

<<网络渗透技术攻防高手修炼>>

图书基本信息

书名：<<网络渗透技术攻防高手修炼>>

13位ISBN编号：9787121125737

10位ISBN编号：7121125730

出版时间：2011-1

出版时间：电子工业出版社

作者：武新华 等编著

页数：438

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>

<<网络渗透技术攻防高手修炼>>

内容概要

本书由浅入深、图文并茂地再现了网站入侵与脚本技术快速防杀的全过程，内容涵盖：创建安全测试环境、踩点侦察与漏洞扫描、渗透入侵数据库的web脚本攻击、木马欺骗、渗透入侵的“通道”、缓冲区溢出实现渗透入侵与提权、溢出后开辟控制通道、cookies欺骗与防御技术、xss跨站脚本攻击技术、横向提权的暗道渗透、渗透入侵中的嗅探与欺骗技术、拒绝服务攻击技术、网络渗透技术的系统防护、网络渗透技术的终极防范等应用技巧，并通过一些综合应用案例，向读者讲解了黑客网络渗透技术攻防工具多种应用的全面技术。

本书内容丰富全面，图文并茂，深入浅出，面向广大网络爱好者，同时可作为一本速查手册，也适用于网络安全从业人员及网络管理者。

<<网络渗透技术攻防高手修炼>>

书籍目录

第1章 初识网络渗透测试	1.1 网络渗透概述	1.1.1 什么是网络渗透攻击	1.1.2
学习网络渗透测试的意义	1.2 渗透测试需要掌握的知识	1.2.1 进程、端口、服务	
1.2.2 文件和文件系统概述	1.2.3 dos系统常用的命令	1.3 形影不离的“渗透测试”与攻击	
1.3.1 网络渗透测试与攻击的分类	1.3.2 渗透测试过程与攻击的手段	1.4 专家点拨(常见问题与解答)	
1.3.1 网络渗透测试与攻击的分类	第2章 创建安全测试环境	2.1 安全测试环境概述	
2.1.1 为什么需要安全测试环境	2.1.2 虚拟机软件与虚拟系统	2.2 创建安全测试环境	
2.2.1 虚拟机软件:vmware的安装	2.2.2 配置虚拟机	2.2.3 在虚拟机中安装操作系统	
2.2.4 vmware tool的安装	2.2.5 在虚拟机上架设iis服务器	2.2.6 在虚拟机中安装网站	
2.3 入侵测试前的自我保护	2.3.1 设置代理服务器	2.3.2 使用代理服务器	
2.3.3 使用代理跳板	2.4 专家点拨(常见问题与解答)	第3章 踩点侦察与漏洞扫描	
3.1 踩点与侦察范围	3.1.1 确定侦察范围	3.1.2 实施踩点的具体流程	
3.1.3 如何堵塞漏洞	3.2 确定扫描范围	3.2.1 确定目标主机ip地址	
3.2.2 确定可能开放的端口服务	3.2.3 常见的端口扫描工具	3.2.4 有效预防端口扫描	
3.3 扫描操作系统信息和弱口令	3.3.1 获取netbios信息	3.3.2 获取snmp信息	
3.3.3 制作黑客字典工具	3.3.4 弱口令扫描工具	3.4 扫描注入点	
3.4.1 注入点扫描实例	3.4.2 注入点扫描防御	3.4.1 注入点扫描实例	
3.4.2 注入点扫描防御	3.5 专家点拨(常见问题与解答)	第4章 渗透入侵数据库的web脚本攻击	
4.1 实现sql注入攻击	4.1.1 sql注入攻击基础	4.1.2 my sql注入攻击	
4.1.3 sql server数据库注入攻击	4.1.4 口令破解/暴力破解攻击	4.1.5 常见的注入工具	
4.2 web脚本注入攻击	4.2.1 保护sql server的安全	4.2.2 防止sql数据库攻击	
4.2.3 防止sql注入攻击	4.3 文件上传为渗透铺路	4.3.1 上传功能导致的漏洞	
4.3.2 利用google发起rtf攻击	4.3.3 本地提交上传流程分析	4.3.4 wscokexpert与上传漏洞攻击	
4.3.5 文件上传漏洞攻击实例	4.4 专家点拨(常见问题与解答)	第5章 木马欺骗,渗透入侵的“通道”	
5.1 webshell后门与提权	5.1.1 让asp木马躲过杀毒软件的查杀	5.1.2 暗藏webshell后门	
5.1.3 全面提升asp木马权限	5.1.4 利用serv-u全面提升webshell权限	5.2 木马渗透:从分站渗透到主站服务器	
5.2.1 无处不在的网页木马	5.2.2 百度搜索霸与挂马漏洞	5.2.3 网页木马之星,万能溢出所有目标	
5.3 封锁关口,追踪入侵者	5.3.1 封锁关口:揪出隐藏的asp木马后门	5.3.2 木马分析:追踪入侵者	
5.3.4 防患于未然:拦截网页木马	5.4 专家点拨(常见问题与解答)	第6章 缓冲区溢出实现渗透入侵与提权	
6.1 剖析缓冲区溢出攻击	6.1.1 一个缓冲区溢出简单实例	6.1.2 功能强大的万能溢出工具——metasploit	
6.2 身边的缓冲区溢出实例	6.2.1 rpc服务远程溢出漏洞攻击	6.2.2 idq缓冲区溢出攻击	
6.2.3 webdav缓冲区溢出攻击	6.2.4 即插即用功能远程控制缓冲区溢出攻击	6.3 安全防线上的溢出漏洞	
6.3.1 不可信任的http connect代理“请求”	6.3.2 一击即溃的诺顿防火墙	6.4 防止缓冲区溢出	
6.4.1 防范缓冲区溢出的根本方法	6.4.2 普通用户防范缓冲区溢出的方法	6.5 专家点拨(常见问题与解答)	
7.1 清除障碍,打通渗透通道	7.1.1 获取目标主机密码口令	7.1.2 建立隐蔽账号	
7.1.3 清空复制账号登录信息	7.1.4 开启3389通道	7.1.5 后门程序的上传与隐藏	
7.1.6 端口转发渗透内网	7.1.7 清除入侵记录	7.2 灰鸽子内网渗透实战	
7.2.1 生成灰鸽子木马	7.2.2 木马操作远程计算机文件	7.2.3 控制远程计算机鼠标键盘	
7.2.4 木马修改控制系统设置	7.3 专家点拨(常见问题与解答)	第8章 cookies欺骗与防御技术	
8.1 透析cookies	8.1.1 cookies的定义及用途	8.1.2 探秘系统中的cookies	
8.2 cookies欺骗攻击案例	8.2.1 cookies欺骗原理与技术实现步骤	8.2.2 cookies欺骗攻击安全模拟	
8.3 cookies注入	8.3.1 数据库与cookies的关系	8.3.2 cookies注入典型步骤	
8.3.3 手工cookies注入案例与中转工具使用			

<<网络渗透技术攻防高手修炼>>

8.4 cookies欺骗和注入的防范	8.4.1 cookies欺骗与防范的代码实现	8.4.2 cookies注入防范
8.5 专家点拨(常见问题与解答)	第9章 xss跨站脚本攻击技术	9.1 xss产生根源和触发条件
9.2 跨站漏洞的利用	9.3 xss攻击案例模拟	9.3.1 盗用用户权限攻击案例模拟
9.3.2 xss挂马攻击案例模拟	9.3.3 xss提权攻击案例模拟	9.3.4 xss钓鱼攻击分析
9.4 跨站脚本攻击的防范	9.5 专家点拨(常见问题与解答)	第10章 横向提权的暗道渗透
10.1 snmp信息安全技术	10.1.1 snmp威胁windows网络安全	10.1.2 绕过防火墙刺探系统信息
10.1.3 snmp服务防范	10.2 远程终端入侵的常见手法	10.2.1 开启远程终端
10.2.2 远程终端入侵的常见手法	10.2.3 溢出窗口下的终端开启	10.2.4 远程桌面入侵的技巧
10.2.5 远程终端安全防范	10.3 弱口令打开暗藏的入侵通道	10.3.1 等同于虚设的密码
10.3.2 ftp弱口令漏洞	10.3.3 radmin与4489“肉鸡”	10.4 专家点拨(常见问题与解答)
第11章 渗透入侵中的嗅探与欺骗技术	11.1 功能强大的嗅探器sniffer	11.1.1 嗅探器鼻祖tcpdump
11.1.2 用于捕获数据的snifferpro嗅探器	11.1.3 可实现多种操作的spynetsniffer嗅探器	11.1.4 网络嗅探器:影音神探
11.1.5 局域网嗅探工具:iris嗅探器	11.2 arp欺骗嗅探的渗透	11.2.1 arp嗅探欺骗概述
11.2.2 交换型网络嗅探器winarpspoof	11.2.3 内网dns欺骗工具cain	11.3 arp欺骗嗅探的防御
11.3.1 瑞星arp防火墙	11.3.2 金山arp防火墙	11.3.3 arp防火墙
11.3.4 绿盾arp防火墙	11.3.5 arp卫士	11.4 dns欺骗攻击
11.4.1 dns欺骗原理	11.4.2 dns欺骗的实现过程	11.4.3 dns攻击的防御
11.5 专家点拨(常见问题与解答)	第12章 拒绝服务攻击技术	12.1 利用漏洞进行d.o.s攻击
12.1.1 ping of death攻击	12.1.2 d.o.s攻击的其他实现方式以及防御	12.2 披上伪装进行syn flood攻击
12.2.1 syn flood攻击的原理	12.2.2 使用工具进行syn flood攻击	12.2.3 syn flood攻击防御
12.3 分布式拒绝服务d.d.o.s攻击	12.3.1 分布式拒绝服务入侵简介	12.3.2 著名的d.d.o.s入侵工具介绍
12.3.3 d.d.o.s攻击的防御	12.4 专家点拨(常见问题与解答)	第13章 网络渗透技术的系统防护
13.1 寻找攻击目标的扫描器	13.1.1 专业漏洞扫描工具shadow security scanner	13.1.2 扫描器中的佼佼者nmap
13.1.3 自制简单群ping扫描工具	13.1.4 代理扫描工具x-way	13.2 系统管理工具
13.2.1 进程查看器:procxp	13.2.2 网络监测工具:capsa professional	13.2.3 注册表监视工具:regmon
13.2.4 端口查看器:active ports	13.2.5 木马检测工具:icesword	13.3 网络渗透中的入侵检测防护
13.3.1 基于网络的入侵检测	13.3.2 基于主机的入侵检测	13.3.3 实用入侵检测范例
13.4 专家点拨(常见问题与解答)	第14章 网络渗透技术的终极防护	14.1 不可忽视的安全细节问题
14.1.1 端口及服务	14.1.2 ipsec与端口认证	14.1.3 严格控制关键系统文件
14.2 秒杀危害溢出攻击	14.2.1 扫描漏洞隐患	14.2.2 自动为系统打补丁
14.2.3 强制安装补丁	14.3 专家点拨(常见问题与解答)	参考文献

<<网络渗透技术攻防高手修炼>>

章节摘录

版权页：插图：渗透测试是受信任的第三方进行的一种评估网络安全的活动，它通过运用各种黑客攻击方法与工具，对企业网络进行各种手段的攻击，以便找出系统存在的漏洞，给出网络系统存在的安全风险，是一种攻击模拟行为。

网络渗透攻击与普通网络攻击的不同在于：普通的网络攻击只是单一类型的攻击；网络渗透攻击则与此不同，它是一种系统渐进型的综合攻击方式，其攻击目标是明确的，攻击目的往往不那么单一，危害性也非常严重。

例如，在普通的网络攻击事件中，攻击者可能仅仅是利用目标网络的Web服务器漏洞，入侵网站更改网页或在网页上挂马。

也就是说，这种攻击是随机的，而其目的也是单一而简单的。

在渗透入侵攻击过程中，攻击者会有针对性地对某个目标网络进行攻击，以获取其内部的商业资料，进行网络破坏等。

其实施攻击的步骤是非常系统的，假设其获取了目标网络中网站服务器的权限，则不会仅满足于控制此台服务器，而是会利用此台服务器继续入侵目标网络，获取整个网络中所有主机的权限。

另外，为了实现渗透攻击，攻击者往往综合运用远程溢出、木马攻击、密码破解、嗅探、ARP欺骗等多种攻击方式，逐步控制网络。

总之，网络渗透攻击与普通网络攻击相比，网络渗透攻击具有攻击目的明确性、攻击步骤逐步与渐进性、攻击手段的多样性和综合性等特点。

目前，网络渗透测试已经成为安全工作者中的一个课题，其发展前景不可估量。

作为一名网络管理员或安全工作者，如果有能力实施基本渗透测试的话，那么其价值将是极大的，一切日常安全维护操作将更加有针对性，也更加有效。

<<网络渗透技术攻防高手修炼>>

编辑推荐

《反黑风暴·网络渗透技术攻防高手修炼》：超大容量超值享受，理论+实战图文+视频=让读者不会也会，任务驱动式讲解，揭秘多种黑客攻击手法，攻防互参，全面确保用户网络安全，挑战自我。享受黑客攻防的乐趣。

<<网络渗透技术攻防高手修炼>>

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>