<<堡垒主机搭建全攻略与流行黑客 >

图书基本信息

书名：<<堡垒主机搭建全攻略与流行黑客攻击技术深度分析>>

13位ISBN编号：9787030262561

10位ISBN编号：7030262565

出版时间：2010-1

出版时间：科学出版社

作者：郝永清

页数：414

前言

攻防技术辩证一体辩证的看，网络安全技术包含两个方面，正面是防御，反面是攻击，二者缺一不可：没有了攻击技术，防御技术无从谈起；没有了防御技术，攻击技术就成为摆设，没有丝毫存在的意义。

本系列书籍从始至终贯彻这一基本要点，和其他同类图书的最大区别就在于此：我们虽然会详细模拟攻击者的攻击过程，但其目的是为了在防御的时候更加清楚的明白需要防御的“缺口”在什么地方；我们也会详细讲解防御体系的搭建思路和过程，但是也会讨论突破这样的防御体系的新的攻击技术和思路，进而再推出适当的防御技术。

更多的时候，本系列书籍的角度是在攻击者和防御者两者之间进行切换模拟——就好比现在工作在岗位上的网络安全技术工程师一样，经常都需要扮演攻击测试者和防护者的双重身份。

贯彻始终的“黑客”思维正面导向有圈内人曾用“妖魔化”来形容今天的黑客，很贴切但本质很荒谬、很无奈。

原本作为褒义的“黑客”一词，是指热心于计算机技术，水平高超的电脑专家。

在负面新闻不明真相的炒作下，在无数恶意攻击事件的曝光之后，在利欲熏心者的盲目追崇中，目前几乎已经完全沦为贬义的破坏者的代名词。

网络需要发展，技术需要进步。

让这样歪曲的思维误导的长期后果，就是越来越多的人远离“黑客”，远离本来可能为网络发展、技术进步而提供非常大助力的群体，让原本正面积极的群体变得愈加孤僻，越加“妖魔”，甚至沦陷。

所以，本系列书籍坚持正面积极的正确“黑客”思维导向，并将贯彻始终，力争明晰恶意攻击者和善意黑客之间的区别，力争将攻击技术这把锋利的刀用在推动技术进步之上，力争让更多即将误入歧途的被误导者看到光明的希望！

内容概要

在网络快速发展的情况下，对网络安全的技术要求已经越来越高，针对网络安全的细节要求和极致防御，国外开始出现防御能力极强的“堡垒主机”，并在极短的时间内风靡网络，受到托管机房、网络管理员等的信任。

本书以具有广泛意义的windows 2003 server为例，网络上流传着很多系统安全配置方法，但是仔细分析就会发现极不全面，很多配置甚至完全不合理，还有很大的安全隐患。
所以本书站在巨人的肩膀上，以全面、细致的方式，以各项安全配置可能遇到的攻击技术相辅助，结合藏锋者网络安全网(www．cangfengzhe．com)上的部分精华资料，完整的进行堡垒主机的搭建全过程，力求让读者深刻明白安全设置的目的、作用。

本书作者通过长年的网络安全工作经验，总结了最优化的堡垒主机安全设置，所有配置均在实际工作中经过详细调试，力求让读者通过简单、直接的方式，快速搭建出符合实际工作需求的、高安全度的堡垒主机！

本书适合对网络安全技术有兴趣并想从事相关行业的大学生；就读于网络信息安全相关专业的研究生；负责企业、公司网络信息安全的从业者；网络安全技术专业研究人员；所有对网络安全有兴趣的爱好者参考阅读。

作者简介

郝永清 CISSP、CISP、MCSE资深讲师，藏锋者网络安全网(www．cangfengzhe．com)核心成员之一，主要从事信息安全相关工作，负责深入分析用户安全需求；有近十年的授课经验，为300多家企业千余IT经理及IT技术人员做过安全培训；有丰富的项目经验，同时密切跟踪国内外的安全动态，对严重安全事件进行快速响应；对各种恶意软件进行分析，提供检测和解决方案，并完成产品的安全评估，如防火墙、入侵检测、漏洞扫描等；参与众多公司网络的渗透测试项目，并对病毒和木马有深入了解。

<<堡垒主机搭建全攻略与流行黑客 >

书籍目录

章节摘录

插图：1.1人员接触控制人员接触控制是所有有安全要求的计算机的第一项必备保护措施。
堡垒主机首先是一台服务器，是一台设备，是一个死物，然后才能在管理员的配置和管理之下，成为能发挥作用的系统平台。
如果可以让任何人没有限制地物理接触、控制、操作这个服务器，那无疑没有任何安全可言。
所以，在综合考虑堡垒主机的方方面面安全之前，首先需要对堡垒主机的物理人员访问进行一定程度的限制和规范。
国内目前比较流行的各大托管机房中，都或多或少的存在一些人员访问、接触的控制措施，但是一个标准而细致的具体方案是什么？
很难有人能说清楚，这一节主要就解决这个问题。
就普通的企业网络管理员、工程师来说，如果是大型企业，可能需要自己搭建专属机房，或者是将企业的服务器群组放置在托管机房，不管是什么情况，对人员的接触控制都应该有一个很明确、很细致的管理规范。
如果是企业自己的机房，需要使用这些人员接触控制规范来约束和管理：如果是托管在别人的机房，则需要使用这些规则来对机房进行评测，以便明确目标机房的服务质量。
国内大型的托管机房一般都具备比较完善的人员接触控制机制，当然根据控制力度的不同而收费也有所不同，网络管理员或者网络工程师需要根据实际情况来进行选择，以便在资金成本能够允许的条件下，尽量选择一个高质量的机房。
本节将主要涉及出入登记、门禁系统、视频监控、区域管理与比较特殊但却非常有用的电话记录、维护授权和身份审核等内容，选取了网络工程师在日常的工作中经常会遇到的问题作为例子进行讲述。
不管是企业自己的机房，还是托管机房，都应该有很完善而严密的出入登记策略，这是最基本也是很有必要的一项简单而有效的物理保护措施。
1.1.1.1 出入登记的作用出入登记是最简单的一种记录进出人员的方法，通过出入登记可以记录来访人员的身份、时间、目的、携带物品等，也可以记录该人员离开机房的时间，确认携带物品等。
一般出入登记和身份审核是一体的，也就是说在出入登记的同时，完成基本的身份审核。

后记

堡垒主机的相关技术涉及非常多的方面，本书前面的章节尽量选择了具有共通性的、实用的、效果好的一些技术进行讲解，目的是构建一个实用级的堡垒主机——但是限于篇幅，很多内容无法涉及，某些上文中的技术详情也无法一一列举和阐述，还需要读者通过自己的实际动手操作进行融会贯通。
对一个干净的堡垒主机来说，进行完本书上面几个章节的设置以后，还应该进行以下步骤的操作（限于篇幅，这里无法详述）：“ 重新修补一次补丁 ”在优化、配置的过程中，可能出现改动系统文件或者删除某些文件的情况，等所有设置完成以后，管理员应该及时使用“ 自动更新 ”功能进行完整的一次补丁更新。
“ 进行第一次完整备份 ”上述操作完成以后，需要管理员对堡垒主机系统的驱动、服务、数据进行完整备份。
最方便的方式是直接将整个操作系统进行完整备份，使用Ghost等相关备份程序，将备份好的数据刻录到光盘上，并妥善存放。
“ 安装服务并进行服务相关安全配置 ”上文的所有设置均是在干净的操作系统上进行的，没有涉及其他服务、组件、的安全，而Windows系统的庞大造成了它的任何组件如果要做到“ 安全 ”，都必须进行深刻、细致的安全配置，所以在确保堡垒主机已经配置完毕且进行了备份以后，开始进入各服务的安全配置和优化步骤吧！

编辑推荐

《堡垒主机搭建全攻略与流行黑客攻击技术深度分析》：物理安全保护+系统文件减肥+系统性能优化+服务透彻剖析+最小化安全网络+极限化系统安全=堡垒主机。

版权说明