信息安全技术丛书

用 Nmap 检查网络脆弱性、资产调研、服务运行状况及安全审计

众多实例让读者快速掌握 Nmap，详解 Zenmap 及 Nmap 使用技巧，轻松掌握 NSE 脚本使用及编写

防火墙逃逸攻防剖析，Nmap 指纹识别让目标无以遁形，还原真实场景让读者身临其境


# Nmap

# 渗透测试指南

商广明 编著

中国工信出版集团

人民邮电出版社
POSTS & TELECOM PRESS

信息安全技术丛书


# Nmap

# 渗透测试指南

商广明 编著
北方工业大学图书馆

人 民 邮 电 出 版 社
北 京

**图书在版编目（CIP）数据**

Nmap渗透测试指南 / 商广明编著. -- 北京 : 人民邮电出版社, 2015.10
ISBN 978-7-115-40395-7

Ⅰ. ①N… Ⅱ. ①商… Ⅲ. ①计算机网络－安全技术－指南 Ⅳ. ①TP393.08-62

中国版本图书馆CIP数据核字(2015)第225785号

## 内 容 提 要

本书专门介绍 Nmap 渗透测试的有关内容，全书共分 12 章，从最基础的 Nmap 下载、安装开始介绍，由浅入深地对 Nmap 的功能作了完整详细的说明。同时书中还包括了大量的实践案例，更有利于读者对 Nmap 使用的理解。本书主要内容包括：Nmap 基础、Nmap 工作原理、扫描指定段、Nmap 主机发现、TCP ACK Ping 扫描、ARP Ping 扫描、路由跟踪、探索网络、从 Nmap 识别端口状态、隐蔽扫描、指纹识别与探测、重量级扫描、调整探测报文的并行度、防火墙/IDS 逃逸、源端口欺骗、信息收集、检索系统信息、数据库渗透测试、渗透测试、Zenmap 应用、Nmap 技巧、Nmap 保存和输出等核心技术。

本书适合计算机安全爱好者、程序员、计算机安全研究人员的参考用书，也适合大专院校相关专业师生的学习用书和培训学校的教材。

◆ 编　　著　商广明
责任编辑　张　涛
责任印制　张佳莹　焦志炜

◆ 人民邮电出版社出版发行　　北京市丰台区成寿寺路 11 号
邮编　100164　　电子邮件　315@ptpress.com.cn
网址　http://www.ptpress.com.cn
北京天宇星印刷厂印刷

◆ 开本：800×1000　1/16
印张：17.5
字数：316 千字　　2015 年 10 月第 1 版
印数：1－3 000 册　　2015 年 10 月北京第 1 次印刷

定价：49.00 元

读者服务热线：(010)81055410　印装质量热线：(010)81055316
反盗版热线：(010)81055315

# 推荐序

当你看了《黑客帝国 2》《谍影重重 3》《虎胆龙威 4》这些耳熟能详的好莱坞巨片时，你想到了什么？也许是梦幻般的科幻镜头，也许是刺激的动作，还可能是暴力！而我想到了一个“伟大的工具”，它便是由 Gordon Lyon 先生创建并维护的著名安全工具——Nmap。在上面提到的这些好莱坞巨片中均出现过黑客们使用 Nmap 的镜头。而据 nmap.org 官方统计，各种出现 Nmap 镜头的影片有 17 部以上。

我之所以把 Nmap 称为“伟大的工具”，有以下几点原因。

- 第一个原因是它的“年龄”。Nmap“诞生”于 1996 年，目前已经 18 岁。但在这个信息爆炸的互联网时代，Nmap 依然保持着充沛的活力以及旺盛的生命力！Nmap 至今依然保持着平均 2 至 3 个月更新一次版本的速度成长着。而几乎所有黑客还非常频繁地使用着它。
- 第二个原因是它的“知名度”。Nmap 的知名度让我有胆量可以在这样一个公开场合告诉大家，如果某人不知道 Nmap，那么他绝对不可能被称为一名黑客。Nmap 绝对是著名的网络安全工具！
- 第三个原因是它强大的“功能”。也许 Nmap 在不少人眼中是一个网络端口扫描以及远程操作系统、服务鉴别工具。其实除了这些基础功能外，Nmap 还具备有相对完整的信息收集、数据库渗透、网络渗透测试等功能。Nmap 在强大的脚本支持下几乎可以做到我们想做的任何网络扫描测试。
- 第四个原因是它传奇般的“家族”。Nmap 的“兄弟”包括 NetCat（另一个神奇的工具）、Nping 以及 Zenmap，Nmap 的“姐妹”包括 Nmap.Org、SecLists.Org、SecTools.Org、Insecure.Org 等著名网络安全站点。
- 第五个原因是它伟大的“精神”。Nmap 是网络安全业界坚持 GNU GPL 并一直开放源代码的典范之一，它在 18 年间一直是“黑客精神”的最好典范之一。

基于以上原因，我建议所有对网络以及网络安全有兴趣的朋友必须了解并熟练使用 Nmap。此书是我见过的第一本由中国人编写并公开发行的 Nmap 专著。本书从最基础的 Nmap 下载、安装开始介绍，通过 12 个章节由浅入深地对 Nmap 的功能作了完整详细的说明。同时

书中还包括了大量的实践案例，更有利于读者对 Nmap 使用的理解。

因此，我认为本书是网络安全新手入门的必备读物之一，也是网络安全从业人员的常备工具书之一。如果需要我对此书提出建议的话，我建议售价更低一些，让更多的读者能够购买它，让更多有兴趣的朋友可以进入网络安全这个人才奇缺的行业。

彭泉，中国黑客的探索者，知名信息安全专家，网名 PP

# 前　言

我很荣幸可以撰写国内第一本有关 Nmap 的书籍。在众多的书籍之中，与渗透有关的书籍比比皆是，有介绍工具的书籍，也有介绍技巧的书籍，可偏偏没有一本介绍 Nmap 的书籍。宏观看来，在国内，大多数安全人员仅用 Nmap 进行端口扫描，这让一款优秀强大的工具失去了本应该有的光彩与能力。

渗透技术更像是一本失传已久的“武林秘籍”，大家无不争相修炼。渗透技术已从单纯的技术交流演变为黑色产业链，经历了许多坎坷。安全技术是一把双刃剑，伤人也会伤己，利用得当就会保障网络安全，否则会破坏网络安全。随着“江湖”上的各类黑客层出不穷，渗透技术出现了低端化的趋势，越来越多的人投入到技术的海洋中，近些年，黑客工具的不断涌现使网络安全形势堪忧，这种状况让现在很多企业、公司越来越重视网络安全。

Nmap 具有强大的功能及应对渗透测试的能力，随着近几年的发展 Nmap 不断成熟，从只能扫描端口的小工具逐步成为了现在进行渗透测试时不可或缺的部分，日益扮演着越来越重要的角色。虽然如此，很多人并没有转变对 Nmap 的认识，他们对 Nmap 的使用也仅仅局限于对端口的扫描。这并不能将 Nmap 的功能发挥出来，Nmap 蕴藏的能量或许超乎你的想象。

我在撰写这本书的时候经常与 Nmap 参考指南（Man Pege）的作者 Fyodor 先生和 Fei Yang 先生聊起书中的内容，他们希望我更多地去参考、引用 Nmap 参考指南（Man Pege）的内容，以便可以更好地帮助读者了解并使用 Nmap，所以，我在本书的前一部分引用了 Nmap 参考指南（Man Pege）的内容并与 Fyodor 先生和 Fei Yang 先生探讨其中的一部分细节，这里再次感谢 Fyodor 先生与 Fei Yang 先生对 Nmap 的贡献。

我时常用一句诗来形容渗透技术——“路漫漫其修远兮，吾将上下而求索”，这句诗出自屈原的《离骚》，意为：在追寻真理方面，前方的道路还很漫长，但我将百折不挠，不遗余力地去追求和探索。追求真理如此，追求渗透技术亦是如此。渗透技术无疑是一本上乘“武林秘籍”，想要悟透其中道理已是不易，若想将渗透技术修炼得出神入化，这其中还有很长的道路要走。学习渗透技术应该有百折不挠、不遗余力的精神，希望这本书可以起到抛砖引玉的作用，也希望各位“道友”可以有一本参考的资料。本书将 Nmap 进行了较为详细的剖析，剖析 Nmap

的各个功能以及在实战中的使用方式。也希望业界“大牛”可以撰写出更为精彩和详细的文章与我们分享。

## 感谢

首先我要感谢我的父母，感谢他们含辛茹苦地把我抚养长大，感谢在这 20 多年中对我的谆谆教导，正是他们的鼓励让我顺利编写完此书；感谢爷爷、奶奶在背后的支持；感谢婧婧在我编写本书时的陪伴，每当编写进入困境时，婧婧总是很有耐心地劝导我、鼓励我；感谢 Fyodor 先生与 Fei Yang 先生的支持；感谢人民邮电出版社编辑老师不辞辛苦地审稿，共同与我解决本书的问题；感谢 PP 先生为此书写序并指导！

## 读者对象

网络与系统安全领域的技术爱好者与学生。

渗透测试、漏洞分析研究与网络安全管理方面的从业人员。

开设信息安全、网络安全与执法等相关专业的高等院校的本科生及研究生。

期望在信息安全领域就业的技术人员。

想成为一位自由职业渗透测试师的人。

## 指正

本书编写之处不免会有用词或表达方面的问题，请读者发现后及时与我联系，笔者恳请读者对本书批评指正。编辑联系邮箱：zhangtao@ptpress.com.cn。

## 赠言

技术在于不断地追求与探索！

——商广明

非宁静无以致远 非淡泊无以明志

# 目　录

# 第 1 章　Nmap 基础学习

本章知识点

- Nmap 介绍
- Windows 下安装 Nmap
- Linux/Unix 源码编译安装 Nmap
- Linux 通过 RPM 软件包安装 Nmap
- Mac OS 安装 Nmap
- Nmap 语法
- Nmap 全面扫描
- Nmap 扫描指定段

本章节将介绍在几大主流平台中如何安装 Nmap，并介绍多种安装方式，通过对每一步的演示进行解说，让初学者可以很快地掌握安装 Nmap 技巧，以及如何简单地使用 Nmap 扫描一个目标地址、一个 IP 段，从而迈入 Nmap 渗透测试的大门。

本章选项

表 1.1　　第一章所需选项

| 选　项 | 解　释 |
| --- | --- |
| -A | 全面扫描/综合扫描 |

## 1.1 Nmap 介绍

Nmap 的英文全称是“Network Mapper”，中文为“网络映射器”。Nmap 是一款开放源代

码的网络探测和安全审核的工具，它的设计目标是快速地扫描大型网络，当然用它扫描单个主机也没有问题。Nmap 以新颖的方式使用原始 IP 报文来发现网络上有哪些主机，这些主机提供什么服务（应用程序名和版本），服务运行在什么操作系统（包括版本信息），它们使用什么类型的报文过滤器/防火墙，以及一些其他功能。虽然 Nmap 通常用于安全审核，许多系统管理员和网络管理员也用它来做一些日常的工作，比如查看整个网络的信息、管理服务升级计划，以及监视主机和服务的运行。

Nmap 的基本功能有 3 个，一是探测一组主机是否在线，其次是扫描主机端口，嗅探所提供的网络服务，还可以推断主机所用的操作系统。Nmap 可用于扫描仅有两个节点的 LAN，直至 500 个节点以上的网络。Nmap 还允许用户定制扫描技巧。通常，一个简单的使用 ICMP 协议的 Ping 操作可以满足一般需求；也可以深入探测 UDP 或者 TCP 端口，直至主机所使用的操作系统；还可以将所有探测结果记录到各种格式的日志中，供进一步分析操作。

Nmap 输出的是扫描目标的列表，以及每个目标的补充信息，至于是哪些信息则依赖于所使用的选项。Open（开放的）意味着目标机器上的应用程序正在该端口监听连接/报文。Filtered（被过滤的）意味着防火墙，过滤器或者其他网络障碍阻止了该端口被访问，Nmap 无法得知它是 Open（开放的）还是 Closed（关闭的）。Closed（关闭的）端口上面没有应用程序监听，但是它们随时可能开放。

Nmap——Script 功能的使用。在 Nmap 的安装目录的 share/nmap/scripts 中，已经有多种写好的脚本提供，使用这些脚本可以轻易地发起渗透测试。

## 1.2 Windows 下安装 Nmap

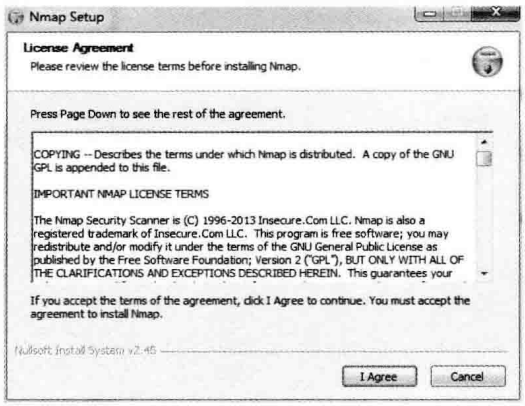
Nmap 可以运行在所有的 Windows NT 版本中，包括 Windows 2000、Windows XP、Windows 2003、Windows Vista、Windows 7 等。

在浏览器中打开网址“http://nmap.org/download.html”，在 Microsoft Windows binaries 中选择下载。

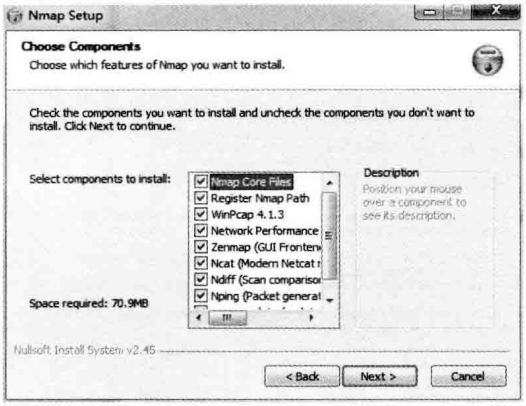
下载完毕后双击安装文件即可安装。

如图 1.1 所示，阅读 Nmap 许可协议，点击“I Agree”进行下一步安装。

如图 1.2 所示，选择所需要安装的组建，如果不需要安装某些组件可以勾选掉，一般默认安装所有组件，确实无误后点击“Next”进行下一步安装。



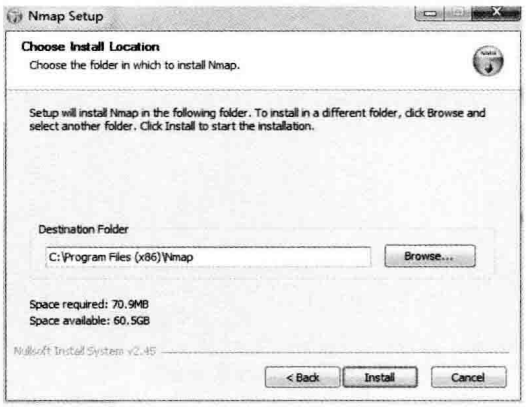

▲图 1.1 Nmap 许可协议



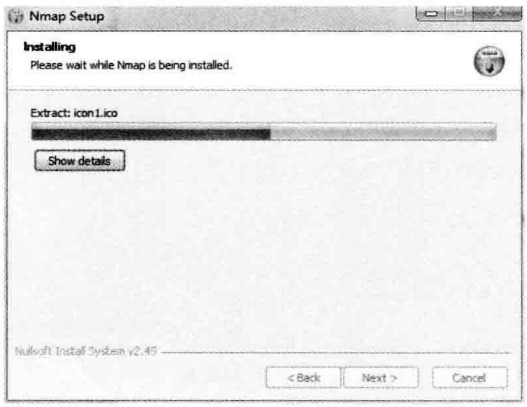

▲图 1.2 Nmap 组件选择

如图 1.3 所示，选择 Nmap 安装路径，一般保持默认即可。

如图 1.4 所示，Nmap 正在安装中。




▲图 1.3 Nmap 安装路径




▲图 1.4 Nmap 安装

如图 1.5 所示，在 Nmap 安装过程中会弹出对话框，询问某些组件的许可协议，选择“I Agrree”进行安装。

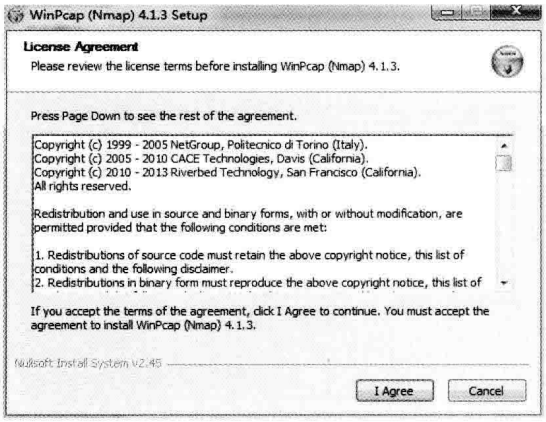
如图 1.6 所示，选择“Next”进行下一步安装。

如图 1.7 所示，选择您所需要的选项，点击“Next”进行下一步。

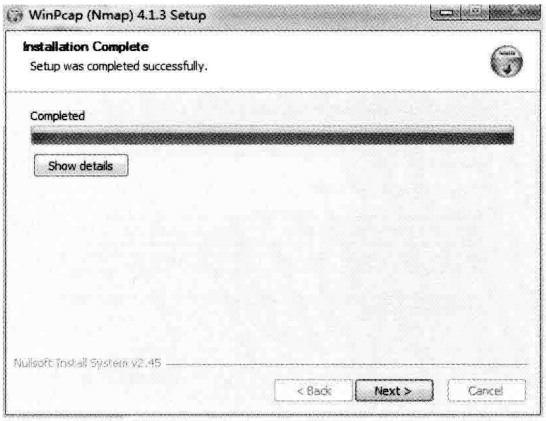
如图 1.8 所示，点击“Finish”完成安装。

在如图 1.9 所示的对话框中选择创建快捷方式，这里保持默认，点击“Next”进行下一步安装。

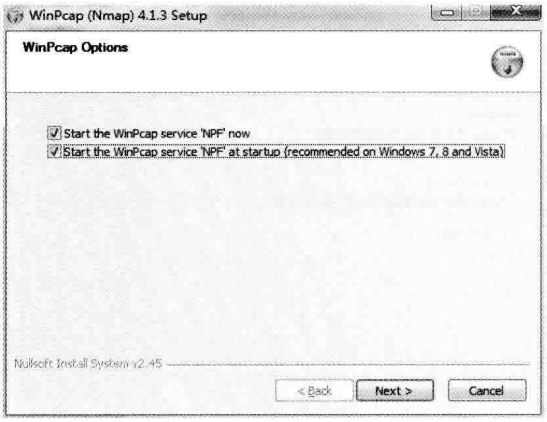
如图 1.10 所示，点击“Finish”完成安装。



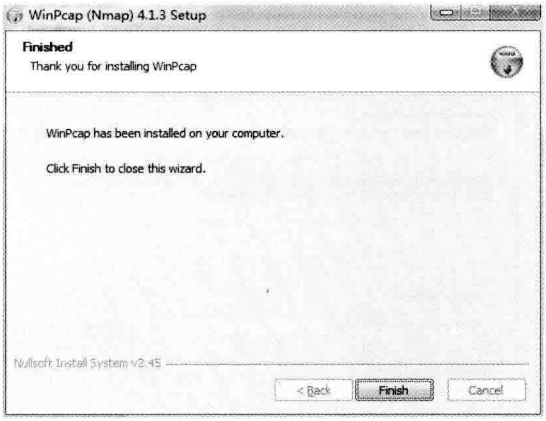

▲图 1.5　Nmap 组件许可



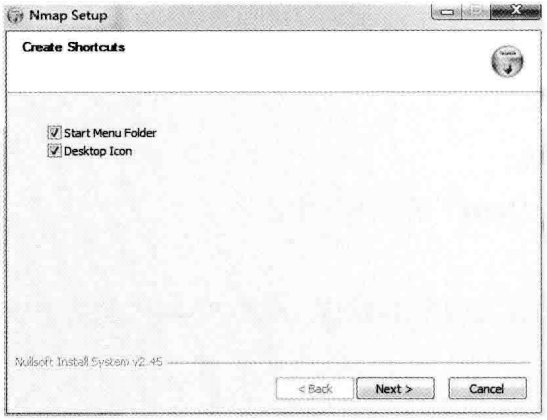

▲图 1.6　Nmap 安装



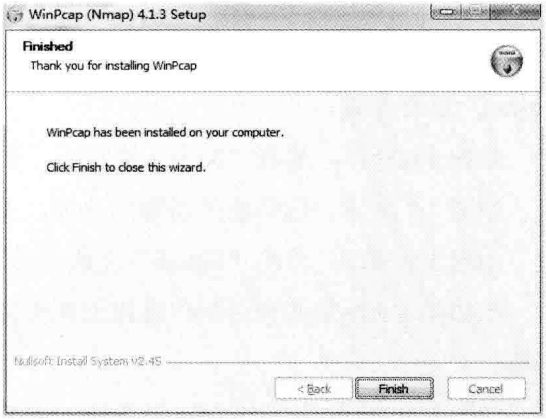

▲图 1.7　Nmap 选项选择




▲图 1.8　Nmap 安装完成




▲图 1.9　Nmap 创建快捷方式




▲图 1.10　Nmap 安装完成

## 1.3 Linux/Unix 源码编译安装 Nmap

在 Linux/Unix 中我们可以很方便地通过源码编译安装 Nmap，首先在“http://nmap.org/download.html”中选择源码进行下载。下载完毕后首先解压压缩包。

```
root@ubuntu:/home# bzip2 -cd nmap-6.46.tar.bz2 | tar xvf -
nmap-6.46/zenmap/zenmapCore/I18N.py
nmap-6.46/zenmap/zenmapCore/Version.py
nmap-6.46/zenmap/zenmapCore/Paths.py
nmap-6.46/zenmap/COPYING_HIGWIDGETS
…省略…
root@ubuntu:/home#
```

切换到 Nmap 目录进行编译。

```
root@ubuntu:/home# cd nmap-6.46
root@ubuntu:/home/nmap-6.46# ./configure
…省略…
checking whether we are using the GNU C++ compiler... no
checking whether g++ accepts -g... no
no
configure: creating ./config.status
config.status: creating Makefile
config.status: WARNING:  'Makefile.in' seems to ignore the --datarootdir setting
config.status: creating config.h
          .      .
          \`-"'"-'/
           } 6 6 {
          ==. Y ,==
            /^^^\  .
           /    \  )  Ncat: A modern interpretation of classic Netcat
          ( )-( )/
          -""---""---   /
         /   Ncat    \_/
        (     ____
         \_.=|____E
Configuration complete.
   ( )   /\   _                (
    \ |  (  \ ( \.(              )                  _____
  \  \ \  `  `   ) \            (  ___              / _  \
 (_`    \+   . x  ( .\           \/   \____-----------/ (o)   \_
- .-              \+  ;          (  O                         \____
(__               +- .( -'.- <.   \_____________  `             \  /
(_____            ._._: <_ - <- _-  _  VVVVVVV VV V\             \/
  .    /./.+-  . .- /  +--  - .     (--_AAAAAAA__A_/              |
  (__ ' /x  / x _/ (               \_________________//_           \_______
```

```
, x / ( '  . / .  /                                    \___'          \     /
   /  /  _/ /    +                                      |           \   /
  '  (__/                                              /             \/
                                                     /                \
            NMAP IS A POWERFUL TOOL -- USE CAREFULLY AND RESPONSIBLY
Configuration complete.  Type make (or gmake on some *BSD machines) to compile.
root@ubuntu:/home/nmap-6.46# make
root@ubuntu:/home/nmap-6.46# make install
```

编译完成后就可以使用 Nmap 进行渗透测试。

## 1.4 Linux 通过 RPM 软件包安装 Nmap

在 http://nmap.org/download.html 页面下载 RPM 安装包，查看一下 RPM 安装包并安装。

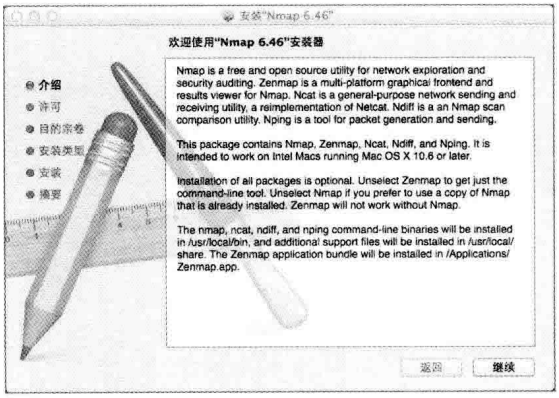
```
root@ubuntu:~# cd /home/
root@ubuntu:/home# ls
apache  nmap-6.46-1.i386.rpm
root@ubuntu:/home# rpm -ivh nmap-6.46-1.i386.rpm
```

## 1.5 Mac OS 安装 Nmap

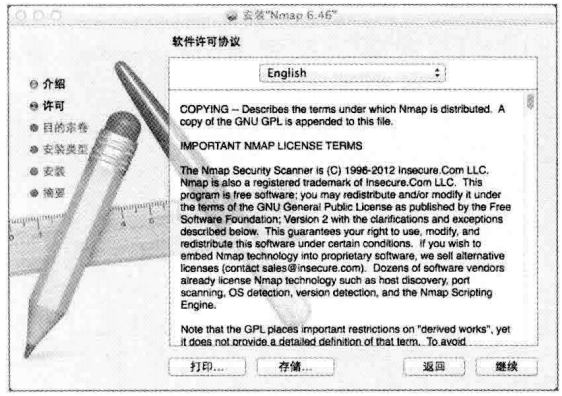
在 http://nmap.org/download.html 页面下载 Mac OS 版本的 DMG 文件，下载完毕后进行安装。

图 1.11 所示为 Nmap 的介绍页面，点击“继续”进行下一步。

阅读如图 1.12 所示的许可协议，点击“继续”进行下一步安装。



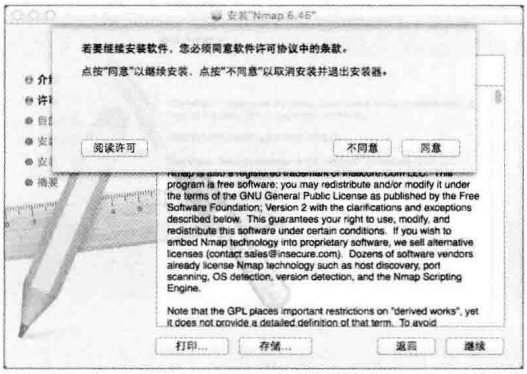

▲图 1.11　Nmap 介绍



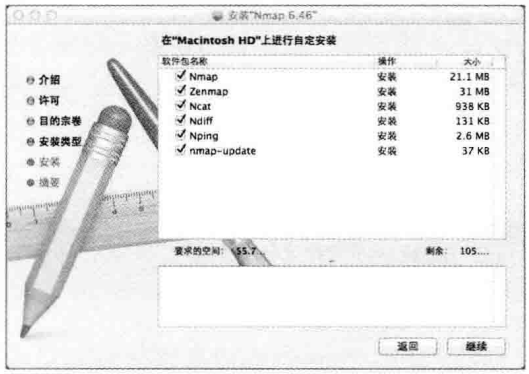

▲图 1.12　Nmap 许可协议

如图 1.13 所示，安装程序进行许可协议的再次确认，点击“同意”进行下一步。

如图 1.14 所示，选择您所需要的组件，在一般情况下保持默认即可。




▲图 1.13　Nmap 许可协议




▲图 1.14　Nmap 组件选择

如图 1.15 所示，确认有充足的空间安装 Nmap，点击“安装”。

如图 1.16 所示，看到此页面则表示安装成功。


▲图 1.15　确认安装空间


▲图 1.16　Nmap 安装完成

如图 1.17 所示，在 Shell 终端中输入 Nmap 命令可以成功打开 Nmap 并使用。至此在 Mac OS 下的安装就已经完成。


▲图 1.17　Nmap 在 MAC OS 下使用