郝永清［藏锋者］ 编著

网络安全攻防实用技术深度案例分析

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

科学出版社
www.sciencep.com

网络安全攻防实用技术深度案例分析

堡垒主机搭建全攻略与流行黑客攻击技术深度分析

郝永清［藏锋者］ 编著

科学出版社

北京

内 容 简 介

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。

图书在版编目（CIP）数据

堡垒主机搭建全攻略与流行黑客攻击技术深度分析 / 郝永清编著. —北京：科学出版社，2010

（网络安全攻防实用技术深度案例分析）

ISBN 978-7-03-026256-1

Ⅰ.堡… Ⅱ.郝… Ⅲ.计算机网络–安全技术 Ⅳ.TP393.08

中国版本图书馆 CIP 数据核字（2009）第 233397 号

责任编辑：田慎鹏 霍志国 / 责任校对：刘小梅

责任印制：钱玉芬 / 封面设计：耕者设计工作室

科学出版社出版

北京东黄城根北街 16 号

邮政编码：100717

http://www.sciencep.com

骏走印刷厂印刷

科学出版社发行 各地新华书店经销

*

2010 年 1 月第 一 版 开本：787×1092 1/16

2010 年 1 月第一次印刷 印张：27

印数：1—4 000 字数：514 000

定价：52.00 元

（如有印装质量问题，我社负责调换）

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。

丛 书 序

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！

专注于热点技术的追踪和普及

时代在变，技术也在变，技术热点的推陈出新本质就是技术进步的演变过程。

关注并专注于最新的攻防技术，并将这些新的、热的网络安全技术普及给大众，这就是本系列书籍的重要目标之一。

就当下的网络安全状况来看，针对 Web 服务的攻防、针对服务器的渗透攻防、针对个人计算机长期精准的控制和安全、针对网络协议的缺陷研究和修补等，都是攻击者、防御者们津津乐道的话题——自然也就是本系列书籍关注的话题。

需要提出注意的是，本系列书籍是动态的，是持续变化的，是跟随着热点变化而进步的，所以本系列书籍将长期、持续、及时地推出！

案例化和可操作性的实现尝试

就本质来说，计算机技术是一门需要动手能力比较强的学科。作为书籍来说，可操作性的优劣将决定此书的成败。

我们采用案例化的方式来进行技术讨论，针对网络安全技术的攻击和防御两方面，采用有针对性的、螺旋上升的“攻防”对立案例进行演示，力求让各技术体系毫发毕现的出现在读者面前——注意这不是空泛的理论交锋，这是可以做到“按图索骥”一步一步攻击和防御操作的详细记录！

最大化的提升书籍的易用性

任何事情的起步都是艰辛的，作为过来人的编者深刻明白迈出第一步的艰辛，所以，对于刚刚接触网络安全相关领域的新手，对于理解书中相关概念略显吃力的读者，我们尽量将一些关键的概念以“基本概念解释”的方式贯穿在文中，并在书末提供速查表。目的只是为了提高系列书籍的易读性，让读者更能贴切的理解各种案例和操作中的原理所在。

系列书籍中，类似于“基本概念解释”的还有适当位置的“技巧”、“提示”，以及序言之后的“本书使用方法”，还有文末的基本概念速查、书中所用演示平台和工具的汇总介绍等项。

希望读者能将这些小项目利用起来，让其为深刻理解书中技术而起到应有的辅助作用。

辅助在线技术交流平台

作为人力有限的编者来说，遗漏在所难免，所以为了更好的为读者服务，也为了除了书籍之外读者还有更方面的解惑、交流、讨论平台，本书和藏锋者网络安全网（www.cangfengzhe.com）合作，由之提供在线技术交流平台，以便本系列书籍读者更快、更好、更方便的提升技术层次——当然，这个平台肯定是免费的。

部分资料来源于藏锋者

任何技术都存在表现形式上的共性，网络安全技术也不例外。正是因为存在这样的共性，在案例的选取上，本系列书籍使用了部分藏锋者网络上的相关资料。

这样做的原因一来是很多经典资料的确很能明白的说明问题，二来是因为很多典型技术的推出就是因为存在这样的典型案例，三则是出于对实用性的考虑——我们倡导的方式是读者在通读全书后，去藏锋者网站下载并搭建书中案例的相关环境，使用相关工具进行模拟攻击和模拟防护，以达到真正的将书中的技术纳为己有的目的。

纠错及感谢

编著过程仓促，难免有所遗漏或者错误，如有发现，欢迎读者使用上述的网络交流平台与编者联系，提前致谢。

在系列书籍编著过程中，得到很多藏锋者网络上的技术伙伴们的支持和帮助，在此一并感谢。

最重要的是，系列书籍的出版和推出，得到科学出版社的大力支持。特别是责任编辑田 sir，事前、事中、事后均提供了莫大的支持，鞠躬谢过。

郝永清

2009 年 9 月于北京

本书使用方法

请用虚拟机

对任何一个网络安全技术爱好者来说，虚拟机都是必须的，也是必要的。

如果读者对本书中所讲案例有兴趣，想亲手操作，以达到最佳的阅读和理解效果，请使用虚拟机在本地虚拟相关系统，并在虚拟机上使用相关工具进行攻击和防御测试。

使用虚拟机的最大目的在于保障读者自身的系统安全；

其次是为了杜绝不经意间由读者兴趣而引发的网络恶意攻击；

然后是为了读者更深刻的理解不同身份的攻击者和防御者的操作平台、操作方法和操作目的；

最后是为了读者养成网络安全技术的基本构建、调试习惯，为以后可能遇到的网络安全问题提供最基本的环境支持。

基本概念解释

文中适当位置将出现“基本概念解释”，一般情况下是对上文中和本书主题无关，但却因为案例需要而有所涉及的理论概念。

整个网络安全体系庞大到难以想象，对于有一定经验的读者来说，将文中所述技术和其他相关概念联系在一起是很有裨益的，对技术层次的提升和某方面技术的全面透彻的理解尤为重要。

对于刚刚接触网络安全技术的读者来说，直接的案例风格书籍虽然可以很方便的提高读者的操作兴趣，快速让读者获得某一领域的相关技术理解，但是未免太过于片面，太过于单调。所以，对于新手来说，“基本概念解释”将是一个比较有用的全面的理解网络安全体系的机会，有关联的相关概念更能让新手在脑中构建完整的网络安全体系图。

当然，如果是已经有深入研究的读者，阅读此书只是因为想了解其中最新的技术，那大可略过这些内容。

提示

书中适当位置将有“提示”出现，“提示”的作用是编者对特定环境和情况的

说明。

比如是为了演示这个案例而进行的非常规操作，在实际情况中不建议使用这样的操作。

简单来说“提示”就是编者因为行文需要，为了避免误导读者而做的防护措施。

技巧

和“基本概念解释”、“提示”不同，需要特别指出的是，“技巧”一般是以攻击者的角度给出的说明，这些说明一般是针对特定环境的非常有效的攻击手法。

书中可能出现为了全盘需要，模拟攻击者进行攻击的时候，没有使用最好的、最灵巧的、最直接的攻击方式，而是采用了和书中相关概念深度符合的基本手法进行攻击模拟，所以以“技巧”的方式补充说明。

案例相关工具和程序平台

网络安全技术很多时候在明白原理之后，不用自己编写相关工具，网络上已经有很多前人编写了适当的攻击和防御工具，所以“站在巨人的肩上”是最好的快速进步的法门。

书中的相关工具除了在对应的章节出现以外，还在文末有统一的附件形式速查。

另外藏锋者网络也专门为本书提供了相关工具和程序平台的下载支持，读者可以浏览并下载。

编者建议读者在虚拟机中搭建这样的相关环境，然后同样是在虚拟机中使用相关工具进行攻击模拟和防御模拟。

在线交流

为了给各技术层次的读者提供及时在线的交流平台，本书和藏锋者合作提供了一个免费的在线交流平台。

读者可以通过登录藏锋者网站（www.cangfengzhe.com）进行技术交流。

编者邮件

编著过程比较仓促，难免出错，欢迎发现错误的读者与编者联系：cangfengzhe@live.cn。

目　录

概　述

1．什么是堡垒主机

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。

“堡垒主机”这个概念最初由美国 Marcus J.Ranum 在《Thinking About Firewalls V2.0：Beyond Perimeter Security》一书中提出。堡垒主机就是一个以最小化安全定义的网络节点，拥有强悍的网络攻击防御力，理想状态下可以抵御任何网络攻击和入侵。

在实用级的网络中，堡垒主机一般承担着某种单一而且固定的网络服务，比如 Web、FTP、DNS 或者数据库等。在堡垒主机上运行的这些服务拥有基本可以杜绝所有攻击者攻击的防御能力，可以让运行于堡垒主机上的服务丝毫不惧攻击者的攻击——不管这些攻击和入侵技术是古老的，还是新兴的。

非常关键的是，一般情况下堡垒主机都不会借助防火墙等硬件、软件的保护，而是以“裸机”的形态出现在网络中，纯粹依靠防御技术的完整、细致进行网络安全方面的保护。

2．堡垒主机的作用

通常，堡垒主机是一台独立应用的服务器主机，有极大的价值，可能蕴含着用户的敏感信息，经常提供重要的网络服务，这些服务大都极其重要，如银行、证券、政府单位用来实现业务、发布信息的平台等。

在国内的网络安全技术现状下，即使投入大量的金钱，使用种类繁多的硬件防火墙等相关设备来进行防御，依然有被攻破的极大可能，因为滞后的网络防御技术、陈旧的硬件级防御设备和呆板单一的防御思维往往对新兴的、变异的网络攻击无从下手，导致大量资金成本的浪费。从这一角度来看，不管是针对大型企业的服务器群，还是中小企业的少量服务器，在防御强度、设备成本等因素的综合考虑下，与其投入大量资金却得不到完善、仔细、全面的保护，还不如从技术角度入手，构建防御力度超强的堡垒主机，节省大量的资金而且以一种动态的、

可更新维护的、及时性高的防御策略来进行网络安全的防御。

堡垒主机通常用作 Web 服务器、域名系统(DNS)服务器、文件传输协议(FTP)服务器、简单邮件传输协议（SMTP）服务器和网络新闻传输协议（NNTP）服务器等。理想情况下，堡垒主机应该只执行这些服务中的某一个功能，因为它扮演的角色越多，出现安全漏洞的可能性就越大。

安全堡垒主机的配置与通常的主机相比明显不同，所有不必要的服务、协议、程序和网络接口都将被禁用或删除，以达到“最小化安全”，而且每台堡垒主机通常被配置成只承担一个特定角色，使用此方式强化堡垒主机，会极大地限制可能出现的网络攻击。

国外最受欢迎的网络服务商都在提供各种堡垒主机的服务，甚至一些小型的“虚拟主机”服务商也在积极地提供堡垒主机服务，让用户以极低的价格就可以享受到极好地网络安全保护。

3. 本书的主要目的

在网络时代中，技术才是第一生产力，而承载技术的人员无疑才应该是网络整体进步的保障。作为有志于成为某一方面专家的技术人才，掌握一种足可以媲美甚至超越昂贵的硬件级防御技术是必要也是必须的——这是本书的主要目的。

单纯就技术角度而言，不管是常规的 Linux、UNIX 或者 Windows 操作系统，均可以以完善细致的安全设置，实现最小化安全，并且成为网络中强悍的堡垒主机。这无疑极大地提高了堡垒主机相关技术的适用范围，大大地提高了实用性。

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，完整地进行堡垒主机的搭建，力求让读者深刻明白安全设置的目的、作用。

4. 本书特点：实用、易用、严谨、完善

本书主要内容涉及机房物理保护、系统最小化、网络最小化等方面的防护内容，同时根据实际工作经验，对系统的性能优化、安全策略实施等进行了一些有别于传统意义的更新和改动，完全从一个实用的角度进行相关的安全技术实现。

考虑到服务器操作系统的选择，本书以典型而广泛的 Windows 2003 Server 为例，通读本书，读者可以明白在 Windows 2003 Server 中，通过谨慎、合理、完全的配置，完全可以获得足够的安全性，达到“堡垒主机”的安全高度。

另外，因为堡垒主机的安全设置的复杂性，同时网络服务存在多样性，本书

充分考虑的是扎实构建“最小化”系统，并没有涉及具体的服务构建，后续书籍中会有详细的各种服务级堡垒主机的具体搭建内容，但是基本的最小化系统均以本书为基础。

同时，充分考虑到网络上各种各样攻击的存在，为了使各项措施更有针对性，本书每个技术实施细节均有相关的攻击方法概述或者案例简单模拟，力求“知其然且知其所以然”。

在本书最后，为了方便读者在实际工作过程中遇到某一问题的时候可以快速查阅，特意将本书中的各种防御措施整理成了简表，方便读者快速地查阅和检索知识。

第 1 章　强化机房物理安全保护

章节内容提点与概述

本章主要内容：

- ■ 人员接触控制
- ■ 自然灾害防御
- ■ 物理事件防御

本章典型案例：

- □ 出入登记与身份审核
- □ 视频监控
- □ 防盗窃和防破坏
- □ 电话维护与身份审核
- □ 防雷击
- □ 防火
- □ 防水和防潮
- □ 电磁与静电防御
- □ 电力供应

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。

1.1.1 出入登记与身份审核

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。