Nmap 应用指南

Nmap 应用指南

Nmap 是一个著名的开源工具，它是在 20 世纪 90 后期出现的。2003 年，在电影《黑客帝国 2》中 Tritnity 曾用 Nmap 2.54BETA25 版攻击 SSH 服务器， 破坏发电厂的安全，Nmap 因此受到了普遍关注。在现实生活中，Nmap 主要用于确定网络上的主机，主机提供的服务，以及扫描网络的开放端口等等。Nmap 是安全专家用以映射他们的网络和测试安全漏洞的有价值的工具，有人担心黑客帝国中的情况的出现，因为 Nmap 也是恶意黑客的利用的工具，被用来查找可以攻击的开放端口。本专题将给安全专家提供一些指南，包括在企业环境中，如何在 windows 和 Linux 平台上安装 Nmap，以及 Nmap 的设置，运行和评估。

黑客帝国中的 Nmap

Nmap 的简介

Nmap（Network Mapper，网络映射器）是 Fyodor 编写的，目前已经升级到了第四版。它是一种免费的开源软件工具，允许许多网络管理员在不增加预算的情况下，运行自己的扫描并且找到开放的端口，测试安全漏洞。

- **Nmap：有价值的开源软件网络安全工具**
- **Nmap 4.01 改善了多种功能**

Nmap 的安装和设置

Nmap 原来是用于 Unix 系统的命令行应用程序。但是，自从 2000 年以来，这个应用程序就有了 Windows 版本。 而 Linux 是运行 Nmap 工具软件最常用的平台。事实上，大多数 Linux 发布版都包含 Nmap，尽管 Nmap 也许不是默认安装的。

- **在 Windows 中安装和设置 Nmap**
- **在 Linux 中安装和设置 Nmap**

Nmap 的端口扫描技术和应用

Nmap 是进行一种简单的网络目录或者安全漏洞评估的理想的工具。按照默认的设置，Nmap 能够进行同步扫描。这种扫描可依靠任何合适的 tcp 栈，而不是依靠具体平台的性质。此外，Nmap 还提供 Nmap 的 TCP Null (选项 -sN)、 FIN (选项 -sF)和 Xmas (选项 -sX)等选项扫描。而 IPID 空闲扫描(选项 -sI) 能够在某些环境中穿过数据包过滤器。Nmap 还提供另一种扫描，也就是 TCP ACK 扫描(选项 -sA)，来帮助描绘出防火墙的规则。

- **Nmap：扫描端口和服务**
- **Nmap：更多的端口扫描技术**

- **Nmap：防火墙设置测试**
- **Nmap：改善扫描时间的技术**
- **Nmap：Nmap 扫描结果说明与作用**
- **Nmap：语法分析器和界面**

Nmap 优劣比较

在决定使用什么软件工具执行什么具体任务的时候，重要的是评估什么软件能够做到，确保这个软件工具的功能符合你的需求，理解能够提供什么帮助和支持，对拥有的总成本进行一次评估。Nmap 已经出现好几年了，赢得了许多奖励，并且能够应用于许多操作系统，使它成为了网络探索和安全审计的工具选择。Nmap 是一种优秀的工具，如果说它没有超过市场的任何商业性软件，至少它与那些商业软件是同样好的。

- **Nmap 与开源软件的争论**

Nmap 应用指南之一：有价值的开源软件网络安全工具

要争取增加你的 IT 安全预算通常是一件很困难的任务。因此，许多网络管理员使用免费的开源软件工具来帮助他们完成任务。但是，他们如何依靠没有商业性技术支持并且从来没有经过测试版的软件呢?如果你那样想的话，你需要再考虑一下。许多开源软件工具目前在功能、可靠性和帮助论坛方面都比商业性软件有优势。特别是 Nmap 已经成为许多网络和安全管理员选择的工具。他们要用这个工具映射他们的网络和测试安全漏洞。

Nmap (Network Mapper，网络映射器)安全扫描器是 Fyodor 编写的，目前已经升级到了第四版。这个软件工具提供了广泛的端口扫描技术，旨在快速扫描大小网络，进行网络探查和安全检查。这个具有多种功能的工具能够确定网络上有什么主机，这些主机提供什么服务，正在使用的是什么类型的数据包过滤器和防火墙。这个工具还能够远程识别一台机器的操作系统。这个工具软件支持大多数 Unix 和 Windows 平台，还支持 Mac OS X 和若干种掌上设备。这个软件有命令行和图形用户界面两种模式，对于不熟悉命令提示符的那些系统管理员来说这是很幸运的。

那么，你为什么需要一个网络扫描器呢?Nmap 是一种人们喜爱的黑客工具。因此，运行你自己的扫描并且找到开放的端口，看看你的网络正在向潜在的攻击者泄露什么信息，是很有意义的。例如，一台 Windows 计算机能够使用数百个端口与其它的机器进行通信，每一个端口都是攻击者进入你的网络的潜在的途径。使用 Nmap 进行扫描是找到哪一个端口处于开放状态、这些端口正在运行什么服务以及你的防御弱点在哪里的有效方法。当你找到开放的端口时，你可以关闭任何不须要得端口，从而减少可能被利用的服务的数量。当你已经映射你的网络的时候，你还可以看看自从上一次扫描之后发生了什么意料之外的变化。例如，一台被蠕虫感染的机器将设法打开端口以便听从蠕虫的控制者发出的指令。

Nmap获得了许多奖，其中包括“Linux Journal”杂志的最佳安全工具编辑选择奖。其它荣誉还包括电影《黑客帝国 2:重装上阵》中使用了介绍了这个软件的功能，此外，美

国总统布什视察国家安全局的照片上也出现了这个软件。因此，如果你要把这个用途最多的网络工具增加到你的工具箱中，并且要发现黑客能够从你的网络中了解到什么信息，你应该在www.insecure.org网站下载这个软件。

（作者：Michael Cobb　来源：TT 中国）

网络工具介绍:Nmap 4.01 改善了多种功能

Nmap 也许是一种最著名的端口扫描器和许多其它扫描工具进行对照的标准。Nmap 是 Insecure.org 根据 GPL 许可证协议免费提供的，能够在现有的任何操作系统上运行，从微软的 Windows 到你喜欢的 Linux/Unix 操作系统都可以。

在 Nmap 软件的生命周期中，Nmap 4.01 的核心端口扫描引擎是成熟的、功能强大的、能够扫描 IPv4 和 IPv6 主机，而且不管这些主机是否受到防火墙的保护。

我们实验室在一台运行 SUSE 9 Linux 操作系统的工作站平台上进行了一次测试，结果表明 Nmap 4.01 比 Nmap 3.81 发布版的速度提高了大约 10%。考虑到每个端口的 SYN 扫描大约需要 1.5 秒，当扫描少量的端口时，这个差别用户可能是察觉不到的。

Nmap 4.01 发布版的大的改进是在服务和操作系统识别方面。如果你愿意让 Nmap 在主机上花大量的时间(根据主机上打开端口/服务的数量以及使用的命令行选项，我们测试结果是用 15 秒至 90 秒)，这个应用软件能够告诉你有关被扫描的目标服务器上运行的服务的大量信息，包括服务类型和版本号等(如 Microsoft IIS 6.0)。

Nmap 已经把它的数据库扩大到了包含大约 380 个服务协议的 3000 多个签名。这是一种非常方便的工具，可用来确定主机是否在运行有安全漏洞的版本的服务，并且能够告诉你需要采取什么步骤来修复这些安全漏洞。

Nmap 4.01 中的操作系统识别结果比我们在 Nmap 3.81 版中获得结果要好一些，但是，这个漂亮的功能仍有改进的空间，如速度和准确性等。例如，Nmap 能够准确识别一台 VMware ESX 服务器上运行的 Windows 2003 SP1 VMware 目标，但是，不能在不同的 ESX 服务器上识别出 Windows NT SP6a 目标(它只能把后者识别为一般的 Windows 主机)。

Nmap 的服务和操作系统识别部分是安全团体最感兴趣的。因此，我们预计这些功能在未来的版本中将会得到改善。

应用程序源代码和二进制安装数据包这两种方式都有，因此，你应该能够通过标准的方法安装和运行这个应用程序，包括用于 Linux 的 RPM 安装程序。如果你不打算自己汇编这个程序，你还简单地解开 Windows 二进制压缩文件就可以使用。

Linux 版本提供了图形用户接口，能够帮助用户熟悉“开始”菜单的各种选择和运行 Nmap。这个图形用户接口非常好，不过，坦率地说，它只是一个覆盖在 Nmap 程序支持的丰富的指令行标识上面的一层皮，仅仅对一些新手有价值。如果你还不熟悉这个软件，你要尽快学习这个命令行接口，这样，你将能够从这个多功能工具中得到更多的价值。

Nmap 是许多系统管理员工具箱中不可缺少的工具，是利用管理良好和有用的开源软件计划完成任务的最好的例子之一。这个软件是免费的。如果你到目前为止还没有使用过这个软件，你可以现在就下载并且开始研究它高深莫测的能力。

（作者：Peter Giannacopolous　来源：TT 中国）

Nmap 应用指南之二：在 Windows 中安装和设置 Nmap

本文是关于如何在企业环境中使用 Nmap 安全工具的系列应用指南的第二讲。

Nmap 原来是用于 Unix 系统的命令行应用程序。但是，自从 2000 年以来，这个应用程序就有了 Windows 版本。本指南将介绍这个开源软件网络扫描器的 Windows 版本的安装和设置。

虽然你可以从Zip文件下载和安装Nmap，但是，最新版本还需要安装免费的WinPcap数据包捕捉库。我建议你选择使用Nmap Windows安装程序。这个安装程序能够为你处理WinPcap安装。这个安装程序的文件名是nmap-4.01-setup.exe，下载网址是http://www.insecure.org/nmap/download.html。这个安装程序不向程序菜单增加Nmap的快捷方式，因为你需要在DOS命令提示符下面运行nmap.exe。虽然添加/删除模板中没有出现WinPcap程序，但是，如果你要删除Nmap程序，你需要在Nmap文件夹中运行卸载程序。这个程序全部安装完毕之后仅占用 2.6MB的空间。

这个软件默认的安装目录是 C:\Program Files\Nmap\。但是，由于安装程序在计算机的“路径”变量环境中增加了 Nmap 程序，你可以在任何目录下执行 Nmap 程序。因此，要运行和测试 Nmap，你可以打开命令提示符窗口，然后输入如下命令:nmap -A -T4 scanme.insecure.org，就可以开始扫描 scanme.insecure.org 网站主机。

A 和 T4 的选项启动了操作系统和版本检测，并且把时间模板设置为“积极的”。这个程序有数百个命令行选项，其中一些选项我们将在今后的应用指南中介绍。请注意，命令行是区分大小写的。

在Windows平台上的Nmap程序没有在Unix平台上的效率高，特别是连接扫描(-sT)经常是速度非常慢，因为Windows的网络应用程序接口有缺陷。你可以用鼠标双击Nmap目录中的nmap_performance.reg文件来提高连接扫描的性能。这个操作将在注册表中做出三个修

改，以便增加为Nmap等应用程序保留的临时端口数量，减少一个关闭的连接的重新使用之前的时间。如果你在运行Windows平台的Nmap软件时遇到了问题，你可以查看Windows事件记录中的错误信息，然后查看http://seclists.org/#nmap-dev网站的“Nmap-dev”列表中是否包含了这个错误。还有一个网页上有许多Nmap软件的技术支持文件，网址是http://www.insecure.org/nmap/docs.html。订阅Nmap-黑客邮件列表也是值得的。

Nmap作为一个命令行的应用程序的主要优势是，这个程序很容易从脚本程序运行，不需要设置许多不同的选项就能够进行准确的扫描。然而，新手和不常使用这个程序的人会感到很害怕。虽然这个软件有用于Unix平台的图形用户接口，但是，还没有用于Windows平台的稳定的接口。幸运的是这种情况今年将发生变化。目前还没有正式的发布日期。但是，Nmap的制作者Fyodor希望今年推出一个兼容Windows版本的NmapFE。NmapFE是最流行的用于Unix的图形用户接口。目前还有一些跨平台的图形用户接口正在开发之中，如UMIT (http://umit.sourceforge.net/)。

(作者：Michael Cobb 来源：TT中国)

Nmap 应用指南之三：在 Linux 中安装和设置 Nmap

Linux 用户可以选择源代码安装，或者选择由分销商提供的 RPM 等二进制软件包安装。源代码安装更灵活一些，可以确定如何建立 Nmap 程序，并且按照你的系统进行优化。

本文是关于如何在企业环境中使用 Nmap 安全工具的系列应用指南的第三讲。

Linux 是运行 Nmap 工具软件最常用的平台。事实上，大多数 Linux 发布版都包含 Nmap，尽管 Nmap 也许不是默认安装的。即使你的系统已经有了一个 Nmap 软件，你还应该考虑升级到最新的版本，下载的网址是:http://www.insecure.org/nmap/download.html(注:并非所有的 Nmap 发布版都有一种特殊的 Nmap 计划签名密钥。这个密钥可以从这个网站获得:http://www.insecure.org/nmap/data/nmap_gpgkeys.txt)

Linux 用户可以选择源代码安装，或者选择由分销商提供的 RPM 等二进制软件包安装。源代码安装更灵活一些，可以确定如何建立 Nmap 程序，并且按照你的系统进行优化。二进制软件包的安装速度更快，更方便，通常是按照分销商提供的标准目录路径和设置进行个性化安装。在涉及到在系统上升级软件的问题时，这些软件包还能够进行更简单的管理。Nmap 软件包仅包含命令行的可执行命令和数据文件，而 Nmap 前端数据包还包括一个可以选择的名为“NmapFE”的 X-Window 图形用户接口。

从源代码汇编和安装 Nmap 是安装这个软件的一种最有力的方法，可以保证你有最新的版本，而且 Nmap 还能够适应你的具体系统的库和目录结构。这个构建的系统旨在尽可能地进行自动检测，但是，还有几十个命令行参数和环境变量能够影响 Nmap 的构建方式。我建议你运行“./configure”命令来看一下帮助文件。

通过 RPM 安装 Nmap 也很简单。但是，如果你确实有问题，例如，如果你的库版本与最初建立 RPM 用的库版本有很大不同，你可以从原来的 RPM 建立和安装你自己的二进制 RPM。

要运行和测试 Nmap，输入:nmap -A -T4 scanme.insecure.org

这个命令将在外壳提示符下扫描主机 scanme.insecure.org。A 和 T4 选项启动操作系统和版本检测，并且把时间模板设置为“积极的”。命令行选项有一百多个，其中一些选项我们将在以后的指南中介绍。

如果你在运行Nmap程序时发生了问题，滚动输出屏幕并且查看第一个错误信息。然后，查看http://seclists.org/#nmap-dev网站的Nmap-dev列表存档文件中是否包含这个问题。http://www.insecure.org/nmap/docs.html网站还有许多Nmap的技术支持文件，因此订阅Nmap-黑客邮件列表是值得的。

由于Nmap是一个命令行的应用程序，因此它很容易从脚本程序运行，而且不需要设置许多不同的选项就能够进行准确的扫描。然而，对于那些不适应命令提示符操作的管理员来说，还有一些用于Linux的图形用户接口。NmapFE是最常用的。它提供了许多选项，全部可以用来建立一个适当的Nmap命令。在构建的过程中，窗口的底部将显示Nmap命令行。这是学习命令行参数的一种有用的方法。最后，Nmap支持许多掌上电脑，包括夏普的Zaurus和Compaq IPAQ。要进一步了解这些信息，请参考http://www.insecure.org/nmap/install/inst-pda.html网站的教学。

(作者：Michael Cobb 来源：TT 中国)

Nmap 应用指南之四：扫描端口和服务

这是在企业环境中如何使用 Nmap 的系列应用指南的第四部分。

Nmap 是进行一种简单的网络目录或者安全漏洞评估的理想的工具。按照默认的设置，Nmap 能够进行同步扫描。这种扫描可依靠任何合适的 tcp 栈，而不是依靠具体平台的性质。Nmap 能够用来快速扫描数千个端口，它能够清楚地和可靠地区分端口是处于打开、关闭和过滤的状态。

对主机www.yourorg.com进行同步扫描，你可以使用这个命令

nmap www.yourorg.com

虽然这并不是很重要，但是，如果你有你的Unix或者Linux服务器的root访问权限，或者在一台Windows机器上使用管理员账号，那就是最好的。因为大多数类型的扫描都是发送和接收原始数据包，因此，这些数据包仅提供给有权限的用户。如果你没有必要的权限，或者你在扫描一个IPv6 网络，你可以使用这个命令“nmap -sT www.yourorg.com”进行一次TCP连接扫描。Nmap最多可以扫描 1024 个端口，以及在Nmap服务文件中列出的更多的端口。你可以使用“-p”指定你要扫描的端口，如:nmap -p U:53,T:21-25 www.yourorg.com。这个命令就是仅扫描UDP端口 53 和TCP端口 21 至 25。

一旦你发现一台机器的可以看到的端口，你需要知道这些端口在运行什么服务，以便把这些端口做成目录或者确定利用哪一个端口可以对机器实施攻击。“-sV”选项能够启动版本检测查询，但是，更好的选项是“-A”。这个选项即可以检测操作系统又可以检测版本。下面使用 Nmap 服务检测数据库设法确定服务协议、应用程序名称、版本号码、主机名、设备类型、操作系统系列和其它详细的情况，如 SSH 协议版本或者一台 X 服务器是否开放了连接:

nmap -A www.yourorg.com

如果 Nmap 程序支持 OpenSSL，它甚至能够连接到一台 SSL 服务器以推测在那个加密层后面监听到服务。运行版本检测的另一个好处是 Nmap 将设法得到 TCP 或者 UDP 端口回答简单的扫描不能确定的端口是处于打开状态还是过滤状态。如果获得成功，Nmap 将把这个状态改为打开。

Nmap 为人类和机器的消费提供各种输出格式，包括 XML 格式。这些数据可以移植到数据库中或者让 Nmap 图形用户接口 NmapFE 的程序进行解析。例如，可以增加下列选项:“-oX”和“-oN”。

你可以保存正常的输出用于自己查阅，同时把同样的扫描结果存储为 XML 版本以便进行编码分析。如:

nmap -A -oX scanreport.xml -oN scanreport.txt www.yourorg.com

还有一些控制输出细节以及各种调试信息的选项。如果持续可很长时间的扫描由于某种原因一直不能完成，在恢复扫描的时候这个扫描将从它上一次停止时查询的地方接着进行扫描。遗憾的是，这种功能不支持 XML 格式的输出。

在下一期 Nmap 应用指南中，我们将介绍更多的 Nmap 扫描技术，包括空闲扫描。

(作者：Michael Cobb 来源：TT 中国)

Nmap 应用指南之五：更多的端口扫描技术

这是在企业环境中如何使用 Nmap 的系列应用指南的第五部分。

我们在上一期指南中介绍了扫描网络和服务的基本的 Nmap 命令。在这一期应用指南中，我要介绍一些利用某些具体平台或者协议的性质进行的扫描以便更好地区分打开的和关闭的端口。

Nmap 的 TCP Null (选项 -sN)、 FIN (选项 -sF)和 Xmas (选项 -sX)等选项扫描 RFC 793 介绍的 TCP 协议技术规范中的细小的安全漏洞。当扫描符合这个 RFC 标准(如大多数基于 Unix 的系统)的系统时，如果这个端口是关闭的，任何不包含 SYN、RST 或者 ACK 等固定字节的数据包都会返回一个 RST(重置)数据包。如果这个端口时打开的，那就什么都不会返回。如果收到一个 RST 数据包，这个端口就被认为是关闭的。如果没有反应，就意味着这个端口是打开的或者可能是过滤的。这些扫描的关键好处是它们能够穿过某些非监控状态的防火墙和过滤数据包的路由器。

能够在某些环境中穿过数据包过滤器的另一种扫描是 IPID 空闲扫描(选项 -sI)。通过使用网络上的另一种设备(一般称作“zombie”)，Nmap 的空闲扫描不用从自己的 IP 地址发送一个数据包就能够从一台远程设备上收集到端口信息。任何入侵检测系统都将把无辜的“zombie”报告为攻击者。但是，更重要的是这种扫描能够用来描绘出机器之间基于 IP 地址的可信赖的关系，因为空闲扫描结果是从“zombie”机器的角度显示打开的端口。例如，对一个数据库服务器的扫描可能显示没有打开的端口。但是，通过使用一台文件服务器的 IP 地址作为这个“zombie”机器，数据库服务器上与数据库相关的服务端口也许会显示端口已打开并且暴露可信赖的关系。如果通过使用 Nmap 探索你的网络，你将意识到这可能是与 IPID 有关的攻击，然后，你需要设置或者调整你的防火墙和路由器规则以拒绝假冒源地址发来的数据包。另外，你应该启用出口过滤功能阻止欺骗性的数据包离开你的网络。阻止你的内部用户发动这种类型的攻击。

Nmap 还提供另一种扫描，也就是 TCP ACK 扫描(选项 -sA)，来帮助描绘出防火墙的规则。这种扫描不能确定端口是打开还是关闭的。但是，这种扫描能够告诉你这个端口是不是过滤的，这个设备过滤的端口是否处于监控状态。

我们在下一期应用指南中将研究防火墙回避问题，同时，你可以通过发出带有各种不同的标识设置(flag settings)的探测类型来测试和分析你的防火墙。尽管 Nmap 包含几种不同类型的扫描，你还可以使用定制的 TCP 扫描(选项-- scanflags)来指定任意的 TCP 标识来设计你自己的扫描。例如，你可以使用如下命令运行一个 SYN|FIN 扫描:

```
nmap -sF --scanflags SINFIN -p20-25 www.yourorg.com.
```

(作者：Michael Cobb 来源：TT 中国)

Nmap 应用指南之六：防火墙设置测试

本文是如何在企业环境中使用 Nmap 软件的系列应用指南的第六讲。

在到目前为止的应用指南中，我们考察了如何使用 Nmap 映射一个网络和检查 Nmap 暴露的潜在的攻击者的什么信息。在本期应用指南中，我们将研究如何使用 Nmap 测试你的防火墙配置的有效性。

理解你的防火墙如何处理不请自来的通讯的最佳方法之一是验证你的防火墙的过滤器和规则正在按照你的预期工作。例如，例如，许多管理员在制定允许通讯穿过防火墙的规则时犯的错误之一是仅仅根据其来源端口的编号就信任这个通讯，如端口 53 的 DNS 应答或者端口 20 的 FTP 等。要测试你的防火墙是否允许所有的通讯经过一个特定的端口，你可以充分利用 Nmap 的 TCP 扫描功能，包括 SYN 扫描，对欺骗性的源端口号码选择进行扫描。仅仅提供一个端口号码， Nmap 就会从那个端口发送数据包。例如，使用下面的命令将运行一次 FIN 扫描，使用一个欺骗性的源端口号码 25(SMTP)，把输出结果存储名为“firewallreport.txt”的文件。

```
nmap -sF -g 25 -oN firewallreport.txt www.yourorg.com
```

测试你的防火墙应付碎片数据包通讯的能力也是值得的。攻击者经常把 TCP 头文件分为几个数据包，使数据包过滤器和入侵检测系统很难检测到这种攻击。虽然碎片数据包不能通过对所有的 IP 碎片进行排列检查的数据包过滤器和防火墙，但是，许多设备为了避免性能下降在默认的状态下都关闭了排列检查功能。可以增加“-f”选项来设置扫描发送碎片式的 IP 数据包。

在审查你的防火墙的时候，我建议你按照数字的顺序(选项 -r)进行扫描。这样，在分析 Nmap 输出文件时就很容易跟上通讯流。然而，在测试防火墙和入侵检测系统的效率时，你可以使用默认的方式进行扫描，也就是随机的端口顺序。在随机顺序的端口扫描

中，可以使用随机的主机选项对主机进行扫描，随机的主机的缩写字是“-rH”。这个选项与我们将在下个星期介绍的减缓时间的选项结合在一起将使你拥有的任何网络监视设备努力工作以检测扫描的结果。测试你的网络防御能力的一个命令的例子是:

```
nmap -sS --scan-delay 500 -f -rH firewallreport.txt www.yourorg.com
```

一旦你发现任何没有过滤的端口或者其它问题，你应该审查你的防火墙规则以确保对所有服务的访问在控制之下，过滤器和规则正在按计划发挥作用。经过修改之后，再一次运行 Nmap，以检查你取得满意结果的机会。Nmap 提供了许多饶过配置不佳的防火墙的功能，因此可以扮演一个攻击者的角色并且发现你的网络防御是否能够应付 FTP 反弹扫描、空闲扫描和碎片攻击。

（作者：Michael Cobb　来源：TT 中国）

Nmap 应用指南之七：改善扫描时间的技术

这是在企业环境中如何使用 Nmap 软件的系列应用指南的第七讲。

你运行 Nmap 扫描的目标将决定你让它如何运行:缓慢而安静地、快速而激烈地、或者以介于两者之间的方式。因此，Nmap 包括各种定时选项，能够让你影响到扫描的几乎每一个方面。

按照默认的设置，Nmap 不会因为时间问题中途停止进行扫描，无论这个扫描需要多长时间才能完成。主机超时选项(-- host_timeout)能够使这个扫描失效。这个选项在放弃对一个 IP 地址的扫描之前将设定扫描的时间总长度。当在一个速度慢的连接上扫描一台设备时或者在扫描一台反应速度慢的设备时，这个功能是有用的。

Nmap 其它的定时选项基本上可以分为四类:往返时间、延迟、并行主机扫描和并行端口扫描。往返时间是接收 Nmap 请求反应所需要的毫秒数。在扫描的时候，Nmap 自动调整其反应时间的超时。然而，你可以强制它使用较大的超时值。例如，如果你的网络掉数据包的时候，你可以使用最低往返时间超时选项(--min_rtt_timeout)。在速度慢或者有问题的网络上进行扫描时，这个选项能够使扫描更准确。

探测之间的最小延迟选项(--scan_delay)能够让你设置每一次探测帧之间的延迟，以便根据需要加快或者减缓扫描的速度。例如，这个选项让你能够在速度慢的链路上进行扫描，或者避开一台入侵探测设备。同样，你可以使用探测之间的最大延迟选项(--max_scan_delay)来设置 Nmap 在每一次请求之间延迟的上限时间。这个选项能够显著减慢总的扫描时间。但是，这个选项对于速度慢的或者阻塞的广域网连接是非常有用的。并行托管的扫描和并行端口扫描选项用于设置同时扫描的端口的最大和最小数量。这些选项可以用来改善无人看管的批量扫描的效率，或者通过减少同时扫描主机的数量让 Nmap 更快地显示结果。

如果你不想单独设置这些选项，你可以使用预先定义的定时政策替代这些设置。这些范围从缓慢、平静到准确到快速、大声和不太准确。这些定时政策选项(--timing)对于测试入侵检测和入侵防御系统是很有用的。通过运行每一个定时政策，你可以根据何时和是否报警或者数据包过滤事件是否发生等情况调整你的网络监视标准。与Nmap的其它指令不同，定时选项在命令行中的位置是非常重要的，因为最后一个选项要优先执行。这就意味着你可以把定时政策放在命令行的开始位置，随后指定其它单个的定时选项并且创建一个定制的定时的组合，而不必在命令行中指定每一种可能的定时选项。例如，下面的设置是把扫描延迟设置为三分钟，而不是把“paranoid”设置为五分钟，同时保持其它政策设置不变:nmap --timing paranoid --scan_delay 3000 scanreport.txt www.yourorg.com。

(作者：Michael Cobb 来源：TT中国)

Nmap 应用指南之八：Nmap 扫描结果说明与作用

这是如何在企业网络中使用 Nmap 软件的系列应用讲座的第八讲。

你使用 Nmap 执行的正常的任务之一是验证你的防火墙规则正在按照预定要求执行。要做到这一点，运行一次扫描查看那些对外界打开的端口，检查那些端口是否进行了过滤。一次简单的防火墙审计扫描操作大致是这样的：

```
nmap -v -sA -ff -r -n www.yourorg.com -oA firewallaudit
```

上述指令的含义是，Nmap TCP ACK 扫描(-sA)证实数据包是否可以不经过过滤通过你的防火墙。通过增加-ff 选项，你还可以测试它如何处理分段的通讯。要方便地跟踪防火墙是如何处理这些数据包的，最好是按照数字顺序扫描端口。通过增加-r 选项可以实现这个目的。我还使用-oA 输出选项，这样，你可以创建一个可以检索的 grepable 文件以及一个 XML 文件用于做适当的记录和报告。你可以使用这些输出文件评估通讯流量通过任何未经过滤的端口的情况，然后根据需要修改你的防火墙设置。如果你确实修改了你的防火墙，重新运行审计扫描确认你的修改是成功的。定期运行这种审计扫描保证你的防火墙设置没有被意外地修改是一个好主意。

由于大多数新病毒和间谍软件程序在受感染的机器上制造开放的端口，在接到病毒爆发的消息之后，你应该使用Nmap软件扫描开放的端口。你可以使用一个ICMP ping (-PE)、TCP SYN和UDP扫描以及-sS和-sU选项。使用-p选项仅仅搜索特定的恶意软件专门使用的端口。一个这样的Nmap指令:nmap -PE -sS -sU -sV -p U:2140,T:2745 www.yourorg.com/24 -oG infected创建一个名为“infected”的输出文件。这个文件可用来搜索“开放的”这个词汇。在开放端口拥有未经授权的应用程序的任何机器都能够被隔离和检查。你可以使用-sV选项找出在那台机器中运行的那个应用程序。

由于许多机构有远程和虚拟办公室，定期对连接网络的设备进行审计扫描，检查安全和软件许可证问题，是非常重要的。下列扫描将产生一个客户机、服务器、以及路由器、交换机和打印机的分类目录：

```
nmap -vv -sS -O -n www.yourorg.com/24 -oA inventory
```

SYN scan (-sS)同步扫描与操作系统扫描(-O)结合在一起使用很少的数据包，同时仍然可以收集到需要的信息。如果你在一个连接速度较慢的线路上审计一个远程办公室，你可以增加一个定时的政策，如-T 2，放慢扫描速度，在目标机器上使用较少的带宽和资源。最后，当你在运行一次 Nmap 扫描的时候，你可以在不放弃扫描和重新运行扫描的情况下修改某些选项或者要求状态信息。例如，输入 V 将增加冗长的信息输出，同时，大多数键值将向你提供最新的状态，显示主机扫描已完成以及预计的剩余时间。

（作者：Michael Cobb 来源：TT 中国）

Nmap 应用指南之九：语法分析器和界面

这是如何在企业网络环境中使用 Nmap 软件的系列应用技巧讲座的第九讲。

对于一个有用的安全工具来说，你必须要能够理解这个软件告诉你的有关你的系统或者网络的设置、安全或者弱点。使用 Nmap 软件，你可以进行非常广泛的测试。要分析这个结果，你的输出记录最好采用 XML 格式，这样，这些数据就很容易移植到数据库或者转换为 HTML 格式进行分析和供人类使用。

你可以在你的Nmap命令中增加-oX选项，把Nmap软件的输出内容存储为XML格式。如:nmap -A -oX scanreport.xml www.yourorg.com

要编辑并且使这个 XML 输出更漂亮，你可以使用样式表选项(--stylesheet)。这个 XML 文件将指向一个使用 XSL 语言进行格式化和转换的样式表。XSL 语言能够解释应该如何显示 XML 文件。Nmap 包含一个名为 nmap.xsl 的默认的 XSL 样式表。你还可以参考这个最新版本的文件，在命令行加入完整的链接:

nmap -A -oX --stylesheet http://insecure.org/nmap/data/nmap.xsl scanreport.xml www.yourorg.com

参考位于 Web 上的样式表能够让你看到在一台没有安装 Nmap 或者 nmap.xsl 软件的计算机上正确格式化的结果。当然，你还可以选择使用你自己的样式表。

Nmap 作为命令行应用程序的主要好处是它能够方便地从脚本运行，并且不必使用许多不同的选项就可以进行准确的扫描。然而，这对于新手和不常使用这个软件的用户来说是很可怕的。NmapFE 是 Nmap 软件的一个前端图形 X 窗口。它的选项大多数都与 Nmap 的选项直接对应的，让你选择你的目标、设置扫描选项和查看扫描结果。它还能够向你显示在命

令行之下创建的 Nmap 命令。这对于学习创建复杂的 Nmap 命令行指令是一种非常好的方法。

(作者：Michael Cobb　来源：TT 中国)

Nmap 应用指南之十：Nmap 与开源软件的争论

本文是如何在企业网络环境中使用 Nmap 应用程序的系列讲座的最后一讲。

在决定使用什么软件工具执行什么具体任务的时候，重要的是评估什么软件能够做到，确保这个软件工具的功能符合你的需求，理解能够提供什么帮助和支持，对拥有的总成本进行一次评估。让我们看看 Nmap 是如何提供支持的。

由于 Nmap 是免费的，它在成本方面显然优于其它网络映射器。然而，许多 IT 管理员对开源软件仍持谨慎态度，他们在向高级管理层推荐涉及开源软件工具的建议时经常把缺少质量保证当作开源软件的一个缺点。对于重要的应用程序，如网络操作系统，许多人认为开源软件风险太大。然而，专有软件供应商也极少保证它们的软件能够向你提供不间断的和没有错误的运行。虽然 Nmap 没有提供质量保证，但是，它得到了热情的开发和用户支持团体的支持。尽管如果你遇到问题或者需要咨询的时候没有昂贵的热线，Nmap 还有非常好的存档文件，有最新的帮助网页、白皮书和教学资料。

成熟的开源软件，特别是在IT安全领域的软件，通常是专有软件可行的替代者。英国政府赞助的在实施开源软件方面进行的一系列试验(www.opensourceacademy.org.uk/solutions/casestudies)产生了一些有趣的结果，其结论是:用于具体任务的开源软件应用程序通常适用于这个目的，并且强调了这样一个事实，就是购买专业软件可能导致购买者遭受“隐性锁定”。然而，由于大多数开源软件是在基于Unix的机器上开始工作的，通常在原来的基础库上建立起来的Windows移植版本不能像专门为Windows编写的软件那样充分利用Windows 环境的优势。开源软件落后于专有软件竞争对手的另一个方面是集成的GUI(图形用户界面)。应该感谢的是一些GUI是为Nmap开发的，为那些喜欢不使用命令行的人开发的。

Nmap 是根据自由软件基金会发表的 GNU 一般公共许可证第二版开发的，并且还一起推出了完整的源代码。你可以根据这个许可证条款修改和重新发布。从法律的观点看，你应该阅读 Nmap 代码是如何使用的。

我肯定不是宣传开源软件是每一种情况的答案。但是，事实是，Nmap 已经出现好几年了，赢得了许多奖励，并且能够应用于许多操作系统，使它成为了网络探索和安全审计的工具选择。Nmap 是一种优秀的工具，如果说它没有超过市场的任何商业性软件，至少它与那些商业软件是同样好的。

（作者：Michael Cobb　来源：TT 中国）