

<<终端安全>>

图书基本信息

书名：<<终端安全>>

13位ISBN编号：9787121084867

10位ISBN编号：7121084864

出版时间：2009-6

出版时间：卡德里奇、伍前红、余发江、杨颢 电子工业出版社 (2009-06出版)

作者：卡德里奇

页数：269

版权说明：本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问：<http://www.tushu007.com>

## <<终端安全>>

### 内容概要

尽管在安全技术和培训中已经投入了大量人力和资金，但黑客们总是能成功攻击网络中最薄弱的环节——终端。

《终端安全》作者、顶级安全专家MarkS.Kadrich系统地阐述了终端安全是影响信息系统安全的根源这个学术观点，同时提出了以过程控制模型构建网络安全的方法。

同时《终端安全》也从实际出发，介绍了如何通过过程控制技术来帮助读者保护所有的终端设备，从MicrosoftWindows、AppleOSX、Linux到PDA、智能电话、嵌入式设备。

在《终端安全》中，作者还介绍了许多实际的信息安全技术、软件和工具，对读者有很高的参考和应用价值。

《终端安全》特别适合用作信息安全、计算机、通信、电子工程等领域的科技人员的技术参考书，或作为相关专业的教材。

<<终端安全>>

作者简介

作者：(美国)卡德里奇 译者：伍前红 余发江 杨颀

## 书籍目录

第1章定义终端1.1概要1.2特别注意1.3Windows终端1.4非Windows终端1.5嵌入式终端1.6移动电话和个人数字助理(PDA)1.7Palm1.8WindowsCE——WindowsMobile1.9SYMBIAN操作系统1.10黑莓1.11消失的边界——骗人1.11.1边界在变化1.11.2快速移动不等于消失1.11.3终端是新的边界1.11.4保护数据1.12关键点1.12.1终端是新的战场1.12.2对人类来说变化太快第2章安全防护为什么会失败2.1概要2.2特别注意2.3设定舞台2.4商业利益驱动的过程2.4.1解决过去问题的方案2.4.2我们没有严格地质问厂商2.5病毒、蠕虫、木马和僵尸程序2.5.1今天的恶意软件：大、快而且危险2.5.2引人瞩目的失败2.5.3攻击利用的是什么2.5.4僵尸程序2.6可以料想的悲惨结果2.6.1比以往更多的花费2.6.2我们无法获得预期的成功2.6.3我们仍然很诧异2.7有什么遗漏吗2.7.1我们做错了什么2.7.2我们错过了一些线索吗2.8关键点2.8.1恶意软件继续肆虐2.8.2厂商没有帮上忙2.8.3我们需要问更难的问题2.8.4我们遗漏了什么吗第3章缺失之处3.1概要3.2特别注意3.3现有尝试已经失败(目前的模型)3.4我们不明白为什么失败3.5我们还在沿用旧的思想3.6像控制问题那样定义网络3.6.1将控制模型与技术对应3.6.2确定反馈路径3.6.3识别出影响其他度量的那些度量3.6.4规划业务途径和技术路线3.6.5我们可以建立一个更好的模型吗3.7确定控制节点3.7.1将技术和控制节点对应3.7.2将控制节点与控制模式对应3.7.3测定时间常数3.7.4控制路径与业务过程3.8完成图释3.9关键点3.9.1我们需要更好的思想3.9.2信任与风险3.9.3过程控制有助于建立模型3.9.4不能忽视业务过程3.9.5我们需要共同的语言第4章查明缺失的环节4.1概要4.2特别注意4.3两个数据点蕴含一个解决方案4.3.1攻击载体4.3.2过程控制分析4.4联系似乎就是终端4.4.1恶意软件的目标4.4.2允许网络接入4.5需要做些什么4.5.1基本的阻断和治理4.5.2管理主机的完整性4.5.3控制接入网络4.6网络访问控制4.6.1验证最低限度的信任4.6.2只允许可信系统4.6.3亡羊补牢4.6.4利用技术强制实施决策4.7关键点4.7.1终端是关键4.7.2必须利用技术4.7.3网络是比例过程控制解决方案的一部分第5章终端与网络集成5.1概要5.2特别注意5.3体系是关键5.4基础5.4.1多老才算过时5.4.2网络分区仍然有效5.5我需要铲车吗5.5.1升级的代价不菲5.5.2一种花销较少的方法5.5.3技术展望与未来5.6终端支持5.6.1认证5.6.2厂商支持5.7安全漏洞与修复5.7.1检测5.7.2漏洞跟踪服务5.7.3漏洞管理5.7.4修复5.7.5渗透测试5.8签约客户与访客5.9关键点5.9.1了解你的体系结构5.9.2三种基本的网络访问控制模型5.9.3谨慎选择厂商5.9.4不要相信未来5.9.5允许受控接入是重要的5.9.6漏洞管理在安全过程中有一席之地5.9.7技术,流程,然后闭合回路第6章信任的起点6.1概要6.2特别注意6.3从一个安全的创建环境开始6.3.1过程是关键6.3.2在安全明亮的地方创建6.3.3需要一个安全底线6.3.4控制你的源代码6.4必要的工具6.4.1软件防火墙6.4.2反病毒6.4.3补丁管理6.4.4入侵检测6.4.5入侵防御6.4.6主机完整性6.4.7加密6.5信任,但要验证6.5.1测试,测试,测试6.5.2跟踪你的结果6.6关键点6.6.1起点安全6.6.2必需的工具6.6.3检查你的结果第7章威胁载体7.1概要7.2特别注意7.3保护操作系统7.3.1一些内置的保护7.3.2一些内在的弱点7.4“杀手级”应用7.4.1P2P攻击7.4.2让我们“聊聊”它7.5关键点7.5.1操作系统是你最好的敌人7.5.2软件是你最坏的朋友第8章MicrosoftWindows8.1概要8.2特别注意8.3简单说说Vista8.4最初的安全检查8.4.1系统扫描8.4.2查找Rootkit包8.4.3系统文件8.4.4交换数据流8.4.5检查注册表8.4.6关于进程8.4.7间谍软件8.4.8查看日志8.4.9网络欺骗8.4.10扫尾工作8.5加固操作系统8.5.1独立系统8.5.2检查你的反病毒软件8.5.3上紧螺丝8.6应用程序8.6.1软件限制策略8.6.2IE浏览器8.6.3网络会议8.6.4终端服务8.6.5WindowsMessenger8.6.6Windows更新8.7企业安全8.8服务器8.9闭合回路8.10工具和厂商8.11关键点8.11.1从新鲜环境开始8.11.2Rootkit包8.11.3安全装备竞赛8.11.4Windows可以是安全的8.11.5过程是关键8.11.6闭合回路第9章AppleOSX9.1概要9.2特别注意9.3最初的安全检查9.3.1系统扫描9.3.2查找rootkit包9.3.3系统文件9.3.4处理你的进程9.3.5网络上有些什么9.3.6间谍软件和其他恶意软件9.3.7查看日志文件9.4加固操作系统9.5应用程序9.6网络9.7工具和厂商9.7.1Apple远程桌面9.7.2LittleSnitch9.7.3反病毒软件9.7.4Symantec9.7.5Virex9.7.6ClamXav9.8闭合回路9.9关键点9.9.1网络9.9.2应用程序9.9.3Rootkit包9.9.4数据保护9.9.5检查日志9.9.6主机完整性9.9.7安全工具9.9.8闭合回路第10章Linux10.1概要10.2特别注意10.2.1支持10.2.2应用10.2.3FEDORA10.2.4XANDROS10.2.5支持的应用10.2.6漫谈10.2.7合适与完美10.2.8不是背书10.3初始安全检查10.3.1系统扫描10.3.2查找ROOTKIT包10.3.3系统文件10.3.4进程10.3.5网络10.3.6间谍软件和恶意软件10.3.7查看日志10.4加固操作系统10.4.1安装10.4.2清除无用软件(Dunselware)10.4.3更新和补丁10.4.4网络10.4.5访问控制10.5应用10.5.1读,写,算10.5.2远程管理10.6网络10.6.1NETBIOS的不幸10.6.2无线网络10.6.3网络应用10.6.4802.1X10.7企业管理10.8工具和

## &lt;&lt;终端安全&gt;&gt;

厂商10.9闭合回路10.10关键点10.10.1两个极端的对比10.10.2XANDROS运行NETBIOS10.10.3更新FEDORA10.10.4用户依然是问题10.10.5为成功而筹划10.10.6闭合回路的可能性第11章PDA与智能电话11.1概要11.2注意11.2.1当前的严重威胁11.2.2有趣的解决方法11.2.3连接11.2.4新领域11.3操作系统11.3.1Windows Mobile11.3.2SYMBIANOS11.3.3黑莓11.3.4PALM11.3.5移动Linux11.3.6初始安全检查11.4手持设备安全保护11.4.1Windows Mobile11.4.2SYMBIANOS11.4.3PALM11.4.4黑莓11.4.5同步11.5应用11.5.1电子邮件11.5.2短信11.5.3浏览11.6网络11.6.1WiFi11.6.2蓝牙安全11.6.3蜂窝协议11.7工具与厂商11.7.1GOOD11.7.2BLUEFIRE安全技术11.7.3SMOBILE系统11.7.4移动ARMOR11.7.5反病毒厂商11.7.6非企业用户11.7.7WEB站点11.8闭合回路11.9关键点11.9.1行业尚未成熟11.9.2手持设备将是下一个攻击目标11.9.3网络的不幸11.9.4解决方案和安全分歧11.9.5强制措施将会启用11.9.6还没有实现闭环过程控制第12章嵌入式设备12.1概要12.2特别注意12.3什么是嵌入式系统12.4哪里有嵌入式系统12.5为什么担心12.6嵌入式安全威胁12.7初始安全检查12.8应用12.9网络12.10工具及厂商12.11嵌入式安全12.12闭合回路12.13关键点12.13.1我们被嵌入式系统包围12.13.2没有真正的安全12.13.3TPM没给嵌入式解决方案帮上忙12.13.4闭合回路12.13.5你可以做一些工作第13章终端安全失败案例研究13.1概要13.2案例研究113.2.1失败模式：出了什么问题13.2.2终端如何卷入其中13.2.3影响13.2.4过程控制缺失13.2.5如何避免13.3案例研究213.3.1失败模式：出了什么问题13.3.2终端如何卷入其中13.3.3影响13.3.4过程控制缺失13.3.5如何避免13.4案例研究313.4.1失败模式：出了什么问题13.4.2终端如何卷入其中13.4.3影响13.4.4过程控制缺失13.4.5如何避免13.5案例研究413.5.1失败模式：出了什么问题13.5.2终端如何卷入其中13.5.3影响13.5.4过程控制缺失13.5.5如何避免13.6关键点13.6.1不同点和相似点13.6.2闭环过程控制哲学13.6.3余下的工作附录：术语

## <<终端安全>>

### 编辑推荐

无论你是否是一名安全工程师、安全顾问、网管、架构师、经理或者是首席安全官，这本书中都有一直在寻觅的东西：一种管用的全面的终端安全策略。

尽管在安全技术和培训中投入了大量的人力和物力，黑客们总是能成功攻击网络中最薄弱的环节——终端。

本书中，作者并不是给出传统的千篇一律的解决方案，而是针对每一种终端的唯一特性，从它的应用软件到应用环境，制定不同的方法。

作者为WindowsPC、笔记本、UNIX / Linux工作站、苹果机、手机、嵌入式设备等提出了特定的定制的安全策略。

通过本书读者将学会： 识别常规终端安全策略中存在的安全隐患 辨别好的产品、工具和流程，选择它们保护自己的设备和基础设施 配置新的终端安全，重新配置已有终端，优化安全措施 快速识别和修复有危险隐患的终端设备 系统地防御针对终端的新恶意软件和病毒 改善终端与网络接入点的安全

#### 版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:<http://www.tushu007.com>