第一图书网, tushu007.com

<<暗战亮剑>>

图书基本信息

书名：<<暗战亮剑>>

13位ISBN编号：9787115228284

10位ISBN编号：7115228280

出版时间：2010-7

出版时间：人民邮电出版社

作者：张晓

页数：316

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

前言

多年以前，我开始学习网络攻防技术的时候是没有师傅带的，知识全部来自于图书、杂志、网络，再加上自己的试验和摸索，终于略有所得。
因为不想让其他人再走我走过的弯路，所以就有了把自己的经验写成书的想法。
本书力图从实用的角度剖析网络入侵与反入侵技术的方方面面，从ASP、PHP、ASPX、JSP脚本漏洞攻防，到服务器渗透和浏览器端攻防，详细阐述了相关的安全技术。
另外，还撰写了其他书籍很少涉及的特色内容，如开源程序的后门攻防剖析以及社会工程学和手机攻防知识。
本书主要内容如下。
第一篇攻防基础知识，包括第l章和第2章。
第1章讲解了网络硬件、TCP和UDP、端口、进程、系统服务等网络安全入门知识。
第2章介绍了QQ安全、QQ密码攻防、利用hash登录保护QQ密码、QQ尾巴生成器、QQ强制聊天、QQ炸弹剖析、QQ聊天记录防护、MSN安全、MSN密码的防护、MSN保护盾、查看和嗅探MSN聊天记录剖析、键盘记录与防护、Windows密码安全、Word文档加解密防护、查看Access数据库密码攻防等内容。
第二篇脚本攻防，包括第3章～第5章。
第3章讲解了ASP脚本漏洞及防御知识，其中包括SQL注入的成因、ASP注入的防御、关于权限的问题、自动化注入工具安全检测等，第4章是PHP脚本漏洞及防御，主要讲解PHP的SQL注入基础、PHP注入的判断、PHP脚本漏洞的形成及防御、如何避免PHP注入、远程文件包含漏洞及防御等。
第5章介绍了ASPX与JSP脚本漏洞及防御，主要包括ASPX脚本漏洞及防御、著名ASPX木马WebAdmin、JSP脚本漏洞及防御、JSP脚本的注入测试等。
第三篇入侵剖析与反入侵技术，包括第6章和第7章。
在第6章服务器渗透安全测试及防御知识中主要讲解信息收集、扫描器、DNS反向查询、网站常见弱点、挖掘“鸡”、SQLServer提权及防御、Linux提权及防御、内网渗透及防御、WebShell的查杀等。
在第7章浏览器端攻击及防御中，主要讲解挂马及防御、跨站脚本及防御、几种常见的XSS类型、网络钓鱼及防御、内网ARP欺骗挂马剖析及防御。
第四篇后门和远程控制，包括第8章和第9章。
第8章讲解了蠕虫和后门及其免杀的危害，并给出相应的防范技术，剖析了穿墙下载者、粘滞键后门、HackerDefender的编译及其免杀防范等。
在第9章远程控制软件及其免杀攻防中，讲解了运行控制软件、加壳与脱壳、加花以及基于：B／S模式的远程控制软件的攻防内容。

内容概要

《暗战亮剑：黑客攻防入门与进阶全程实录》系统性地从网络入侵与反入侵技术的基本概念、基本原理讲起，一步步地介绍了网络安全的有关知识。
但《暗战亮剑：黑客攻防入门与进阶全程实录》不是一本简单的入门图书，各个相应部分都有提高的内容，涉及目前较新、较实用的网络安全技术。
《暗战亮剑：黑客攻防入门与进阶全程实录》内容分为5篇共11章，另外，还有供读者参考使用的附录。
第一篇攻防基础知识，包括第1章和第2章，讲解了网络安全入门知识以及攻防技术，包括进程、QQ安全、QQ密码防护、QQ聊天记录防护、MSN密码防护、Windows密码安全等内容。
第二篇脚本攻防，主要包括第3章～第5章，讲解了脚本漏洞及防御，如PHP脚本漏洞、ASPX和JSP脚本漏洞及防御等内容。
第三篇入侵剖析与反入侵技术，包括第6章和第7章，主要阐述了服务器渗透攻防，如信息收集、扫描器、浏览器端攻防技术等。
第四篇后门和远程控制，包括第8章和第9章，主要剖析了蠕虫和后门及其免杀的危害性，并给出防范方法，以及远程控制软件安全防范技术。
第五篇高级实战技术，包括第10章和第11章，通过7个完整的综合案例，如Discuz！
论坛安全分析、PHP程序漏洞防范和内网渗透剖析等，全面讲解了黑客的防御知识。
附录部分则包括常用的命令和字符编码的转换知识。
《暗战亮剑：黑客攻防入门与进阶全程实录》配套光盘中附赠教学视频，以便读者易学、易用。
《暗战亮剑：黑客攻防入门与进阶全程实录》适合作为网络安全爱好者、渗透测试人员、网络安全专业技术人员参考用书。

作者简介

张晓，特立独行的85后网络高手，网名人鱼姬。
高中时代在数学、物理方面展现出特长，两度获得国家级竞赛二等奖；进入大学后开始涉足网络安全领域，读研期间为专业杂志撰写黑客安全技术文章数十篇。
目前正在攻读博士学位，在黑客安全技术方面具有深入的研究。

书籍目录

第一篇　攻防基础知识第1章　网络安全入门1.1　网络的定义1.2　网络分类1.3　OSI模型和TCP/IP模型1.4　IP地址1.5　网络硬件1.6　TCP和UDP1.7　端口1.8　进程1.9　系统服务第2章　初级攻防2.1　QQ安全2.1.1　QQ密码的安全攻防2.1.2　QQ医生2.1.3　利用hash值登录保护QQ密码2.1.4　QQ尾巴生成器2.1.5　QQ强制聊天2.1.6　QQ炸弹攻防剖析2.1.7　IP地址的泄露与保护2.1.8　查看QQ聊天记录与防护2.2　MSN安全2.2.1　MSN密码的安全攻防2.2.2　MSN保护盾2.2.3　本地保存的MSN密码防护2.2.4　查看、嗅探MSN聊天记录2.2.5　MSN 监视程序的使用2.3　Windows系统安全攻防2.3.1　键盘记录与防护2.3.2　拒绝服务剖析及防御2.3.3　无需密码进入本地主机安全攻防2.3.4　邮箱炸弹与查看发件人IP安全攻防2.3.5　局域网IP冲突攻击器2.3.6　远程桌面的使用2.3.7　系统注册表监视程序2.3.8　查看端口情况2.3.9　利用组策略提高系统安全性2.3.10　打补丁保证系统安全2.3.11　代理的使用2.3.12　清除上网痕迹2.4　Windows密码安全2.4.1　管理员登录密码防护2.4.2　查看星号密码2.4.3　查看IE浏览器保存的密码2.4.4　查看本地拨号密码2.4.5　查看本地保存的邮箱密码2.4.6　查看保存的远程桌面密码2.4.7　查看注册表中保存的表单内容2.4.8　查看本地VNC密码2.4.9　查看Firefox浏览器保存的密码2.4.10　简单嗅探密码2.4.11　Word文档加解密防护2.4.12　查看Access数据库密码第二篇　脚本攻防第3章　ASP脚本漏洞及防御3.1　SQL注入基础3.1.1　SQL注入的成因3.1.2　绕过密码验证3.1.3　判断是否存在注入3.1.4　区分系统中Access和SQL Server数据库3.2　针对Access数据库的漏洞利用防范3.2.1“ %5C ”暴库剖析3.2.2　下载默认数据库3.2.3　手动注入剖析3.3　针对SQL Server数据库的漏洞利用攻防剖析3.3.1　SQL Server的存储扩展3.3.2　备份获得一句话木马3.4　ASP注入的防御及绕过3.5　ASP木马的使用及免杀3.5.1　一句话木马剖析3.5.2　海阳顶端网ASP木马剖析3.5.3　关于权限的问题3.5.4　SQL Rootkit攻防3.5.5　Windows 2003上以“ .asp ”结尾的文件夹安全问题3.5.6　ASP木马的免杀剖析3.6　自动化注入工具剖析第4章　PHP脚本漏洞及防御4.1　PHP程序的SQL注入基础4.1.1　PHP程序文件变量注入攻防4.1.2　验证的绕过4.1.3　PHP注入的判断4.2　PHP脚本漏洞的利用及防御4.2.1　表内查询4.2.2　跨表查询4.2.3　PHP暴路径剖析4.2.4　利用注入点读文件剖析4.2.5　导出文件4.2.6　利用注入点导出一句话木马4.2.7　PHPMyAdmin一句话木马剖析4.2.8　如何避免PHP注入4.2.9　远程文件包含漏洞及防御4.2.10　本地文件包含漏洞及防御4.2.11　Apache错误造成的漏洞剖析4.2.12　多字节编码漏洞剖析4.3　PHPShell的使用及免杀剖析4.3.1　微型PHP后门剖析4.3.2　新型PHP一句话木马剖析4.3.3　在线管理程序PhpSpy4.3.4　PHPShell的免杀剖析4.4　自动化工具的使用第5章　ASPX与JSP脚本漏洞及防御5.1　ASPX脚本漏洞及防御5.1.1　暴路径剖析5.1.2　注入剖析5.1.3　SQL Server存储扩展5.1.4　数据库备份一句话木马剖析5.2　ASPX木马及免杀剖析5.2.1　ASPX一句话木马剖析5.2.2　著名ASPX木马WebAdmin攻防5.2.3　ASPX木马的免杀剖析5.3　JSP脚本漏洞及防御5.3.1　暴JSP脚本源码剖析5.3.2　JSP脚本的注入剖析5.3.3　有趣的UTL_HTTP.request函数5.4　JSP木马及其免杀剖析5.4.1　JSP一句话木马剖析5.4.2　JSP木马Jfolder剖析5.4.3　JFolder的免杀剖析第三篇　入侵剖析与反入侵技术第6章　服务器渗透及防御6.1　信息收集6.1.1　判断操作系统6.1.2　扫描器6.1.3　DNS反向查询6.1.4　整站程序源码的判断6.2　网站常见弱点6.2.1　注入点剖析6.2.2　Web扫描器WScan的使用6.2.3　Google Hack应用6.2.4　挖掘“ 鸡 ”6.2.5　Cookie欺骗攻防6.2.6　后台获取WebShell6.3　网络硬件入侵及防御6.4　Windows提权及防御6.4.1　FIP服务器软件Serv-U提权及防御6.4.2　远程控制软件pcAnywhere提权及防御6.4.3　远程控制软件Radmin提权及防御6.4.4　SQL Server提权及防御6.4.5　MySQL提权及防御6.4.6　跨平台远程控制软件VNC提权及防御6.4.7　本地溢出及防御6.4.8　替换系统服务6.4.9　破解工具SAMInside应用6.4.10　FTP客户端密码文件的解密6.4.11　C:\WINDOWS\system32\LogFiles\MSFTPSVC1\的安全问题6.4.12　远程桌面的开启6.5　Linux提权及防御6.6　内网渗透及防御6.6.1　常用的嗅探工具应用6.6.2　ARP欺骗篡改网页及防御6.6.3　利用Cain进行ARP Sniff及防御6.6.4　DNS欺骗剖析6.6.5　远程溢出及防御6.6.6　端口映射6.7　清理日志及制作跳板6.7.1　清理日志6.7.2　制作跳板6.8　WebShell的查杀6.9　Windows注册表取证6.10　小结第7章　浏览器端攻击及防御7.1　挂马及防御7.1.1　挂马代码剖析7.1.2　两种常见的网页加密7.2　跨站脚本及防御7.2.1　什么是跨站7.2.2　跨站脚本剖析7.2.3　几种常见的跨站脚本攻击(XSS)类型7.2.4　跨站利用剖析7.2.5　跨站的过滤和绕过剖析7.2.6　另类分隔关键词7.2.7　跨站脚本攻击工具XSS Shell剖析7.3　网

络钓鱼及防御7.3.1　虚假网站7.3.2　电子邮件钓鱼攻防7.4　会话复制7.5　内网ARP欺骗挂马及防御7.6　社会工程学7.6.1　社会工程学应用实例7.6.2　操控术第四篇　后门和远程控制第8章　蠕虫和后门及免杀8.1　穿墙下载者剖析　08.2　粘滞键后门剖析8.3　熊猫烧香核心程序剖析8.4　Hacker Defender的编译及免杀剖析8.4.1　概念澄清8.4.2　编译Hacker Defender并免杀剖析8.4.3　Hacker Defender的使用第9章　远程控制软件及免杀9.1　远程控制软件gh0st的编译及免杀剖析9.1.1　编译RESSDT.sys和免杀剖析9.1.2　编译svchost.dll和免杀剖析9.1.3　编译install.exe和免杀剖析9.1.4　对付启发式杀毒剖析9.1.5　编译客户端gh0st9.1.6　map文件的使用9.1.7　gh0st的上线方式9.1.8　gh0st使用方法9.2　特征码定位器MyCCL的使用9.3　加壳与脱壳9.4　加花剖析9.5　手动杀毒9.6　基于B/S模式的远程控制软件第五篇　高级实战技术第10章　实战攻防案例分析10.1　案例一10.1.1　Discuz!论坛安全分析10.1.2　案例防御分析10.2　案例二10.2.1　PHP远程文件漏洞防范10.2.2　案例防御分析10.3　案例三10.3.1　oblog4.6漏洞的攻防10.3.2　案例防御分析10.4　案例四10.4.1　内网渗透剖析10.4.2　案例防御分析10.5　案例五10.5.1　Discuz! NT 2.5社区软件注入剖析10.5.2　案例防御分析10.6　案例六10.6.1　My SQL的load_file()函数列目录安全分析10.6.2　案例防御分析10.7　案例七10.7.1　Oracle的搜索型注入攻防10.7.2　案例防御分析第11章　手机攻防11.1　手机间谍11.2　蓝牙安全11.2.1　蓝牙渗透工具Super Bluetooth Hack11.2.2　手机漏洞检查工具Blooover II11.2.3　蓝牙拒绝服务软件Bluetooth Terror11.3　编程获取通话记录剖析11.4　基于手机的窃听器剖析11.5　手机杀毒与手机防火墙应用附录A　破解MD5附录B　字符编码的转换附录C　命令行知识

章节摘录

所谓操控术，就是按自己的意愿引导别人行事的技术，使用这些技术无需个人魅力和地位优势，也无需成为能言善辩的高手。
在地位平等的二者之间（同学、同事、陌生人等），一方不能命令另一方必须去做什么，这时可以运用操控术来达到某些目的。
下面简述3种操控术的方法和实例。
（1）诱发。
诱发就是先隐瞒部分真相，然后在恰当的时机和盘托出，让人不好拒绝。
以下是两个例子。
比如老师请你帮他做个测试，但是他并没有说具体的时间和地点，你出于热心就张口答应了。
当晚老师就给你打电话说，你需要早起并到一个很远的地方做这个测试，问你答应不答应，此时老师并没有强迫你，但你是不是觉得不好意思拒绝了呢？
当然，你也可以怀着内疚的心情拒绝老师，但是老师的办法无疑增加了你同意的概率。
如果他一开始就要求你早起并到一个很远的地方去做测试，你还会答应吗？
再比如父母要你去离家不远的超市买些东西回来，你觉得很快就能回来，所以就答应了。
但当你骑上自行车的那一刻，父母突然要你顺便去离家5公里的地方取个东西回来，你是不是也觉得难以拒绝呢？
假如一开始就要你去5公里外的地方，你大概会不情愿吧。
（2）潜移默化。
所谓潜移默化，就是前后两次使用同类型的请求（前一次简单，后一次复杂，而且后一次是真实目的），不必是同一人实施的，第二个请求要让对方想起第一个请求，两个请求之间可以相隔几天。
看到这里，或许大部分人还不能完全理解，下面举个例子。
假如你在家接到了这样的一个电话，某调查组要你回答几个关于家庭布置的问题，这是个很简单的请求，在你回答之后你就将此事忘了。
但是过几天，又有电话打来，还是上次的调查组，他们想到你家来参观一下，你可能就会比较容易答应。
如果没有上面的第一个请求，而是直接要求来你家参观，你就会觉得难以接受。
实际上，这是一个心理学家做过的试验，与省略第一次请求的22%的成功率相比，使用两次请求将主人允许调查组进入他家参观的成功率提高到了50%。

编辑推荐

QQ密码安全防护、MSN密码防护、Windows安全等　　蠕虫、后门和木马的防御策略　　全程展现从服务器渗透攻防到浏览器攻防的真实内幕　　7个精彩实战攻防案例分析　　100个黑客安全工具使用介绍　　200个黑客攻防技巧　　500分钟语音视频教程　　国内著名网络安全媒体《黑客防线》鼎力推荐

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