网络安全

安全工具（三）

小未 主编

目　录

扫描之王 Nmap

许多人认为端口扫描器是黑客们才需要关心的工具，其实不然，知己知彼，才能百战不殆，端口扫描器是帮助你了解自己系统的绝佳助手。象 Windows2K/XP 这样复杂的操作系统支持应用软件打开数百个端口与其他客户程序或服务器通信，端口扫描是检测服务器上运行了哪些服务和应用、向 Internet 或其他网络开放了哪些联系通道的一种办法，不仅速度快，而且效果也很不错。

目前支持 Win2K/XP 的端口扫描器已经有不少，部分还提供 GUI（图形用户界面）。在诸多端口扫描器中，Nmap 是其中的佼佼者——它提供了大量的命令行选项，能够灵活地满足各种扫描要求，而且输出格式丰富。Nmap 原先是为 Unix 平台开发的，是许多 Unix 管理员的至爱，后来才被移植到 Windows 平台。NmapforWindows 最新的稳定版本是 3.27，可以从 www.insecure.org/nmap/免费下载。

一、安装 Nmap

Nmap 要用到一个称为“Windows 包捕获库”的驱动程序 WinPcap——如果你经常从网上下载流媒体电影，可能已经熟悉这个驱动程序——某些流媒体电影的地址是加密的，侦测这些电影的真实地址就要用到 WinPcap。WinPcap 的作用是帮助调用程序（即这里的 Nmap）捕获通过网卡传输的原始数据。WinPcap 的最新版本在 http://netgroup-serv.polito.it/winpcap，支持 XP/2K/Me

/9x 全系列操作系统，下载得到的是一个执行文件，双击安装，一路确认使用默认设置就可以了，安装好之后需要重新启动。

接下来从 www.insecure.org/nmap/nmap_download.html 下载 Nmap（国内各大软件网站也有，但一般版本更新略有滞后）。下载好之后解开压缩，不需要安装。除了执行文件 nmap.exe 之外，它还有下列参考文档：

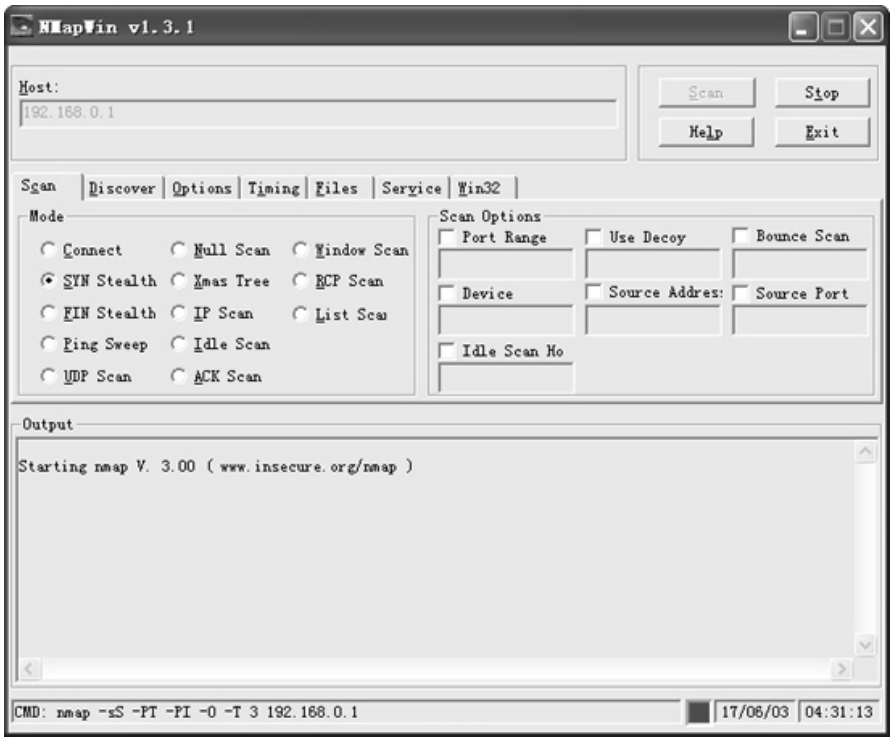
㈠nmap-os-fingerprints：列出了 500 多种网络设备和操作系统的堆栈标识信息。

㈡nmap-protocols：Nmap 执行协议扫描的协议清单。

㈢nmap-rpc：远程过程调用（RPC）服务清单，Nmap 用它来确定在特定端口上监听的应用类型。

㈣nmap-services：一个 TCP/UDP 服务的清单，Nmap 用它来匹配服务名称和端口号。

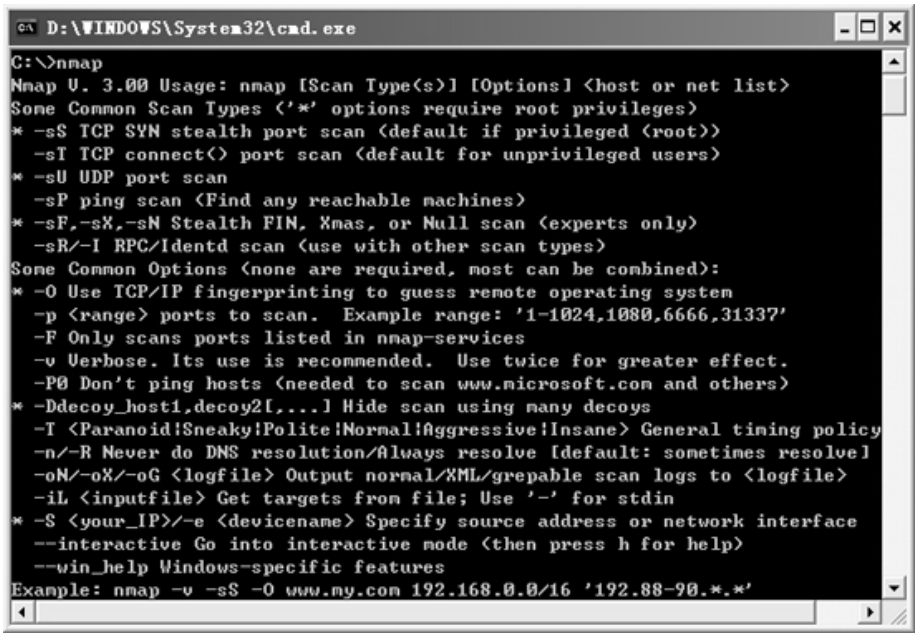
除了命令行版本之外，www.insecure.org 还提供了一个带 GUI 的 Nmap 版本。和其他常见的 Windows 软件一样，GUI 版本需要安装，图一就是 GUI 版 Nmap 的运行界面。GUI 版的功能基本上和命令行版本一样，鉴于许多人更喜欢用命令行版本，本文后面的说明就以命令行版本为主。



图一

二、常用扫描类型

解开 Nmap 命令行版的压缩包之后，进入 Windows 的命令控制台，再转到安装 Nmap 的目录（如果经常要用 Nmap，最好把它的路径加入到 PATH 环境变量）。不带任何命令行参数运行 Nmap，Nmap 显示出命令语法，如图二所示。



图二

下面是 Nmap 支持的四种最基本的扫描方式：

⑴TCPconnect()端口扫描（-sT 参数）。

⑵TCP 同步（SYN）端口扫描（-sS 参数）。

⑶UDP 端口扫描（-sU 参数）。

⑷Ping 扫描（-sP 参数）。

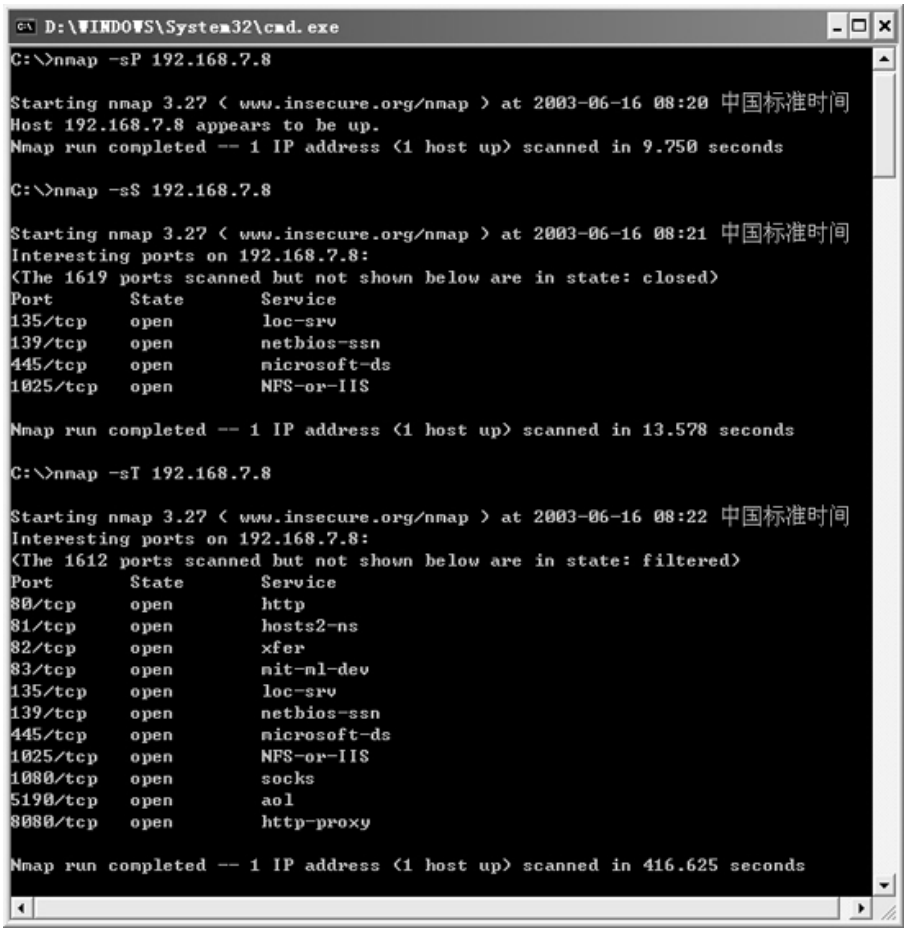
如果要勾画一个网络的整体情况，Ping 扫描和 TCP SYN 扫描最为实用。Ping 扫描通过发送 ICMP（Internet ControlMessageProtocol，Internet 控制消息协议）回应请求数据包和 TCP 应答（Acknowledge，简写 ACK）数据包，确定主机的状态，非常适合于检测指定网段内正在运行的主机数量。

TCPSYN 扫描一下子不太好理解，但如果将它与 TCPconnect()扫描比较，就很容易看出这种扫描方式的特

点。在 TCPconnect()扫描中，扫描器利用操作系统本身的系统调用打开一个完整的 TCP 连接——也就是说，扫描器打开了两个主机之间的完整握手过程（SYN，SYN-ACK，和 ACK）。一次完整执行的握手过程表明远程主机端口是打开的。

TCPSYN 扫描创建的是半打开的连接，它与 TCPconnect()扫描的不同之处在于，TCPSYN 扫描发送的是复位（RST）标记而不是结束 ACK 标记（即，SYN，SYN-ACK，或 RST）：如果远程主机正在监听且端口是打开的，远程主机用 SYN-ACK 应答，Nmap 发送一个 RST；如果远程主机的端口是关闭的，它的应答将是 RST，此时 Nmap 转入下一个端口。

图三是一次测试结果，很明显，TCPSYN 扫描速度要超过 TCPconnect()扫描。采用默认计时选项，在 LAN 环境下扫描一个主机，Ping 扫描耗时不到十秒，TCPSYN 扫描需要大约十三秒，而 TCPconnect()扫描耗时最多，需要大约 7 分钟。



图三

Nmap 支持丰富、灵活的命令行参数。例如，如果要扫描 192.168.7 网络，可以用 192.168.7.x/24 或 192.168.7.0-255 的形式指定 IP 地址范围。指定端口范围使用-p 参数，如果不指定要扫描的端口，Nmap 默认扫描从 1 到 1024 再加上 nmap-services 列出的端口。

如果要查看 Nmap 运行的详细过程，只要启用 verbose 模式，即加上-v 参数，或者加上-vv 参数获得更加详细的信息。例如，nmap-sS192.168.7.1-255-p20,21,53-11

0,30000--v 命令，表示执行一次 TCPSYN 扫描，启用 verbose 模式，要扫描的网络是 192.168.7，检测 20、21、53 到 110 以及 30000 以上的端口（指定端口清单时中间不要插入空格）。再举一个例子，nmap-sS192.168.7.1/24 -p80 扫描 192.168.0 子网，查找在 80 端口监听的服务器（通常是 Web 服务器）。

有些网络设备，例如路由器和网络打印机，可能禁用或过滤某些端口,禁止对该设备或跨越该设备的扫描。初步侦测网络情况时，-host_timeout<毫秒数>参数很有用，它表示超时时间，例如 nmapsShost_timeout10000192.168.0.1 命令规定超时时间是 10000 毫秒。

网络设备上被过滤掉的端口一般会大大延长侦测时间,设置超时参数有时可以显著降低扫描网络所需时间。Nmap 会显示出哪些网络设备响应超时，这时你就可以对这些设备个别处理,保证大范围网络扫描的整体速度。当然，host_timeout 到底可以节省多少扫描时间，最终还是由网络上被过滤的端口数量决定。

Nmap 的手册（man 文档）详细说明了命令行参数的用法（虽然 man 文档是针对 UNIX 版 Nmap 编写的，但同样提供了 Win32 版本的说明）。

三、注意事项

也许你对其他端口扫描器比较熟悉，但 Nmap 绝对值得一试。建议先用 Nmap 扫描一个熟悉的系统，感觉一下 Nmap 的基本运行模式，熟悉之后，再将扫描范围扩大到其他系统。首先扫描内部网络看看 Nmap 报告的结果，然后从一个外部 IP 地址扫描，注意防火墙、入侵检测系统（IDS）以及其他工具对扫描操作的反应。通常，TCPconnect()会引起 IDS 系统的反应，但 IDS 不一

定会记录俗称“半连接”的 TCPSYN 扫描。最好将 Nmap 扫描网络的报告整理存档，以便随后参考。

如果你打算熟悉和使用 Nmap，下面几点经验可能对你有帮助：

㈠避免误解。不要随意选择测试 Nmap 的扫描目标。许多单位把端口扫描视为恶意行为，所以测试 Nmap 最好在内部网络进行。如有必要，应该告诉同事你正在试验端口扫描，因为扫描可能引发 IDS 警报以及其他网络问题。

㈡关闭不必要的服务。根据 Nmap 提供的报告（同时考虑网络的安全要求），关闭不必要的服务，或者调整路由器的访问控制规则（ACL），禁用网络开放给外界的某些端口。

㈢建立安全基准。在 Nmap 的帮助下加固网络、搞清楚哪些系统和服务可能受到攻击之后，下一步是从这些已知的系统和服务出发建立一个安全基准，以后如果要启用新的服务或者服务器，就可以方便地根据这个安全基准执行。

防火墙功能指标详解

产品类型：从防火墙产品和技术发展来看，分为三种类型：基于路由器的包过滤防火墙、基于通用操作系统的防火墙、基于专用安全操作系统的防火墙。

LAN 接口：列出支持的 LAN 接口类型：防火墙所能保护的网络类型，如以太网、快速以太网、千兆以太网、ATM、令牌环及 FDDI 等。

支持的最大 LAN 接口数：指防火墙所支持的局域网络接口数目，也是其能够保护的不同内网数目。

服务器平台：防火墙所运行的操作系统平台（如 Linux、UNIX、WinNT、专用安全操作系统等）。

协议支持：支持的非 IP 协议：除支持 IP 协议之外，又支持 AppleTalk、DECnet、IPX 及 NETBEUI 等协议。

建立 VPN 通道的协议：构建 VPN 通道所使用的协议，如密钥分配等，主要分为 IPSec，PPTP、专用协议等。

可以在 VPN 中使用的协议：在 VPN 中使用的协议，一般是指 TCP/IP 协议。

加密支持：支持的 VPN 加密标准：VPN 中支持的加密算法,例如数据加密标准 DES、3DES、RC4 以及国内专用的加密算法。

除了 VPN 之外，加密的其他用途：加密除用于保护传输数据以外，还应用于其他领域，如身份认证、报文完整性认证，密钥分配等。

提供基于硬件的加密：是否提供硬件加密方法，硬件加密可以提供更快的加密速度和更高的加密强度。

认证支持：支持的认证类型：是指防火墙支持的身份认证协议，一般情况下具有一个或多个认证方案，如 RADIUS、Kerberos、TACACS/TACACS＋、口令方式、数字证书等。防火墙能够为本地或远程用户提供经过认证与授权的对网络资源的访问，防火墙管理员必须决定客户以何种方式通过认证。

列出支持的认证标准和 CA 互操作性：厂商可以选择自己的认证方案，但应符合相应的国际标准，该项指所支持的标准认证协议，以及实现的认证协议是否与其

他 CA 产品兼容互通。

支持数字证书：是否支持数字证书。

访问控制：通过防火墙的包内容设置：包过滤防火墙的过滤规则集由若干条规则组成，它应涵盖对所有出入防火墙的数据包的处理方法，对于没有明确定义的数据包，应该有一个缺省处理方法；过滤规则应易于理解，易于编辑修改；同时应具备一致性检测机制，防止冲突。IP 包过滤的依据主要是根据 IP 包头部信息如源地址和目的地址进行过滤，如果 IP 头中的协议字段表明封装协议为 ICMP、TCP 或 UDP，那么再根据 ICMP 头信息（类型和代码值）、TCP 头信息（源端口和目的端口）或 UDP 头信息（源端口和目的端口）执行过滤，其他的还有 MAC 地址过滤。应用层协议过滤要求主要包括 FTP 过滤、基于 RPC 的应用服务过滤、基于 UDP 的应用服务过滤要求以及动态包过滤技术等。

在应用层提供代理支持：指防火墙是否支持应用层代理，如 HTTP、FTP、TELNET、SNMP 等。代理服务在确认客户端连接请求有效后接管连接，代为向服务器发出连接请求，代理服务器应根据服务器的应答，决定如何响应客户端请求，代理服务进程应当连接两个连接（客户端与代理服务进程间的连接、代理服务进程与服务器端的连接）。为确认连接的唯一性与时效性，代理进程应当维护代理连接表或相关数据库（最小字段集合），为提供认证和授权，代理进程应当维护一个扩展字段集合。

在传输层提供代理支持：指防火墙是否支持传输层代理服务。

允许 FTP 命令防止某些类型文件通过防火墙：指是

否支持 FTP 文件类型过滤。

用户操作的代理类型：应用层高级代理功能，如 HTTP、POP3。

支持网络地址转换(NAT)：NAT 指将一个 IP 地址域映射到另一个 IP 地址域，从而为终端主机提供透明路由的方法。NAT 常用于私有地址域与公有地址域的转换以解决 IP 地址匮乏问题。

在防火墙上实现 NAT 后，可以隐藏受保护网络的内部结构，在一定程度上提高了网络的安全性。

支持硬件口令、智能卡：是否支持硬件口令、智能卡等，这是一种比较安全的身份认证技术。

防御功能：支持病毒扫描：是否支持防病毒功能，如扫描电子邮件附件中的 DOC 和 ZIP 文件，FTP 中的下载或上载文件内容，以发现其中包含的危险信息。

提供内容过滤：是否支持内容过滤，信息内容过滤指防火墙在 HTTP、FTP、SMTP 等协议层，根据过滤条件，对信息流进行控制，防火墙控制的结果是：允许通过、修改后允许通过、禁止通过、记录日志、报警等。过滤内容主要指 URL、HTTP 携带的信息：JavaApplet、JavaScript、ActiveX 和电子邮件中的 Subject、To、From 域等。

能防御的 DoS 攻击类型：拒绝服务攻击(DoS)就是攻击者过多地占用共享资源，导致服务器超载或系统资源耗尽，而使其他用户无法享有服务或没有资源可用。防火墙通过控制、检测与报警等机制，可在一定程度上防止或减轻 DoS 黑客攻击。

阻止 ActiveX、Java、Cookies、Javascript 侵入：属于 HTTP 内容过滤，防火墙应该能够

从 HTTP 页面剥离 JavaApplet、ActiveX 等小程序及从 Script、PHP 和 ASP 等代码检测出危险代码或病毒，并向浏览器用户报警。同时，能够过滤用户上载的 CGI、ASP 等程序，当发现危险代码时，向服务器报警。

安全特性：支持转发和跟踪 ICMP 协议（ICMP 代理）:是否支持 ICMP 代理，ICMP 为网间控制报文协议。

提供入侵实时警告：提供实时入侵告警功能，当发生危险事件时，是否能够及时报警，报警的方式可能通过邮件、呼机、手机等。

提供实时入侵防范：提供实时入侵响应功能，当发生入侵事件时，防火墙能够动态响应，调整安全策略，阻挡恶意报文。

识别/记录/防止企图进行 IP 地址欺骗：IP 地址欺骗指使用伪装的 IP 地址作为 IP 包的源地址对受保护网络进行攻击，防火墙应该能够禁止来自外部网络而源地址是内部 IP 地址的数据包通过。

管理功能：通过集成策略集中管理多个防火墙：是否支持集中管理，防火墙管理是指对防火墙具有管理权限的管理员行为和防火墙运行状态的管理，管理员的行为主要包括：通过防火墙的身份鉴别，编写防火墙的安全规则，配置防火墙的安全参数，查看防火墙的日志等。防火墙的管理一般分为本地管理、远程管理和集中管理等。

提供基于时间的访问控制：是否提供基于时间的访问控制。

支持 SNMP 监视和配置：SNMP 是简单网络管理协议的缩写。

本地管理：是指管理员通过防火墙的 Console 口或

防火墙提供的键盘和显示器对防火墙进行配置管理。

远程管理：是指管理员通过以太网或防火墙提供的广域网接口对防火墙进行管理，管理的通信协议可以基于 FTP、TELNET、HTTP 等。

支持带宽管理：防火墙能够根据当前的流量动态调整某些客户端占用的带宽。

负载均衡特性 :负载均衡可以看成动态的端口映射，它将一个外部地址的某一 TCP 或 UDP 端口映射到一组内部地址的某一端口,负载均衡主要用于将某项服务(如 HTTP）分摊到一组内部服务器上以平衡负载。

失败恢复特性（failover)：指支持容错技术，如双机热备份、故障恢复，双电源备份等。

记录和报表功能：防火墙处理完整日志的方法：防火墙规定了对于符合条件的报文做日志，应该提供日志信息管理和存储方法。

提供自动日志扫描：指防火墙是否具有日志的自动分析和扫描功能，这可以获得更详细的统计结果，达到事后分析、亡羊补牢的目的。

提供自动报表、日志报告书写器：防火墙实现的一种输出方式，提供自动报表和日志报告功能。

警告通知机制：防火墙应提供告警机制，在检测到入侵网络以及设备运转异常情况时，通过告警来通知管理员采取必要的措施，包括 E－mail、呼机、手机等。

提供简要报表（按照用户 ID 或 IP 地址）:防火墙实现的一种输出方式，按要求提供报表分类打印。

提供实时统计：防火墙实现的一种输出方式，日志分析后所获得的智能统计结果，一般是图表显示。

列出获得的国内有关部门许可证类别及号码：这是

防火墙合格与销售的关键要素之一，其中包括：公安部的销售许可证、国家信息安全测评中心的认证证书、总参的国防通信入网证和国家保密局的推荐证明等。

防火墙安全及效能分析

网络防火墙早已是一般企业用来保护企业网络安全的主要机制。然而，企业网络的整体安全涉及的层面相当广，防火墙不仅无法解决所有的安全问题，防火墙所使用的控制技术、自身的安全保护能力、网络结构、安全策略等因素都会影响企业网络的安全性。

在众多影响防火墙安全性能的因素中，有些是管理人员可以控制的，但是有些却是在选择了防火墙之后便无法改变的特性，其中一个很关键的就是防火墙所使用的存取控制技术。目前防火墙的控制技术大概可分为：封包过滤型(PacketFilter)、封包检验型(StatefulInspectionPacketFilter)以及应用层闸通道型(ApplicationGateway)。这三种技术分别在安全性或效能上有其特点，不过一般人往往只注意防火墙的效能而忽略了安全性与效率之间的冲突。本文针对防火墙这三种技术进行说明，并比较各种方式的特色以及可能带来的安全风险或效能损失。

封包过滤型：封包过滤型的控制方式会检查所有进出防火墙的封包标头内容，如对来源及目地 IP、使用协定、TCP 或 UDP 的 Port 等信息进行控制管理。现在的路由器、SwitchRouter 以及某些操作系统已经具有用 PacketFilter 控制的能力。封包过滤型控制方式最大的好处