HZ BOOKS

Hack Attacks Testing
How to Conduct Your Own Security Audit

网络与信息安全技术丛书

黑客攻击
测试篇

(美) John Chirillo 著
黄江海 李宏平 骆智 等译

附赠 CD-ROM

机械工业出版社
China Machine Press

Hack Attacks Testing
How to Conduct Your Own Security Audit

网络与信息安全技术丛书

黑客攻击
测试篇

(美) John Chirillo 著
黄江海 李宏平 骆智 等译

机械工业出版社
China Machine Press

本书由著名安全专家John Chirillo撰写而成，讲解了如何自己进行安全审核。本书内容针对性强，采取循序渐进的方式，向读者介绍了“老虎盒”操作系统的安装和配置，同时讲述了当前最流行的安全审核软件套件，讨论了通用的和定制的安全审核用法，以及扫描方式和对每个过程的报告，分析了单个漏洞扫描器的结果，并对各扫描器针对目标网络上的一组故意设置的安全漏洞的测试结果进行了比较。

本书内容翔实，讲解透彻，不仅适合作为系统管理员、安全工程师、网络管理员、网络工程师的参考书，而且也适用于感兴趣的普通读者。

John Chirillo：Hack Attacks Testing: How to Conduct Your Own Security Audit（ISBN: 0-471-22946-6）.

版权登记号：图字：01-2003-2620

图书在版编目（CIP）数据

黑客攻击测试篇/（美）切里罗（Chirillo, J.）著；黄江海等译. -北京：机械工业出版社，2004.1
（网络与信息安全技术丛书）
书名原文：Hack Attacks Testing: How to Conduct Your Own Security Audit
ISBN 7-111-13031-6

Ⅰ.黑… Ⅱ.①切… ②黄… Ⅲ.计算机网络-安全技术-测试 Ⅳ.TP393.08

中国版本图书馆CIP数据核字（2003）第080764号

机械工业出版社（北京市西城区百万庄大街22号 邮政编码 100037）
责任编辑：迟振春
北京昌平奔腾印刷厂印刷·新华书店北京发行所发行
2004年1月第1版第1次印刷
787mm×1092mm 1/16·25.25印张
印数：0 001 - 4 000 册
定价：55.00元（附光盘）

凡购本书，如有倒页、脱页、缺页，由本社发行部调换
本社购书热线电话：（010）68326294

前　言

本书的目的是填补大多数安全书籍中的空白：通过示例和实际模拟来说明如何进行安全测试。具有简单图形用户界面和自动化的审核工具正日趋流行，其中很多宣称是管理员和安全顾问用于网络安全测试的一揽子解决方案。不过实际上，精确的、最新的评估需要多种工具组合构成的“老虎盒”分析/监控系统。“老虎盒”是设计用来提供必要工具的系统，这些工具通过对安全漏洞的发现、扫描和某些情况下进行渗透来揭示潜在的安全隐患。本书覆盖了Windows以及Unix和Linux（*NIX）双启动配置，解释了如何利用当今高质量的、最流行的工具构建和操作自己的漏洞分析系统。

本书逐步地讲解了如何建立“老虎盒”操作系统，安装、配置其他最流行的审核软件套件。讨论了通用的和定制的用法，以及扫描方式和对每个过程的报告。本书还分析了单个漏洞扫描器的结果，并在评价矩阵中对各扫描器针对目标网络上的一组故意设置的安全漏洞的测试结果进行了比较。

光盘内容

如果你想获得使用书中所讨论的扫描器的实际经验，只需参看本书附带的光盘，它包含了书中的交互练习内容。光盘中覆盖了扫描器的基本用法，其中一些包含了交互式报告，读者可以借此熟悉它们的界面。

本光盘的内容从真实使用模拟的角度介绍扫描器。如果想得到更多的经验，可以从每部分的链接下载产品的评估版。

本书读者对象

本书讲解了如何执行自己的安全审核，包含了从没有工具使用经验的初学者到高级用户所必需了解的内容。本书适合作为系统管理员、安全工程师、网络管理员、网络工程师的参考书，同时也适用于感兴趣的普通读者。

致谢

要想获得成功，一定要和最优秀的人一起工作。首先，我要感谢我的妻子在本书创作过程中对我的不断支持和耐心。另外，还要感谢全家和朋友给予我的鼓励和信心。

我还要感谢Carol Long、Adaobi Obi、Micheline Frederick、Erica Weinstein、Ellen Reavis、Kathryn Malm、Janice Borzendowski以及John Wiley & Sons出版社的所有人员。

全书由黄江海、李宏平、骆智、吴新鸣、张小冰、李海涛、文静、李祥、刘海宁、丁镇兴、万仁伟、刘晶晶、方平、邓盛骋、陈小冲、郭龙永、王冶、李鹃君、常欣、李桦等进行翻译，最后由宋涛统稿。

关于作者

John Chirillo 12岁时就开始了他的计算机生涯，经过一年的自学后，他编写了一个名为Dragon's Tomb的游戏。该游戏发布后，在Color Computer System市场上销售了几千份。在接下来的5年里，John编写了一些其他软件包，包括The Lost Treasure（一个游戏编写教程）、Multimanager（一个记账、库房和财务管理软件套件）、Sorcery（RPG探险游戏）、PC Notes（用来教授数学的GUI，范围从代数到微积分）、Falcon's Quset I 和II（可以发音的图形化探险游戏）以及Genius（一个完全基于Windows的点击操作系统）。John学习并获得了多种编程语言的证书，包括QuickBasic、VB、C++、Pascal、Assembler和Java。John后来开发了PC Optimization Kit（可以把标准Intel 486芯片的速度提高到200%）。

在开办两家公司（Software Now和Geniusware）之后，John成为多家久负盛名的公司的顾问，专门进行安全和嗅探器分析以及LAN/WAN设计、实现和故障检修。在此期间，他获得了多项网络方面的证书，包括CCNA、CCDA、CCNP、Intel Certified Solutions Consultant、Compaq ASE Enterprise Storage、Unix、CISSP以及即将获得的CCIE等。他现在是某技术管理公司的高级网络工程师。

John写了几本关于安全和网络方面的书，包括John Wiley & Sons出版社的*Hack Attacks*（黑客攻击）系列丛书。

目　录

第三部分 用于*NIX和Mac OS X的安全分析工具

第四部分 漏洞评估

附 录

第一部分

构建多系统的“老虎盒”

在国际信息系统安全认证联盟（the International Information Systems Security Certification Consortium，IISSCC）的公共知识体系（Common Body of Knowledge，CBK）领域中，识别系统问题的审核过程的一部分是网络防御性测试技术中的漏洞扫描和渗透测试。换句话说，应该实施定期的安全审核，特别是在进行整个企业（从大到小的办公室/家庭办公室）资产安全保护过程中。有效的安全实现由几个生命期组件构成，包括安全策略、边界防御以及灾难恢复计划等等。不过，对安全控制效果的审核是至关重要的。

本书的目的是提供发现漏洞和渗透测试方面的技术。首先，来看看美国国家安全技术委员会（the National Institute of Security Technology，NIST）所列举的有关计算机安全的八个要素：

1) 计算机安全应该支持组织的使命。

2) 计算机安全是健全管理的有机组成部分。

3) 计算机安全要有好的成本效益。

4) 计算机安全的责任和义务必须清晰。

5) 系统拥有者具有自己组织之外的计算机安全责任。

6) 计算机安全需要综合及一体化的方法。

7) 计算机安全应该进行周期性的评估。

8) 计算机安全受到社会因素的约束。

无论计算机安全控制是否到位，通过分析都能够对安全解决方案如何保护关键的系统和数据予以更好的理解。网络（包括那些没有连接到Internet上的）可能存在安全漏洞以及其他问题，如果不解决就可能使得秘密数据遭受非授权的访问。本书介绍了最常用的计算机安全评估工具，说明和实际模拟它们用于本地和远程评估的做法，并且报告发现和改进过程。

注意　本书将遵从信息系统评估的信息安全准则和方法（the InfoSec Criteria and Methods of Evaluations of Information Systems），特别是信息技术安全评估准则中对评估对象（Target of Evaluation，TOE）进行有效评估的如下方法：1) TOE要有适当的安全实施功能来对抗在安全目标（Security Target，ST）中所标识的威胁；2) TOE的安全实施功能和机制应以相互支持的方式绑定，从而形成集成、有效的整体；3) TOE的安全机制要有经受直接攻击的能力；4) 构建及运行中的TOE实际上是否有会破坏TOE安全的已知漏洞；5) TOE不能够以一种不安全而管理员或是终端用户却想当然地认为是安全的方式被配置和使用。

安全分析的七个阶段

无论家庭还是企业，也无论新近上网还是早就连网的基础设施，安全分析都能够帮助确定系统是否受到了足够的保护，免遭入侵。执行安全分析的典型过程是开发计划，进行审核，以及报告结果。本部分提出了进行详细安全审核的通用评估阶段，如下所示：

- 站点扫描，测试端口和应用层，检查内部防御设施。
- 远程审核，测试外部服务—例如ISP（Internet Service Provider）托管、服务器和管道。
- 渗透测试，测试Internet安全性以及验证当前的风险。你要弄清和测试相关的特定目标、需求和时间框架，小心地进行测试以免破坏数据和系统，通知目标站点测试过程中产生的任何漏洞，以及在站点要求时立即停止测试。
- 网际协议（IP）、邮件哄骗和垃圾邮件测试。

• 拨号审核，以确保诸如PC Anywhere、Reachout和/或Citrix等应用远程访问连接的安全性。

外部审核应该远程执行，也就是说，从站点外或保护边界（例如防火墙）的外部进行。应该从盲测试开始，即没有关于该网络基础设施的详细资料。

接着开始第一阶段的评估，基于知识的渗透测试将决定外部攻击的程度和风险（如果有的话）。这种审核对边界安全机制配置的测试是很有用的，包括Web、文件传输协议（FTP）、电子邮件以及其他服务。扫描和模拟的攻击通过Internet远程执行。较好的情况下，该阶段应该在有限的了解下进行（不详细了解但是有选择的管理），作为非预期的外部渗透评估。

多次的渗透测试应该局限于被动的探测，以免对企业造成破坏。可选的情况下，渗透测试可以包括对调制解调器拨号以及物理安全的攻击和评估，这可以通过称为拨号器（wardialing）的方式完成，该机制用于扫描和检测错误配置的拨号及终端服务器，以及不道德的人和/或非授权的调制解调器连接。

当审核是针对Web站点时，应该进行对公共网关接口（Common Gateway Interface，CGI）、Java、JavaScript以及ActiveX脚本的源代码审核。在执行审核时，要维护关于整个活动的详细的、带时间戳的日志记录。通过对审核日志和目标站点日志进行比较，该日志将进一步用于测试当前站点日志工具的工作情况。最重要的是，如果是为某种非个人的原因执行审核，一定要从公司领导那里得到书面许可。

安全审核应该定期执行。根据一些参考书籍，例如《黑客攻击揭密篇》（Hack Attacks Revealed）[⊖] 第2版中介绍的技术、工具和软件，一个好的分析过程可以分为7个阶段。

第一阶段：盲测试

在盲测试或者远程测试中，测试人员预先没有目标网络基础设施的详细资料。

站点扫描

站点扫描包括如下内容：

• 网络发现。
• 对发现阶段确定的所有端口进行端口扫描。
• 应用扫描以确定绑定在所发现的端口上的系统服务。
• 进行吞吐量扫描来得到端口的利用率级别以判断漏洞。
• 文档记录结果。

远程审核

远程审核中需要进行以下活动：

• 对边界防御、外部ISP服务以及任何其他通过防火墙或是代理作为管道的网络服务进行配置、稳定性和漏洞测试。
• 文档记录结果。

渗透测试

渗透测试中需要进行以下活动：

• 带着渗透的目的，对站点扫描和远程审核过程中确定的所有对象的物理安全进行攻击和评估。
• 审核CGI、JavaScript和ActiveX脚本源代码。
• 从客户标识的数据库中启动对象数据库连接（Object Database Connectivity, ODBC）调用。
• 进行IP泛洪（flood）测试。

⊖ 该书已由机械工业出版社引进出版。——编辑注

- 发起标准的Windows NT、Novell Netware和Unix IOS攻击。
- 执行域名服务（Domain Name Service，DNS）哄骗。
- 进行被动嗅探器（sniffer）探测以捕获网络流量。
- 文档记录结果。

IP、邮件哄骗和垃圾邮件测试

在IP、邮件哄骗（spoof）和垃圾邮件（spam）测试中需要进行以下活动：

- 进行渗透攻击使得网络基础设施设备进入受损害的状态或是泄漏敏感信息（例如口令字）。
- 测试伪造电子邮件，并控制任何简单邮件传输协议（Simple Mail Transfer Protocol, SMTP）、邮局协议（Post Office Protocol, pop3）以及Internet消息访问协议版本4（Internet Message Access Protocol Version 4, IMAP4）服务器，以利用用户昂贵的带宽发送外部邮件攻击的能力。
- 文档记录结果。

第二阶段：基于知识的渗透测试

在基于知识的渗透测试阶段，测试人员具有目标网络基础设施的知识。该阶段的测试包括以下活动或内容：

- IP和IPX（Internetwork Packet Exchange）寻址机制。
- 协议。
- 网络/端口地址转换机制。
- 拨号信息（例如用户、拨号号码和接入方式）。
- 互联（设备）操作系统的配置。
- 特权接入点。
- 详细的外部配置（例如ISP和Web托管）。
- 文档记录结果。
- 站点扫描，包括：
  - 网络发现。
  - 对发现阶段确定的所有端口进行端口扫描。
  - 应用扫描以确定绑定在所发现的端口上的系统服务。
  - 进行吞吐量扫描来得到端口的利用率级别以判断漏洞。
  - 文档记录结果。
- 远程审核，包括：
  - 对边界防御、外部ISP服务以及任何其他通过防火墙或是代理作为管道的网络服务进行配置、稳定性和漏洞测试。
  - 文档记录结果。
- 渗透测试，包括：
  - 带着渗透的目的，对站点扫描和远程审核过程中确定的所有对象的物理安全进行攻击和评估。
  - 审核CGI、JavaScript和ActiveX脚本源代码。
  - 从客户标识的数据库中启动ODBC调用。
  - 进行IP泛洪测试。
  - 发起标准的Windows NT、Novell Netware和Unix IOS攻击。

- 执行域名服务哄骗。
- 进行被动嗅探器探测以捕获网络流量。
- 文档记录结果。

- IP、邮件哄骗和垃圾邮件测试，包括：
  - 进行渗透攻击使得网络基础设施设备进入受损害的状态或是泄漏敏感信息（例如口令字）
  - 测试伪造电子邮件，并控制任何SMTP、POP3以及IMAP4服务器，以利用用户昂贵的带宽发送外部邮件攻击的能力。
  - 文档记录结果。

第三阶段：Internet安全和服务的测试

第三阶段中进行渗透测试，包括以下活动：

- 带着渗透的目的，对站点扫描和远程审核过程中确定的所有对象的物理安全进行攻击和评估。
- 审核CGI、JavaScript和ActiveX脚本源代码。
- 从客户标识的数据库中启动ODBC调用。
- 进行IP、超文本传输协议（Hypertext Transfer Protocol, HTTP）和Internet控制消息协议（Internet Control Message Protocol, ICMP）泛洪测试。
- 执行域名服务哄骗。
- 文档记录结果。

第四阶段：拨号审核

在拨号审核阶段中，包括以下活动：

- 利用拨号器来扫描、检测错误配置的拨号和终端服务器（例如PC Anywhere、Reachout以及Citrix），以及不道德的人或任何非授权的桌面调制解调器。
- 文档记录结果。

第五阶段：本地基础设施审核

本地基础设施审核是对各部分交付报告的编辑，包括如下内容：

用户问题报告。其中包括诸如启动时间缓慢、文件/打印困难、低的带宽可用性以及自发的连接终止等。

协议系列的流量合成。捕获阶段中所发现的协议比例详细分类。每帧按照协议系列归类。多种协议的帧根据所分析的最高协议归类。这样，例如封装在帧中继中的TCP/IP帧将归为TCP/IP类；帧中所有的字节作为TCP/IP比例的一部分。

网段/站点与特征。对所发现的网站和特征的详细分类，包括每个网络的错误或是特征数量。可能被检测到的特征包括：

- 帧冻结（frame freeze），指示挂起的应用或是不运行的站点。
- 文件重传，指示整个文件或是文件的一部分已经被重新传送，通常由没有有效利用网络的应用引起。
- 低吞吐量，根据文件传送的平均吞吐量计算。
- 重定向主机，指示站点正在接收路由器或是网关的ICMP重定向消息，通知站点更好的路由存在或是不可用。

带宽利用率。指示在分析会话过程中站点利用的整个带宽。根据这些数据，可以建议增加吞吐量和效率。

第六阶段：广域网审核

广域网（WAN）审核是对各部分交付报告的编辑。包括如下内容：

互联设备的发现。所发现的当前的硬件互联设备，包括交换机、路由器、防火墙和代理。

告警和阈值。该功能实时地跟踪所有HTTP、FTP、POP3、SMTP和NNTP（Network News Transfer Protocol）流量，以及对定制站点的访问信息。其他监控的访问信息包括：以小结形式记录的网络负载、每个用户访问的数量和频率以及对访问企图的拒绝。

告警/事件的日志记录。引用自分析会话过程中的实际日志文件。

第七阶段：报告结果

报告阶段是对每个阶段交付报告的汇总、编辑。包括如下内容：

- 所有发现的详细文档记录。
- 每个事件的图表或者屏幕快照。
- 根据“老虎队”技术所推荐的防御机制的增强措施。
- 对构成直接威胁的漏洞列出的要求或是可选的增强措施。

安全分析的交付报告应该合并分析阶段项目综述中所包括的所有功能。每次交付应该以一种详细报告的形式，分成诸如扫描、哄骗、垃圾邮件、泛洪、审核、渗透、发现、网络信息、系统信息、漏洞评估以及对提高网络安全的推荐（要求的或是可选的）等部分。对发现结果应按分配时间来组织，接下来的补救阶段也是如此。应该将漏洞扫描器（例如NAI公司的CyberCop扫描器或Nessus安全扫描器）的结果合并入报告中。在本书后面章节将更详细地讲述扫描器。

发挥Windows、Linux和Solaris的能力

在详细讨论漏洞和渗透评估之前，将讲述一下测试系统（即“老虎盒”）的最低需求和结构。“老虎”这一术语来自安全专家小组。最初，“老虎队”是指一组受雇佣的专业人员，他们的目的是对边界安全进行渗透并且测试或分析组织的内部安全策略。他们对计算机系统、电话系统、保险柜等进行攻击，以帮助公司对自己安全系统的有效性进行评估并且学习如何有效地提高自己的安全策略。

不过最近“老虎队”已经用于代表评估安全问题的任何官方检查组或者特别行动组。“老虎队”中包括专业黑客和骇客，他们通过网络或者设想的安全通信通道进行远程攻击来测试计算机的安全。此外，“老虎队”也对程序代码的完整性进行测试。很多软件开发公司在将软件投放市场前会外请“老虎队”进行严格的动态代码测试。“老虎队”使用其“老虎盒”提供必要的发现潜在安全漏洞的工具。“老虎盒”包括发现、扫描和进行某种安全漏洞渗透的工具。

“老虎盒”的核心元素是操作系统。一等的“老虎盒”为多启动配置设置，包括*NIX和Windows操作系统。目前，用于Windows操作系统的“老虎盒”工具没有用于*NIX操作系统的多，不过在这一点上Windows正在提高其竞争力。最初由AT&T贝尔实验室开发的Unix是被科学计算、工程和学术团体所使用的强大的操作系统。Unix是一个灵活的、可移植的多用户、多任务环境，提供了电子邮件、联网、编程、文字处理以及科学计算能力。多年来，形成了两种主要的Unix开发版本：AT&T开发的Unix System V和加利福尼亚大学伯克利分校开发的BSD Unix，每种Unix又有多种变种。除了Sun公司的Solaris，还有新的Unix变种—Linux，也是“老虎盒”中的常见配置。Linux提供对OS命令行的直接控制，包括实现软件稳定性和灵活性的定制代码编译。Linux由多家厂商定制、封装和分发，这些厂商包括：

RedHat Linux（www.redhat.com）

Slackware（www.slackware.org）

Debian（www.debian.org）

TurboLinux（www.turbolinux.com）

Mandrake（www.linux-mandrake.com）

SuSE（www.suse.com）

Trinux（www.trinux.org）

MkLinux（www.mklinux.org）

LinuxPPC（www.linuxppc.org）

SGI Linux（www.oss.sgi.com/projects/sgilinux11）

Caldera OpenLinux（www.caldera.com）

Corel Linux（www.linux.corel.com）

Stampede Linux（www.stampede.org）

“老虎盒”组件

在本书第一部分给出了配置“老虎盒”操作系统的逐步指导。如果你技术娴熟或是已经安装了“老虎盒”操作系统并且配置了Windows或是*NIX操作系统，可以直接进入第二部分。

前面提到过多操作系统，多启动配置使得在一个“老虎盒”中启动不同的操作系统更为容易（注意，为了简单起见Windows要在*NIX之前安装和配置）。在写本书时，Windows最稳定的版本包括Windows 2000、Windows 2000专业版和Windows 2000服务器版。*NIX中最灵活和被支持的是Red Hat Linux（www.redhat.com）版本7.3/8，以及SUN公司的Solaris 8（www.sun.com/software/solaris/）。好消息是除了微软的操作系统，Linux和Solaris都可以免费得到二进制代码。

如果用于多启动的第三方产品工作不正常，Red Hat提供做启动盘的选择，该盘包括安装核心的副本和用于启动系统的所有模块。启动盘也用来加载急救盘。这样，要执行Windows，就不带启动盘重启系统；要执行Linux，就用启动盘重启系统。缺乏经验的用户可以使用诸如PowerQuest公司的BootMagic（www.powerquest.com/products/index.html）等工具，它提供了图形界面的简单多启动安装。

最低系统需求

硬件需求根据使用“老虎盒”的目的决定，例如，系统是否用于开发和脚本编程以及系统是否使用网络服务。当前，完成大多数情况的最低配置如下：

处理器：Pentium II以上。

内存：128MB。

硬盘驱动器：10GB。

视频卡：至少支持1 024 x 768分辨率和16 000种颜色。

网络：双网卡（Network Interface Card，NIC），至少其中一个支持被动或所谓的混杂（promiscuous）模式（当接口处于混杂模式时，无论包的地址是否针对“老虎盒”，都可以接收所有的网络包）。

其他：三键鼠标、光驱和软盘驱动器。

本书第一部分将开始指导你进行Windows 2000和服务器“老虎盒”操作系统的安装和配置。

第1章 Windows 2000/Windows 2000 Server的基本安装和配置

本章将带领你逐步安装基于Windows的“老虎盒”操作系统。虽然本章以配置Windows 2000 Server为主，但是这些介绍同样适用于Windows 2000和Windows 2000专业版。

1.1 安装Windows 2000 Server

要安装Windows 2000 Server，首先将安装光盘放入主光驱中，并启动系统。确保系统指定的启动顺序是先从光驱启动。然后，按照以下的步骤执行：

步骤1：在欢迎屏幕上，有三个选项：

- 要开始安装Windows 2000，请按Enter键。
- 要修复Windows 2000的安装，请按R键。
- 要停止安装Windows 2000并退出安装程序，请按F3键。

这里，我们按Enter键继续进行安装。

步骤2：许可协议（License Agreement）。通过按Page Down键来查看整个Windows 2000的许可协议。在协议的最后，按F8键接受并继续安装。

步骤3：选择安装位置和驱动器格式。为Windows选择一个安装位置。在这个步骤中，可能要创建或删除硬盘活动分区，然后选择打算安装操作系统的分区并按Enter键。在按Enter键的时候，可能选择了用文件分配表（FAT）系统或NT文件系统（NTFS）格式来格式化分区。这里，我们选择NTFS。

FAT还是NTFS？这是个问题

FAT格式是Windows支持的最简单的文件系统。因为它有很小的开销，因此最适合于400MB以下的驱动器或分区。它以固定大小存放在硬盘上分配的存储空间或卷的顶部。为了安全的目的，保存着两份FAT的副本，以防止出现一个副本被破坏的情况。

FAT系统建立了一张操作系统用于定位磁盘文件的表。即使一个文件被分段存储在许多扇区中（也就是分散存储在磁盘里），FAT也可以利用这个表来监控和找到所有的扇区。

FAT格式是以组或者簇来分配空间的，每一簇的大小是由相应卷的尺寸来决定的。例如，当创建一个文件的时候，系统会在目录和第一簇码中设置一个认可过的条目。这个条目显示的不是

一个文件的末尾，就是指向下一簇。

注意FAT要定期地更新，这是很重要的；否则，可能导致数据的丢失。然而，也应该注意在每次更新FAT的时候，磁盘读头应该重定位在驱动器的逻辑零磁道上。这是个费时的过程。同样，由于FAT目录结构没有特定的组织方式，因此一般把文件放在驱动器第一个可用的位置上。应该注意到，为了成功地启动系统，FAT和根目录存储在一个预定的位置上是很重要的。

FAT支持的文件属性只有只读、隐藏、系统和存档这四个。文件名或目录名最多只能有8个字符，紧跟一个句点（.），并有一个不超过3个字符的扩展名。FAT使用传统的8.3格式文件名约定——即文件名必须使用ASCII码字符集。所有的FAT名称必须以一个字母或数字开始，也可以包括除以下字符外的其他字符：

句点（.）

双引号（""）

斜杠和反斜杠（/\）

方括号（[]）

冒号（:）

分号（;）

竖杠（|）

等号（=）

逗号（,）

FAT有以下两个主要的优点：

- 当出现硬盘故障的时候，一个可启动的软盘就可以访问分区来进行故障诊断。
- 在Windows下，执行反删除恢复是不可能的。然而，如果文件存放在FAT格式的分区中，那么只要系统可以重新启动到MS-DOS环境下，这个文件就可以恢复。

FAT有以下两个缺点：

- 当驱动器的容量增加的时候，FAT的性能会下降；因此，在驱动器或分区大于400MB的情况下，不推荐使用FAT文件系统。
- 存储在FAT分区中的文件不能设置安全权限，而且在Windows环境下，限制FAT分区中的文件大小最大为4GB。

NTFS文件系统改进了可管理性，包括处理日志和文件安全性来解决磁盘错误。可以对目录或单个文件设置访问控制权限。对于大空间的需求，NTFS可以支持分散卷（spanning volume），也就是可以将文件和目录分散在不同的物理硬盘上。由于随着空间的增加，NTFS文件系统的性能并没有降低，因此非常适合在400MB或更大的卷上使用。

NTFS文件系统中文件名和目录名允许最多255个字符，其中包括用句点（.）分开的扩展名。虽然名称中保留键入时候的大小写，但是这些名称并不是大小写敏感的。NTFS的名称必须以一个字母或数字开始，也可以包括除以下字符外的其他字符：

问号（?）

双引号（""）

斜杠和反斜杠（/\）

星号（*）