<<黑客远程控制服务攻击技术与安>>

图书基本信息

书名：<<黑客远程控制服务攻击技术与安全搭建实战>>

13位ISBN编号：9787030262714

10位ISBN编号：7030262719

出版时间：2010-1

出版时间：科学出版社

作者：郝永清

页数：351

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！

<<黑客远程控制服务攻击技术与安>>

内容概要

黑客对互联网上的服务器攻击，不管是基于WEB、FTP还是其他方式，其核心目的，都是通过普通的攻击技术，想要获取服务器的远程控制权限，进而方便、快捷地进行偷窃、攻击、欺骗等行为。
从近几年的网络攻击案例比例来看，针对服务器远程控制服务的攻击正在逐步增加，有愈演愈烈的态势。
同时，因为普通的网络安全管理员或者服务器所有者对新兴的远程控制服务本身的攻击比较陌生，对黑客的远程服务攻击技术不了解，进而造成很大损失。
本书独辟蹊径，以发展的眼光看待黑客攻击，紧扣远程控制服务攻防技术。
书中以Windows系统远程终端服务(3389)、Pcanywhere、VNC这三种国内外使用率最广的远程控制服务系统为例，辅以藏锋者网络安全(WWW．cangfengzhe．com)上的各种案例程序的搭建和模拟，深入分析黑客使用的密码攻击、权限攻击、漏洞攻击等方式，采取极具针对性的防范策略，构建一个安全、实用的远程控制服务器。
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。

<<黑客远程控制服务攻击技术与安>>

书籍目录

丛书序本书使用方法第1章 远程桌面（3389）攻防案例剖析 1.1 远程桌面（3389）组件的安装与使用 1.1.1 远程桌面（3389）组件简介 1.1.2 启用各操作系统上的远程桌面 1.1.3 本地远程桌面连接测试 1.1.4 使用Web页面进行远程桌面连接 1.1.5 远程桌面连接的“.rdp”文件分析 1.2 渗透攻击中的“.rdp”文件破解 1.2.1 网络渗透技术简介 1.2.2 渗透攻击中的“.rdp”文件破解案例模拟 1.3 不同网络环境下的远程桌面暴力破解案例 1.3.1 暴力破解简介 1.3.2 制作密码字典 1.4 远程桌面（3389）密码嗅探实战 1.4.1 嗅探简介 1.4.2 远程桌面（3389）密码嗅探与协议解密第2章 pcAnywhere攻击案例模拟 2.1 pcAnywlaere安装与使用 2.1.1 pcAnywhere简介与工作原理 2.1.2 pcAnywhere管理器介绍 2.2 pcAnywlaere攻防案例模拟 2.2.1 长盛不衰的pcAnywhere密码破解 2.2.2 通杀pcAnywhere各版本的提权攻击案例第3章 最简便的跨系统远程控制：VNC攻防案例 3.1 VNC安装与使用 3.1.1 Windows下VNC的安装与使用 3.1.2 Linux下VNC server安装与使用 3.2 VNC攻防案例模拟 3.2.1 功能强大的VNC攻击工具：vncpwdump 3.2.2 VNC的远程验证绕过漏洞案例 3.2.3 注册表中的VNC本地密码破解第4章 实用级远程控制服务安全策略 4.1 构建方便灵活而又足够安全的远程桌面（3389） 4.1.1 修改远程桌面默认端口提高安全级别 4.1.2 使用专用账户登录远程桌面 4.1.3 取消上次远程登录的用户名记录 4.1.4 使用强壮的密码防止暴力破解 4.1.5 使用防火墙或IPSEC限定访问者 4.2 使用SecunID双重认证打造安全的pcAnywhere 4.2.1 构建pcAnywhere的Serial ID双重认证案例附录1 vncpwdump经典源代码附录2 RealVNC远程认证绕过漏洞利用程序源代码附录3 本书涉及基本概念速查表附录4 案例涉及程序速查表

章节摘录

插图：1.3不同网络环境下的远程桌面暴力破解案例新手网络安全爱好者常常会问：网络中是否存在一种可以攻克所有系统的攻击方法？
针对这一总是出现在眼帘的问题，很多安全专家发起了广泛的讨论，答案是肯定存在这样的攻击方法的。
原因很简单，因为“暴力破解（或者说穷举）”的存在，注定网络攻击是永远没有尽头的。
有目光长远的专家认为暴力破解的方法是可能杜绝的，因为暴力破解是基于现在的计算机认证模式而出现的，也就是说现在的认证模式一般都是通过账户、密码的方式来进行，这样的方式如果从计算机使用的所有领域中排除、推出新的非账户密码认证的安全机制，那就可能杜绝暴力破解的攻击——很不幸的是，就短期来看（这个“短期”是相对计算机技术发展而言），估计在我们的有生之年都无法看到计算机技术的这一种彻底性的革命了。
本节后续的内容中，将和大家一起来探讨暴力破解这一看似简单，实际上却是“无敌”的攻击方法在远程桌面攻击中的运用。
在当今攻防技术不断的发展中，有一种称得上是“古老”的攻击技术却～直顽强而固执地存在着，而且它非但没有跟不上技术的发展而淘汰，反而是随着技术的发展、硬件设备性能的提升，越来越体现出攻击的强悍和防护的无奈——这就是暴力破解，也叫穷举。
1.3.1.1暴力破解（穷举）基本概念暴力破解在计算机领域叫Exhaustive Attack method，即穷举攻击方法。
简单来说就是将密码进行逐个推算、尝试直到找出真正的密码为止。
暴力破解是一种针对于账户密码认证方式的破解、攻击方法，这种方法很像数学上的“完全归纳法”，因为目前计算机技术还处于账户密码认证方式的广泛应用期，所以这种攻击方法在密码破译方面得到了非常广泛的应用。
暴力破解用时间上的牺牲换来了全面性的保证，尤其是随着计算机运算速度的飞速发展，穷举法的形象已经不再是最低等和原始的无奈之举，一跃成为真正意义上的“万能”攻击。

编辑推荐

《黑客远程控制服务攻击技术与安全搭建实战》：·不为人知的3389攻防技术揭秘·pcAnyvvhere各版本缺陷分析·国外最新VNC攻击技术与工具展现·打造实用级安全远程控制服务

版权说明