信息安全
技术大讲堂

从实践中学习
Kali Linux
网络扫描

大学霸IT达人◎编著

从理论、应用和实践三个维度讲解网络扫描的相关知识
通过128个操作实例手把手带领读者从实践中学习网络扫描
从协议工作原理到应用方式，再到扫描策略，逐步讲解

机械工业出版社
China Machine Press

信息安全
技术大讲堂

从实践中学习
Kali Linux
网络扫描

大学霸IT达人◎编著

机械工业出版社
China Machine Press

图书在版编目（CIP）数据

从实践中学习Kali Linux网络扫描/大学霸IT达人编著. —北京：机械工业出版社，2019.7

（信息安全技术大讲堂）

ISBN 978-7-111-63036-4

Ⅰ. 从… Ⅱ. 大… Ⅲ. Linux操作系统－安全技术 Ⅳ. TP316.85

中国版本图书馆CIP数据核字（2019）第126611号

从实践中学习 Kali Linux 网络扫描

出版发行：机械工业出版社（北京市西城区百万庄大街 22 号 邮政编码：100037）

责任编辑：欧振旭 李华君 责任校对：姚志娟

印 刷：中国电影出版社印刷厂 版 次：2019 年 7 月第 1 版第 1 次印刷

开 本：186mm×240mm 1/16 印 张：15.5

书 号：ISBN 978-7-111-63036-4 定 价：69.00 元

凡购本书，如有缺页、倒页、脱页，由本社发行部调换

客服热线：（010）88379426 88361066 投稿热线：（010）88379604

购书热线：（010）68326294 读者信箱：hzit@hzbook.com

前言

网络扫描是发现网络和了解网络环境的一种技术手段。借助网络扫描，我们可以探测网络规模，寻找活跃主机，然后对主机进行侦查，以便了解主机开放的端口情况。基于这些信息，可以判断该主机的操作系统和运行服务等信息。

本书详细讲解了网络扫描涉及的各项理论知识和技术。书中首先从理论层面帮助读者明确扫描的目的和方式，然后从基本协议的角度讲解了通用的扫描技术，最后过渡到特定类型网络环境的专有扫描技术。在先期扫描完成后，本书继续深入讲解了如何借助响应内容识别目标，并对常见的服务给出了扫描建议。在最后的相关章节，本书详细讲解了高效的数据整理和分析方式。

本书特色

1. 内容实用，可操作性强

在实际应用中，网络扫描是一项操作性极强的技术。本书将秉承这个特点，合理安排内容，从第 1 章开始就详细地讲解了扫描环境的搭建和靶机建立。在后续的章节中，将对每个扫描技术都配以操作实例，以带领读者动手练习。

2. 充分讲解网络扫描的相关流程

网络扫描的基本流程包括探测主机存活、端口/服务发现、目标识别。同时，作为渗透测试的一个环节，往往还要进行后续的信息整理和分析。本书将详解这四个流程，手把手带领读者完成网络扫描的相关任务。

3. 由浅入深，容易上手

本书充分考虑到了初学者的情况，首先从概念讲起，帮助他们明确网络扫描的目的和基本扫描思路；然后详细讲解了如何准备实验环境，例如需要用到的软件环境、靶机和网络环境。这样可以让读者更快上手，理解网络扫描的作用。

4. 环环相扣，逐步讲解

网络扫描是一个理论、应用和实践三者紧密结合的技术。任何一个有效的扫描策略都由对应的理论衍生应用，并结合实际情况而产生。本书遵循这个规律，从协议工作机制开

始讲解，然后依次讲解应用方式，最后结合实例给出扫描策略。

5. 提供完善的技术支持和售后服务

本书提供了 QQ 交流群（343867787）供读者交流和讨论学习中遇到的各种问题，另外还提供了服务邮箱 hzbook2017@163.com。读者在阅读本书的过程中若有疑问，可以通过 QQ 群或邮箱来获得帮助。

本书内容

第 1 章网络扫描概述，主要介绍了网络扫描的基本概念和学习环境的准备，如网络扫描的目的、扫描方式、配置靶机、配置网络环境及法律边界等问题。

第 2 章扫描基础技术，主要介绍了常见的通用扫描技术，以及这些技术所依赖的理论基础，这些技术包括 ICMP 扫描、TCP 扫描、UDP 扫描和 IP 扫描。

第 3~5 章主要介绍了特定网络的专有扫描技术，主要包括局域网扫描、无线网络扫描和广域网扫描技术。例如，局域网支持 ARP 扫描和 DHCP 扫描；无线网络支持无线监听方式，以实现网络扫描。

第 6 章目标识别，主要介绍了当发现主机时，如何通过指纹信息识别系统和服务的版本。同时，还介绍了通过 SNMP 和 SMB 这两种服务分析目标信息的方法。

第 7 章常见服务扫描策略，主要介绍了 7 大类共 27 种常见服务的判断和版本识别方法，如网络基础服务、文件共享服务、Web 服务、数据库服务和远程登录服务等。

第 8 章信息整理及分析，主要介绍了网络扫描后数据的整理和分析方式。本章简要讲解了如何使用 Maltego 以思维导图的形式归纳数据，并拓展、延伸出新的信息。

附录 A 特殊扫描方式，介绍了 FTP 弹跳扫描和僵尸扫描两种特殊扫描方式。

附录 B 相关 API，介绍了用户在安装某个第三方 Transform 时，需要使用的 API Key。

本书配套资源获取方式

本书涉及的工具和软件需要读者自行下载，下载途径有以下几种：

- 根据图书中对应章节给出的网址自行下载；
- 加入技术讨论 QQ 群（343867787）获取；
- 登录华章公司网站 www.hzbook.com，在该网站上搜索到本书，然后单击“资料下载”按钮，即可在页面上找到“配书资源”下载链接。

本书内容更新文档获取方式

为了让本书内容紧跟技术的发展和软件更新，我们会对书中的相关内容进行不定斯更

新，并发布对应的电子文档。需要的读者可以加入 QQ 交流群（343867787）获取，也可以通过华章公司网站上的本书配套资源链接下载。

本书读者对象

- 渗透测试技术人员；
- 网络安全和维护人员；
- 信息安全技术爱好者；
- 计算机安全技术自学者；
- 高校相关专业的学生；
- 专业培训机构的学员。

本书阅读建议

- Kali Linux 内置了 Nmap 和 Maltego 等工具，使用该系统的读者可以跳过第 1.3.1 节、8.1.1 节和 8.1.2 节的内容。
- 学习阶段建议多使用靶机进行练习，以避免因为错误操作而影响实际的网络环境。
- 由于安全工具经常会更新、增补不同的功能，因此建议读者定期更新工具，以获取更稳定和更强大的环境。

本书作者

本书由大学霸 IT 达人技术团队编写。感谢在本书编写和出版过程中给予我们大量帮助的各位编辑！

由于作者水平所限，加之写作时间较为仓促，书中可能还存在一些疏漏和不足之处，敬请各位读者批评指正。

编著者

目录

第 1 章　网络扫描概述

随着互联网络的飞速发展，网络入侵行为日益严重，网络安全已成为人们的关注点。在实施渗透测试过程中，网络扫描是收集目标系统信息的重要技术之一。通过实施网络扫描，可以发现一个网络中活动的主机、开放的端口及对应服务等。本章将介绍网络扫描的目的和方式。

1.1　扫 描 目 的

通过网络扫描，用户能够发现网络中活动的主机和主机上开放的端口，进而判断出目标主机开放的服务。然后通过对服务的扫描，还可以获取到目标主机的操作系统类型、服务欢迎信息和版本等信息。本节将介绍网络扫描的目的。

1.1.1　发现主机

通过对一个网络中的主机实施扫描，即可发现该网络中活动的主机。当发现网络中活动的主机后，用户就可以在扫描时重新规划扫描范围，而不需要对所有主机进行扫描，这样将会节约大量的时间和资源，而且扫描的结果更精确。这样用户可以针对活动主机做进一步扫描，以探测开放的端口，进而推断出开放的服务信息等。

1.1.2　探测端口

当用户扫描到网络中活动的主机后，即可探测该活动主机中开放的所有端口。这里的端口指的不是物理意义上的端口，而是特指 TCP/IP 协议中的端口，它是逻辑意义上的端口。在 TCP/IP 协议中，最常用的协议是 TCP 和 UDP 协议，由于这两个协议是独立的，因此各自的端口号也相互独立。例如，TCP 有 235 端口，UDP 也可以有 235 端口，且两者并不冲突。

在 TCP/IP 协议中的端口，可以根据它们的用途进行分类。因此下面将介绍一下端口的类型，以方便用户判断端口所对应的程序。

1. 周知端口（Well Known Ports）

周知端口是众所周知的端口号，范围为 0～1023。例如，WWW 服务默认端口为 80，FTP 服务默认端口为 21 等。不过，用户也可以为这些网络服务指定其他端口号，但是有些系统协议使用固定的端口号，是不能被改变的。例如，139 端口专门用于 NetBIOS 与 TCP/IP 之间的通信，不能手动改变。

2. 动态端口（Dynamic Ports）

动态端口的范围是 49152～65535。之所以称为动态端口，是因为它们一般不固定分配某种服务，而是根据程序申请，系统自动进行动态分配。

3. 注册端口

1024～49151 端口，是用来分配给用户进程或应用程序的。这些进程主要是用户所安装的一些应用程序，而不是已经分配好了公认端口的常用程序。这些端口在没有被服务器资源占用的时候，可以供用户端动态选用。

1.1.3 判断服务

在计算机网络中，每个服务默认都有对应的端口。例如，FTP 服务默认端口为 21，SSH 服务默认端口为 22，HTTP 服务默认端口为 80 等。所以，如果用户探测出目标主机开放的端口后，即可判断出对应的服务了。为了帮助用户能够快速地判断出开放端口所对应的服务，这里将以表格形式列出一些常见的服务及其对应端口，如表 1.1 所示。

表 1.1 常见的TCP端口号及服务

端 口	服 务	协 议	说 明
20、21	FTP	TCP	FTP为档案传输协议。20/TCP是FTP Data使用；21/TCP是FTP Control使用
22	SSH	TCP	Secure Shell（SSH）是一种较安全的远程连接协议
23	Telnet	TCP	Telnet为远程签入协议，如BBS
25	SMTP	TCP	Simple Mail Transfer Protocol（SMTP）是Internet的信件传送协议，用于不同邮件服务器间或使用者到服务器间数据传输

（续）

端 口	服　　务	协　　议	说　　明
53	DNS	TCP、UDP	DNS服务器的名称查询
80	HTTP	TCP	World Wide Web Service
88	Kerberos	TCP、UDP	网络账号验证协议
110	POP3	TCP	收信软件（Client端）协议
119	NNTP	TCP	Usenet新闻讨论群组协议，即News服务器使用的网络通信协议
135	RPC	RPC	网络上Windows平台计算机网络服务彼此间沟通用的协议。例如，邮件客户端连到Exchange Server时，先透过port 135建立RPC连接，接着再使用port 1024以上某个动态范围的port进行数据传输
137	NetBIOS Name Server	TCP、UDP	WINS Server就是NetBIOS Name Server，透过WINS Server做名称解析得知网络主机的IP地址
138	NetBIOS Datagram	UDP	是NetBIOS over TCP/IP的一部分，用于网络登入（NetLogon）及网络浏览（Browsing）功能。例如，网上邻居的使用
139	NetBIOS Session Services	TCP	是NetBIOS over TCP/IP的一部分，用于档案分享及网络打印机打印功能
143	IMAP4	TCP	邮件存取协议，类似POP3协议。例如，使用邮件客户端软件可以设定使用IMAP4来连接支持IMAP4邮件服务
161	SNMP	UDP	Simple Network Management Protocol（SNMP）是网络管理时所使用的协议。网管软件及网络接口设备与操作系统平台间透过SNMP协议进行必要的网络管理信息交换
162	SNMP Trap	UDP	使用SNMP做网络管理时，Trap可以使被管理的设备在系统发生紧急状况时通知网管系统
194	IRC	TCP	Internet Relay Chat Protocol（IRC），网络聊天协议
389	LDAP	LDAP	Lightweight Directory Access Protocol，AD透过LDAP连到DC对AD数据库查询
443	HTTPS	TCP	SSL使用的port，透过SSL，使用者端的Browser与WWW Server可以达到安全、加密的数据传输目的
593	RPC over HTTP	TCP	使用在COM+的服务上
993	IMAP	TCP	使用SSL加密的IMAP联机
995	POP3	TCP	使用SSL加密的POP3联机
1433	SQL Server	TCP、UDP	SQL Server是一种数据库服务，使用通信端网络链接库透过TCP/IP进行通信
1434	SQL Monitoring	TCP	用来监控SQL Server的性能

（续）

端 口	服　务	协　议	说　明
3306	MySQL	TCP	MySQL数据库服务
3389	RDP	TCP	Remote Desktop Protocol（RDP）

1.2 扫描方式

用户可以使用三种扫描方式来实施网络扫描，分别是主动扫描、被动扫描和第三方扫描。本节将分别介绍这三种扫描方式。

1.2.1 主动扫描

主动扫描就是用户主动发送一些数据包进行扫描，以找到网络中活动的主机。其中，用于主动扫描的工具有很多，如 Netdiscover、Nmap 和 Ping 等。例如，当用户使用 Ping 命令实施主动扫描时，将会发送一个 ICMP Echo-Request 报文给目标主机，如果目标主机收到该请求，并回应一个 ICMP Echo-Reply 报文，则说明该目标主机是活动的。

1.2.2 被动扫描

被动扫描是通过长期监听广播包，来发现同一网络中的活动主机。一般情况下发送广播包，主要有两个原因。一个原因是，应用程序希望在本地网络中找到一个资源，而应用程序对该资源的地址又没有预先储备。例如 ARP 广播包，用于获取局域网内某 IP 对应的 MAC 地址。另一个原因是由于一些重要的功能。例如，路由器要求把它们的信息发送给所有可以找到的邻机。

1.2.3 第三方扫描

用户还可以借助第三方主机来实施扫描。例如，使用公开的网络服务或者控制其他主机/设备来实施扫描。下面将介绍一些第三方扫描方式。

1. Shodan的使用

Shodan 是目前最强大的搜索引擎。但是，它与 Google 这种搜索网址的搜索引擎不同，

Shodan 是用来搜索网络空间中在线设备的，用户可以通过 Shodan 搜索指定的设备，或者搜索特定类型的设备。其中，Shodan 上最受欢迎的搜索内容是 webcam、linksys、cisco、netgear 和 SCADA 等。Shodan 搜索引擎的网址为 https://www.shodan.io/，界面如图 1.1 所示。

图 1.1　Shodan 搜索引擎

该界面就是 Shodan 搜索引擎的主界面。这里就像是用 Google 一样，在主页的搜索框中输入想要的内容即可。例如，这里搜索一个 SSH 关键词，显示结果如图 1.2 所示。

从该界面中可以看到搜索到的结果，主要包括两个部分：其中，左侧是大量的汇总数据，包括 TOTAL RESULTS（搜索结果总数）、TOP COUNTRIES（使用最多的国家）、TOP SERVICES（使用最多的服务/端口）、TOP ORGANIZATIONS（使用最多的组织/ISP）、TOP OPERATING SYSTEMS（使用最多的操作系统）和 TOP PRODUCTS（使用最多的产品/软件名称）；中间的主页面就是搜索结果，包括 IP 地址、主机名、ISP、该条目的收录时间、该主机位于的国家和 Banner 信息等。如果想要了解每个条目的具体信息，则需要单击每个条目下方的 Details 按钮即可。此时，URL 会变成这种格式 https://www.shodan.io/host/[IP]，如图 1.3 所示，所以用户也可以通过直接访问指定的 IP 来查看详细信息。

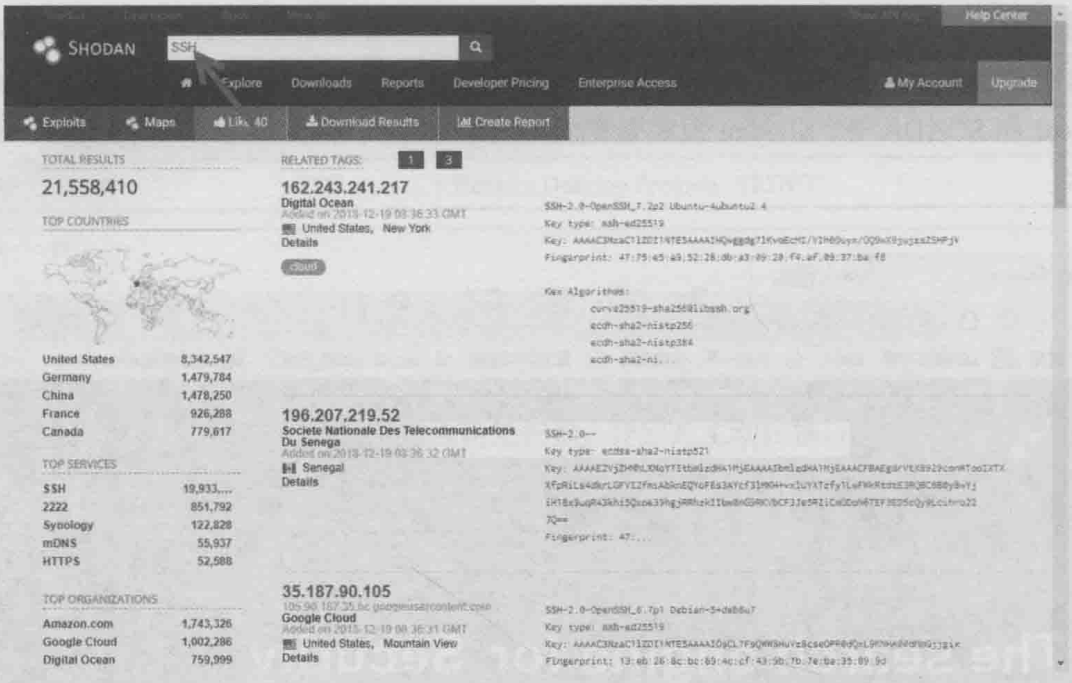

图 1.2　搜索结果

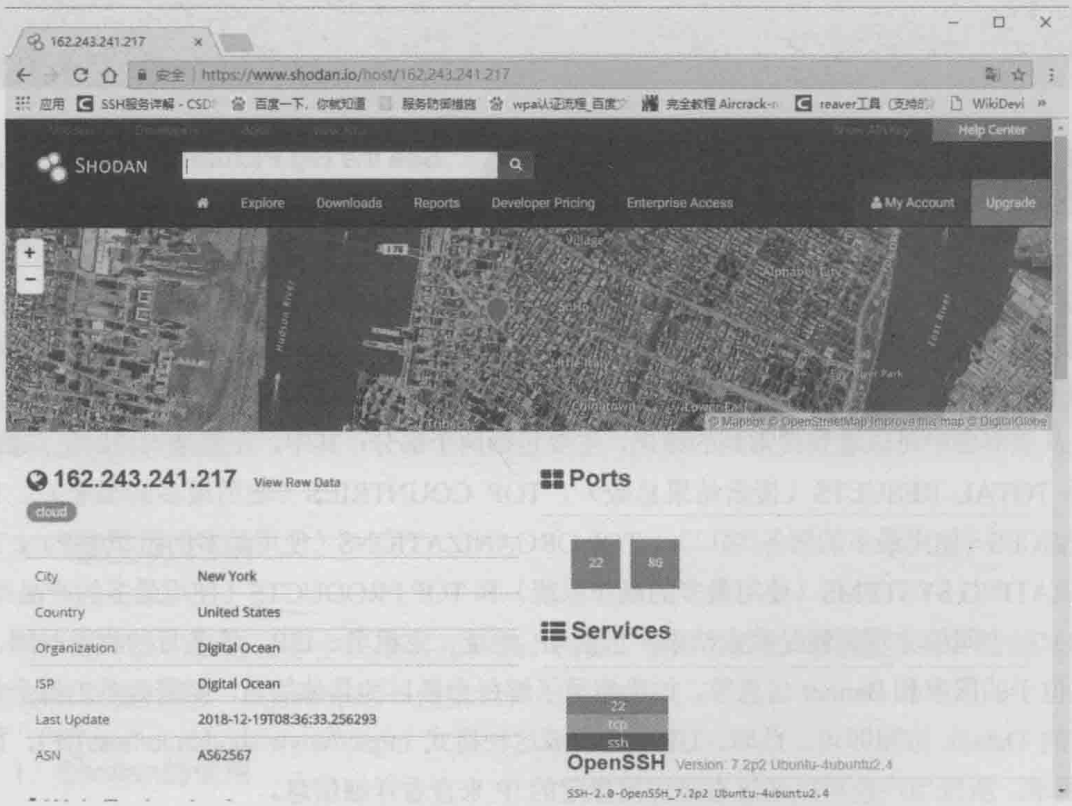

图 1.3　搜索结果的详细信息