HZ BOOKS
华章科技

学电脑从入门到精通

THE SECRETS OF BEING AN EXPERT
IN COMPUTER FROM A BEGINNER

黑客攻防
从入门到精通
（攻防与脚本编程篇）

天河文化 编著

- 高效模式：全程图解模式可彻底克服攻防操作的学习障碍
- 内容合理：精选攻防入门最迫切需要的知识点，形成一个实用、完整的知识体系
- 实例为主，易于上手，模拟真实攻防环境，解决各种疑难问题

入门到精通丛书
累计销售
30万册

机械工业出版社
China Machine Press

黑客攻防

从入门到精通

（攻防与脚本编程篇）

天河文化 编著

机械工业出版社
China Machine Press

图书在版编目（CIP）数据

黑客攻防从入门到精通（攻防与脚本编程篇）/ 天河文化编著 . —北京：机械工业出版社，2015.3

ISBN 978-7-111-49193-4

I. 黑… II. 天… III. 计算机网络－安全技术 IV. TP393.08

中国版本图书馆 CIP 数据核字（2015）第 051244 号

黑客攻防从入门到精通（攻防与脚本编程篇）

出版发行：机械工业出版社（北京市西城区百万庄大街 22 号 邮政编码：100037）

责任编辑：李华君 陈佳媛 责任校对：殷 虹

印 刷：北京瑞德印刷有限公司 版 次：2015 年 4 月第 1 版第 1 次印刷

开 本：185mm×260mm 1/16 印 张：27

书 号：ISBN 978-7-111-49193-4 定 价：69.00 元

凡购本书，如有缺页、倒页、脱页，由本社发行部调换

客服热线：（010）88378991 88361066 投稿热线：（010）88379604

购书热线：（010）68326294 88379649 68995259 读者信箱：hzjsj@hzbook.com

前言

我们常听说某个网站存在漏洞，某个网站又被黑客攻击了，但是黑客们是如何进行攻击的呢？本着让所有计算机使用者能够防患于未然的主旨，本书着重而详细地介绍了各种黑客入侵 PHP 网页的手法，虽然不能说是涵盖了全部的入侵手段，但已经能够概括绝大部分的攻击方式。本书详细解说了每个攻击手法的原理与实际操作，以及如何有效地防范这些入侵。读者只有在了解黑客攻击知识的基础上，才能最大限度地做到“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。

主要内容

本书共 13 章，第 1 章介绍黑客入门基础知识，包括进程、端口、黑客常见术语及命令、TCP/IP 协议、创建虚拟测试环境以及介绍常见的黑客攻击流程以及网络防御技术。

第 2 章介绍黑客的攻击方式，包括网络欺骗攻击、口令猜解攻击以及缓冲区溢出攻击。

第 3 章介绍 Windows 系统编程与网站脚本，包括黑客常用的编程语言、网络通信编程、文件操作编程、注册表编程、进程和线程编程以及 Web 脚本的入侵与防范。

第 4 章介绍后门程序编程基础，包括后门的发展历史及后门的分类、编写简单的 cmdshell 程序、编写简单的后门程序以及实现自启动功能的编程技术。

第 5 章介绍高级系统后门编程技术，包括远程线程注入后门和端口复用后门基本实现过程以及通过编程来编辑出这两种后门。

第 6 章介绍黑客程序的配置和数据包嗅探，包括文件生成技术、黑客程序配置

以及数据包嗅探等三方面的内容。

第 7 章介绍编程攻击与防御实例，包括 VB 木马编写以及防范措施、基于 ICMP 的 VC 木马编写、基于 Delphi 的木马编写、计算机扫描技术的编程以及隐藏防拷贝程序的运行。

第 8 章介绍 SQL 注入与防范技术，包括 SQL 注入前的准备，啊 D、NBSI、Domain、ZBSI 等常见注入工具实现注入攻击的方法，‘or’ = ‘or’ 经典漏洞攻击曝光，针对缺失单引号与空格的注入攻击方式，Update 注入攻击，以及 SQL 注入攻击的防范方法等。

第 9 章介绍数据库入侵与防范技术，包括常见的数据库入侵及其防御方式、两种常见的数据库入侵技术：下载漏洞攻击和暴库漏洞攻击。

第 10 章介绍 Cookie 攻击与防范技术，包括 Cookie 欺骗攻击、数据库与 Cookie 的关系、Cookie 欺骗与上传攻击、ClassID 的欺骗入侵、用户名的欺骗入侵以及 Cookie 欺骗的防范措施。

第 11 章介绍网络上传漏洞的攻击与防范，包括多余映射与上传攻击、点与 Windows 命名机制的漏洞攻击、二次循环产生的漏洞、借助 WSockExpert 工具进行上传攻击等。

第 12 章介绍恶意脚本入侵与防御，包括恶意脚本论坛入侵与防御、剖析恶意脚本的巧妙运用以及常见恶意脚本入侵的防御措施。

第 13 章介绍数据备份升级与恢复，包括备份与还原操作系统、备份与还原常用数据，全面了解数据恢复以及 Recuva、FinalData 和 FinalRecovery 三款数据恢复软件的使用等。

本书特色

本书以情景教学、案例驱动与任务进阶为鲜明特色，在书中可以看到一个个生动的情景案例。通过完成一个个实践任务，读者可以轻松掌握各个知识点，在不知不觉中快速提升实战技能。

高效模式——全程图解模式可彻底克服攻防操作的学习障碍。

内容合理——精选入门读者最迫切需要掌握的知识点，构成一个实用、充分、完整的知识体系。

举一反三——根据初学者学习中习惯机械记忆、不求甚解的特点，力求通过一个个知识点的讲解，让读者彻底理解和掌握类似场合的应对思路。

读者对象

- 计算机初、中级用户
- 计算机爱好者、提高者
- 各行各业从事网络维护的人员
- 网络管理员
- 大中专院校相关专业学生

目录

第2章 黑客的攻击方式曝光 / 40

第3章 Windows系统编程与网站脚本 / 64

第4章 后门程序编程基础 / 94

第5章 高级系统后门编程技术 / 140

第6章 黑客程序的配置和数据包嗅探 / 156

第9章 数据库入侵与防范技术 / 264

第10章 Cookie攻击与防范技术 / 285

第13章 数据备份升级与恢复 / 378

第1章 黑客入门基础知识

随着互联网在人们日常生活中影响的深入，网络的安全问题也引起了人们高度关注。而黑客则是网络世界中很神秘的一类人，他们有时会义务地维护网络的安全，有时却又以网络破坏者的形象出现。

本章要点：

- 了解并掌握进程、端口、文件和文件系统、Windows 注册表等黑客入门基础知识。
- 掌握黑客常用术语及 Ping 命令、Netstat 命令、Net 命令、Telnet 命令、FTP 命令、IPConfig 命令等黑客常用命令。
- 掌握 TCP/IP 协议簇、IP 协议、ARP 协议、ICMP 协议等常见的网络协议。
- 掌握如何安装 Vmware 虚拟机以及如何用 Vmware 创建虚拟环境、安装虚拟工具等。
- 了解常见的黑客攻击流程以及网络防御技术。

很多人由于对计算机安全防御和黑客入侵原理缺乏必要的了解，常常被黑客攻击了还蒙在鼓里。希望通过本章的学习，读者可以对黑客入门知识有个大概的了解。

1.1 成为黑客需要学习的基础知识

1.1.1 认识进程

进程是程序在计算机上的一次执行活动。当运行一个程序时，就启动了一个进程。显然，程序是静态的，进程是动态的。进程可以分为系统进程和用户进程两种。凡是用于完成操作系统的各种功能的进程就是系统进程，它们就是处于运行状态下的操作系统本身；用户进程就是所有由用户启动的进程。进程是操作系统进行资源分配的单位。

在 Windows 系统中按 Ctrl+Shift+Esc 组合键，即可打开“任务管理器”窗口。切换到“进程”选项卡，即可看到本机中开启的所有进程，如图 1-1 所示。如果想设置进程显示的内容，则选择“查看”→“选择列”菜单项，在“选择进程页列”对话框中勾选相应的复选框，如图 1-2 所示。

图 1-1 本机中开启的进程

图 1-2 “选择进程页列”对话框

1.1.2 端口的分类和查看

端口（Port）可以认为是计算机与外界通信交流的出口。其中硬件领域的端口又称接口，如 USB 端口、串行端口等。软件领域的端口一般指网络中面向连接服务和无连接服务的通信协议端口，是一种抽象的软件结构，包括一些数据结构和 I/O（输入输出）缓冲区。

端口是传输层的内容，是面向连接的，它们对应着网络上常见的一些服务。这些常见的服务可划分为使用 TCP 端口（面向连接，如打电话）和使用 UDP 端口（无连接，如写邮件）两种。

在网络中可以被命名和寻址的通信端口是一种可分配资源，由网络 OSI（Open System Interconnection ReferenceModel，开放系统互联参考模型）协议可知，传输层与网络层的区别

是传输层提供进程通信能力，网络通信的最终地址不仅包括主机地址，还包括可描述进程的某种标识。因此，当应用程序（调入内存运行后一般称为进程）通过系统调用与某端口建立连接（Binding，绑定）之后，传输层传给该端口的数据都被相应进程所接收，相应进程发给传输层的数据都从该端口输出。

1. 端口的分类

在网络技术中，端口大致有两种意思：一是物理意义上的设备，如集线器、交换机、路由器等用于连接其他的网络设备的接口；二是逻辑意义上的端口，一般指 TCP/IP 协议中的端口，范围为 0 ～ 65535，如浏览网页服务的 80 端口，用于 FTP 服务的 21 端口等。

逻辑意义上的端口有多种分类标准，常见的分类标准有如下两种。

（1）按端口号分布划分

按端口号分布划分可以分为“公认端口”、“注册端口”以及“动态和 / 或端口”等。

1）公认端口（Well Known Ports）。公认端口也称为常用端口，端口号为 0 ～ 1023，它们紧密地绑定于一些特殊的服务。通常，这些端口的通信明确地表明了某种服务协议，不可再重新定义它的作用对象。例如 21 端口分配给 FTP 服务，23 号端口分配给 Telnet 服务专用，25 号端口分配给全 SMTP（简单邮件传输协议）服务，80 端口是 HTTP 通信使用的，135 端口分配给 RPC（远程过程调用）服务等，通常不会被像木马这样的黑客程序利用。

2）注册端口（Registered Ports）。注册端口的端口号为 1024 ～ 49151，它们松散地绑定一些服务，即有许多服务绑定于这些端口。这些端口同样用于许多其他目的，且多数没有明确定义对象，不同的程序可以根据需要自己定义。记住这些常见程序端口，在木马程序的防护和查杀上非常有用。

3）动态和 / 或私有端口（Dynamic and/or Private Ports）。动态和或私有端口的端口号为 49152 ～ 65535，理论上不应该把常用服务分配在这些端口上，但实际上有些较为特殊的程序，特别是一些木马程序就非常喜欢使用这些端口，因为这些端口常常不会引起人们的注意，容易隐蔽。

（2）按协议类型划分

根据所提供的协议类型，端口又可分为“ TCP 端口”和“ UDP 端口”两种。一般直接与接收方进行的连接方式，大多采用 TCP 协议。只是把信息放在网上发布出去而不去关心信息是否到达的连接（即“无连接方式”），则大多采用 UDP 协议。

使用 TCP 协议的常见端口主要有如下几种：

1）FTP 协议端口。定义了文件传输协议，使用 21 端口。某计算机开了 FTP 服务便启动了文件传输服务，下载文件和上传主页都要用到 FTP 服务。

2）Telnet 协议端口。一种用于远程登录的端口，用户可以自己的身份远程连接到计算机上，通过这种端口可提供一种基于 DOS 模式的通信服务。如支持纯字符界面 BBS 的服务器会将 23 端口打开，以对外提供服务。

3）SMTP 协议端口。现在很多邮件服务器都是使用这个简单邮件传送协议来发送邮件。

如常见的免费邮件服务中使用的就是此邮件服务端口，所以在电子邮件设置中经常会看到有SMTP端口设置栏。服务器开放的是25号端口。

4）POP3协议端口。POP3协议用于接收邮件，通常使用110端口。只要有相应使用POP3协议的程序（如Outlook等），就可以直接使用邮件程序收到邮件（如使用126邮箱的用户就没有必要先进入126网站，再进入自己的邮箱来收信）。

使用UDP协议的常见端口主要有如下几种：

1）HTTP协议端口。这是用户使用得最多的协议，即“超文本传输协议”。当上网浏览网页时，就要在提供网页资源的计算机上打开80号端口以提供服务。通常的“WWW服务”、“Web服务器”等使用的就是这个端口。

2）DNS协议端口。DNS用于域名解析服务，这种服务在Windows NT系统中用得最多。Internet上的每一台计算机都有一个网络地址与之对应，这个地址就是IP地址，它以纯数字形式表示。但由于这种表示方法不便于记忆，于是就出现了域名，访问计算机时只需要知道域名即可，域名和IP地址之间的变换由DNS服务器来完成（DNS用的是53号端口）。

3）SNMP协议端口。SNMP即简单网络管理协议，它用来管理网络设备，使用161号端口。

4）QQ协议端口。QQ程序既提供服务又接收服务，使用无连接协议，即UDP协议。QQ服务器使用8000号端口侦听是否有信息到来，客户端使用4000号端口向外发送信息。

提示

在计算机的6万多个端口中，通常把端口号在1024以内的称为常用端口，这些常用端口所对应的服务通常是固定的。

2. 查看端口

为了查看目标主机上都开放了哪些端口，可以使用某些扫描工具对目标主机一定范围内的端口进行扫描。只有掌握目标主机上的端口开放情况，才能进一步对目标主机进行攻击。

在Windows系统中，可以使用Netstat命令查看端口。在“命令提示符”窗口中运行netstat -a -n命令，即可看到以数字形式显示的TCP和UDP连接的端口号及其状态，如图1-3所示。

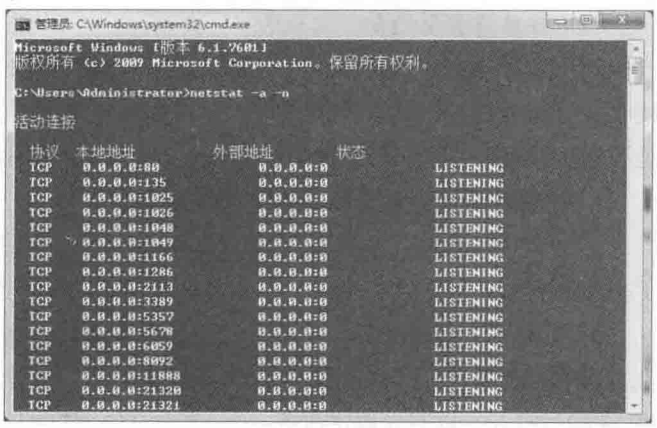

图1-3 查看端口状态

如果攻击者使用扫描工具对目标主机进行扫描，即可获取目标计算机开放的端口情况，并了解目标计算机提供了哪些服务。根据这些信息，攻击者即可对目标主机有一