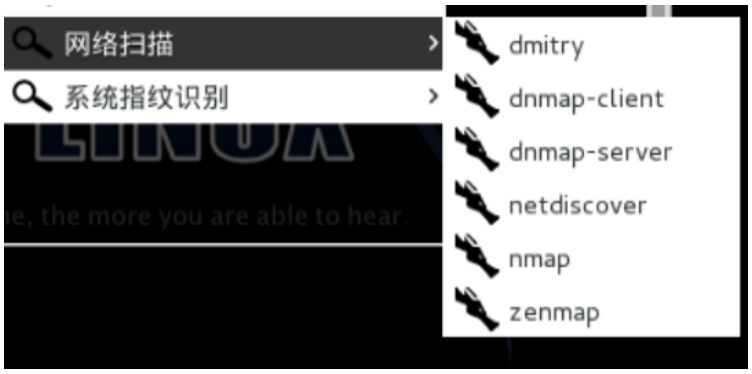
路由分析工具

情报分析包含如下工具：



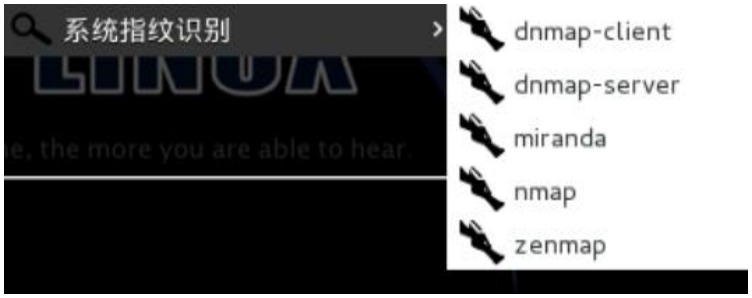
情报分析工具

网络包含如下工具：



网络扫描工具

系统指纹识别包含如下工具：



系统指纹识别工具

扩展—指纹识别：

在实际的生产环境中 ,应用程序返回的软件、服务器、操作系统的相关信息，很有可能是伪装过的。比如请求一台 apathe 服务器，如果它在 http 响应中返回的是 IIS 6.0 的信息，如果我们简单的认为它是 iis 服务器，并以此为依据继续接下来的渗透工作，岂不是南辕北辙？指纹识别技术应运而生，向测试对方发送特殊的请求，根据响应内容的不同来做出正确的识别，这种技术称之为指纹识别技术。常用的操作系统指纹识别技术为 IP 协议栈。

链接：http://nmap.org/book/osdetect-fingerprint-format.html 是 Nmap 操作系统指纹识别的基本原理

2.漏洞分析

漏洞分析工具集

漏洞分析工具集 ,共分为 6 个小类 ,分别为 Cisco 工具集、Fuzzing 工具集、OpenVAS、开源评估软件、扫描工具集、数据库评估软件。

Cisco 工具集包含如下工具：

Cisco 工具集

Fuzzing 工具集下包含如下工具：

fuzzing 工具集

扩展—Fuzzing

模糊测试 （fuzz testing, fuzzing）是一种软件测试技术。其核心思想是自动或半自动的生成随机数据输入到一个程序中，并监视程序异常，如崩溃，断言(assertion)失败，以发现可能的程序错误，比如内存泄漏。模糊测试常常用于检测软件或计算机系统的安全漏洞。

模糊测试工具主要分为两类，变异测试（mutation-based）以及生成测试（generation-based）。模糊测试可以被用作白盒，灰盒或黑盒测试。[3]文件格式与网络协议是最常见的测试目标，但任何程序输入都可以作为测试对象。常见的输入有环境变量，鼠标和键盘事件以及 API 调用序列。甚至一些通常不被考虑成输入的对象也可以被测试，比如数据库中的数据或共享内存。

参考：https://www.owasp.org/index.php/Fuzzing

OpenVAS 包含如下工具：

扩展—OpenVAS

OpenVAS 是一款开放式的漏洞评估工具，主要用来检测目标网络或主机的安全性。与安全焦点的 X-Scan 工具类似，OpenVAS 系统也采用了 Nessus 较早版本的一些开放插件。OpenVAS 能够基于 C/S(客户端/服务器),B/S(浏览器/服务器)架构进行工作，管理员通过浏览器或者专用客户端程序来下达扫描任务，服务器端负载授权，执行扫描操作并提供扫描结果。

参考：http://www.openvas.org/

开源评估软件包含如下工具：

开源评估软件工具

扫描工具集包含如下工具：

扫描工具

数据库评估软件包含如下工具：

数据库评估工具

3.Web 程序

Web 程序下主要包含 CMS 识别、IDS/IPS 识别、Web 漏洞扫描、Web 爬行、Web 应用代理、Web 应用漏洞挖掘、Web 库漏洞利用共 7 个类别。

web 程序工具集

4.密码攻击

密码攻击主要包括 GPU 工具集、Passing the Hash、离线攻击、在线攻击。

密码攻击工具集

扩展—Passing the Hash

Passing the Hash ,中文一般翻译为 Hash 传递攻击。在 windows 系统中，系统通常不会存储用户登录密码，而是存储密码的 Hash 值。在我们远程登录系统的时候，实际上向远程传输的就是密码的 Hash。当攻击者获取了存储在计算机上的用户名和密码的 hash 值 的时候，他虽然不知道密码值，但是仍然可以通过直接连接远程主机，通过传送密码的 hash 值来达到登录的目的。

5.无线攻击

无线攻击包含 RFID/NFC 工具集、Software Defined Radio、蓝牙工具集、其他无线工具、无线工具集。

扩展-- Software Defined Radio

软件无线电（Software Defined Radio，SDR）是一种实现无线通信的新概念和体制。一开始应用在军事领域，在 21 世纪初，由于众多公司的努力，使得它已从军事领域转向民用领域，成为经济的、应用广泛的、全球通信的第三代移动通信系统的战略基础。

由 于无线通信领域存在的一些问题，如多种通信体系并存，各种标准竞争激烈，频率资源紧张等，特别是无线个人通信系统的发展，使得新的系统层出不穷，产品生产 周期越来越短，原有的以硬件为主的无线通信体制难以适应这种局面，迫使软件无线电的概念的出现。它的出现，使无线通信的发展经历了由固定到移动，由模拟到 数字，由硬件到软件的三次变革。

参考：

http://zh.wikipedia.org/wiki/%E8%BD%AF%E4%BB%B6%E6%97%A0%E7%BA%BF%E7%94%B5

6.漏洞利用工具集

漏洞利用工具集，主要包含了几个流行的框架，和其他工具。

BeEF XSS Framework ,官方站点 http://beefproject.com/。全称 Browser Exploitation Framework，它是专注于 web 浏览器的渗透测试框架。

Metasploit，官方站点 http://www.metasploit.com/。著名的渗透测试框架，是渗透测试人员的必修课。

7.嗅探/欺骗

嗅探、欺骗 包含 VoIP、Web 嗅探、网络欺骗、网络嗅探、语言监控五个工具集。

嗅探、欺骗工具集

8.权限维持

权限维持包含 Tunnel 工具集、Web 后门、系统后门三个子类。

其中 Tunnel 工具集包含了一系列用于建立通信隧道、代理的工具。

9.逆向工程

逆向工程，包含了 Debug 工具集、反编译、其他逆向工具集三个子类。

10.压力测试

压力测试包含 VoIP 压力测试、Web 压力测试、网络压力测试、无线压力测试四个子类。

11.硬件 Hacking

硬件 Hacking 包括 Android 工具集、Arduino 工具集两个子类。

12.数字取证

数字取证工具集包含 PDF 取证工具集、反数字取证、密码取证工具集、内存取证工具集、取证分割工具集、取证分析工具集、取证哈希验证工具集、取证镜像工具集、杀毒取证工具集、数字取证、数字取证套件。

13.报告工具集

报告工具集，主要用于生成、读取、整理渗透测试报告的工具，包含 Domentation、媒体捕捉、证据管理。

14.系统服务

系统服务是系统上的服务程序，包括 BeFF、Dradis、HTTP、Metasploit、MySQL、OpenVas、SSH。

默认情况下，网络和数据库服务是关闭的，需要重新开启。

15.小结

上面对 Kali Linux 的默认工具集进行的了大致的浏览，由于本书只关注于渗透测试，对逆向工程、压力测试、硬件 Hacking、数字取证这些工具不会涉及。

下一节介绍虚拟机下的系统安装和简单配置。