Secrets of Nmap
Network Security Audit
Technology

诸神之眼

Nmap网络安全审计技术揭秘

一线网络安全教师撰写，凝聚自己多年教学与实践开发经验，系统且深入阐释Nmap在网络安全管理方面的方法与应用，以及Nmap强大的脚本编写功能等

由浅入深剖析使用Nmap进行网络安全审计的相关技术，涉及活跃主机发现、端口扫描、Zenmap、NSE脚本开发等

清华大学出版社

Secrets of Nmap
Network Security Audit
Technology

诸神之眼

Nmap网络安全审计技术揭秘

李华峰◎编著

清华大学出版社
北京

内 容 简 介

Nmap是目前非常受关注的网络安全审计技术工具，是绝大多数从事网络安全人员的必备工具。本书由一线网络安全教师亲笔撰写，凝聚了作者多年教学与实践开发经验，内容涉及网络安全审计的作用、价值、方法论，Nmap在网络安全管理方面的方法与应用，以及Nmap强大的脚本编写功能等。本书内容并不局限于某个具体功能的使用，而是系统深入地结合Nmap与网络审计原理进行讲解，帮助网络安全人员全面深入了解使用Nmap进行网络安全审计的相关技术。本书讲解的内容通俗易懂、深入浅出，特别是书中所用示例的设计，它们不仅可以让读者理解某个知识点的用法，更能让读者明白具体知识点所使用的场景，从而更深入地理解具体内容。

本书内容安排合理，架构清晰，注意理论与实践相结合，适合那些希望学习Nmap进行网络安全审计的网络安全渗透测试人员、运维工程师、网络管理人员、网络安全设备设计人员、网络安全软件开发人员、安全课程培训人员、高校网络安全专业方向的学生等阅读。

图书在版编目 (CIP) 数据

诸神之眼——Nmap网络安全审计技术揭秘 / 李华峰编著. —北京：清华大学出版社，2017

ISBN 978-7-302-47236-0

Ⅰ. ①诸… Ⅱ. ①李… Ⅲ. ①计算机网络—安全技术 Ⅳ. ① TP393.08

中国版本图书馆CIP数据核字 (2017) 第122603号

责任编辑： 杨如林　秦　健

封面设计： 李召霞

责任校对： 徐俊伟

责任印制： 沈　露

出版发行：清华大学出版社

网　　址：http://www.tup.com.cn，http://www.wqbook.com

地　　址：北京清华大学学研大厦A座　　邮　　编：100084

社 总 机：010-62770175　　邮　　购：010-62786544

投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn

质 量 反 馈：010-62772015，zhiliang@tup.tsinghua.edu.cn

印 装 者：三河市铭诚印务有限公司

经　　销：全国新华书店

开　　本：186mm × 240mm　　印　　张：15.75　　字　　数：343千字

版　　次：2017年9月第1版　　印　　次：2017年9月第1次印刷

印　　数：1 ~ 3500

定　　价：49.00元

产品编号：072303-01

Preface 前　言

为什么要写这本书

很多人在年少时，都曾经有一个黑客梦。

还记得我第一次接触“黑客”这个词是在很早的一部名为《战争游戏》的电影，虽然那时我甚至还没见过真正的计算机，但是里面的情节却深深地印在了我的脑海之中。从那以后，我开始对每部电影中出现的黑客情节都十分感兴趣，也经常推敲电影中这些情节在现实中的可行性。1999 年，一部名为《黑客帝国》的影片风靡了整个世界。对我来说，这部影片的意义更为深刻，在这部影片中，我居然见识到了一个真实中存在的极客工具——Nmap。这个发现让我兴奋不已。

要知道，极客技术在外人看起来神奇无比，对于这方面的学习者来说却是头疼无比。数量众多的知识需要学习，各种各样的工具需要掌握，在我刚开始接触极客技术的时候，几乎每天都将精力用在对各种工具的掌握上。不过，很快我也意识到了自己的失误——在“鱼”与“渔”之间，错误地选了“鱼”。我缺乏的不是一款万能的黑客工具，而是一个能将自己想法快速实现的工具，而这个问题随着 Nmap 的出现迎刃而解。

Nmap 是网络安全方面极为常用的工具，它的使用相当广泛。凡是从事网络安全技术的人员几乎都接触过这款工具。Nmap 作为世界渗透测试行业公认最优秀的网络安全审计工具，它可以通过对设备的探测来审计其安全性，而且功能极为完备，单是对端口状态的扫描技术就有数十种。不过很可惜的是，由于国内 Nmap 方面的学习资料相对匮乏，很多人都将 Nmap 作为一种普通的端口扫描工具来使用，却忽略 Nmap 中强大的编程能力。NSE 是 Nmap 中革命性的创新。通过 Nmap 强大的脚本引擎（NSE），每一个用户都可以向 Nmap 中添加自己编写的代码，从而将 Nmap 打造成用户自由定制功能的强大工具。可以这样说，NSE 的使用才是真正的“授人以渔”。

在本书的编写过程中，我一直在学校从事网络安全的教学工作。这使得每当我在进行一个章节编写时，可以预先在课堂上进行讲授，从而直接感受到学生对此的反映，他们其实是

本书的第一批读者。现在成书之时，也正值他们毕业之际。在这里希望书中的知识能够为他们以后的工作提供一些帮助。同样也希望这本书能为读者们带来帮助。

本书特色

Nmap 的强大功能是毋庸置疑的，它几乎是当前的极客必备工具，你几乎可以在任何经典的网络安全图书中找到它的名字，甚至可以在大量的影视作品（例如《 Matrix | 黑客帝国》《极乐空间》《谍影重重》《虎胆龙威 4》等）中看到它的身影。目前，国内对于 Nmap 的研究越来越热。近年来正是国内网络安全飞速发展的阶段，Nmap 这个曾经只有顶尖高手才能使用的“旧时王谢堂前燕”，到如今终于飞入了普通网络安全工作人员的“寻常百姓家”，受到广大网络安全行业从业人员的喜爱，假以时日，它必将成为国内最为流行的网络安全审计工具之一。本人从 2009 年开始正式涉足网络渗透领域，对于 Nmap 的使用，花费了大量的时间和精力进行研究，尤其是阅读了大量国外的相关文献。在本书中将会分享自己学习 Nmap 的使用经验、方法和总结，希望可以减少其他 Nmap 学习者的学习成本。

本书是第一本系统深入将 Nmap 应用实例与网络原理相结合进行讲解的工具书，不仅仅讲述 Nmap 的实际应用方法，更从网络原理的角度来分析 Nmap 实现网络安全审计的技术，将各种网络协议、各种数据包格式等知识与 Nmap 的实践应用相结合，真正做到理论与实践相结合。本书还将对 Nmap 强大的脚本引擎（NSE）进行系统而又深入的讲解，以达到通过 Lua 编程来扩展 Nmap 的功能，将 Nmap 打造成为用户可以自由定制功能的强大工具，真正地做到“授人以渔”。这里之所以将本书命名为“诸神之眼”，就是暗示 Nmap 在网络中强大的信息收集能力。

读者对象

本书的读者群主要是网络安全渗透测试人员、运维工程师、网络管理人员、网络安全设备设计人员、网络安全软件开发人员、安全课程培训人员、高校网络安全专业方向的学生等，其他读者还包括各种非专业但却热衷于网络安全研究的人员。

目前随着极客文化的盛行，以及网络安全爱好者日益增多，本书将对网络安全的宣传与教育起到重要作用。

如何阅读本书

本书可分为三大部分。

基础知识：从 Nmap 的基础讲起，系统讲述了网络安全审计的作用、价值、方法论，Nmap 在网络安全管理上的应用，以及 Nmap 在实现这些应用时相关的网络原理和技术等。

网络安全审计：结合实例讲解使用 Nmap 进行网络安全审计的方式和方法，以及在实际渗透中的各种应用。

脚本：介绍 Nmap 的强大脚本编写功能，使读者可以最终将 Nmap 打造成为个性化的工具。

阅读本书的建议

- 没有 Nmap 基础的读者，建议从第 1 章顺次阅读并演练每一个实例。
- 有一定 Nmap 基础的读者，可以根据实际情况有重点地选择阅读各个技术要点。
- 对于每一个知识点和项目案例，先通读一遍有个大概印象，然后将每个知识点的示例代码都在开发环境中操作一遍，加深对知识点的印象。

勘误和支持

由于作者的水平有限，编写时间仓促，书中难免会出现一些错误或者不准确的地方，恳请读者批评指正。欢迎您通过清华大学出版社网站（www.tup.com.cn）与我们联系，同时也欢迎大家与作者交流，作者的邮箱是 lihuafeng1999@163.com，期待能够得到你们的真挚反馈。

致谢

首先要感谢我的单位提供的自由而又宽松的科研工作环境，正是这种完全自由的氛围才使得年少时的梦想成为我现实生活中的工作。

感谢清华大学出版社的秦健编辑，在本书的编写过程中始终支持我的写作，你的鼓励和帮助引导我能顺利完成全部书稿。

最后感谢我的母亲，是她将我培养成人，并在人生的每一个关键阶段帮助我成长，感谢我深爱的妻子、我可爱的儿子，感谢你们在我编写本书的时候给予的无条件的理解和支持。

谨以此书献给我最亲爱的家人以及众多热爱极客技术的朋友们！

Contents 目　录

CHAPTER 01

第 1 章 走近 Nmap

刘开缓缓地睁开眼睛。

此刻他正处在一个阴冷的房间内，这个房间除了一扇门之外再无任何出口。

“这是在哪里？”

刘开支撑着身体慢慢坐了起来，他注意到身边只有一台笔记本电脑。

他站起身，走向门口，试图打开门，然而这一切都是徒劳的，门是锁着的，无论怎么撞都无法打开。房子十分密实，屋里的声音根本传不出去，呼救也只能是徒劳无功。

在仔细检查这个房间后再也没有找到任何其他东西，唯一可以利用的只有那台笔记本电脑，他只好返身回来，蹲下身子，将笔记本电脑打开。

刚刚开机，笔记本电脑就发出了电量过低，将在 20 分钟后自动关机的警报。

随即笔记本电脑屏幕上赫然出现了一行如同鲜血写成的文字！

“房间的门锁由一台计算机 X 控制，在网络上找到并侵入它，在取得它的控制权之后，就可以打开门锁。否则你将永远被关在这个房间里！”

这是一个看起来很像密室逃生故事的开头，不过不同的是，故事中的刘开不再像其他电影中的人物一样要找出一些隐藏的物品，在这个空荡的房间里，他可以依靠的只有这一台笔记本电脑，而仅有的这一丝希望也将会在 20 分钟后因停电而消失。

在这仅有的 20 分钟内，刘开该如何才能成功逃脱呢？

好了，我们正在开始一个精彩的故事，随着剧情的进展，你将领略到网络世界的神奇，并掌握保卫这个世界的技能。

在这一章中，除了开头这个紧张的故事之外，还将学习以下内容。

- ❑ 传奇般的安全审计工具 Nmap。
- ❑ Nmap 的下载与安装。
- ❑ Nmap 的基本操作。
- ❑ Nmap 扫描范围的确定。

1.1 Nmap 简介

对于已经陷入困境的刘开，什么能够给他带来一丝希望呢？如果没有从天而降的救兵的话，刘开所能依靠的只有自己娴熟的技术，以及某个强大的工具。此时，刘开最希望得到的工具又是什么呢？

如果可以选择，Nmap（Network Mapper）绝对是此时刘开的最佳选择。作为当今顶尖的网络审计工具，Nmap 在国外已经被大量的网络安全人员所使用，它的身影甚至出现在很多优秀影视作品中，其中影响力最大的要数经典巨著《黑客帝国》系列。在《黑客帝国 2》中，影片中的女主人公 Tritnity 就曾使用 Nmap 攻击 SSH 服务，从而破坏了发电厂的工作，如图 1-1 所示。

图 1-1 《黑客帝国 2》中女主人公 Tritnity 正在使用 Nmap 攻击 SSH 服务

Nmap 是由 Gordon Lyon 设计并实现的，于 1997 开始发布。Gordon Lyon 最初设计 Nmap 的目的只是希望打造一款强大的端口扫描工具。但是随着时间的发展，Nmap 的功能越来越全面。2009 年 7 月 17 日，开源网络安全扫描工具 Nmap 正式发布了 5.00 版，这是自 1997 年以来最重要的发布，代表着 Nmap 从简单的网络连接端扫描软件变身为全方面的安全和网络工具组件。目前 Nmap 已经更新到 7.30 版。

现在的 Nmap 已经具备了如下各种功能。

- **主机发现功能**：向目标计算机发送特制的数据包组合，然后根据目标的反应来确定它是否处于开机并连接到网络的状态。
- **端口扫描**：向目标计算机的指定端口发送特制的数据包组合，然后根据目标端口的反应来判断它是否开放。
- **服务及版本检测**：向目标计算机的目标端口发送特制的数据包组合，然后根据目标的反应来检测它运行服务的服务类型和版本。
- **操作系统检测**：向目标计算机发送特制的数据包组合，然后根据目标的反应来检测它的操作系统类型和版本。

除了这些基本功能之外，Nmap 还实现一些高级审计技术，例如伪造发起扫描端的身份，进行隐蔽扫描，规避目标的安全防御设备（例如防火墙），对系统进行安全漏洞检测，并提供完善的报告选项等。在后来的不断发展中，随着 Nmap 强大的脚本引擎（NSE）的推出，任何人都可以向 Nmap 中添加新的功能模块。

如果使用 Nmap 对一台计算机进行审计，最终可以获得目标如下的信息。

- 目标主机是否在线。
- 目标主机所在网络的结构。
- 目标主机上开放的端口，例如 80 端口、135 端口、443 端口等。
- 目标主机所使用的操作系统，例如 Windows 7、Windows 10、Linux 2.6.18、Android 4.1.2 等。
- 目标主机上所运行的服务以及版本，例如 Apache httpd 2.2.14、OpenSSH 5.3p1、Debian 3、Ubuntu 4 等。
- 目标主机上所存在的漏洞，例如弱口令、ms08_067、ms10_054 等。

收集目标信息是整个安全审计环节中至关重要的一部分工作。如此一来，对目标的信息将了若指掌。

1.2　Nmap 的下载与安装

在开始正式工作之前，首先需要从 Nmap 的官方网站（https://Nmap.org/download.html）下载这款软件，要注意这个页面中提供了对应不同操作系统的软件版本，在使用的时候选择对应所使用的操作系统的版本。

1.2.1　在 Windows 系统下安装与下载 Nmap

步骤 1：下载 Nmap。在 Windows 下安装 Nmap 时，注意网站提供两个版本的 Nmap，

一个是最新版，另一个是稳定版。这里以稳定版 Nmap-7.12-setup.exe 为例，图 1-2 给出了适用于 Windows 操作系统的 Nmap 下载地址。

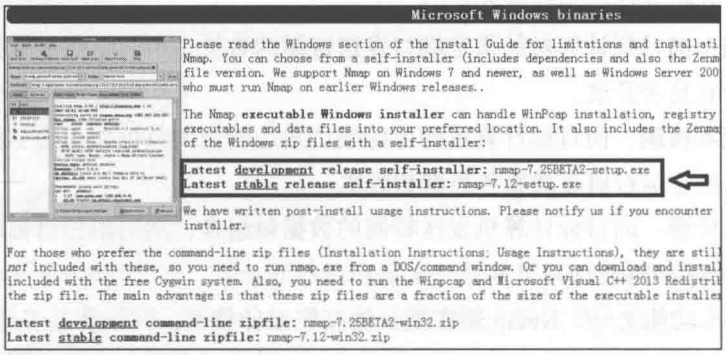

图 1-2　适用于 Windows 操作系统的 Nmap 下载地址

步骤 2：启动 Nmap 安装程序，选择默认安装（推荐），就可以自动将如图 1-3 所示全部的组件都装好。

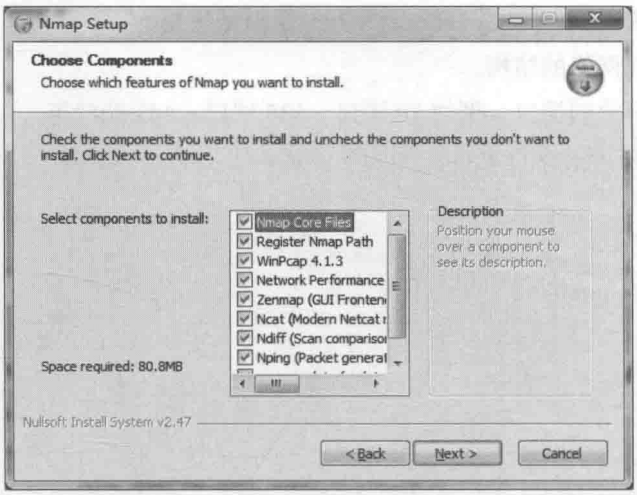

图 1-3　Nmap 安装过程中的组件选择

步骤 3：在安装过程中，将会安装一个 WinPcap 插件，如果之前没有安装过 WinPcap，就需要对其进行安装。如果之前你的计算机上安装过处理数据包的软件，将会弹出一个如图 1-4 所示的对话框，只需要单击“确定”按钮就可以了。

步骤 4：之后的操作只需要一路单击 Next 按钮即可，直到完成安装，如图 1-5 所示。

步骤 5：安装完成以后，可以在 Windows 命令行窗口中输入 Nmap 命令启动 Nmap，如图 1-6 所示。

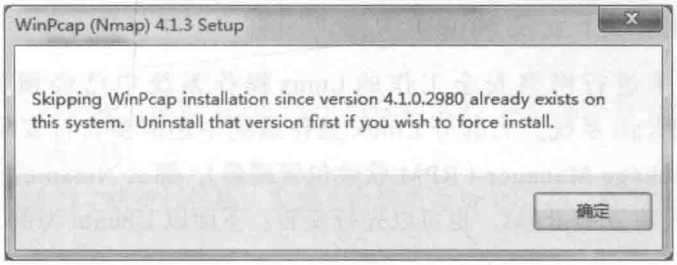

图 1-4　Nmap 安装所需要的 WinPcap

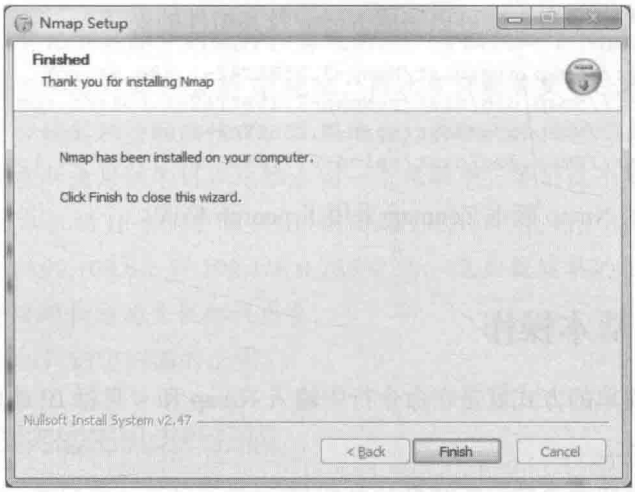

图 1-5　Nmap 安装完毕

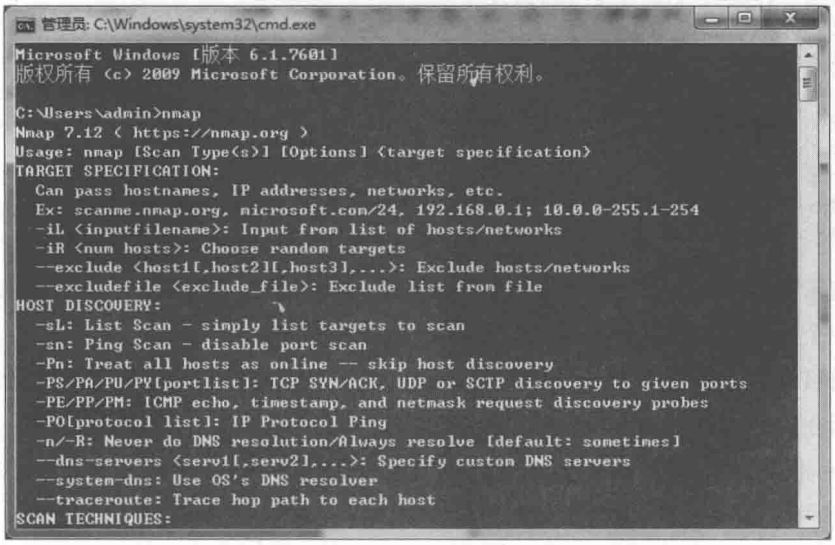

图 1-6　Windows 工作环境下 Nmap 的运行界面

1.2.2 在 Linux 系统下安装 Nmap

一些专门用来进行网络安全工作的 Linux 操作系统中已经预装了 Nmap，比如 BackTrack 系统和 Kali 系统。大部分 Linux 操作系统中还需要自行安装。如果系统中已经安装了 RPM Package Manager（RPM 软件包管理器），那么 Nmap 的安装将会变得十分简单。如果系统没有安装 RPM，也可以先行安装。下面以 Ubuntu 为例，使用如下命令安装 RPM。

```
sudo apt-get install rpm
```

之后只需要输入如下命令就可以完成 Nmap 及其组件的安装。

```
rpm -vhU https://Nmap.org/dist/Nmap-7.25BETA2-1.x86_64.rpm
rpm -vhU https://Nmap.org/dist/zeNmap-7.25BETA2-1.noarch.rpm
rpm -vhU https://Nmap.org/dist/ncat-7.25BETA2-1.x86_64.rpm
rpm -vhU https://Nmap.org/dist/nping-0.7.25BETA2-1.x86_64.rpm
```

注意，图形化的 Nmap 版本 Zenmap 采用了 noarch 格式。

1.3 Nmap 的基本操作

使用 Nmap 最简单的方式就是在命令行中输入 Nmap 和 < 目标 IP 地址 >，例如：

```
Nmap 192.168.0.1
```

下面就是执行这条命令的扫描结果。

```
Starting Nmap 7.12 ( https://Nmap.org ) at 2016-09-07 09:39                    ①
Nmap scan report for 192.168.0.1                                               ②
Host is up (0.030s latency).                                                   ③
Not shown: 997 closed ports                                                    ④
PORT        STATE      SERVICE                                                 ⑤
23/tcp      open       telnet                                                  ⑥
80/tcp      open       http
5431/tcp    open       park-agent
MAC Address: D8:FE:E3:B3:87:A9 (D-Link International)                          ⑦
Nmap done: 1 IP address (1 host up) scanned in 4.71 seconds                    ⑧
```

扫描结果中，①给出了当前使用的 Nmap 版本为 7.12，扫描开始时间为 2016-09-07 09:39。

②是一个标题，生成的是关于 192.168.0.1 主机的报告。

③给出目标主机的状态为 up（意味着这台主机处于开机并连上了互联网的状态）。

④表示在进行检查的 1000 个端口中，有 997 个是关闭的。

⑤是一张表，这张表中一共有三个字段，分别是 PORT、STATE、SERVICE，其中 PORT 指的是端口，STATE 指的是状态，SERVICE 指的是运行的服务。

例如，⑥中 PORT 列的值为 23/tcp，STATE 列的值为 open，SERVICE 列的值为 telnet，