<<更安全的Linux网络>>

图书基本信息

书名：<<更安全的Linux网络>>

13位ISBN编号：9787121082214

10位ISBN编号：7121082217

出版时间：2009-3

出版时间：电子工业出版社

作者：恒逸资讯，陈勇勋 著，刘立群 等改编

页数：481

字数：806

前言

Linux是一个注重实用的系统，像是练拳术一般，虽然你会练习花哨的套路，但终究是为了实战的目的。
Linux这样的系统，它不好“看”，但却扎扎实实。
我常看到IT人员拿LinUX在企业内部做各种不同的应用，除了常见的Web server、File server之类的应用之外，还有一个特殊的用途，那就是当做企业IT系统的防护罩。

目前企业的信息安全防护有个“流行”的现象，那就是在企业日常运营系统外面搭建了一层坚固异常的系统防护罩，许多企业因而会采用Linux做最外层或其中一层防火墙，以降低被入侵的几率。
Linux作为安全防护的机制颇为契合企业的实际用途，类似的实际功用只有Linux好手才知其中的诀窍。
除了防火墙机制之外，企业还有常见的Proxv服务器，你知道可以拿Linux当做“反向”proxy服务器，反过来保护Windows server的IIS Web服务器吗？
诸如此类的实际应用，通常都是企业所需，如果你是企业内部的IT管理人员，建议你对于此类的技术议题可以多加涉猎。

虽然Linux可以为企业带来许多好处，但毕竟是“马有千里之程，无人不能自往”，企业IT人员若不具备相关技术，给你再好的武器都派不上用场，而今即使IT人员愿意好好研究Linux相关技术，但可能也苦于参考数据的不够充足。
针对Linux应用在企业内部网络与系统安全之议题，现在终于有了一本专书呈现在各位读者面前。
本书作者Iacky。
是恒逸信息著名的Linux讲师之一，他授课的最大特色是会让学员觉得像是朋友股的在教授你技术知识。

<<更安全的Linux网络>>

内容概要

这是一本将理论与实务完美结合的书，由网络的基本概念开始，采取以由浅入深的讲解方式，逐步引导读者进入网络安全的世界。
让读者从无到有地快速向下扎根，以帮助有心跨入网络安全领域的IT技术人员，能够完整且正确地构建企业网络的安全屏障。
本书内容包括Netfilter/Iptables（Linux系统下功能最为强大且扩充能力最强的防火墙系统）；Squid Proxy（能够加速企业外连带宽，以及保护Microsoft IIS Web Server的重要机制）；Nessus、Snort及Guardian（Nessus为OpenSource下功能最为完整的弱点扫描工具，可帮助我们快速且完整找出企业中有安全漏洞的服务器，进而提出问题解决的方法；Snort则是OpenSource下功能最为强大的入侵检测系统，甚至可以结合Guardian，以构成企业内部的入侵防御系统，自动将入侵者封锁于企业防火墙之外）；虚拟专用网（企业e化已是当今企业生存的关键，然而网络封包的窃听已成为使用网络的一大隐忧，如何在企业e化与信息安全中取得平衡点？
虚拟专用网可以完全解决以上所有困扰）。
本书适合系统管理与网络管理从业人员、网络安全及系统安全工作者参考学习。

<<更安全的Linux网络>>

书籍目录

第1章 防火墙的基本概念 1.1 TCP/IP的基本概念 1.2 封包的传递 1.3 ARP通信协议 1.4 TCP、UDP及Socket的关系 1.5 什么是防火墙 1.6 防火墙的判别依据 1.7 防火墙的分类 1.8 常见的防火墙结构 第2章 Linux防火墙基础篇 2.1 什么是Kernel 2.2 什么是Netfilter 2.3 Netfilter与Linux的关系 2.4 Netfilter工作的位置 2.5 Netfilter的命令结构 2.6 Netfilter的Filter机制 2.7 规则的匹配方式 2.8 Netfilter与Iptables的关系 2.9 Iptables工具的使用方法 2.10 以Filter机制来构建简单的单机防火墙 2.11 以Filter机制来构建网关式防火墙 2.12 Netfilter的NAT机制 2.13 Netfilter的Mangle机制 2.14 Netfilter的RAW机制 2.15 Netfilter的完整结构 2.16 实战演练 第3章 Netfilter 模块的匹配方式与处理方法 3.1 匹配方式 3.2 处理方法 3.3 实战演练 第4章 Netfilter/Iptables的高级技巧 4.1 防火墙性能的最佳化 4.2 Netfilter连接处理能力与内存的损耗 4.3 使用RAW Table 4.4 简单及复杂通信协议的处理 4.5 实战演练 第5章 Proxy Server的应用 5.1 什么是Proxy Server 5.2 Proxy Server能够支持的通信协议 5.3 Proxy Server的分类 5.4 Proxy Server的硬件需求 5.5 安装Squid Proxy 5.6 以Squid构建Cache Proxy 5.7 Transparent Proxy 5.8 Reverse Proxy 5.9 实战演练 第6章 使用Netfilter/Iptables保护企业网络 6.1 防火墙结构的选择 6.2 防火墙的本机安全 6.3 防火墙规则定义 6.4 入侵与防御的其他注意事项 第7章 弱点扫描及入侵检测 第8章 VPN 基础篇 第9章 VPN 实务篇 第10章 VPN： L2TP Over IPSec 附录A VMware Server 的安装及使用

章节摘录

不过，要解决以上的问题其实一点也不困难，只要稍微了解ICMP封包的结构就可以很容易解决这个问题，ICMP并不像TCP或UDP协议可以使用Port来区别封包的应用差别，例如，Port 3342送到Port 80，我们可以很轻易判断这是由Client送给Server的封包，但在ICMP封包的应用中，不管是Client送给Setver或是Server回应给Client，都是以ICMP封包来沟通，因此，我们无法单独就协议来区分某个ICMP封包是Client端主动送给server端，又或者是Setver端主动送给Client端。

接着，我们来观察ICMP封包的内容，或许就可以轻易知道解决这个问题的方法，图3-2是“ICMP请求”封包的内容，此外，图3-3为“ICMP响应”封包的内容，从图中我们可以发现“请求”与“响应”封包之间的差异，事实上，ICMP有很多不同的应用，为了区别某个ICMP封包的应用，在ICMP封包的包头内会有Type及code两个字段，其内容都为数字，而每个不同数字的组合都代表某一种特定的应用，若你对所有ICMP封包的应用有兴趣，不妨可参考RFC 793和RFC 2463，即可查询到所有Type及code的组合及应用。

学员通过学习与实践还可参加国家职业技能资格的考核认证，获得国家统一的职业资格证书。

如果需要进一步了解职业技能培训、鉴定和考核的相关信息，或需要相关技术资格。

<<更安全的Linux网络>>

编辑推荐

《更安全的Linux网络》适合系统管理与网络管理从业人员、网络安全及系统安全工作者参考学习。

<<更安全的Linux网络>>

版权说明