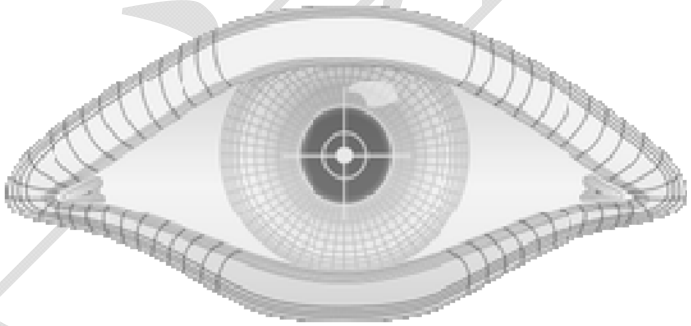
Nmap 扫描基础教程

（内部资料 v1.0）



大学霸
www.daxueba.net

前　言

Nmap（Network Mapper，网络映射器）是一款免费开放的网络扫描和嗅探工具包。Nmap 工具可以用来发现主机，扫描电脑上开放的端口和运行的程序，并且可以推出计算机运行的操作系统。通过使用该工具，可以评估网络系统安全。所以，Nmap 是大部分用户所必要的工具之一。

为了帮助用户更好的使用 Nmap 工具，本教程根据 Nmap 工具的功能，进行了详细介绍。如发现主机、扫描端口、识别服务、操作系统及 Nmap 脚本的使用等。

1.学习所需的系统和软件

- ❑ 安装 Windows 7 操作系统
- ❑ 安装 RHEL 操作系统
- ❑ 安装 WordPress 操作系统
- ❑ 安装 Nmap 工具

2.学习建议

大家学习之前，可以致信到 xxxxxxxxxxx，获取相关的资料和软件。如果大家在学习过程遇到问题，也可以将问题发送到该邮箱。我们尽可能给大家解决。

目　录

第 1 章　Nmap 基础知识

Nmap 是一个免费开放的网络扫描和嗅探工具包，也叫网络映射器（Network Mapper）。Nmap 工具可以用来扫描电脑上开放的端口，确定哪些服务运行在哪些端口，并且推断出计算机运行的操作系统。通过使用该工具，可以评估网络系统安全。所以，Nmap 是大部分用户所必要的工具之一。本章将对 Nmap 工具的基础知识进行详细介绍。

1.1　Nmap 概述

Nmap 是一款非常不错的网络扫描工具，支持各种操作系统，如 Windows、Linux、Mac OS 等。为了帮助用户更好的使用该工具，本节将对 Nmap 工具做一个简单介绍。

1.1.1　什么是 Nmap

Nmap 是一款开源免费的网络发现（Network Discovery）和安全审计（Security Auditing）工具。软件名字 Nmap 是 Network Mapper 的简称。Nmap 最初是由 Fyodor 在 1997 年创建的。随后在开源社区众多的志愿者参与下，该工具逐渐成为最为流行安全必备工具之一。目前，Nmap 工具的最新版本是 6.47。

由于 Nmap 工具具有许多优点，所以该工具被广泛应用。其中，Nmap 工具的优点如下所示：

- 灵活：支持数十种不同的扫描方式，支持多种目标对象的扫描。
- 强大：Nmap 可以用于扫描互联网上大规模的计算机群。
- 可移植：支持主流的操作系统，如 Windows、Linux、Unix、Mac OS 等；并且其源码开放，方便移植。
- 简单：提供默认的操作能覆盖大部分功能，如基本端口扫描，全面扫描。
- 自由：Nmap 作为开源软件，在 GPL License 的范围内可以自由的使用。
- 文档丰富：Nmap 官网提供了详细的文档描述。Nmap 作者及其它安全专家编写了多部 Nmap 参考书籍。
- 社区支持：Nmsp 背后有强大的社区团队支持。
- 赞誉有加：获得很多的奖励，并在很多影视作品中出现（如黑客帝国 2、Die Hard4 等）。
- 流行：目前 Nmap 已经被成千上万的安全专家列为必备的工具之一。

1.1.2　Nmap 的功能

Nmap 主要包括四个方面的扫描功能，分别是主机发现、端口扫描、应用与版本侦测、操作系统侦测。这四项功能之间，又存在大致的依赖关系。通常情况下顺序关系，如图 1.1 所示。

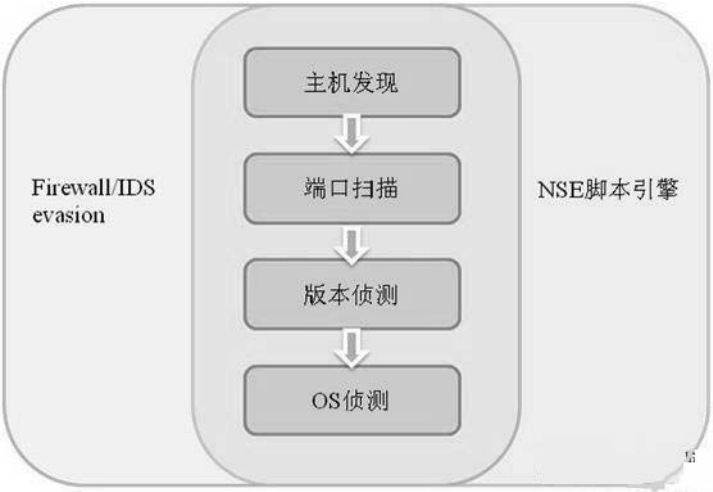


图 1.1　Nmap 功能架构图

下面将详细介绍以上 Nmap 各功能之间的依赖关系。如下所示：

（1）首先用户需要进行主机发现，找出活动的主机。然后，确定活动主机上端口状况。

（2）根据端口扫描，以确定端口上具体运行的应用程序与版本信息。

（3）对版本信息侦测后，对操作系统进行侦测。

在这四项基本功能的基础上，Nmap 提供防火墙与 IDS（IntrusionDetection System，入侵检测系统）的规避技巧，可以综合应用到四个基本功能的各个阶段；另外 Nmap 提供强大的 NSE（Nmap Scripting Language）脚本引擎功能，脚本可以对基本功能进行补充和扩展。

1.1.3　Nmap 工作原理

Nmap 使用 TCP/IP 协议栈指纹准确地判断目标主机的操作系统类型。首先，Nmap 通过对目标主机进行端口扫描，找出有哪些端口正在目标主机上监听。当侦测到目标主机上有多于一个开放的 TCP 端口、一个关闭的 TCP 端口和一个关闭的 UDP 端口时，Nmap 的探测能力是最好的。Nmap 工具的工作原理如表 1-1 所示。

表 1-1　Nmap工作原理

测试	描述
T1	发送TCP数据包（Flag=SYN）到开放的TCP端口上
T2	发送一个空的TCP数据包到开放的TCP端口上
T3	发送TCP数据包（Flag=SYN，URG，PSH，FIN）到开放的TCP端口上
T4	发送TCP数据包（Flag=ACK）到开放的TCP端口上
T5	发送TCP数据包（Flag=SYN）到关闭的TCP端口上
T6	发送TCP数据包（Flag=ACK）到开放的TCP端口上
T7	发送TCP数据包（Flag=URG，PSH，FIN）到关闭的TCP端口上

Nmap 对目标主机进行一系列测试，如表 1-1 所示。利用得出的测试结果建立相应目标主机的 Nmap 指纹。最后，将此 Nmap 指纹与指纹库中指纹进行查找匹配，从而得出目标主机的操作系统类型。

1.1.4　Nmap 扫描类型

Nmap 常见的扫描类型如表 1-2 所示。

表 1-2　Nmap主要扫描类型

Ping扫描	端口扫描
TCP SYN扫描	UDP扫描
操作系统识别	隐蔽扫描

1.2　获取 Nmap 安装包

当用户对 Nmap 工具有一个清晰的认识后，即可安装并使用该工具了。如果要安装该工具，则必须要先获取其软件包。本节将介绍如何获取 Nmap 工具的安装包。

Nmap 工具的官网是 http://nmap.org/。在该官网提供了 Nmap 各种类型包的下载地址。其中，下载地址是：

https://nmap.org/download.html

在浏览器中输入以上地址后，将打开如图 1.2 所示的界面。

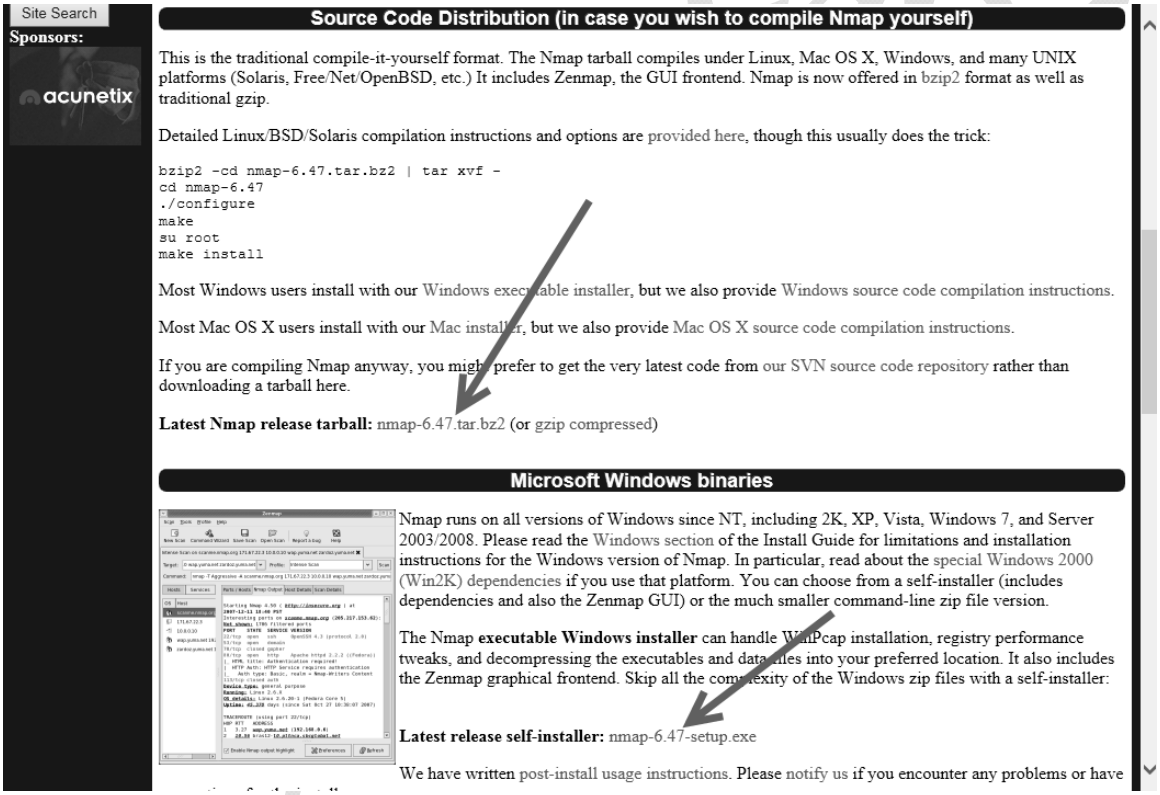


图 1.2　Nmap 下载页面

在该界面根据自己的系统版本，选择相应的软件包。由于章节的原因，上图只截取了一部分（包括源码包和 Windows 二进制包的下载地址）。

1.3　安装 Nmap 工具

通过上一节的介绍，用户可以顺利的获取到 Nmap 工具的安装包。接下来，用户就可以在操作系统

中安装该工具了。为了使任何所有用户都可以很好的使用该工具，下面将分别介绍在 Windows 和 Linux 操作系统中安装 Nmap 工具的方法。

1.3.1　在 Windows 下安装

【示例 1-1】下面将介绍在 Windows 下安装 Nmap 工具的方法。具体操作步骤如下所示：

（1）在 Windows 下双击下载的 Nmap 软件包，本例中的软件包名为 nmap-6.47-setup.exe。双击该软件包后，将弹出许可协议对话框，如图 1.3 所示。

（2）该界面显示了安装 Nmap 工具的许可证协议。这里单击 I Agree 按钮，将弹出选择组件对话框，如图 1.4 所示。

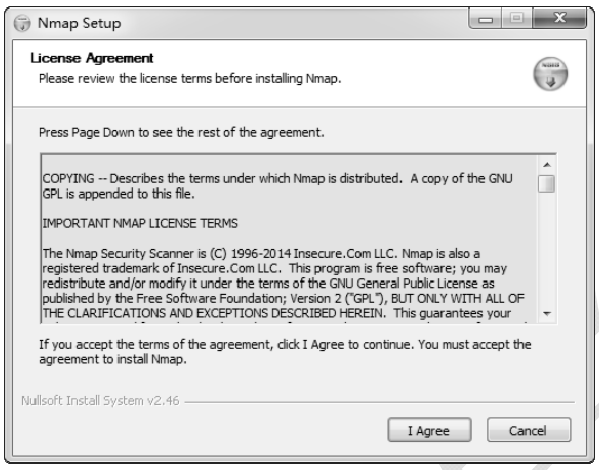


图 1.3　许可证协议对话框

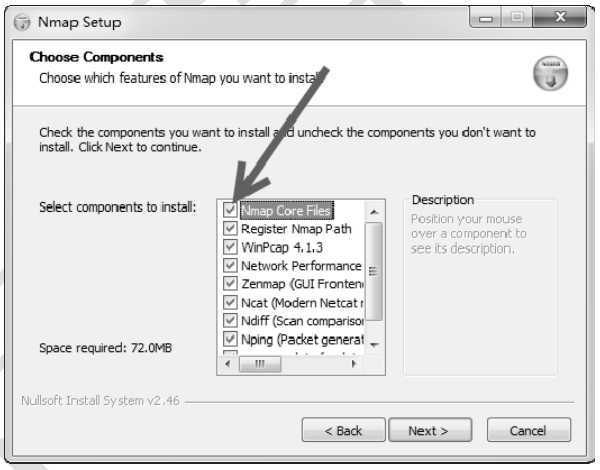


图 1.4　选择组件对话框

（3）在该界面选择安装 Nmap 其它功能的一些组件，如 Zenmap、Ndiff、Nping 等。如果用户不想安装某组件的话，将组件名前面复选框中的对勾去掉即可。这里选择默认设置，安装所有组件。然后，单击 Next 按钮，将弹出安装位置选择对话框，如图 1.5 所示。

（4）该界面是用来设置 Nmap 安装位置的。如果用户希望安装到其它位置的话，则单击 Browse 按钮，选择要安装的位置。这里使用默认的位置，然后单击 Install 按钮，将弹出 WinPcap 许可协议对话框，如图 1.6 所示。

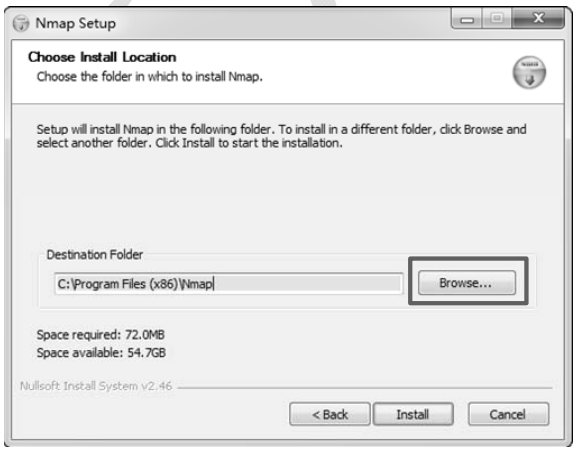


图 1.5　安装位置选择对话框

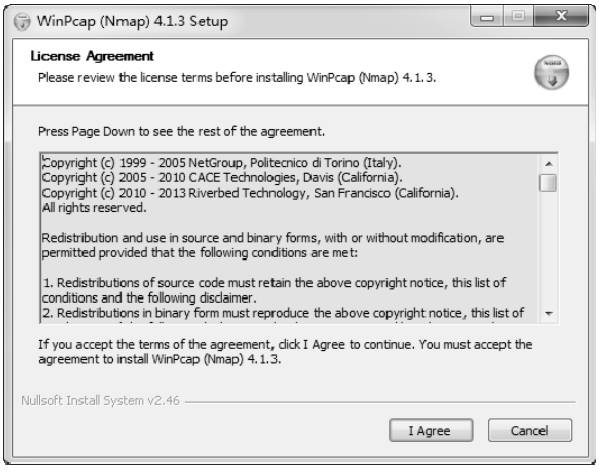


图 1.6　WinPcap 许可证协议对话框

（5）该界面显示了安装 WinPcap 组件的许可证协议。WinPcap 是重要的组件，用来实现数据包捕获和网络分析。所以，必须安装。这里单击 I Agree 按钮，将显弹出 WinPcap 安装完成提示信息对话框，如图 1.7 所示。

（6）该界面显示 WinPcap 组件已经完成。此时，单击 Next 按钮，将弹出 WinPcap 选项对话框，如图 1.8 所示。

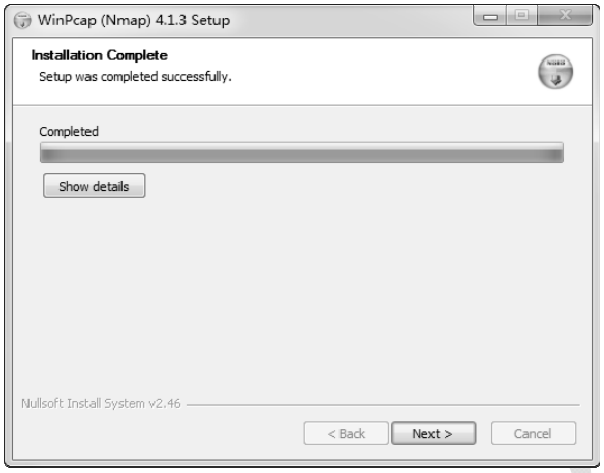


图 1.7　WinPcap 安装完成信息

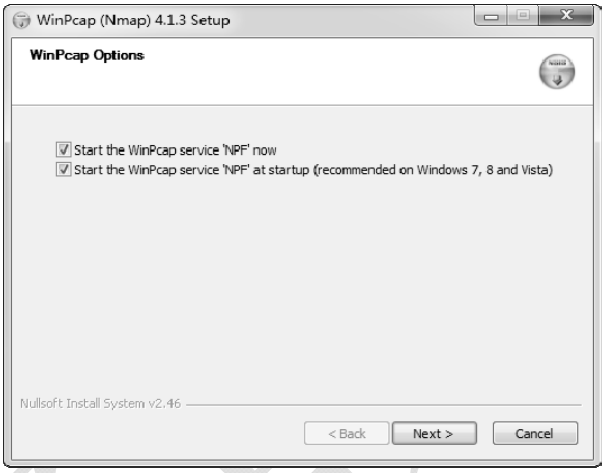


图 1.8　WinPcap 选项对话框

（7）该界面用来设置启动 NPF 选项。这里使用默认设置，然后单击 Next 按钮，将弹出完成对话框，如图 1.9 所示。

（8）该界面提示 WinPcap 组件已设置完成。此时，单击 Finish 按钮，将显示开始安装 Nmap 工具。安装完成后，将弹出 Nmap 安装完成提示信息对话框，如图 1.10 所示。

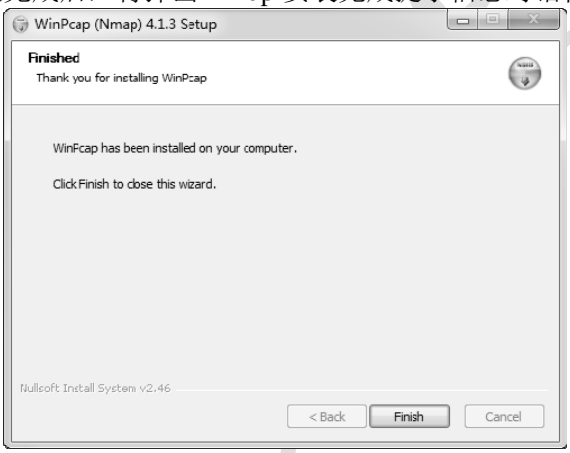


图 1.9　WinPcap 组件设置完成

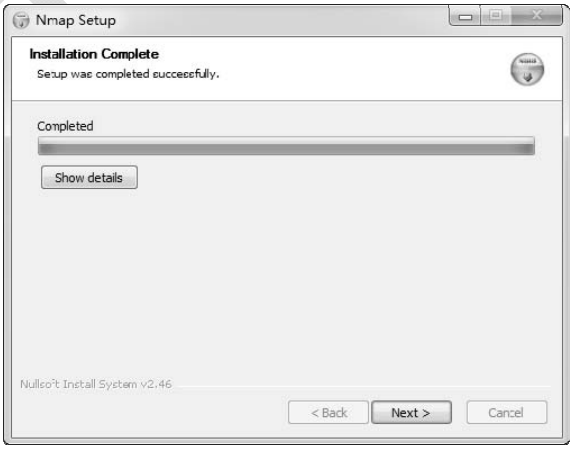


图 1.10　Nmap 安装完成信息

（9）从该界面可以看到 Nmap 工具已经安装完成。此时，单击 Next 按钮，将弹出创建快捷方式的对话框，如图 1.11 所示。

（10）该界面用来设置 Nmap 工具创建快捷方式的位置。默认是在启动菜单栏和桌面上创建快捷方式，这里使用默认设置。然后，单击 Next 按钮，将弹出 Nmap 完成对话框，如图 1.12 所示。

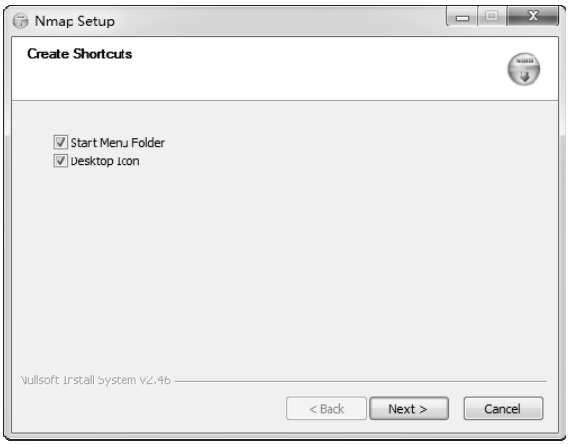


图 1.11　创建快捷方式对话框

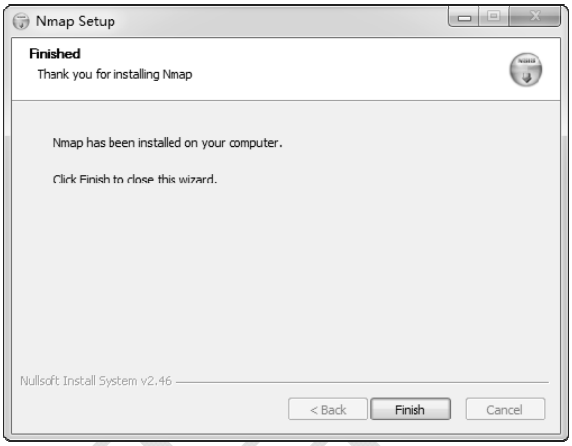


图 1.12　Nmap 设置完成

（11）从该界面可以看到 Nmap 工具已设置完成。此时，单击 Finish 按钮，退出 Nmap 安装向导。

提示：如果用户当前系统中已经安装 WinPcap 的话，将不会弹出图 1.6 所示的对话框，而是弹出如图 1.13 所示的对话框。

图 1.13　WinPcap 已经安装

从该界面可以看到提示 WinPcap 组件在当前系统中已经安装，接下来将跳过 WinPcap 组件安装。此时，单击“确定”按钮，将显示如图 1.10 所示的界面。如果用户不希望弹出图 1.13 对话框的话，在图 1.4 中去掉 WinPcap 4.1.3 组件前面复选框中的对勾即可。

1.3.2　在 Linux 下安装

在 Linux 下可以使用两种方法来安装。其中，一种是使用二进制包，另一种就是源码包。但是，在 Linux 中二进制包的安装有两大流派，分别是 Red Hat 的 rpm（Redhat Package Management）和 Debian 的 dpkg。所以，对于使用二进制包安装，则需要根据系统的类型选择相应的包进行安装。下面分别介绍这两种类型包的安装方法。

1.Red Hat 系列系统安装

【示例 1-2】在 Red Hat 系列系统中安装 Nmap 工具。下面以 RHEL 操作系统为例，演示 Nmap 的安装方法。执行命令如下所示：

```
[root@RHEL ~]# rpm -ivh nmap-6.47-1.i386.rpm
Preparing...                ########################################### [100%]
   1:nmap                   ########################################### [100%]
```

看到以上输出信息，则表示 Nmap 工具安装成功。在以上命令中，rpm 是命令，表示安装.rpm 格式

的软件包；-ivh 是-i、-v 和-h 三个选项的组合，其中-i 表示安装、-v 显示详细信息、-h 用来显示安装进度；nmap-6.47-1.i386.rpm 是软件包名。

2.Debian 系列系统安装

【示例 1-3】在 Debian 系列系统中安装 Nmap 工具。下面以 Ubuntu 操作系统为例，演示 Nmap 的安装方法。执行命令如下所示：

```
test@testtual-machine:~$ sudo dpkg -i nmap_6.47-4_i386.deb
[sudo] password for test                          #输入当前登录系统用户的密码
(正在读取数据库 ... 系统当前共安装有 175794 个文件和目录。)
正准备解包 nmap_6.47-4_i386.deb  ...
正在将 nmap (6.47-4) 解包到 (6.47-4) 上 ...
正在设置 nmap (6.47-4) ...
正在处理用于 man-db (2.6.7.1-1ubuntu1) 的触发器 ...
```

看到以上类似输出信息，则表示 Nmap 功能安装成功。

1.3.3 源码包安装

源码包可以在各种系列的 Linux 系统中安装。下面将以 RHEL 操作系统为例，介绍使用源码包安装 Nmap 工具的方法。具体操作步骤如下所示：

（1）解压 Nmap 安装包。执行命令如下所示：

```
[root@RHEL ~]# tar jxvf nmap-6.47.tar.bz2
```

执行以上命令后，将会将源码包中的文件解压的当前目录下 nmap-6.47 文件夹中。

（2）配置 Nmap 工具。执行命令如下所示：

```
[root@RHEL ~]# cd nmap-6.47
[root@RHEL nmap-6.47]# ./configure
```

执行以上命令，表示为 Nmap 工具指定了默认的安装位置。

（3）编译软件包。执行命令如下所示：

```
[root@RHEL nmap-6.47]# make
```

（4）安装软件包。执行命令如下所示：

```
[root@RHEL nmap-6.47]# make install
```

以上命令执行成功的话，将会看到“NMAP SUCCESSFULLY INSTALLED”信息。该信息表示，Nmap 工具安装成功。

第 2 章　基础扫描

当用户对 Nmap 工具了解后，即可使用该工具实施扫描。通过上一章的介绍，用户可知 Nmap 工具可以分别对主机、端口、版本、操作系统等实施扫描。但是，在实施这些扫描工作之前，需要先简单了解下 Nmap 工具的使用，以方便后面实施扫描。所以，本章将通过使用 Nmap 工具实施基础的扫描，来帮助用户了解该工具。

2.1　扫描概述

在实施基本的扫描之前，需要先了解一些 Nmap 网络扫描的基本知识，及需要考虑的一些法律边界问题。本节将对网络基本扫描进行一个简单介绍。

1.网络扫描基础知识

在使用网络扫描之前，需要先理解以下内容：

- 当目标主机上使用了防火墙、路由器、代理服务或其它安全设备时，使用 Nmap 扫描结果可能会存在一些偏差。或者当扫描的远程目标主机不在本地网络内时，也有可能会出现误导信息。
- 在使用 Nmap 实施扫描时，一些选项需要提升权限。在 Unix 和 Linux 系统中，必须使用 root 登录或者使用 sudo 命令执行 Nmap 命令。

2.法律边界问题

在实施网络扫描时，需要考虑一些法律边界问题。如下所示：

- 在扫描互联网服务提供商网络时（如政府或秘密服务器网站），如果没有被允许的话，不要进行扫描。否则，会惹上法律麻烦。
- 全面扫描某些主机时，可能会导致主机崩溃、停机或数据丢失等不良结果。所以，在扫描关键任务时要小心谨慎。

2.2　指定扫描目标

当用户有明确的扫描目标时，可以直接使用 Nmap 工具实施扫描。根据扫描目标的多少，可以分为扫描单个目标、多个目标及目标列表三种情况。本节将依次讲解这三种情况的扫描方式。

2.2.1　扫描单个目标

通过指定单个目标，使用 Nmap 工具可以实现一个基本的扫描。指定的目标可以是一个 IP 地址，也可以是主机名（Nmap 会自动解析其主机名）。其中，语法格式如下所示：

```
nmap [目标]
```

其中，参数[目标]可以是一个 IP 地址，也可以是一个主机名。

【示例 2-4】扫描局域网中 IP 地址为 192.168.1.105 的主机。执行命令如下所示：

```
root@localhost:~# nmap 192.168.1.105
Starting Nmap 6.47 ( http://nmap.org ) at 2015-05-05 18:44 CST
Nmap scan report for localhost (192.168.1.105)
Host is up (0.00010s latency).
Not shown: 995 closed ports
PORT     STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
111/tcp   open  rpcbind
445/tcp   open  microsoft-ds
MAC Address: 00:0C:29:31:02:17 (VMware)
```

```
Nmap done: 1 IP address (1 host up) scanned in 0.87 seconds
```

从输出信息中，可以看到目标主机 192.168.1.105 上开启的端口有 21、22、23、111、445，及这些端口所对应的服务。而且，还可以看到该目标主机的 MAC 地址为 00:0C:29:31:02:17。从最后一行信息，可以看出目标主机是活动的（up），并且扫描该目标主机共用了 0.87 秒。

提示：Nmap 工具默认扫描前 1000 个端口，即 1-1000。如果用户想扫描 1000 以上端口的话，需要使用-p 选项来指定。关于如何使用 Nmap 的一些选项，将在后面章节介绍。

由于 IP 地址分为 IPv4 和 IPv6 两类。所以，使用 Nmap 工具扫描单个目标时，指定的 IP 地址可以是 IPv4，也可以是 IPv6。上例中指定扫描的目标是使用 IPv4 类地址。如果用户指定扫描目标地址是 IPv6 类地址时，需要使用-6 选项。例如，扫描 IP 地址为 fe80::20c:29ff:fe31:217 的目标主机，则执行命令如下所示：

```
[root@router ~]# nmap -6 fe80::20c:29ff:fe31:217
```

执行以上命令后，将显示如下所示的信息：

```
Starting Nmap 6.47 ( http://nmap.org ) at 2015-05-06 15:07 CST
Nmap scan report for fe80::20c:29ff:fe31:217
Host is up (0.000017s latency).
Not shown: 995 closed ports
PORT    STATE SERVICE
22/tcp    open    ssh
23/tcp    open    telnet
111/tcp open    rpcbind
139/tcp open    netbios-ssn
445/tcp open    microsoft-ds
Nmap done: 1 IP address (1 host up) scanned in 0.16 seconds
```

从以上输出信息中，可以看到 IPv6 地址为 fe80::20c:29ff:fe31:217 的主机是活动的，并且开放了 22、23、111、139、445 端口。

提示：如果要使用 IPv6 类地址作为目标时，则扫描主机和目标主机都必须支持 IPv6 协议。否则，无法实施扫描。

2.2.2 扫描多个目标

Nmap 可以用来同时扫描多个主机。当用户需要扫描多个目标时，可以在命令行中同时指定多个目标，每个目标之间使用空格分割。其中，语法格式如下所示：

```
nmap [目标 1  目标 2 ...]
```

【示例 2-5】使用 Nmap 工具同时扫描主机 192.168.1.1、192.168.1.101 和 192.168.1.105。执行命令如下所示：

```
root@localhost:~# nmap 192.168.1.1 192.168.1.101 192.168.1.105
Starting Nmap 6.47 ( http://nmap.org ) at 2015-05-05 19:07 CST
Nmap scan report for localhost (192.168.1.1)
Host is up (0.00094s latency).
Not shown: 997 closed ports
PORT          STATE SERVICE
80/tcp          open   http
1900/tcp        open   upnp
49152/tcp       open   unknown
MAC Address: 14:E6:E4:84:23:7A (Tp-link Technologies CO.)
Nmap scan report for localhost (192.168.1.101)
```

```
Host is up (0.0060s latency).
All 1000 scanned ports on localhost (192.168.1.101) are closed
MAC Address: 14:F6:5A:CE:EE:2A (Xiaomi)
Nmap scan report for localhost (192.168.1.105)
Host is up (0.00038s latency).
Not shown: 995 closed ports
PORT     STATE SERVICE
21/tcp     open   ftp
22/tcp     open   ssh
23/tcp     open   telnet
111/tcp    open   rpcbind
445/tcp    open   microsoft-ds
MAC Address: 00:0C:29:31:02:17 (VMware)
Nmap done: 3 IP addresses (3 hosts up) scanned in 1.00 seconds
```

从以上输出信息，可以看到共扫描了三台主机，并且依次显示了每台主机的扫描结果。在以上信息中，将扫描的每台主机地址行已加粗，方便用户了解其扫描结果。下面分别介绍这三台主机的扫描结果，如下所示：

- 192.168.1.1：从输出信息中可以看到该主机开启了三个端口，MAC 地址为 14:E6:E4:84:23:7A。根据 MAC 地址后面括号中的信息，可以推断出该主机是一个 Tp-link 路由器。
- 192.168.1.101：从输出信息中，可以看到该主机上前 1000 个端口是关闭的。但是，可以看到该主机的 MAC 地址为 14:F6:5A:CE:EE:2A，设备类型为 Xiaomi。由此可以判断出，该主机是一个小米手机设备。
- 192.168.1.105：从输出信息中，可以看到该主机上 995 个端口是关闭的，五个端口是开启的。其中，MAC 地址为 00:0C:29:31:02:17，而且是一台 VMware（虚拟机）操作系统。

提示：当用户同时指定扫描的目标太多时，可以使用简化符号来获取扫描结果。其中，目标地址之间使用逗号（,）分割。例如，同时扫描以上三台主机，则可以使用如下命令：

```
nmap 192.168.1.1,101,105
```

2.2.3　扫描一个目标列表

当用户有大量主机需要扫描时，可以将这些主机的 IP 地址（或主机名）写入到一个文本文件中。然后，使用 Nmap 工具进行扫描。这样避免在命令行中手工输入目标。其中，语法格式如下所示：

```
nmap -iL [IP 地址列表文件]
```

以上语法中的-iL 选项，就是用来从 IP 地址列表文件中提取所有地址的。其中，IP 地址列表文件中包含了一列被扫描的主机 IP 地址。并且，在 IP 地址列表文件中的每个条目必须使用空格、Tab 键或换行符分割。

【示例 2-6】使用 Nmap 工具扫描 list.txt 文件中所有的主机。具体操作步骤如下所示：

（1）创建 list.txt 文本文件，并将扫描的主机 IP 地址写入到该文本文件中。如下所示：

```
root@localhost:~# vi list.txt
192.168.1.1
192.168.1.100
192.168.1.101
192.168.1.102
192.168.1.103
192.168.1.104
```

```
192.168.1.105
```

以上就是在 list.txt 文件中，指定将要扫描的目标地址。

（2）扫描 list.txt 文件中指定的所有主机。执行命令如下所示：

```
root@localhost:~# nmap -iL list.txt
Starting Nmap 6.47 ( http://nmap.org ) at 2015-05-06 10:53 CST
Nmap scan report for localhost (192.168.1.1)
Host is up (0.00045s latency).
Not shown: 997 closed ports
PORT          STATE SERVICE
80/tcp          open  http
1900/tcp        open  upnp
49152/tcp       open  unknown
MAC Address: 14:E6:E4:84:23:7A (Tp-link Technologies CO.)
Nmap scan report for localhost (192.168.1.100)
Host is up (0.00023s latency).
Not shown: 986 closed ports
PORT    STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
443/tcp   open  https
445/tcp   open  microsoft-ds
902/tcp   open  iss-realsecure
912/tcp   open  apex-mesh
1033/tcp open   netinfo
1034/tcp open   zincite-a
1035/tcp open   multidropper
1038/tcp open   mtqp
1040/tcp open   netsaint
1075/tcp open   rdrmshc
2869/tcp open   icslap
5357/tcp open   wsdapi
MAC Address: 00:E0:1C:3C:18:79 (Cradlepoint)
Nmap scan report for localhost (192.168.1.103)
Host is up (0.00028s latency).
Not shown: 977 closed ports
PORT STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp open   rmiregistry
1524/tcp open   ingreslock
```

```
2049/tcp open   nfs
2121/tcp open   ccproxy-ftp
3306/tcp open   mysql
5432/tcp open   postgresql
5900/tcp open   vnc
6000/tcp open   X11
6667/tcp open   irc
8009/tcp open   ajp13
8180/tcp open   unknown
MAC Address: 00:0C:29:F8:2B:38 (VMware)
Nmap scan report for localhost (192.168.1.104)
Host is up (0.00028s latency).
Not shown: 997 closed ports
PORT STATE SERVICE
22/tcp   open   ssh
80/tcp   open   http
443/tcp open   https
MAC Address: 00:0C:29:C3:1F:D7 (VMware)
Nmap scan report for localhost (192.168.1.105)
Host is up (0.00034s latency).
Not shown: 995 closed ports
PORT STATE SERVICE
21/tcp   open   ftp
22/tcp   open   ssh
23/tcp   open   telnet
111/tcp open   rpcbind
445/tcp open   microsoft-ds
MAC Address: 00:0C:29:31:02:17 (VMware)
Nmap scan report for localhost (192.168.1.102)
Host is up (0.0000080s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
80/tcp    open   http
9876/tcp open   sd
Nmap done: 7 IP addresses (6 hosts up) scanned in 1.05 seconds
```

从输出的信息中，可以看到依次扫描了 list.txt 文件中的每台主机，并且显示了每台主机的扫描结果。从最后一行信息，可以看到共扫描了七个 IP 地址。其中，六个主机是活动的，并且整个扫描过程共用了 1.05 秒。

2.2.4　扫描随机目标

Nmap 工具提供了一个-iR 选项，可以用来选择随机的互联网主机来扫描。Nmap 工具将会随机的生成指定数量的目标进行扫描。其中，语法格式如下所示：

```
nmap -iR [主机数量]
```

【示例 2-7】使用 Nmap 工具随机选择两个目标主机进行扫描。执行命令如下所示：

```
root@localhost:~# nmap -iR 2
Starting Nmap 6.47 ( http://nmap.org ) at 2015-05-06 11:07 CST
Nmap scan report for suncokret.vguk.hr (161.53.173.3)
```

```
Host is up (0.43s latency).
Not shown: 984 closed ports
PORT     STATE    SERVICE
21/tcp   open     ftp
25/tcp   open     smtp
53/tcp   open     domain
80/tcp   open     http
81/tcp   open     hosts2-ns
110/tcp  open     pop3
135/tcp  filtered msrpc
139/tcp  filtered netbios-ssn
143/tcp  open     imap
443/tcp  open     https
444/tcp  open     snpp
445/tcp  filtered microsoft-ds
593/tcp  filtered http-rpc-epmap
2002/tcp open     globe
3306/tcp open     mysql
4444/tcp filtered krb524
Nmap done: 3 IP addresses (1 host up) scanned in 29.64 seconds
```

从输出信息中，可以看到 Nmap 工具随机生成了三个 IP 地址。但是，只有主机 161.53.137.3 是活动的，并且显示了对该主机的扫描结果。

提示：一般情况下，不建议用户实施随机扫描。除非，你是在做一个研究项目。否则，经常实施随机扫描可能会给自己的互联网服务提供商带来麻烦。

2.3 指定扫描范围

当用户不确定扫描主机的地址时，可以通过指定一个地址范围实施扫描。通过指定扫描范围，从扫描结果中可以获取到活动的主机及相关信息。用户在指定一个扫描范围时，还可以排除单个或多个扫描目标。本节将介绍使用 Nmap 工具实施指定地址范围的扫描方法。

2.2.1 IP 地址范围扫描

用户在指定扫描范围时，可以通过 IP 地址或子网的方式来实现。下面将介绍使用 IP 地址指定扫描范围的方法。其中，语法格式如下所示：

```
nmap [IP 地址范围]
```

在以上语法中，IP 地址范围之间使用短连字符（-）。

【示例 2-8】使用 Nmap 工具扫描 192.168.1.1 到 100 之间的所有主机。执行命令如下所示：

```
root@localhost:~# nmap 192.168.1.1-100
Starting Nmap 6.47 ( http://nmap.org ) at 2015-05-05 19:40 CST
Nmap scan report for localhost (192.168.1.1)
Host is up (0.0014s latency).
Not shown: 997 closed ports
PORT     STATE SERVICE
80/tcp   open  http
```

```
1900/tcp   open   upnp
49152/tcp open   unknown
MAC Address: 14:E6:E4:84:23:7A (Tp-link Technologies CO.)
Nmap scan report for localhost (192.168.1.100)
Host is up (0.00025s latency).
Not shown: 986 closed ports
PORT     STATE SERVICE
135/tcp   open   msrpc
139/tcp   open   netbios-ssn
443/tcp   open   https
445/tcp   open   microsoft-ds
902/tcp   open   iss-realsecure
912/tcp   open   apex-mesh
1033/tcp open   netinfo
1034/tcp open   zincite-a
1035/tcp open   multidropper
1037/tcp open   ams
1039/tcp open   sbl
1041/tcp open   danf-ak2
2869/tcp open   icslap
5357/tcp open   wsdapi
MAC Address: 00:E0:1C:3C:18:79 (Cradlepoint)
Nmap done: 100 IP addresses (2 hosts up) scanned in 3.34 seconds
```

从以上输出信息中，可以看到 192.168.1-100 之间，只有 192.168.1.1 和 192.168.1.100 两台主机是活动的。

用户也可以指定扫描多个网络/子网范围的主机。例如，扫描 C 类 IP 网络 192.168.1.*到 192.168.100.*之间的所有主机。则执行命令如下所示：

```
nmap 192.168.1-100.*
```

以上命令中星号（*）是一个通配符，表示 0-255 之间所有有效的主机。

2.2.2　整个子网扫描

Nmap 也可以使用 CIDR（无类别域间路由，Classless Inter-Domain Routing）格式来扫描整个子网。CIDR 将多个 IP 网络结合在一起，使用一种无类别的域际路由选择算法，可以减少由核心路由器运载的路由选择信息的数量。其中，语法格式如下所示：

```
nmap [CIDR 格式的网络地址]
```

以上语法中的 CIDR 是由网络地址和子网掩码两部分组成，并且中间使用斜杠（/）分割。其中，CIDR 和子网掩码对照表如表 2-1 所示。

表 2-3　CIDR对照表

子网掩码	CIDR	子网掩码	CIDR
000.000.000.000	/0	255.255.128.000	/17
128.000.000.000	/1	255.255.192.000	/18
192.000.000.000	/2	255.255.224.000	/19
224.000.000.000	/3	255.255.240.000	/20
240.000.000.000	/4	255.255.248.000	/21
248.000.000.000	/5	255.255.252.000	/22
252.000.000.000	/6	255.255.254.000	/23

254.000.000.000	/7	255.255.255.000	/24
255.000.000.000	/8	255.255.255.128	/25
255.128.000.000	/9	255.255.255.192	/26
255.192.000.000	/10	255.255.255.224	/27
255.224.000.000	/11	255.255.255.240	/28
255.240.000.000	/12	255.255.255.248	/29
255.248.000.000	/13	255.255.255.252	/30
255.252.000.000	/14	255.255.255.254	/31
255.254.000.000	/15	255.255.255.255	/32
255.255.000.000	/16	255.255.128.000	/17

【示例 2-9】使用 Nmap 扫描 192.168.1.1/24 整个子网中的所有主机。执行命令如下所示：

```
root@localhost:~# nmap 192.168.1.1/24
Starting Nmap 6.47 ( http://nmap.org ) at 2015-05-05 19:41 CST
Nmap scan report for localhost (192.168.1.1)
Host is up (0.00064s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE
80/tcp    open  http
1900/tcp  open  upnp
49152/tcp open  unknown
MAC Address: 14:E6:E4:84:23:7A (Tp-link Technologies CO.)
Nmap scan report for localhost (192.168.1.100)
Host is up (0.00022s latency).
Not shown: 986 closed ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
443/tcp  open  https
445/tcp  open  microsoft-ds
902/tcp  open  iss-realsecure
912/tcp  open  apex-mesh
1033/tcp open  netinfo
2869/tcp open  icslap
5357/tcp open  wsdapi
MAC Address: 00:E0:1C:3C:18:79 (Cradlepoint)
Nmap scan report for localhost (192.168.1.101)
Host is up (0.0041s latency).
All 1000 scanned ports on localhost (192.168.1.101) are closed
MAC Address: 14:F6:5A:CE:EE:2A (Xiaomi)
Nmap scan report for localhost (192.168.1.103)
Host is up (0.00027s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
```

```
445/tcp   open   microsoft-ds
512/tcp   open   exec
513/tcp   open   login
......
49157/tcp open   unknown
MAC Address: 00:0C:29:DE:7E:04 (VMware)
Nmap scan report for localhost (192.168.1.102)
Host is up (0.0000040s latency).
Not shown: 998 closed ports
PORT     STATE SERVICE
80/tcp    open   http
9876/tcp open   sd
Nmap done: 256 IP addresses (9 hosts up) scanned in 3.39 seconds
```

从输出信息中，可以看到共扫描了 256 个地址。其中，九台主机是活动的，并且共用时间为 3.39 秒。由于章节的原因，以上只列举了五台主机的扫描结果。其中，中间部分内容，使用省略号（.....）代替了。

2.2.3　排除扫描目标

当用户指定一个扫描范围时（如局域网），在该范围内可能会包括自己的主机，或者是自己搭建的一些服务等。这时，用户为了安全及节约时间，可能不希望扫描这些主机。此时，用户就可以使用--exclude 命令将这些主机排除。其中，排除单个目标的语法格式如下所示：

```
nmap [目标] --exclude [目标]
```

【示例 2-10】扫描 192.168.1.1/24 网络内除 192.168.1.101 以外的所有主机。执行命令如下所示：

```
root@localhost:~# nmap 192.168.1.1/24 --exclude 192.168.1.101
Starting Nmap 6.47 ( http://nmap.org ) at 2015-05-05 19:44 CST
Nmap scan report for localhost (192.168.1.1)
Host is up (0.00068s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE
80/tcp      open   http
1900/tcp   open   upnp
49152/tcp open   unknown
MAC Address: 14:E6:E4:84:23:7A (Tp-link Technologies CO.)
Nmap scan report for localhost (192.168.1.100)
Host is up (0.00025s latency).
Not shown: 986 closed ports
PORT     STATE SERVICE
135/tcp   open   msrpc
139/tcp   open   netbios-ssn
443/tcp   open   https
445/tcp   open   microsoft-ds
902/tcp   open   iss-realsecure
912/tcp   open   apex-mesh
1033/tcp open   netinfo
1034/tcp open   zincite-a
1035/tcp open   multidropper
1037/tcp open   ams
```

```
1039/tcp open    sbl
1041/tcp open    danf-ak2
2869/tcp open    icslap
5357/tcp open    wsdapi
MAC Address: 00:E0:1C:3C:18:79 (Cradlepoint)
Nmap scan report for localhost (192.168.1.103)
Host is up (0.00036s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE
21/tcp     open    ftp
22/tcp     open    ssh
23/tcp     open    telnet
25/tcp     open    smtp
53/tcp     open    domain
80/tcp     open    http
111/tcp    open    rpcbind
139/tcp    open    netbios-ssn
445/tcp    open    microsoft-ds
512/tcp    open    exec
513/tcp    open    login
514/tcp    open    shell
......
Nmap scan report for localhost (192.168.1.105)
Host is up (0.00026s latency).
Not shown: 995 closed ports
PORT STATE SERVICE
21/tcp    open    ftp
22/tcp    open    ssh
23/tcp    open    telnet
111/tcp open    rpcbind
445/tcp open    microsoft-ds
MAC Address: 00:0C:29:31:02:17 (VMware)

Nmap scan report for localhost (192.168.1.106)
Host is up (0.00039s latency).
Not shown: 996 closed ports
PORT    STATE SERVICE
135/tcp    open    msrpc
139/tcp    open    netbios-ssn
445/tcp    open    microsoft-ds
1025/tcp open    NFS-or-IIS
MAC Address: 00:0C:29:C7:6A:2A (VMware)
......
Nmap scan report for localhost (192.168.1.102)
Host is up (0.0000030s latency).
Not shown: 998 closed ports
PORT     STATE SERVICE
80/tcp     open    http
9876/tcp open    sd
Nmap done: 255 IP addresses (8 hosts up) scanned in 3.05 seconds
```

从输出信息中，可以看到共扫描了 255 个 IP 地址。其中，八个主机是活动的。由于章节的原因，中间省略了一部分内容。

用户使用--exclude 选项，可以指定排除单个主机、范围或者整个网络块（使用 CIDR 格式）。例如，扫描 192.168.1.1/24 网络内，除 192.168.1.100-192.168.1.103 之外的所有主机。则执行命令如下所示：

```
root@localhost:~# nmap 192.168.1.1/24 --exclude 192.168.1.100-103
Starting Nmap 6.47 ( http://nmap.org ) at 2015-05-05 19:45 CST
Nmap scan report for localhost (192.168.1.1)
Host is up (0.0012s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE
80/tcp    open  http
1900/tcp  open  upnp
49152/tcp open  unknown
MAC Address: 14:E6:E4:84:23:7A (Tp-link Technologies CO.)
Nmap scan report for localhost (192.168.1.104)
Host is up (0.00028s latency).
Not shown: 997 closed ports
PORT   STATE SERVICE
22/tcp  open  ssh
80/tcp  open  http
443/tcp open  https
MAC Address: 00:0C:29:C3:1F:D7 (VMware)
Nmap scan report for localhost (192.168.1.105)
Host is up (0.00019s latency).
Not shown: 995 closed ports
PORT   STATE SERVICE
21/tcp  open  ftp
22/tcp  open  ssh
23/tcp  open  telnet
111/tcp open  rpcbind
445/tcp open  microsoft-ds
MAC Address: 00:0C:29:31:02:17 (VMware)
Nmap scan report for localhost (192.168.1.106)
Host is up (0.00017s latency).
Not shown: 996 closed ports
PORT    STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
1025/tcp open  NFS-or-IIS
MAC Address: 00:0C:29:C7:6A:2A (VMware)
Nmap scan report for localhost (192.168.1.107)
Host is up (0.0014s latency).
Not shown: 984 closed ports
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
443/tcp    open  https
445/tcp    open  microsoft-ds
```

```
554/tcp    open   rtsp
902/tcp    open   iss-realsecure
912/tcp    open   apex-mesh
2869/tcp   open   icslap
5357/tcp   open   wsdapi
10243/tcp open   unknown
49152/tcp open   unknown
49153/tcp open   unknown
49154/tcp open   unknown
49155/tcp open   unknown
49156/tcp open   unknown
49157/tcp open   unknown
MAC Address: 00:0C:29:DE:7E:04 (VMware)
Nmap done: 252 IP addresses (5 hosts up) scanned in 2.27 seconds
```

从以上输出信息中，可以看到共扫描了 252 个主机。其中，有五个主机是活动的，其地址分别是 192.168.1.1、192.168.1.104、192.168.1.105、192.168.1.106 和 192.168.1.107。根据输出的信息，可以发现没有对 192.168.1.100-103 之间主机进行扫描。

2.2.4 排除列表中的目标

当用户排除扫描的目标很多时，也可以将这些目标主机的 IP 地址写入到一个文本文件中。然后，使用--excludefile 选项来指定排除扫描的目标。其中，排除扫描列表中目标的语法格式如下所示：

```
nmap [目标] --excludefile [目标列表]
```

【示例 2-11】使用 Nmap 扫描 192.168.1.0/24 网络内主机，但是排除 list.txt 文件列表中指定的目标。具体操作步骤如下所示：

（1）创建 list.txt 文件，并写入要排除扫描目标的 IP 地址。如下所示：

```
root@localhost:~#vi list.txt
192.168.102
192.168.1.103
192.168.1.104
192.168.1.105
```

在以上列表文件中，指定排除扫描以上四个 IP 地址的主机。

（2）实施扫描。执行命令如下所示：

```
root@localhost:~# nmap 192.168.1.0/24 --excludefile list.txt
Starting Nmap 6.47 ( http://nmap.org ) at 2015-05-05 19:46 CST
Nmap scan report for localhost (192.168.1.1)
Host is up (0.0014s latency).
Not shown: 997 closed ports
PORT     STATE SERVICE
80/tcp       open   http
1900/tcp   open   upnp
49152/tcp open   unknown
MAC Address: 14:E6:E4:84:23:7A (Tp-link Technologies CO.)
Nmap scan report for localhost (192.168.1.100)
Host is up (0.00021s latency).
Not shown: 986 closed ports
PORT     STATE SERVICE
```

```
135/tcp   open   msrpc
139/tcp   open   netbios-ssn
443/tcp   open   https
445/tcp   open   microsoft-ds
902/tcp   open   iss-realsecure
912/tcp   open   apex-mesh
1033/tcp open   netinfo
1034/tcp open   zincite-a
MAC Address: 00:E0:1C:3C:18:79 (Cradlepoint)
Nmap scan report for localhost (192.168.1.106)
Host is up (0.00014s latency).
Not shown: 996 closed ports
PORT   STATE SERVICE
135/tcp   open   msrpc
139/tcp   open   netbios-ssn
445/tcp   open   microsoft-ds
1025/tcp open   NFS-or-IIS
MAC Address: 00:0C:29:C7:6A:2A (VMware)
Nmap scan report for localhost (192.168.1.107)
Host is up (0.0010s latency).
Not shown: 984 closed ports
PORT      STATE SERVICE
135/tcp    open   msrpc
139/tcp    open   netbios-ssn
443/tcp    open   https
445/tcp    open   microsoft-ds
554/tcp    open   rtsp
902/tcp    open   iss-realsecure
912/tcp    open   apex-mesh
2869/tcp   open   icslap
5357/tcp   open   wsdapi
10243/tcp open   unknown
49152/tcp open   unknown
49153/tcp open   unknown
MAC Address: 00:0C:29:DE:7E:04 (VMware)
Nmap scan report for localhost (192.168.1.102)
Host is up (0.0000030s latency).
Not shown: 998 closed ports
PORT    STATE SERVICE
80/tcp    open   http
9876/tcp open   sd
Nmap done: 253 IP addresses (5 hosts up) scanned in 3.31 seconds
```

从以上输出信息中，可以看到扫描的所有目标中，共有五台主机是活动的。

2.4　实施全面扫描

在使用 Nmap 工具实施扫描时，使用不同的选项，则扫描结果不同。用户可以使用不同的选项，单独扫描目标主机上的端口、应用程序版本或操作系统类型等。但是，大部分人又不太喜欢记这些选项。

这时候，用户只需要记一个选项-A 即可。该选项可以对目标主机实施全面扫描，扫描结果中包括各种类型的信息。其中，实施全面扫描的语法格式如下所示：

```
nmap -A [目标]
```

【示例 2-12】使用 Nmap 工具对目标主机 192.168.1.105 实施全面扫描。则执行命令如下所示：

```
root@localhost:~# nmap -A 192.168.1.105
Starting Nmap 6.47 ( http://nmap.org ) at 2015-05-06 15:20 CST
Nmap scan report for localhost (192.168.1.105)
Host is up (0.00028s latency).
Not shown: 995 closed ports
PORT    STATE SERVICE    VERSION
21/tcp    open    ftp              vsftpd 2.2.2                                #FTP 服务版本为 2.2.2，供应商是 Vsftpd
| ftp-anon: Anonymous FTP login allowed (FTP code 230)                        #允许匿名登录
|_drwxr-xr-x       2 14          0                4096 Apr 03 06:10 pub      #FTP 服务的根目录为 pub
22/tcp    open    ssh               OpenSSH 5.3 (protocol 2.0)                #SSH 服务版本是 5.3，供应商是 OpenSSH
| ssh-hostkey:                                                               #SSH 服务密钥
|     1024 83:9f:d0:8e:29:3c:7f:d9:11:da:a8:bb:b5:5a:4d:69 (DSA)
|_    2048 2e:ea:ee:63:03:fd:9c:ae:39:9b:4c:e0:49:a9:8f:5d (RSA)
23/tcp    open    telnet          Linux telnetd                               #Telnet 服务
111/tcp open    rpcbind         2-4 (RPC #100000)
| rpcinfo:                                                                   #RPC 详细信息
|     program version        port/proto        service
|     100000    2,3,4          111/tcp          rpcbind
|     100000    2,3,4          111/udp          rpcbind
|     100024    1              34525/tcp        status
|_    100024    1              51866/udp        status
445/tcp open    netbios-ssn Samba smbd 3.X (workgroup: MYGROUP)#Samba 服务版本为 3.X，供应商为 smbd
MAC Address: 00:0C:29:31:02:17 (VMware)                                        #目标主机的 MAC 地址
Device type: general purpose                                                   #设备类型
Running: Linux 2.6.X|3.X                                                      #正在运行的系统
OS CPE: cpe:/o:linux:linux_kernel:2.6 cpe:/o:linux:linux_kernel:3              #操作系统中央处理单元
OS details: Linux 2.6.32 - 3.10                                                #操作系统详细信息
Network Distance: 1 hop                                                        #网络距离
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel                 #服务信息
Host script results:
| smb-os-discovery:                                                          #SMB 操作系统发现
|     OS: Unix (Samba 3.6.9-151.el6)                                         #操作系统为 Unix，Samba 版本为 3.6.9
|     Computer name: router                                                  #计算机名
|     NetBIOS computer name:                                                 #NetBIOS 计算机名
|     Domain name:                                                           #域名
|     FQDN: router                                                           #完全合格域名（FQDN）
|_    System time: 2015-05-06T15:20:28+08:00                                 #系统时间
| smb-security-mode:
|     Account that was used for smb scripts: <blank>
|     User-level authentication
|     SMB Security: Challenge/response passwords supported
|_    Message signing disabled (dangerous, but default)
|_smbv2-enabled: Server doesn't support SMBv2 protocol
TRACEROUTE
HOP RTT       ADDRESS
```

```
1     0.28 ms localhost (192.168.1.105)
OS and Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.51 seconds
```

从以上输出的信息，可以明显看出比前面例子扫描结果更详细。在以上输出信息中，可以看到目标主机上开启的端口、服务器、版本、操作系统版本、内核、系统类型等。根据分析输出的信息，可知目标主机上运行了 FTP、SSH、Telnet 等服务，并且可以看到各服务的版本及权限信息。而且，还可以知道目标主机的操作系统是 Linux，内核版本为 2.6.32 等。