Kali

安全渗透测试实践教程

张宝军　潘瑞芳　俞承杭　俞　斌

编　著

现代教育出版社
Modern Education Press

Kali安全渗透测试实践教程

张宝军　潘瑞芳　俞承杭　俞　斌
编　著

现代教育出版社
Modern Education Press

图书在版编目（CIP）数据

Kali 安全渗透测试实践教程 / 张宝军等编著 . —北京：现代教育出版社，2018.12

ISBN 978-7-5106-6659-9

Ⅰ. ① K… Ⅱ. ①张… Ⅲ. ① Linux 操作系统—安全技术—教材 Ⅳ. ① TP316.85

中国版本图书馆 CIP 数据核字（2018）第 236620 号

Kali 安全渗透测试实践教程

策　　划　刘　媛

编　　著　张宝军　潘瑞芳　俞承杭　俞　斌

责任编辑　刘小华

封面设计　贝壳学术

出版发行　现代教育出版社

地　　址　北京市朝阳区安华里 504 号 E 座

邮　　编　100011

电　　话　010-64246373（编辑部）　010-64256130（发行部）

印　　刷　天津雅泽印刷有限公司

开　　本　710mm × 1000mm　1/16

印　　张　18

字　　数　332 千字

版　　次　2019 年 4 月第 1 版

印　　次　2019 年 4 月第 1 次印刷

书　　号　ISBN 978-7-5106-6659-9

定　　价　72.00 元

内容简介

安全渗透测试是网络空间安全领域一项非常重要的应用，更是该学科专业人才需要掌握的一项重要技能。本书基于流行的 Kali Linux 系统，全面展现了渗透测试的各种核心技术，涉及渗透测试的基础知识、操作系统、网络协议和社会工程学等诸多领域，并结合一些常用的安全工具，以直观的形式由表及里地展示了网络渗透的奥秘。全书遵循渗透测试的基本流程，重点介绍了渗透测试的相关环节及其技术，注重操作，避免纯理论讲解，让读者可以轻松掌握渗透测试的实施方法。

前　言

网络空间安全在我国已经上升到国家安全战略的高度，并在2015年成为工学门类下的一级学科，足见国家对网络空间安全的重视。而网络空间安全又是一门理论和实践结合十分紧密的学科，将理论用于实践，应用相关的安全知识去解决实际的安全问题十分重要。安全渗透测试是网络空间安全领域一项非常重要的应用，更是该学科专业人才需要掌握的一项重要技能。然而在实际的网络安全教学中，适用于本科教育的安全渗透测试教学实践很少，与实践配套的指导教材更少。考虑到学科建设的需要和当前缺乏好的实践教材的问题，我们决定基于当前流行的Kali和主流靶机系统，结合实际教学的需要，对Kali和靶机系统功能进行梳理，编撰一本适用于网络空间安全本科教学的安全渗透测试实践指导教材。

本教材的主要内容涵盖安全渗透测试的一个完整的生命周期，并对一些常见的安全渗透方法进行介绍，提供详尽的实践操作，教材包括Kali与靶机系统介绍、常用工具介绍、信息收集、漏洞扫描、漏洞利用、密码攻击、权限提升、Web渗透、无线网络渗透等基本内容。本教材力求做到理论和实践相结合，在理论上从漏洞介绍、分析、利用、防范、评估等角度对一些常见漏洞进行剖析，在实践上本教材中的每个实践环节、操作步骤都将在平台上进行严格的测试，经过实践的检验，保证结果的真实可靠。最后，希望本教材能够帮助网络空间安全专业的学生更好地去掌握网络安全渗透测试这门专业技能。

本教材的学习要求学生具备计算机网络、TCP/IP协议分析、网络安全技术相关知识，至少掌握一门程序设计语言，熟悉Windows和Linux操作系统的使用。本教材适合网络安全相关专业高年级的学生，可作为其实践教程，或者是网络安全课程的实验指导教程。

张宝军

2018年9月7日于浙传

目 录

第1章　Kali与靶机系统

本章主要介绍 Kali 系统和用于渗透测试的靶机系统，内容包括 Kali 的发展过程、Kali 的功能、Kali 系统的安装和基本设置，以及目前流行的几种靶机系统介绍。

1.1 Kali 简介

信息安全是一门实践性很强的学科，对从事信息安全学习、工作和研究的人员来说，要真正掌握信息安全技术，成为相关领域的专家，除具备扎实的理论基础外，进行大量的信息安全实践是必不可少的，其中就包括各种安全工具的使用。

然而，随着信息技术的发展，信息安全问题日益严重，各种安全工具层出不穷，版本繁多，呈现种类多、数量大、更新快的特点。这些安全工具的甄别、获取本身就给从事信息安全的人员制造了不小的麻烦。“工欲善其事，必先利其器”，如果有这样一个系统，它能够囊括几乎所有常用的安全工具并能够自动升级就好了，这就是 Kali。当然，Kali 不只如此。那么 Kali 到底是什么？让我们通过这本教材逐渐揭开 Kali 的神秘面纱，并利用 Kali 做些有用的事情。

Kali 首先是一个操作系统，更确切地说它是一个基于 Linux Kernel 的操作系统，该系统从 BackTrack 发展而来。而 BackTrack（简称 BT）是 2006 年由 Remote-Exploits.com 推出的一个用于渗透测试及黑客攻防的专用平台，基于 Knoppix（Linux 的一个发行版）开发。BackTrack 从 2006 年的起始版本 BackTrack v.1.0 Beta 开始，到 2012 年推出最终版本 BackTrack 5 R3 release。之后，2013 年 Offensive Security 的 Mati Aharoni 和 Devon Kearns 基于 Debian（Linux 的一个发行版）重新实现了 BackTrack，新的产品命名为 Kali，从此 Kali 成为 BackTrack 的替代者和后继者，而不再提供对 BackTrack 的维护。

Kali 设计的最初目标是一个用于数字取证的操作系统，预装了很多与安全相关的软件，或者说集成了很多黑客工具，几乎囊括了信息安全工具的各个类型，为从事信息安全领域工作的人员提供了极大的便利，避免了寻找、下载、

安装、维护安全工具的烦恼。当然，信息安全工具那么多，一些新的工具层出不穷、推陈出新，Kali 不可能全部囊括，但是作为一个操作系统，用户可以自由方便地安装新的工具，或者从 Kali 众多的安全工具中找到类似的工具作为替代。

Kali 具有以下几个主要特性：① Kali 是一个基于 Debian 的 Linux 发行版；② Kali 预装了大量安全工具；③ Kali 是永久免费的；④ Kali 支持大量的无线设备；⑤ Kali 系统自身是安全的。

目前，Kali 最新的版本是 Kali Linux 2018.2[1]，于 2018 年发布，该版本与之前的版本相比较，最大的改进是具有一个更新的 Linux 内核和添加了两个新的安全特性。

在 Linux 内核方面，Kali Linux 2018.2 采用了全新的 Linux Kernel 4.15 内核，该内核有两个新的特性非常重要。① AMD 安全内存加密支持：对最新的 AMD 处理器提供了安全内存加密功能，实现了 DRAM 的自动加密和解密。该功能使得 Kali 系统更加安全，在理论上避免了遭受冷启动的攻击。因为对内存加了密，即使通过物理方式直接访问内存，也无法读取存储的内容。②增加了内存的限制：内存对系统性能的影响很大，在不断增长的系统功能应用面前，内存往往捉襟见肘。之前的 Linux 内核最多只能支持 64TB 的物理地址空间，虚拟地址空间为 256TB。对于普通用户这已经足够使用，但是对于一些高端的服务器产品，64TB 的内存已经远远不能满足需要。目前最新的处理器将启用 5 级分页技术，能够支持 4PB 的物理内存和 128PB 的虚拟内存，而在 Linux Kernel 4.15 内核中提供了对这一处理器技术功能的支持。

在安全性方面，Kali Linux 2018.2 系统做了两个重要的更新。①软件包更新：Kali 更新了一些重要的软件包，包括 Zaproxy，Secure-Socket-Funneling，Pixiewps，Seclists，Burpsuite，Dbeaver 和 Reaver，去除了 Bug，弥补了漏洞，更新了功能。②Hyper-V 更新：目前 Hyper-V 虚拟机已经是第 2 代，提供了对“统一的可扩展固件接口”（Unified Extensible Firmware Interface，UEFI）的支持，对于那些使用 Hyper-V 运行由 Offensive Security 提供的 Kali 虚拟机的用户，Kali Linux 2018.2 系统提供了以下功能：支持扩展 / 缩小硬盘；Hyper-V 集成服务；支持动态内存；网络监视 / 扩展和复制。

鉴于 Kali Linux 2018.2 的特性，本教程将基于 Kali Linux 2018.2 来讲解，所有的实践都在 Kali Linux 2018.2 平台上进行。

1.2 Kali 的功能

Kali 是一个面向安全的基于 Debian 的 Linux 发行版，预装了大量的安全软

件。其主要功能有以下三个：数字取证、安全审计、渗透测试。

1. 数字取证[2]

数字取证主要是针对各种电子证据进行识别、收集、保存和分析，用来发现网络和系统的各种入侵行为，为进一步的安全处理提供依据。数字取证处理的对象是电子证据，是指以存储的电子化信息资料来证明案件真实情况的电子物品或电子记录。数字取证往往涉及与数字产品相关的犯罪或过失行为，是目前公安机关应对新型计算机和网络犯罪的一种重要手段。Kali系统提供的数字取证工具很多，可分为数据备份、数据恢复、数据分析和文件取证四种类型，比如：数字备份工具Dc3dd，磁盘备份工具Dcfldd，Linux硬盘数据恢复工具dd_rescue，磁盘数据恢复工具Safecopy，文件还原工具Foremost，日志文件系统块查看工具jcat，磁盘镜像分析工具TSK，信息批量提取工具bulk-extractor，磁盘取证工具Guymager等。

2. 安全审计[3]

安全审计是由“专业审计人员根据有关的法律法规、财产所有者的委托和管理当局的授权，对计算机网络环境下的有关活动或行为进行系统的、独立的检查验证，并做出相应评价”。安全审计是通过测试公司信息系统对一套确定标准的符合程度来评估其安全性的系统方法。安全审计涉及四个基本要素：控制目标、安全漏洞、控制措施和控制测试。Kali系统提供的安全审计工具有：安全漏洞审计工具Lynis，无线安全审计工具FruityWifi，Web应用程序安全审计工具箱Watobo等。

3. 渗透测试[4]

渗透测试是Kali系统最主要的功能，它是通过模拟恶意黑客的攻击方法，来评估计算机网络系统安全的一种评估方法。这个过程包括对系统弱点、技术缺陷或漏洞的主动分析，是根据已知可利用的安全漏洞，去发现是否存在的安全问题，注重的是安全漏洞的严重性。渗透测试可分为黑盒测试、白盒测试和灰盒测试三种方式[5]。其中黑盒测试是在对基础设施不知情的情况下进行测试；白盒测试是在完整了解结构的情况下进行测试；灰盒测试则介于黑盒测试与白盒测试之间，是较为隐秘地进行测试。渗透测试有两个主要的特点：首先，渗透测试是一个渐进的并且逐步深入的过程；其次，渗透测试是选择不影响业务系统正常运行的攻击方法进行的测试。渗透测试包括信息收集、漏洞扫描、漏洞利用、密码攻击、权限提升，以及针对特定应用或平台的渗透，如Web渗透、无线网络渗透等。Kali系统提供的渗透测试工具涵盖以上各个方面，主要有：用于信息收集的Nmap，Dnsenum，Amap，Webscrab，Recon-NG等；用于漏洞扫描的Nessus，OpenVAS；用于漏洞利用的Metasploit，w3af；用于

密码攻击的 Hydra，Medusa，Ettercap，Msfconsole，Samdump2，DirBuster，WebSlayer 等；用于权限提升的 Meterpreter，SET；用于 Web 渗透的 BeEF，BURP，OWASP，Fimap，Scapy，TCPReplay，SniffJoke 等；用于无线网络渗透的 Kismet，Aircrack-Ng，Gerix Wifi Cracker，Wifite，Easy-Creds，Arpspoof 等。

本教程的学习目标聚焦在渗透测试上，重点学习渗透测试各个环节工具的使用，并以 Web 和无线网络这两个重要应用为案例，讲解进行安全渗透测试的方法和过程。

1.3 Kali 安装

Kali 是免费的，用户可在 Kali 官方网站上自由下载 Kali 系统，其下载地址如下：https://www.kali.org/downloads/。打开网址如图 1-1 所示：

图1-1　Kali下载网站

从图 1-1 可以看到 Kali 提供了 64 位和 32 位系统，并且提供了针对 VMware，Vbox 和 Hyper-V 三种虚拟机平台的虚拟机镜像系统，极大地方便了系统的安装，用户只需在虚拟机中导入相应的镜像文件就可以使用 Kali 系统。点击虚拟机镜像文件下载的链接，可以进入以下页面，如图 1-2 所示：

Kali Linux VMware Images　Kali Linux VirtualBox Images　Kali Linux Hyper-V Images

Image Name	Torrent	Size	Version	SHA256Sum
Kali Linux Vm 32 Bit [Zip]	Torrent	3.0G	2018.2	73a79b8deaba5ba6c072621528700e104ed46cfce32ca18c402562190fd765a7
Kali Linux Vm 32 Bit [OVA]	Torrent	3.5G	2018.2	24764727b625d53ca456de65bb01a8364aaf0c8044f5948dc97a1166551911f24
Kali Linux Vm 64 Bit [Zip]	Torrent	3.0G	2018.2	4c99418c8e1abfe2c924e0a5f5bb9464637ad8b49ff79a92ef7aa7540e302368
Kali Linux Vm 64 Bit [OVA]	Torrent	3.4G	2018.2	4160fd2fafc1deb51af79e76e4674fc6bce356c4605e06da8b10e59dc971b5e6

图1-2　Kali虚拟机镜像文件下载页面

这里可以分别下载VMware，Vbox和Hyper-V的虚拟机镜像文件，有OVA和ZIP两种格式，32位和64位系统。下载完Kali系统镜像文件后可以用SHA256Sum散列值验证一下，防止文件下载的过程中出现损坏。

Kali系统的安装有以下几种方式[4]：

1. 安装至硬盘

将操作系统直接安装在硬盘上是最为常见的安装方式。优点是运行速度快，不需要使用其他介质，缺点则是安装起来较为复杂，对于一些本来就有操作系统（比如Windows系统）的计算机来说，涉及双系统甚至多系统的安装，需要对硬盘分区进行规划，避免系统覆盖和冲突，另外在运行时需要通过重启系统的方式在多个系统之间切换。Kali 2018.2的安装对硬件要求如下：处理器不小于2GHz，硬盘不小于20G，内存不小于4G，操作系统推荐采用64位，要对无线网络进行渗透测试需要有无线网卡。Kali系统安装到硬盘的过程相关的介绍很多，按照安装向导一步步执行操作即可，这里不再赘述。

2. 安装至U盘

Kali也可以直接安装在U盘上，优点是便于携带，启动系统时更改BIOS设置，将系统启动顺序设置为U盘优先启动即可，类似于WinPE U盘版的概念；缺点是运行速度比硬盘版慢一些，大家知道U盘的访问速度比硬盘要慢。将Kali 2018.2安装在U盘，要求USB 3.0接口（USB 2.0速度会很慢），U盘容量不小于20G。将Kali安装到U盘可参考文献[6]，注意对U盘容量的要求，不同的Kali镜像文件版本，需求的容量不一样，U盘尽量越大越好。

3. 安装至树莓派

树莓派（Raspberry Pi, RPi）是一个为计算机编程教育而设计，只有信用卡大小的微型电脑，其系统基于Linux。它是一款基于ARM的微型电脑主板，以SD/MicroSD卡为内存硬盘，卡片主板周围有1/2/4个USB接口和一个

10/100 以太网接口（A 型没有网口），可连接键盘、鼠标和网线，同时拥有视频模拟信号的电视输出接口和 HDMI 高清视频输出接口，以上部件全部整合在一张仅比信用卡稍大的主板上，具备所有 PC 的基本功能，只需接通电视机和键盘，就能执行如电子表格、文字处理、玩游戏、播放高清视频等诸多功能[7]。随着 Windows 10 IoT 的发布，也将可以用上运行 Windows 的树莓派。安装至树莓派请参考文献[4]。

4. 安装至虚拟机

随着计算机性能的整体提升，虚拟机的应用越来越广泛，它使得在多个不同类型的操作系统之间随意地切换成为可能。需要运行什么操作系统，只需加载相应的操作系统镜像文件即可。而虚拟机镜像文件是可以随意拷贝的。操作系统虚拟机镜像文件的制作也非常便捷，并且即使出错也可以推倒重来，避免了直接安装到硬盘可能导致的系统损伤和崩溃。目前可供选择的虚拟机软件主要有 VMware，VirtualBox，Hyper-V 等，采用这些虚拟机软件，可以像在硬盘上安装操作系统一样将操作系统安装到虚拟机上，制作出相应的虚拟机镜像文件，其过程与安装到硬盘类似。对于 Kali 2018.2 来说，最好为虚拟机预留 20G 磁盘空间，2G 以上内存。

以上四种安装方式各有千秋和应用场合，用户可根据自己实际应用需求来选择。针对 VMware，VirtualBox，Hyper-V 三种不同类型的虚拟机应用软件，Kali 官网上提供有现成的 Kali 虚拟机镜像文件供用户下载使用，本教程采用的是 64 位 Kali VMware 虚拟机镜像文件 kali-linux-2018.2-vm-amd64.zip。

1.4 Kali 设置

Kali 系统的登录账号和密码是缺省的，账号为 root，密码为 toor，用户可以自行修改。登录界面如图 1-3 所示：

图1-3　Kali登录界面

安装并登录 Kali 系统后，需要做一些常规的设置，开启一些服务，使得 Kali 系统能够正常工作。基于 VMware 的 Kali 虚拟机系统在使用之前需要做以下设置。

1.4.1 网络设置

网络设置分为有线网络设置和无线网络设置两部分，当需要对无线网络进行渗透测试时，要设置无线网络。

1. 有线网络设置

VMware 虚拟机连接有线网络的模式有三种：桥接模式（Bridged）、NAT 模式和仅主机模式（Host-Only 模式）。当安装完 VMware WorkStation，它会自动为我们生成两块虚拟网卡，分别是 vmnet1 和 vmnet8，其中 vmnet1 对应于仅主机模式，vmnet8 对应于 NAT 模式。在 Windows 系统命令行下输入 ipconfig 命令，可看到图 1-4 所示的虚拟网卡信息。

```
以太网适配器 VMware Network Adapter VMnet1:

   连接特定的 DNS 后缀 . . . . . . . :
   本地链接 IPv6 地址. . . . . . . . : fe80::a034:3985:4bf6:20d5%9
   自动配置 IPv4 地址 . . . . . . . . : 169.254.32.213
   子网掩码 . . . . . . . . . . . . : 255.255.0.0
   默认网关. . . . . . . . . . . . . :

以太网适配器 VMware Network Adapter VMnet8:

   连接特定的 DNS 后缀 . . . . . . . :
   本地链接 IPv6 地址. . . . . . . . : fe80::c849:525d:56bc:9411%20
   IPv4 地址 . . . . . . . . . . . . : 192.168.137.1
   子网掩码 . . . . . . . . . . . . : 255.255.255.0
   默认网关. . . . . . . . . . . . . :
```

图1-4　VMware虚拟网卡信息

在 VMware 应用软件中打开“编辑”->“虚拟网络编辑器”，可看到如图 1-5 所示虚拟网卡名称及对应类型信息。

虚拟网络编辑器

名称	类型	外部连接	主机连接	DHCP	子网地址
VMnet1	仅主机模式	-	已连接	已启用	192.168.121.0
VMnet8	NAT 模式	NAT 模式	已连接	已启用	192.168.137.0

图1-5　虚拟网络编辑器

（1）桥接模式

在桥接模式下，虚拟机与物理机可看成通过一个虚拟交换机（VMnet0）

相连，两台机器处于同一网段，采用两个不同的 IP 地址（网络号相同，主机号不同）。物理机能够访问外网，虚拟机通过虚拟交换机与物理机连接，同样可以通过物理机访问外网。桥接模式最为简单方便，一般情况下，如果用户想利用 VMWare 在局域网内新建一个服务器，为局域网用户提供 Web 或网络服务，就可以选择桥接模式。

桥接模式的设置过程如下：启动虚拟机进入系统后，在虚拟机右下角任务栏中右键单击有线网络设置图标，在弹出菜单中点击“设置”命令，如图 1-6 所示：

图1-6　VMware虚拟机有线网络设置

在弹出对话框中选择“桥接模式”单选按钮，如图 1-7 所示：

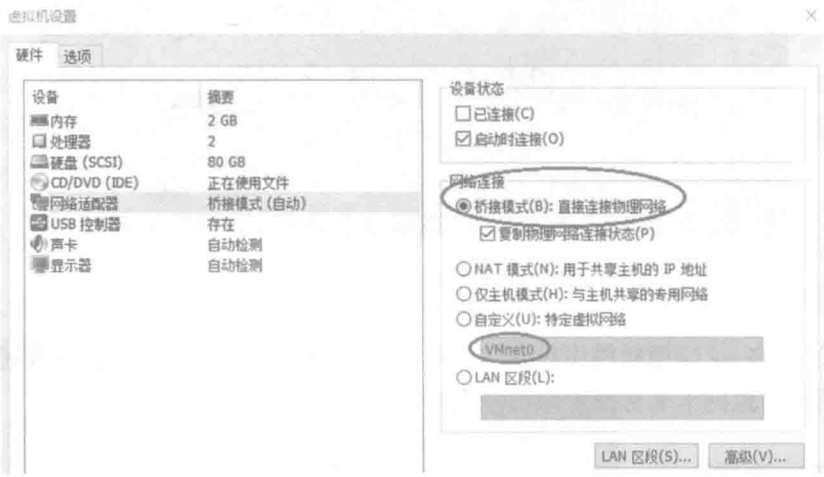

图1-7　桥接模式配置

从图 1-7 可看到虚拟机在桥接模式下默认采用的虚拟网络是 VMnet0，这是一个虚拟交换机，物理机和虚拟机都连接在这个虚拟交换机上。图中“复制物理网络连接状态”是可选项，用于复制物理机的网络连接状态，勾选此项时，当物理机的网络连接断开时，虚拟机也显示为断开状态。

设置好桥接模式后，右键单击有线网络连接图标，在弹出菜单中点击“连

接”命令，打开网络连接，如图 1-8 所示：

图1-8　启动网络连接

此时在 Kali 虚拟机中可看到网络连接的图标已处于连接状态，如图 1-9 所示：

图1-9　Kali虚拟机中网络连接状态

此时虚拟机是否能够上网，可通过查看虚拟机的 IP 地址分配以及 Ping 物理机的网关来确定。在 Kali 虚拟机中打开终端（Terminal），执行 ifconfig 命令，查看 Kali 虚拟机 IP 地址，如图 1-10 所示：

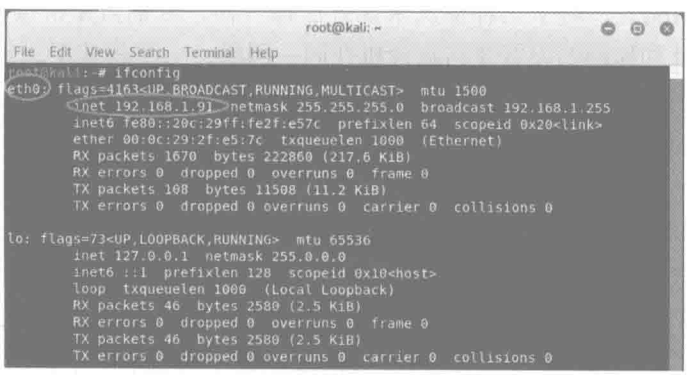

图1-10　查看Kali虚拟机IP地址