第一图书网, tushu007.com

# <<矛与盾>>

## 图书基本信息

书名：<<矛与盾>>

13位ISBN编号：9787111285748

10位ISBN编号：7111285743

出版时间：2010-1

出版时间：武新华、陈艳艳、王英英、 等 机械工业出版社 (2010-01出版)

作者：武新华 等 著

页数：346

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

第一图书网, tushu007.com



## 前言

本书本着防患于未然的主旨，着重而详细地介绍了各种黑客入侵网页的手段，概括绝大部分的攻击方式。
本书虽然详细解说了每个攻击手法的原理与实际操作，但毕竟如何防范这些入侵才是本书的重点。
想要开发安全的PHP应用程序，就赶快拿起这本书仔细地阅读吧！
只有使读者在了解黑客攻击知识的基础上，能够最大限度地做到“知己知彼”，才有可能在遭受黑客攻击时尽量减少自己的损失。
下面简要介绍本书的特点、学习方法以及提供的服务。
本书内容本书以配图、图释、标注、指引线框等丰富的图解手段，再辅以浅显易懂的语言，介绍了黑客攻击计算机的一般方法、步骤，以及所使用的工具。
本书内容主要包括：黑客入门知识基础、黑客的攻击方式、Windows系统编程与网站脚本、后门程序编程基础、高级系统后门编程技术、黑客程序的配置和数据包嗅探、编程攻击与防御实例、SQL注入攻击与防范技术、数据库入侵与防范技术、Cookies攻击与防范技术、网络上传漏洞的攻击与防范、恶意脚本入侵与防御、数据备份升级与恢复等内容。
本书详细地讲述了防护黑客攻击的方法及黑客的攻击与防范技术，使读者在实际应用中碰到黑客攻击时，能够做到“胸有成竹”。
读者运用本书介绍的黑客攻击防守方法去了解黑客，进而防范黑客的攻击，使自己的网络更加安全。
本书几个具体网站例子，已经将具体信息提交给网站进行了修改。
增值服务本书附赠的光盘提供了多种攻防实战的教学视频，汇集了众多高手的操作精华，通过增加读者对主流操作手法感性认识的方式，使读者实现高效学习。
此外，如发现本书中有需要改进之处，还可通过访问http：／／www.newtop01.tom或QQ：274648972与编者进行沟通，编者将衷心感谢提供建议的读者，并真心希望在和广大读者互动的过程中能得到提高。

第一图书网, tushu007.com

# <<矛与盾>>

## 内容概要

《矛与盾：黑客攻防与脚本编程》对每一个入侵步骤作详细的分析，以推断入侵者在每一个入侵步骤的目的以及所要完成的任务，并对入侵过程中常见问题作必要的说明与解答。
全书共分为13章，主要包括黑客入门知识基础、黑客的攻击方式、windows系统编程与网站脚本、后门程序编程基础、高级系统后门编程技术、黑客程序的配置和数据包嗅探、编程攻击与防御实例、SQL注入攻击与防范技术、数据库入侵与防范技术、Cookies攻击与防范技术、网络上传漏洞的攻击与防范、恶意脚本入侵与防御、数据备份升级与恢复等内容。
《矛与盾：黑客攻防与脚本编程》内容丰富全面，图文并茂，深入浅出，面向广大网络爱好者，也适用于网络安全从业人员及网络管理者，同时可作为一本速查手册。

第一图书网, tushu007.com

# <<矛与盾>>

## 书籍目录

前言第1章 黑客攻防知识1.1 黑客基础知识1.1.1 进程、端口和服务1.1.2 文件和文件系统概述1.1.3 DOS系统常用的命令1.1.4 Windows注册表1.2 常见的网络协议1.2.1 TCP／IP1.2.2 IP1.2.3 ARP1.2.4 ICMP1.3 创建安全测试环境1.3.1 安全测试环境概述1.3.2 虚拟机软件概述1.3.3 用VMware创建虚拟环境1.3.4 安装虚拟工具1.3.5 在虚拟机上假设I／S服务器1.3.6 在虚拟机中安装网站1.4 必要的黑客攻防知识1.4.1 常见的黑客攻击流程1.4.2 常用的网络防御技术1.5 专家点拨1.6 总结与经验积累第2章 剖析黑客的攻击方式2.1 网络欺骗攻击2.1.1 攻击原理2.1.2 攻击与防御实战2.2 口令猜解攻击2.2.1 攻击原理2.2.2 攻击与防御实战2.3 缓冲区溢出攻击2.3.1 攻击原理2.3.2 攻击与防御实战2.4 专家点拨2.5 总结与经验积累第3章 Windows系统编程与网站脚本3.1 黑客编程简介3.1.1 黑客编程语言介绍3.1.2 黑客与编程3.2 Windows系统编程概述3.2.1 网络通信编程简介3.2.2 文件操作编程简介3.2.3 注册表编程简介3.2.4 进程和线程编程简介3.3 网站脚本入侵与防范3.3.1 Web脚本攻击概述3.3.2 脚本漏洞的根源与防范3.4.专家点拨3.5 总结与经验积累第4章 后门程序编程基础4.1 后门概述4.2 编写简单的cmdshell程序4.2.1 管道通信技术简介4.2.2 JE~连接后门的编程4.2.3 反向连接后门的编程4.3 编写简单的后门程序4.3.1 编程实现远程终端的开启4.3.2 编程实现文件查找功能4.3.3 编程实现重启、关机和注销4.3.4 编程实现http下载文件4.3.5 编程实现cmdshell和各功能的切换4.4 实现自启动功能的编程技术4.4.1 注册表自启动的实现4.4.2 ActiveX自启动的实现4.4.3 系统服务自启动的实现4.4.4 svchost.exe自动加载启动的实现4.5 专家点拨4.6 总结与经验积累第5章 高级系统后门编程技术5.1 远程线程技术5.1.1 初步的远程线程注入技术5.1.2 编写远程线程注入后门5.1.3 远程线程技术的发展5.2 端口复用后门5.2.1 后门思路5.2.2 具体编程实现5.3 专家点拨5.4 总结与经验积累第6章 黑客程序的配置和数据包嗅探6.1 文件生成技术6.1.1 资源法生成文件6.1.2 附加文件法生成文件6.2 黑客程序的配置6.2.1 数据替换法6.2.2 附加信息法6.3 数据包嗅探6.3.1 原始套接字基础6.3.2 利用ICMP原始套接字实现ping程序6.3.3 基于原始套接字的嗅探技术6.3.4 利用Packet32实现ARP攻击6.4 如何防御黑客进行嗅探6.5 专家点拨6.6 总结与经验积累第7章 编程攻击与防御实例7.1 通过程序创建木马攻防实战7.1.1 VB木马编写与防范7.1.2 基于ICMP的VC木马编写7.1.3 基于Delphi的木马编写7.1.4 电子眼——计算机扫描技术的编程7.2 隐藏防复制程序的运行7.3 专家点拨7.4 总结与经验积累第8章 SQL注入攻击与防范技术8.1 SQL注入攻击前的准备8.1.1 攻击前的准备8.1.2 寻找攻击入口8.1.3 判断SQL注人点类型8.1.4 判断目标数据库类型8.2 常见的注入工具8.2.1 NBSI注入工具8.2.2 啊D注入工具8.2.3 Domain注入工具8.2.4.ZBSI注入工具8.3 ‘ 0r ’ = ‘ or ’ 经典漏洞攻击8.3.1 ‘ 0r ’ = ‘ or ’ 攻击突破登录验证8.3.2 未过滤的request.form造成的注入8.4 缺失单引号与空格的引入8.4.1 转换编码，绕过程序过滤8.4.2 /**/，替换空格的注入攻击8.4.3 具体的防范措施8.5 Update注入攻击8.6 SQtL注入攻击的防范8.7 专家点拨8.8 总结与经验积累第9章 数据库入侵与防范技术9.1 常见数据库漏洞简介9.1.1 数据库下载漏洞9.1.2 暴库漏洞9.2 数据库连接的基础知识9.2.1 ASP与ADO模块9.2.2 ADO对象存取数据库9.2.3 数据库连接代码9.3 默认数据库下载漏洞的攻击9.3.1 论坛网站的基本搭建流程9.3.2 数据库下载漏洞的攻击流程9.3.3 下载网站的数据库9.3.4 数据库下载漏洞的防范9.4 利用Google搜索网站漏洞9.4.1 利用Google搜索网站信息9.4.2 Google暴库漏洞的分析与防范9.5 暴库漏洞攻击实例9.5.1 coRn.asp暴库法9.5.2 %5c暴库法9.5.3 防御暴库攻击9.6 专家点拨9.7 总结与经验积累第10章 Cookies攻击与防范技术10.1 Cookies欺骗攻击实例10.1.1 Cookies信息的安全隐患10.1.2 利用IECookiesView获得目标计算机中的Cookies信息10.1.3 利用Cookies欺骗漏洞掌握网站10.2 深入探讨Cookies欺骗漏洞10.2.1 数据库与Cookies的关系10.2.2 Cookies欺骗与上传攻击10.2.3 ClasslD的欺骗人侵10.2.4 用户名的欺骗人侵……第11章 网络上传漏洞的攻击与防范第12章 恶意脚本入侵与防御第13章 数据备份升级与恢复

第一图书网, tushu007.com


## 章节摘录

插图：1.通过网络监听非法得到用户口令这类方法具有一定的局限性，但危害性极大。
监听者往往采用中途截击的方法来获取用户账户和密码。
当前，很多协议根本就没有采用任何加密或身份认证技术，如在Telnet、FTP、HTIP、SMTP等传输协议中，用户账户和密码信息都是以明文格式传输的，此时若攻击者利用数据包截取工具便可很容易收集到账户和密码。
还有一种中途截击攻击方法，它在同服务器端完成“三次握手”建立连接之后，在通信过程中扮演“第三者”的角色，假冒服务器身份进行欺骗，再假冒向服务器发出恶意请求，其造成的后果不堪设想。
另外，攻击者还可以利用软件和硬件工具时刻监视系统主机的工作，等待记录用户登录信息，从而取得用户密码；或编制有缓冲区溢出错误的SUID程序来获得超级用户权限。
2.利用专门的软件破解口令在知道用户的账号后（如电子邮件@前面的部分）利用一些专门软件强行破解用户口令，这种方法不受网段限制，但攻击者要有足够的耐心和时间。
例如，采用字典穷举法（或称暴力法）来破解用户的密码。
攻击者可以通过一些工具，自动地从电脑字典中取出一个单词，作为用户口令再输入给远端的主机，申请进入系统；弱口令错误就是按序取出下一个单词，进行下一个尝试，并一直循环下去，直到找到正确的口令或字典的单词试完为止。
由于这个破译过程由计算机程序来自动完成，因而几个小时就可以把上十万条记录的字典里所有单词都尝试一遍。
3.利用系统管理员的失误在操作系统中，用户的基本信息存放在passwd文件中，而所有的口令则经过DES加密方法加密后，专门存放在一个叫shadow的文件中。
黑客们获取口令文件后，就会使用专门的破解DES加密法的程序来解口令。
同时，由于为数不少的操作系统都存在许多安全漏洞、.Bug或一些其他设计缺陷，这些缺陷一旦被找出，黑客就可以长驱直人。
为了保护自己密码的安全，用户要慎重设置自己的口令。
要想设置好的口令需要做到如下几点：口不要使用／关于自己的信息作为口令，如执照号码、电话号码、身份证号码、工作证号码、生日、所居住的街道名字等。
不使用简单危险口令，推荐使用口令设置为8位以上的大小写字母、数字和其他符号的组合。
设置口令的一个最好选择就是将两个不相关的词用一个数据字或非字母字符相连。
要定期更换口令，因为8位数以上的字母、数字和其他符号的组合也不是绝对无懈可击的，但更换口令前要确保所使用电脑的安全。
不要把口令轻易告诉任何人。
尽可能避免因为对方是网友或现实生活中的朋友，而把密码告诉他。
避免多个资源使用同一个口令，一旦一个口令泄露，所有的资源都受到威胁。
不要让Windows或者IE保存任何形式的口令，因为“*”符号掩盖不了真实的口令，而且在这种情况下，Windows都会将口令储存在某个文件中。
不要随意保存账号和口令，注意把账号和口令存放在相对安全的位置。
把口令写在台历上、记在钱包上等都是危险的做法。
申请密码保护，即设置安全码，安全码不要和口令设置的一样。
如果没有设置安全码，别人一旦破解密码，就可以把密码和注册资料（除证件号码）全部修改。

第一图书网, tushu007.com

# <<矛与盾>>

## 编辑推荐

《矛与盾:黑客攻防与脚本编程》：披露黑客练功全过程识破黑客入侵小伎俩轻松实现从菜鸟到大虾练就黑客终极必杀技36个知识点多媒体视频讲解让你快速从入门到精通。

第一图书网, tushu007.com



## 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