网络安全

安全技巧（十四）

小未 主编

目　录

WindowsNT 上的 TCP/IP 安装 1
Linux 下的网络扫描利器：NMAP 2
Sunos 使用手册--进出 OPENWINDOW 7
Sunos 使用手册之电子邮件和电子讯息 15
TIS 防火墙详述 17
sniffit 的安装使用简述 46
原码重读--proxyscan 52
原码重读—autopost 58
局域网服务器软件安装 60
ping、trace、finger、whois 的用法 64
Telnet 服务种类 74
Telnet 监控和维护 75
建立 Telnet 连接 76
Trap 的设置 77
show 命令查看系统状态和系统信息 78
网络连接的测试工具 81
SysVinit2.6 的开机过程 87
利用 WINDOWSNT 设置软件路由 106
SUNOS 作业系统简介 111
Windows NT 服务器用作路由器 115
Linux 系统管理员安全 120

WindowsNT 上的 TCP/IP 安装

既然我们对 TCP/IP 及其在网络上的运作已有了一些基本的了解，现在就让我们来看一下它在 WindowsNT 服务器 4.0 上的安装和成形。在这一部分中，我们将运用以下几种基本设想：

你使用的因特网域名是“company.com”

你的服务器的 TCP/IP 主机名是“www”

你的服务器的 IP 地址是 204.176.47.2

你的服务器有一个 255.255.255.0 的子网掩膜

这一特殊服务器只安装了一张网络卡

你设置有一个 WINS 服务器，其 IP 地址是 204.176.47.1

请依照以下步骤来安装 TCP/IP.

1.先单击开始按纽打开开始菜单，选择设置，再单击控制面板。这时会出现一个包括了所有已安装的控制程序的窗口。

2.在控制面板被打开以后，查看所有项目只到你找出象征网络的小图标（图 1.3files/Fig3.gif），双击它，就会出现网络配置的对话框（图 1.4files/Fig4.gif）。选择协议键，再点击添加。

3.接着就会出现网络协议选择对话框（图 1.5files/Fig5.gif）。查看可用协议一览表，直到你看到 TCP/IP 协议。然后，双击它或点“确定”把它添加到你的网络配置中。

4.你将有可能看到一个象图 1.6(files/Fig6.gif)那样的对话框，询问在你的网络上是否有 DHCP 服务器，或

者你是否想使用它来完成动态的 IP 地址工作任务。在大多数情况下，你的服务器需要的都是静态 IP 地址，所以纵然你的网络上有 DHCP 服务器你也只须单击否定就行了。

Linux 下的网络扫描利器：NMAP

NMap 是 Linux 下的网络扫描和嗅探工具包。可以帮助网管人员深入探测 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，为系统安全服务。

正文：

NMap，也就是 NetworkMapper，是 Linux 下的网络扫描和嗅探工具包，其基本功能有三个，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。

一、如何获得并安装 Nmap

一些 Linux 的发行版本提供对 nmap 的安装支持。如果没有，你可以获取并安装其最新版本。这里我们介绍源码的 tgz 安装，当然也可以选择 rpm 格式或者 rpm 源码格式。例如，在 RedHat6.1 下从 http://www.insecur

e.org/nmap 下载 nmap-latest.tgz 到/home 目录，执行 tar-zxvfnmap-latest.tgz，将源码解压到/home 目录下的 nmap-latest 子目录，然后执行 configure,make 和 makeinstall 命令，将 nmap 二进制码安装到/usr/local/bin 目录。这样就可以执行 nmap。

二、Nmap 的使用

1、各种扫描模式与参数

首先你需要输入要探测的主机的 IP 地址作为参数。假如一个 LAN 中有两个节点：192.168.0.1 和 192.168.0.2 如果在命令行中输入：nmap192.168.0.2 结果可能是:

StartingnmapV.2.53byfyodor@insecure.org(www.insecure.org/nmap)

InterestingportsonLOVE(192.168.0.2):

(The1511portsscannedbutnotshownbelowareinstate:closed)

PortStateService

21/tcpopenftp

23/tcpopentelnet

25/tcpopensmtp

79/tcpopenfinger

80/tcpopenhttp

98/tcpopenlinuxconf

111/tcpopensunrpc

113/tcpopenauth

513/tcpopenlogin

514/tcpopenshell

515/tcpopenprinter

6000/tcpopenX11

Nmapruncompleted--1IPaddress(1hostup)scannedin1second

?是对目标主机的进行全面 TCP 扫描后的结果。显示了监听端口的服务情况。这一基本操作不需要任何参数，缺点是运行了日志服务的主机可以很容易地监测到这类扫描。该命令是参数开关-sT 的缺省，即监听 TCP，结果完全一样。

如果不是在本地的 LAN，而是使用拨号上网主机，可以运行 ifconfig 命令，或者从/var/log/messages 文件中检测出你目前的 IP 地址，假如是 202.96.1.1，那么你不妨探测一下你的网上邻居，比如 202.96.1.2。可以输入：nmap-sT202.96.1.2 以上是一些入门的基本操作。假如一些命令选项开关，就可以实现较高级的功能。

-sS 选项可以进行更加隐蔽的扫描，并防止被目标主机检测到。但此方式需要用户拥有 root 权限-sF-sX-sN 则可以进行一些超常的扫描。假如目标主机安装了过滤和日志软件来检测同步空闲字符 SYN，那么-sS 的隐蔽作用就失效了，此时可以采用-sF(隐蔽 FIN),-sX(Xmas Tree)以及-sN(Null)方式的扫描。这里需要注意的是由于微软的坚持和独特，对于运行 Windows95/98 或者 NT 的机器 FIN,Xmas 或者 Null 的扫描结果将都是端口关闭，由此也是推断目标主机可能运行 Windows 操作系统的一种方法。以上命令都需要有 root 权限。

-sU 选项是监听目标主机的 UDP 而不是默认的 TCP 端口。尽管在 Linux 机器上有时慢一些，但比 Window 系统快得多。比如，我们输入上面的例子：

nmap-sU192.168.0.2 结果可能是：

StartingnmapV.2.53byfyodor@insecure.org(www.inse

cure.org/nmap)

InterestingportsonLOVE(192.168.0.2):

(The1445portsscannedbutnotshownbelowareinstate:closed)

PortStateService

111/udpopensunrpc

517/udpopentalk

518/udpopenntalk

Nmapruncompleted--1IPaddress(1hostup)scannedin4seconds

2、操作系统探测

-O 选项用来推断目标主机的操作系统，可以与上述的命令参数联合使用或者单独调用。Nmap 利用 TCP/IP "指纹"技术来推测目标主机的操作系统。还使用前面的例子，我们输入：

nmap-O192.168.0.2 结果可能是：

StartingnmapV.2.53byfyodor@insecure.org(www.insecure.org/nmap)

InterestingportsonLOVE(192.168.0.2):

(The1511portsscannedbutnotshownbelowareinstate:closed)

.....

.....

TCPSequenceprediction:Class=randompositiveincrements

Difficulty=1772042(Goodluck!)

Remoteoperatingsystemguess:Linux2.1.122-2.2.14

nmap 提供了一个 OS 数据库，上例中检测到了 Lin

ux 以及内核的版本号。

3、更进一步的应用

除了一次只扫描一个目标主机，你也可以同时扫描一个主机群，比如

下例：

nmap-sT-O202.96.1.1-50 就可以同时扫描并探测 IP 地址在 202.96.1.1 到 202.96.1.50 之间的每一台主机。当然这需要更多的时间,耗费更多的系统资源和网络带宽。输出结果也可能很长。所以，可以使用下面命令将结果重定向输送到一个文件中：

nmap-sT-O-oNtest.txt202.96.1.1-50

另外的一些命令参数选项包括：

-I 进行 TCP 反向用户认证扫描，可以透露扫描用户信息

-iR 进行随机主机扫描

-p 扫描特定的端口范围

-v 长数据显示，-v-v 是最长数据显示

-h 当然是快捷帮助了

综合了上述参数的例子比如：

nmap-sS-p23,80-oNftphttpscan.txt209.212.53.50-100

4、nmap 的图形用户界面 GUI

nmap 有一些图形用户前端，比如：

NmapFE:GTK 界面，网址：http://codebox.net/nmapfe.html

Kmap:Qt/KDE 前端，网址：http://www.edotorg.org/kde/kmap/

KNmap:KDE 前端，网址：http://pages.infinit.net/rewind/

附录：nmap **资料：**

nmap-**网络嗅测器**（theNetworkMAPper）

作者:Fyodor

需要运行:flex,bison

主页:http://www.insecure.org/nmap

当前版本:2.53

许可:GPL

支持的平台:Linux,FreeBSD,NetBSD,OpenBSD,Solaris,IRIX,

BSDI,SunOS,HP-UX,AIX,DigitalUNIX,CrayUNICOS **以及** WindowsNT.

Sunos 使用手册--进出 OPENWINDOW

一、OpenwindowsWorkspacePrograms **功能表**

视窗和小图形外围的灰色区域就是所谓的工作区(workspace)**，要显示工作区的功能表请将游标移到灰色的工作区上，然後压住滑鼠的右按钮即可。要跳出** workspace **工作表，请将游标移出工作表，在放开滑鼠的右按钮即可。当你在里选一个选项时，这个工具就被载入工作区。你可以载入或开启一个工具许多次。**

二、FileManager

FileManager **视窗由三个主要的部份组成，及一个路径区**(pathpane)**、控制板**(Controlpanel)**和目录区**(floderpane)**。下列将三区加以说明。**

路径区：路径区会显示物前你在档案系统的位置。如果你用 workspace **功能表里的** Programs **启动** FileMana

ger，则会显示你的本目录。要路径显示成树的样子，请将游标移到 View 功能表，按住滑鼠右键，然後将反白移到 Tree 项上面。当你放开右键时，路径区会以树的样子显示档案系统，并且将你的本目录放在底部。

控制板：FileManager 的控制板有六个功能表按钮：File，View，Edit，Props，Home 和 Goto。这些按钮可以让你执行档案的各种操作。要显示这些功能表，只要将游标移到功能按钮上，再按滑鼠就可以了。如果功能表的选项是模糊的，则那个选项不可使用。大部分的情况是，再选择功能表选项之前，必须先选择一个档案。

目录区：路径区所显示的一串目录里的最後一向是你的目前目录，目前目录的内容则显示目录区里代表档案的图形有三种：

档案型态	小图形
目录资料档可执行档	检索卡右上角下摺的一张纸小视窗或应用程式的小图形

选择档案：

要选择档案，请将游标移到所要的档案上，再快速一放滑鼠的左按钮。则此档案已被选取了。选定一个档案或目录後，可以再选择其他的档案或目录，方法是将游标移到其他档案上，再快速压放滑鼠的中间按钮。你可以在所选择的档案、目录和可执行程式上执行好几种操作。例如：开启、拷贝、删除、移动或列印档案，或更改档案特性。开启档案、载入档案和启动应用程式：

可以将指标移到所要开启的档案上，然後快速压放滑鼠左按钮两次，就可以开启资料档或执行档。

用 Goto 按钮切换或搜寻档案：

你可以在 Goto 栏上输入路径名或档名，然後按 Ret

run 或将指标移到 Goto 按钮上，并快速压放滑鼠的左按钮，就会找到档案了。如果你不记的档名或目录，可以用 Goto 功能表里的 Find 选择项来寻找。

建立目录：

建立目录你必须位於要建目录的父目录上，然後将游标移到 File 功能表上按住滑鼠右按钮，再将反白一到 CreateFolder 选择项上，然後放开滑鼠右按钮，就会出现一个名为 NewFolder 的空目录了,并且显示一条底线，底线底端有一个模糊的菱形。

建立文字档：

建立文字档和建立目录的方式很像，只是改用 File 功能表的 CreateDocument 选择项而已。当你键一个文字档後，有一个名为 NewDocument 的档案小图形会出现。

拷贝及移动档案：

拷贝及移动档案的方法有想两个，最简单的是施放小图形，令一个方法是使用 clipboard，那是记忆体里储存资料的地方。

使用施放小图形拷贝：

1.选择要拷贝的档案。

2.按住控制键。

3.按住滑鼠左按钮。

4.将档案拖到目标目录上。

5.放开左按钮就完成拷贝。

Clipboard 的用途：

clipboard 是一个缓冲区，在拷贝或移动档案时，记忆体中暂时存放档案的地方。在 Edit 功能表和 FolderCommands 功能表中都有 clipboard 这个选项。你可以剪或拷贝档案，在把档案黏到其他目录或应用程式上。如果

你要知道 clipboard 里有什堋，可以随时用 Edit 和 FolderCommands 功能表里的 showclipboard 的选项来察看 clipboard 的内容。这个选项会显示内容的前 30 个字元。

列印档案：

你一定有要列印档案的时候，FileManager 有两个方法可以列印档案：

在目录里选择档案，然後从 File 功能表里选择 Printfile 项，当你选择一个档案後，Print 项就变成可以使用了，否则功能表里的 Print 项就会模糊不清。在目录区里选择档案，然後将它拖到 PrintTool 的小图形上，就会用系统预设的指令列印档案。

档案和目录的重新命令：

要更改档名或目录名，只要将游标移到目录或档案上，快速压放滑鼠左按钮，然後将指标移到档名上，再快速压放滑鼠左按钮。这样会使档名加上底线，底线尾端还有脱字符号（^），脱字符号表示插入点。将就档名和目录名删除，然後重新输入新的名字，并且按 Return。则动作完成。

删除档名或目录：

移到你要删除的档案小图形上，按滑鼠左按钮，然後将档案脱到废纸篓。在废纸篓里最多可以存放 100 个档案，丢弃在废纸篓里的档案是存放在一个名叫 wastebasket 里，这个目录是在你的本目录里。档案会一直保留在废纸篓里，直到你从 Edit 功能表或 FolderCommands 功能表里选择了 Rea-llyDelete 选择项时，才真正删除。

更改档案和目录的许可模式：

SunOS 的安全系统是架构在许可模式之上。许可模式可以决定那个使用者可以读取、写入或执行档案，每

个人只可以更改自己的档案许可模式，再档案系统里的每一个目录和档案都设有许可模式，可以用来限制使用档案。要显示 FileProperties 视窗，以便更改档案的许可模式请先选择所要更改的档案，再将指标一到 Props 的功能表按钮上，按住滑鼠右按钮就会有功能表选择项出现，将反白移到 FileProperties 项上，并且放开右按钮。FileProperties 视窗可以让你更改档案和目录的许可模式。

如果你对档案有写入的许可，则可以更改三种人的许可模式：

1.拥有者档案或目录的拥有者（通常是建档人）。

2.团体可以共用档案的一群人的团体名称。

3.其他人网路上的其他使用者。

连结档案：

所谓连结（link）是一种象徵性的连接或指向一个档案的指标，可以让你从许多目录中使用那个档案，而不用跳到档案所在的目录。Edit 功能表里的 Link 指令可以让你建立档案的连结。当档案被连结起来後，被连结的目录会出现一个小图形，就像档案驻再那里一样。

要将一个档案连结到一个目录上，请选择你要连结的档案，并且执行下列步骤：

1.从 Edit 功能表上选择 Link 指令。

2.开启目标目录。

从 FoldersCommands 的 Edit 子功能表选择 Paste 选择项，或使用 Paste 快捷键。

三、ShellToolShellTool 是一个指令解译器，他可一接受、解译、以其执行 SunOS 指令。ShellTool 视窗被称为终端机模拟器，意思是说在那里面工作就像在终端机

的指令提示下工作一样，当它作用时则以实心的矩形表示。

四、Console 视窗

当你用 Openwindows 或 Sunview 时，就会自动开启一个 Console 视窗。Console 视窗适用来显示系统讯息及运用程式讯息的，你可以用 WorkspaceUtilities 子功能表里的 RedisplayAll 项来清除这些讯息。如果不小心跳出 Concole 视窗，也可以用 WorkspaceUtilities 的 Concole 项来开启 Concole 视窗。这好不要同时开启多个 Concole 视窗，因为如果你忘记那一个是最後开启的，就很容易漏失重要资料。

五、CommandTool

CommandTool 就像指令解译器，提供你标准的 Text Edit 所有的功能。CommandTool 的小图形看起来就像 ShellTool 的小图形，但开启後，CommandTool 会显示一个 Scrollbar，以及和 ShellTool 不同的功能表。使用 CommandTool 时，可以用下列步骤将一连串的指令存成一个档案：在提示下输入一个档名，如果所要存放的档案不在目前的目录上，必须加上路径名。将指标移到档名的最前面，并且压放滑鼠的左按钮。将指标移到档名的最尾端，压放滑鼠中间按钮，档名就会呈反白。将指标移到将指标移到 CommandTool 工作区，压住滑鼠又按钮，就会显示 CommandTool 功能表。让 File 选择项反白，将指标往右拖，就会显示 File 子功能表。将指标拖到 StoreasNewFile 项上，使它反白後放开滑鼠右键，这样就会显示 StoreFile 视窗，在 FileName 栏里的档名就会反白。请将指标移到 Apply 按钮上，快速压放滑鼠左按钮，则内容就会存在你第一步骤所指定的档案里。

六、TextEdit **视窗**

TextEdit **会简化编辑动作。你可以很容易的在** Text Edit **和其他文字区之间，直接剪贴内容。**TextEdit **视窗有一个控制板和可以编辑档案的文字区。**TextEdit **视窗表头会一直显示正在编辑的档案名称和路径名。如果还没有为档案命名，就会显示** None**。如果你更改了档案，或尚未存档案，则档名後面的括弧内会显示** edited **字。**

控制板：

TextEdit **的控制板有四个功能表的按钮：**File**、**Vie w**、**Edit **和** Find**。**

1.File **提供了清除、储存、或合并档案的选项。**Vie w **功能表提供了移动游标位置和切换档案的选项。**Edit **功能表及提供了拷贝、移动、删除或取消删除选择项。**Find **功能表提供了在文字区里或在** clipboard **里寻找内容的选项。**

TextEditor **文字区和** TextEditor **功能表：**

所谓文字区(textpane)**是你撰写和编辑文字的地方。将指标放在文字区里，并且按住滑鼠右按钮会显示** Text Editor **功能表。**

将档案载入 TextEditor**：**

你可以将档案的小图形拖放 TextEditor **到是窗中，即可载入档案；亦可用** File **功能表的** LoadFile **选择项载入档案，必须：将指标移到** File **功能表按钮上，并且压住滑鼠右按钮。将指标拖到** LoadFind **选择项上，并且放开滑鼠右按钮，就会显示** LoadFile **视窗了。**

3.**输入目录，并且按** Return**。**

4.**输入你所要载入档名。在** Apply **项上快速压上滑鼠左按钮，档案就会载入** TextEditor **视窗了，并且会取**

代视窗里现有的内容。

储存新档：

当你键一个新档，但尚未将它储存，档案小图形会显示 NoFile 的字。如果以 None 作为档名，则请用 File 功能表的 StoreasNewFile 项来选择一个 StoreFile 视窗。StoreFile 视窗会自动显示 File 栏所选择的档案。如果你没有指定目录，TextEdit 会将它储存在目前的目录。你也可以用 StoreFile 视窗来储存目前档案，请在适当的栏位输入目录和档名，在将指标移到 Alppy 项上，快速压放滑鼠左按钮，将 TextEdit 工作区的内容储存起来。

将以命名的档案储存起来：

File 功能表的 SaveCurrentFile 选择项可以将以命名的档案存起来。请记住，档名及目录会一直显示在 Text Editor 视窗的表头。

输入文字和选择文字：

输入文字和将指标移到文字区的某地方一样简单。如果没有文字出现，请检查看看指标是否在文字区中，并快速压放滑鼠左按钮。下面我们说明个选择方法：单字：将指标移到单字上，并且快速压放两次滑鼠左按钮。段落：将指标移到所要段落上，并且快速压放三次滑鼠中间按钮。一区块：快速压放滑鼠左按钮，以便设定输入点，再将指标移到所选区块的最後面，然後快速压放滑鼠中间按扭。整个档案：指标在档案的任何地方，快速压放两次滑鼠左按钮四次。

用 Clipboard 拷贝、搬移及删除内容：

Edit 功能表和 TextPane 功能表提供了一些标准的编辑功能，可以让你拷贝、搬移及删除内容，你也可以用键盘左边的快捷键来执行这些操作。这时所拷贝或剪下

的内容，是存放在 Clipboard 里的。

重新编辑或取消编辑：

你可以从 Edit 功能表或 TextPane 功能表选择 Again，来重复执行最後一个编辑动作。如果编辑错了，而想要取消最後一个编辑动作，或想要取消上一次储存後的所有编辑，可以用 Edit 功能表或 TextPane 功能表来做。请按住滑鼠右按扭，然後将指标移到功能表的 Undo 项上，然後将指标又右移，你可以用 UndoLast 或 EditUndoAll Edits 来取消上一次编辑，或所有编辑。

Sunos 使用手册之电子邮件和电子讯息

一、收送电子邮件

sunos 亦提供 e-mail 功能，当你执行 mail 时，不管是传出或接收，他都会显示自己的提示符号(&)，这程式提示符号表示你正在 mail 程式上工作。每当你进入 sunos 时，它会先检查信箱，如果你的信箱有邮件，就会有一个 Youhavemail 的讯息显示在萤幕上。此时子可以显示邮件清单，读取邮件，也可以忽略邮件讯息，想看时候再看。

接收邮件

如果有一个讯息通知你，别人利用 sunos 传一份邮件给你时，请在系统的提示下输入：%mail 系统会显示一份邮件讯息标题的清单，以及 mail 程式的提示，如下例：

1kyuWedJun319：13332/1122open

lookupdateN2leeWedJun423：3541/1160Memoryband