<<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

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。

<<暗战亮剑>>

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。

<<暗战亮剑>>

书籍目录

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%。

<<暗战亮剑>>

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