# <<Windows电脑管家>>

## 图书基本信息

书名：<<Windows电脑管家>>

13位ISBN编号：9787113151775

10位ISBN编号：7113151779

出版时间：2012-11

出版时间：中国铁道出版社

作者：《Windows电脑管家:DOS/BIOS/注册表/组策略技术手册》编委会

页数：504

字数：766000

## 内容概要

《Windows电脑管家(DOS\BIOS技术注册表组策略技术手册)》编著者本书编委会。

本书通过大量使用的案例展示,深入浅出的介绍了常见的DOS命令行,BIOS、注册表和组策略的应用技巧,让读者打消畏难心理,做到灵活运用;同时对最新的Windows
7的相关批处理命令和系统优化作了详细介绍。

书中所举案例非常实用，步骤详细，截图清晰，所以学习起来并不难懂，是注册表、BIOS、组策略、DOS爱好者学习的首选指导教程之一。

本书适用于电脑维护人员、电脑软硬件爱好者，可以帮助其较深层次地了解电脑，更有效地管理电脑；同时书中的许多案例对于普通电脑用户和电脑培训班学员有非常好的学习指导意义。

## 书籍目录

## 章节摘录

版权页： 插图： 14.11黑客入侵紧急处理 一旦发现有一个系统被黑客攻击了，不要惊慌。
保持冷静，然后有逻辑地进行处理。
以下的行动计划能帮助减少一些损失。
隔离网络。
关闭网络的所有外部接口，包括Intemet、WAN、VPN和拨号连接，断开路由器、 无线接入点（AP）以及将网络与外界连接起来的任何其他设备的所有线路。
这样做能立即停止当前正受到的攻击，并阻止入侵者危及其他系统的安全。
清理无线设备。
使用无线嗅探器（如Airscanner Mobile Sniffer或NetStumbler.tom的NetStumbler）在所在的区域内查找任何恶意的A_P。
确保嗅探器安装在支持当前所有无线标准（也就是802.11a、802.11b和802.11g）的卡上。
查找其他被攻击了的电脑。
使用上文所述的技术来查找是否有其他电脑已遭受到黑客攻击。
复查防火墙配置。
查找是否存在任何未授权的规则、未授权对外界打开的端口和未授权的网络地址转换（NAT）规则。
检查防火墙日志中是否记录了可疑的活动。
建议始终将出站的通信限制在必要的出站端口，并确保只有经授权的计算机才能通过防火墙向外发送邮件。
检查AD（活动目录）。
查找任何未授权的用户账户并禁用它们。
更改网络中所有账户的密码。
对于有较高权限的账户，建议设置至少15个字符的密码（或密码短语）。
这样长度的密码很难破解，因为LAN管理器（LM）密码HASH不会在服务器上存储超过14个字符的密码。
更换被黑客攻击的计算机上的硬盘。
更换硬盘可以隔离并保留黑客的攻击行为。
可以复查旧硬盘上的数据以获得有关攻击的有用信息。
找出被攻击的弱点。
尽量找出黑客是如何访问网络的，但这通常是很难做到的（并且超出了本文的讨论范围）。
如果不能找到漏洞在哪里，请考虑雇用一位安全顾问来帮助。
重装被攻击的电脑。
彻底清理一个被黑客攻击的计算机几乎是不可能的。
如果电脑上还残留着一种或多种黑客工具，入侵者将会重新获得访问该电脑的能力。
确保电脑完全清理干净的唯一办法是格式化硬盘，并重装整个电脑。
这样确保不会保留了任何先前安装的黑客工具。
应该重新安装所有程序，手工安装所有补丁，只恢复数据文件。
绝对不要从磁带恢复注册表、操作系统或任何程序。
对所有电脑进行全面的病毒扫描。
要注意，防病毒程序有时会把黑客工具当作是合法程序。
如果扫描结果显示电脑是干净的，但还是怀疑它已被攻击，建议重装该电脑。
重新连接WAN线路。
重新连接WAN线路，并仔细监测，以确保关闭了网络的所有漏洞。
注意网络的带宽是否会被大量占用，密切监测防火墙日志，并在所有服务器上启用安全审核。

## 版权说明