

## <<新手学黑客攻防>>

### 图书基本信息

书名：<<新手学黑客攻防>>

13位ISBN编号：9787115245212

10位ISBN编号：7115245215

出版时间：2011-3

出版单位：人民邮电出版社

作者：神龙工作室

页数：208

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>

## <<新手学黑客攻防>>

### 内容概要

本书是指导初学者快速掌握黑客攻防的入门书籍。书中详细地介绍了初学者应该掌握的黑客攻防的基础知识，并对初学者在使用电脑时经常会遇到的问题进行了专家级的指导，以免初学者在起步的过程中走弯路。全书分7章，第1章主要介绍什么是黑客以及黑客的常用命令等内容；第2章主要介绍信息的收集与扫描；第3章主要介绍如何查看电脑的使用记录，以及系统和网页记录等内容；第4章主要介绍如何防范系统攻击；第5章主要介绍如何防范木马攻击；第6章主要介绍如何防范网络安全攻击；第7章主要介绍如何防范黑客攻击。

本书附带一张情景、互动式多媒体教学光盘，它采用了全程语音讲解、情景式教学、详细的图文对照和真实的情景演示等方式，紧密结合书中的内容对各个知识点进行了深入的讲解，大大扩充了本书的知识范围。

本书及配套光盘主要面向电脑初级用户，适合于广大电脑爱好者以及需要学习黑客攻防的读者使用，同时也可以作为电脑培训班的培训教材或者学习辅导用书。

## &lt;&lt;新手学黑客攻防&gt;&gt;

## 书籍目录

## 第1章 拨云见日——了解黑客

在网络世界中有一群神秘的人，他们有时候义务维护网络的安全，有时候却以网络破坏者的面目出现，这就是黑客。

## 1.1 黑客是如何攻击电脑的

## 1. 黑客的由来

## 2. 常见的黑客攻击方式

## 1.2 电脑是怎样联网的

## 1.2.1 认识IP地址

## 1.2.2 认识MAC地址

## 1.3 黑客怎样进入你的电脑

## 1.3.1 黑客进出的门户——端口

## 1.3.2 常用的电脑端口

## 1. 按端口号分类

## 2. 按协议类型分类

## 1.3.3 查看电脑端口的命令

## 1.3.4 怎样关闭端口

## 1. 关闭相应服务阻止访问端口

## 2. 限制端口的方法

## 1.4 木马藏身之处——系统进程

## 1.4.1 认识系统进程

## 1.4.2 打开系统进程

## 1.4.3 关闭和新建系统进程

## 1. 关闭系统进程

## 2. 新建系统进程

## 1.4.4 查看隐藏进程

## 1.4.5 查看远程进程

## 1.5 黑客常用基本命令

## 1.5.1 Ping命令

## 1.5.2 netstat命令

## 1.5.3 net命令

## 1. net localgroup

## 2. net user

## 1.5.4 DOS基本命令

## 1. DIR命令

## 2. CD命令

## 3. MD和RD命令

## 4. DEL命令

## 5. COPY命令

## 新手问题解答

## 第2章 信息的收集与扫描

在互联网中，无论是进攻还是防守，都需要收集尽可能多的信息，只有这样才能做到对战局了然于胸。

## 2.1 搜索网络中的重要信息

## &lt;&lt;新手学黑客攻防&gt;&gt;

## 2.1.1 获取目标主机的IP地址

1. 使用ping命令获取

2. 使用nslookup命令获取

## 2.1.2 获取目标主机的物理地址

## 2.1.3 了解网站备案信息

## 2.2 检测系统漏洞

## 2.2.1 什么是扫描器

1. 扫描器的种类

2. 扫描器的工作原理

3. 扫描器的作用

## 2.2.2 IPScan网段扫描工具

## 2.2.3?LanSee局域网查看工具

## 2.2.4 LanExplorer全能搜索利器

## 2.2.5 MBSA微软基准安全分析器

1. MBSA的功能

2. 扫描单台计算机

3. 扫描多台计算机

4. MBSA使用注意事项

## 2.3 扫描端口

## 2.3.1 ScanPort扫描端口利器

## 2.3.2 SuperScan超级扫描器

1. 域名(主机名)和IP相互转换

2. IP功能的使用

3. 端口检测

## 2.3.3 在线端口扫描

## 2.4 其他工具

## 2.4.1 SSS扫描之王

1. 【Options】选项

2. 【Rules】选项

3. 操作实例

## 2.4.2 X-Scan扫描器

## 2.4.3 爱莎网络监控器

## 2.4.4 流光——扫描利器

1. 流光软件的基本设置

2. 流光软件的使用

## 2.4.5 加壳与脱壳

1. 加壳

2. 脱壳

## 新手问题解答

## 第3章 谁动了我的电脑

系统会将用户在使用电脑过程中的操作记录下来，这样方便了用户查阅以前的操作，但这些记录往往也会成为网络攻击者利用的漏洞。

## 3.1 查看电脑的使用记录

## 3.1.1 查看上网时间

## 3.1.2 查看电脑开关机记?

## 3.1.3 查看系统异常记录

## <<新手学黑客攻防>>

### 3.2 查看系统记录

- 3.2.1 查看程序运行记录
- 3.2.2 查看TEMP文件夹记录
- 3.2.3 查看Windows搜索记录
- 3.2.4 查看【开始】菜单中的文档记录
- 3.2.5 查看回收站
- 3.2.6 查看添加删除程序记录
- 3.2.7 查看注册表编辑器记录

### 3.3 查看网页记录

- 3.3.1 查看Cookies聊天记录
- 3.3.2 查看Internet临时文件记录
- 3.3.3 查看网页历史记录

### 新手问题解答

### 第4章 系统攻防

黑客一般通过系统漏洞和远程控制技术对用户电脑进行攻击和控制，在此过程中，密码起着重要的防范作用。

### 4.1 密码攻防

#### 4.1.1 认识加密技术

- 1. 加密技术的定义
- 2. 加密技术的分类
- 3. 常见的加密算法

#### 4.1.2 系统加密

- 1. 设置CMOS开机密码
  - 2. 设置Windows启动密码
- #### 4.1.3 文件加密
- 1. 使用文件夹加密精灵加密文件夹
  - 2. 使用金锋文件加密器加密文件
  - 3. 使用WinRAR加密文件

#### 4.1.5 密码破解

- 1. 破解Office文档密码
- 2. 破解WinRAR文件的密码

### 4.2 远程控制

- 4.2.1 认识远程控制
- 4.2.2 使用远程控制软件
- 4.2.3 防范远程控制

- 1. 木马程序的运作原理
- 2. 防范/查杀木马程序

### 新手问题解答

### 第5章 木马病毒攻防

木马和病毒攻击是黑客最常用的攻击手段。对于普通的网络用户来说，如何保障自己电脑的安全，拒绝病毒和木马是必须要面对的问题。

### 5.1 木马攻防

#### 5.1.1 认识木马

## <<新手学黑客攻防>>

1. 木马的定义
2. 木马的结构
3. 木马的特征
- 5.1.2 木马的分类
  1. 远程木马
  2. 键盘木马
  3. 密码发送型木马
  4. 破坏型木马
  5. Dos木马
  6. FTP木马
  7. 代理木马
  8. 程序禁用木马
  9. 反弹端口型木马
- 5.1.3 常见的木马入侵和伪装手段
  1. 常见的木马入侵手段
  2. 揭露木马的伪装手段
- 5.1.4 木马诊断
  1. 计算机中木马的表现
  2. 计算机中木马的途径
  3. 木马的防范策略
- 5.1.5 木马制作与防范
  1. 软件捆绑木马
  2. 自解压木马
- 5.2 病毒攻防
  - 5.2.1 认识计算机病毒
    1. 什么是计算机病毒
    2. 计算机病毒的特征
  - 5.2.2 病毒的分类
    1. 引导型病毒
    2. 木马病毒
    3. 可执行文件病毒
    4. 多形性病毒
    5. 语言病毒
    6. 混合型病毒
  - 5.2.3 病毒诊断
    1. 计算机中毒的表现
    2. 计算机中毒的途径
  - 5.2.4 病毒防范
    1. 主要的防范方法
    2. 常见的杀毒软件
- 5.3 恶意代码攻防
  - 5.3.1 认识恶意代码
    1. 恶意代码的定义和特征
    2. 恶意代码的传播方式和趋势
  - 5.3.2 恶意代码分析
    1. 修改IE首页
    2. 修改IE右键菜单

## <<新手学黑客攻防>>

### 5.3.3 恶意代码防范

1. 恶意代码的预防
2. 恶意软件的查杀

### 5.4 U盘病毒攻防

#### 5.4.1 认识U盘病毒

1. U盘病毒的定义
2. U盘病毒的攻击原理
3. U盘病毒的特征

#### 5.4.2 防范U盘病毒

### 新手问题解答

## 第6章 网络安全攻防

网络无处不在，网络攻击也无孔不入。保护好账户和密码，是使用网络的基础课与必修课。

### 6.1 QQ攻防

#### 6.1.1 保护QQ聊天记录

#### 6.1.2 保护QQ密码

1. 设置QQ密码保护
2. 找回丢失的QQ号码

### 6.2 电子邮件攻防

#### 6.2.1 破解电子邮件的登录密码

1. 软件探测
2. 暴力破解

#### 6.2.2 找回邮箱密码

#### 6.2.3 防范邮箱炸弹攻击

### 新手问题解答

## 第7章 防范黑客攻击

黑客技术是不断发展的，我们不能预见明天会出现什么新病毒、新漏洞，但是为了保证计算机的安全，提高防黑意识，防御黑客的攻击势在必行。

### 7.1 提高防黑意识，养成良好习惯

### 7.2 提高系统保护能力

#### 7.2.1 堵住系统漏洞

1. 使用Windows系统自带的自动更新软件
2. 使用360安全卫士

#### 7.2.2 保护注册表安全

1. 限制远程访问
2. 备份与还原注册表

#### 7.2.3 设置组策略

1. 开机策略
2. 安全设置

#### 7.2.4 设置本地计算机安全策略

1. 系统安全管理
2. IP安全策略管理

### 7.3 使用防木马软件和杀毒软件

#### 7.3.1 使用防木马软件

## <<新手学黑客攻防>>

- 1. 360安全卫士
- 2. 金山卫士
- 7.3.2 使用杀毒软件
  - 1. 360杀毒软件
  - 2. 卡巴斯基杀毒软件
- 7.4 使用网络防火墙
  - 7.4.1 使用系统自带的防火墙
    - 1. 防火墙的基本设置
    - 2. 防火墙的高级设置
  - 7.4.2 使用第三方网络防火墙
    - 1. 瑞星个人防火墙主界面
    - 2. 瑞星防火墙规则设置
- 新手问题解答

## &lt;&lt;新手学黑客攻防&gt;&gt;

## 章节摘录

版权页：插图：恶意代码（maliciouscode）是一段程序，它会在用户不察觉的情况下嵌入另一个程序中，从而达到破坏计算机的数据、运行具有入侵性或破坏性的程序及破坏被感染计算机数据的安全性和完整性的目的。

恶意代码的特征恶意代码的编写大多是出于商业或探测他人资料的目的，如宣传某个产品、提供网络收费服务或对他人的计算机直接进行有意的破坏等，总的来说，它具有恶意破坏的目的、其本身为程序，以及通过执行发生作用3个特征。

（1）恶意破坏的目的。

有相当一部分黑客进行恶意代码攻击的目的是从破坏其他用户的系统中得到“成就感”。

但现在更多的黑客则是出于经济利益。

例如，某些广告类代码可以通过用户的上网习惯以提高广告点击率来获取经济利益，而更直接的则是通过窃取其他用户的网上信用卡、银行代码等直接对其进行经济侵犯。

现今又出现了潜伏性的恶意代码，在攻击的同时尽量不被发现，对用户和社会都造成了严重的危害，构成了严重的经济犯罪。

（2）其本身为程序。

恶意代码是一段程序，它可以在很隐蔽的情况下嵌入另一个程序中，通过运行别的程序而自动运行，从而达到破坏被感染计算机的数据、程序以及对被感染计算机进行信息窃取等目的。

（3）通过执行发生作用。

恶意代码与木马一样，只要用户运行就会发作，只不过恶意代码是通过网页进行传播的。

2.恶意代码的传播方式和趋势恶意代码按传播方式可以分为病毒、蠕虫、木马、移动代码和间谍软件等。

其传播的目的已有所变化，传统的攻击活动常常是受好奇心驱使，希望自己的技术可以得到认可，而现在的攻击则以获得经济利益为目的。

这些攻击通常为犯罪行为，例如，为牟取经济利益而非法盗取他人的信息，从而对其造成经济损失。

## <<新手学黑客攻防>>

### 编辑推荐

《新手学黑客攻防》：如果你是第一次接触黑客知识如果你想熟知网络攻防的方法如果你想让电脑更加安全如果你不希望被他人窥探隐私我的第1本黑客攻防入门书，200万读者的共同选择。

<<新手学黑客攻防>>

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>