

从新手到高手

黑客入门与网络安全实用手册  
安全技术全新升级

# 黑客攻防 与网络安全

## 从新手到高手 (实战篇)



网络安全技术联盟 主编  
魏红 副主编

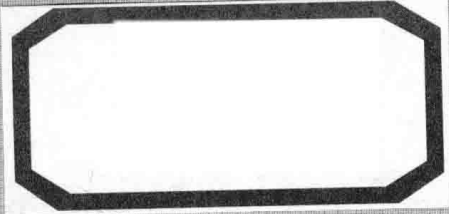


一线网络安全技术联盟倾心打造  
海量王牌资源超值赠送

- |   |                  |   |                         |
|---|------------------|---|-------------------------|
|  超值赠送 1 | 同步微视频            |  超值赠送 6  | 191页Windows 10系统使用和防护技巧 |
|  超值赠送 2 | 精美教学PPT课件        |  超值赠送 7  | 8大经典密码破解工具详解            |
|  超值赠送 3 | 黑客工具(107个)速查手册   |  超值赠送 8  | 加密与解密技术快速入门小白电子手册       |
|  超值赠送 4 | 常用黑客命令(160个)速查手册 |  超值赠送 9  | 网站入侵与黑客脚本编程电子书          |
|  超值赠送 5 | 180页常见故障维修手册     |  超值赠送 10 | 黑客命令全方位详解电子书            |



清华大学出版社



从新手到高手

# 黑客攻防 与网络安全

从新手到高手(实战篇)

网络安全技术联盟 主 编  
魏 红 副主编

RFID



清华大学出版社  
北 京

## 内容简介

本书在剖析用户进行黑客防御中迫切需要或想要用到的技术时，力求对其进行“傻瓜”式的讲解，使读者对网络防御技术有一个系统的了解，能够更好地防范黑客的攻击。全书共分为15章，包括网络安全快速入门、搭建网络安全测试环境、黑客入侵方式与DOS命令、木马病毒的查杀与预防、系统漏洞与用户账户的安全防护、远程控制入侵系统的安全防护、网络账号及密码的安全防护、浏览器的安全防护、有线局域网的安全防护、无线局域网的安全防护、网站系统的安全防护、电子邮箱与邮件的安全防护、操作系统的安全防护、计算机安全的终极防护、黑客后门入侵痕迹的清理等内容。

另外，本书还赠送海量王牌资源，由于赠送的资源比较多，在本书前言部分对赠送资源的具体内容做了详细说明，帮助读者掌握黑客防守方方面面的知识。

本书内容丰富，图文并茂，深入浅出，不仅适用于网络安全从业人员及网络管理员，而且适用于广大网络爱好者，还可作为大中专院校相关专业的参考书。

本书封面贴有清华大学出版社防伪标签，无标签者不得销售。

版权所有，侵权必究。侵权举报电话：010-62782989 13701121933

### 图书在版编目(CIP)数据

黑客攻防与网络安全从新手到高手：实战篇 / 网络安全技术联盟主编. —北京：清华大学出版社，2019  
(从新手到高手)

ISBN 978-7-302-53011-4

I ①黑… II. ①网… III. ①黑客—网络防御 IV. ①TP393.081

中国版本图书馆CIP数据核字(2019)第094003号

责任编辑：张敏

封面设计：杨玉兰

责任校对：胡伟民

责任印制：丛怀宇

出版发行：清华大学出版社

网 址：<http://www.tup.com.cn>，<http://www.wqbook.com>

地 址：北京清华大学学研大厦A座 邮 编：100084

社总机：010-62770175 邮 购：010-62786544

投稿与读者服务：010-62776969，[c-service@tup.tsinghua.edu.cn](mailto:c-service@tup.tsinghua.edu.cn)

质量反馈：010-62772015，[zhiliang@tup.tsinghua.edu.cn](mailto:zhiliang@tup.tsinghua.edu.cn)

印 装 者：北京嘉实印刷有限公司

经 销：全国新华书店

开 本：185mm×260mm 印 张：18.25 字 数：460千字

版 次：2019年10月第1版 印 次：2019年10月第1次印刷

定 价：69.80元

产品编号：082954-01

## 作者简介

### 网络安全技术联盟

“网络安全技术联盟”由众多网络安全高手组成，对系统和网络安全中的漏洞非常熟悉，致力于网络安全技术研究和普及，秉承技术自由、技术创新、技术共享、技术进步的原则，为网络安全爱好者提供一个共同进步的平台。

### 魏红

网络安全工程师，长期从事网络安全、数据通信安全研究工作。

# Preface

## 前言

随着手机、平板计算机的普及，无线网络的防范变得尤为重要，为此，本书除了讲解有线网络的攻防策略外，还把目前市场上流行的无线攻防等热点融入其中。

### 本书特色

**知识丰富全面：**知识点由浅入深，涵盖了所有黑客攻防技术，使读者由浅入深地掌握黑客攻防方面的技能。

**图文并茂：**注重操作，在介绍案例的过程中，每一个操作均有对应的插图。这种图文结合的方式使读者在学习过程中能够直观、清晰地看到操作的过程以及效果，便于更快地理解和掌握。

**案例丰富：**把知识点融汇于系统的案例实训当中，并且结合经典案例进行讲解和拓展，进而达到“知其然，并知其所以然”的效果。

**提示技巧、贴心周到：**本书对读者在学习过程中可能会遇到的疑难问题以“提示”的形式进行了说明，以免读者在学习的过程中走弯路。

### 超值赠送

本书将赠送同步微视频、精美教学PPT课件、黑客工具（107个）速查手册、常用黑客命令（160个）速查手册、180页常见故障维修手册、191页Windows 10系统使用和防护技巧、8大经典密码破解工具详解、加密与解密技术快速入门小白电子手册、网站入侵与黑客脚本编程电子书、黑客命令全方位详解电子书。读者可扫描右方二维码或通过电子邮件zhangmin2@tup.tsinghua.edu.cn获取本书资源。



精美教学  
幻灯片



赠送资源  
8本电子书

### 读者对象

本书不仅适用于网络安全从业人员及网络管理员，而且适用于广大网络爱好者，还可作为大中专院校相关专业的参考书。

### 写作团队

本书由长期研究网络安全知识的网络安全技术联盟主编，魏红任副主编，另外还有王秀英、王英英、刘玉萍、刘尧、王朵朵、王攀登、王婷婷、张芳、李小威、王猛、王维维、李佳康、王秀荣、王天护、皮素芹等人参与编写工作。在编写过程中，尽所能地将最好的讲解呈现给读者，但也难免有疏漏和不妥之处，敬请不吝指正。若您在学习中遇到困难或疑问，或有何建议，可通过电子邮箱zhangmin2@tup.tsinghua.edu.cn及时获得在线指导和本书的资源。

# Contents

## 目 录

<b>第1章 网络安全快速入门</b> .....	1	<b>第2章 搭建网络安全测试环境</b> .....	10
1.1 网络中的相关概念 .....	1	2.1 认识安全测试环境 .....	10
1.1.1 互联网与因特网 .....	1	2.1.1 什么是虚拟机软件 .....	10
1.1.2 万维网与浏览器 .....	1	2.1.2 什么是虚拟系统 .....	10
1.1.3 URL 地址与域名 .....	2	2.2 安装与创建虚拟机 .....	10
1.1.4 IP 地址与 MAC 地址 .....	2	实战1: 下载虚拟机软件 .....	10
1.2 认识网络通信协议 .....	2	实战2: 安装虚拟机软件 .....	11
1.2.1 TCP/IP .....	2	实战3: 创建虚拟机系统 .....	13
1.2.2 IP .....	3	2.3 安装虚拟机软件系统 .....	16
1.2.3 ARP .....	3	实战4: 安装Windows操作	
1.2.4 ICMP .....	3	系统 .....	16
1.3 计算机基本信息的获取 .....	3	实战5: 安装VMware Tools	
实战1: 获取本机的IP地址 .....	3	工具 .....	18
实战2: 获取本机的物理地址 .....	4	实战6: 安装Kali Linux操作	
实战3: 查看系统开放的端口 .....	4	系统 .....	20
实战4: 查看系统注册表信息 .....	4	2.4 实战演练 .....	23
实战5: 获取系统进程信息 .....	5	实战演练1——设置Kail与主机	
1.4 实战演练 .....	5	共享文件夹 .....	23
实战演练1——新建与关闭系统		实战演练2——设置Kali虚拟机的	
进程 .....	5	上网方式 .....	26
实战演练2——全面管理系统进		2.5 小试身手 .....	26
程信息 .....	6	练习1: 显示系统文件的扩	
1.5 小试身手 .....	8	展名 .....	26
练习1: 查看进程起始程序 .....	8	练习2: 查看系统中的ARP	
练习2: 关闭不必要的端口 .....	8	缓存表 .....	26

<b>第3章 黑客入侵方式与DOS命令</b> .. 28	
3.1 黑客常用入侵方式 .. 28	
3.1.1 获取口令入侵 .. 28	
3.1.2 远程控制入侵 .. 28	
3.1.3 木马病毒入侵 .. 29	
3.1.4 系统漏洞入侵 .. 29	
3.1.5 电子邮件入侵 .. 29	
3.1.6 网络监听入侵 .. 29	
3.2 黑客常用DOS命令实战 .. 29	
实战1: 切换当前目录的cd命令 .. 29	
实战2: 列出磁盘目录文件的dir命令 .. 30	
实战3: 检查计算机连接状态的ping命令 .. 31	
实战4: 查询网络状态与共享资源的net命令 .. 32	
实战5: 显示网络连接信息的netstat命令 .. 33	
实战6: 检查网络路由节点的tracert命令 .. 34	
实战7: 显示主机进程信息的Tasklist命令 .. 34	
实战8: 扫描并修复系统错误的sfc命令 .. 35	
3.3 实战演练 .. 36	
实战演练1——使用命令代码清除系统垃圾文件 .. 36	
实战演练2——使用shutdown命令实现定时关机 .. 37	
3.4 小试身手 .. 37	
练习1: 通过滑动鼠标关闭计算机 .. 37	

练习2: 快速锁定Windows桌面 .. 38
--------------------------

<b>第4章 木马病毒的查杀与预防</b> .. 39
4.1 认识病毒与木马 .. 39
4.1.1 常见的木马类型 .. 39
4.1.2 认识网络中的病毒 .. 40
4.1.3 计算机中病毒后的表现 .. 40
4.2 木马自我保护与伪装手段 .. 40
实战1: 通过加壳工具给木马加壳 .. 40
实战2: 使用WinRAR伪装木马 .. 42
实战3: 图片也可能是木马程序 .. 44
4.3 使用木马清除软件清除木马 .. 45
实战4: 使用《金山贝壳木马专杀》清除木马 .. 45
实战5: 使用Spyware Doctor清除木马 .. 46
4.4 使用《360杀毒》软件查杀病毒 .. 49
实战6: 安装《360杀毒》软件 .. 49
实战7: 升级《360杀毒》的病毒库 .. 50
实战8: 快速查杀计算机中的病毒 .. 51
实战9: 自定义查杀计算机中的病毒 .. 52
4.5 使用病毒专杀工具查杀病毒 .. 53
实战10: 查杀异鬼病毒 .. 53
实战11: 查杀CAD病毒 .. 54
实战12: 查杀U盘病毒 .. 54
4.6 实战演练 .. 57
实战演练1——在Word中预防宏病毒 .. 57

实战演练2——使用《360杀毒》查杀宏病毒 .....	58	实战9: 设置Microsoft账户图片密码 .....	73
4.7 小试身手 .....	58	实战10: 重置Microsoft账户登录密码 .....	74
练习1: 删除上网缓存文件 .....	58	5.5 实战演练 .....	76
练习2: 在安全模式下查杀病毒 .....	59	实战演练1——创建用户账户的密码恢复盘 .....	76
<b>第5章 系统漏洞与用户账户的安全防护</b> .....	61	实战演练2——本地账户和Microsoft账户的切换 .....	77
5.1 认识系统漏洞与用户账户 .....	61	5.6 小试身手 .....	79
5.1.1 认识计算机系统漏洞 .....	61	练习1: 设置屏幕保护密码 .....	79
5.1.2 系统漏洞产生的原因 .....	61	练习2: 取消Windows开机密码 .....	80
5.1.3 认识本地管理员账户 .....	61	<b>第6章 远程控制入侵系统的安全防护</b> .....	82
5.1.4 认识Microsoft账户 .....	61	6.1 什么是远程控制 .....	82
5.2 系统漏洞的安全防护 .....	62	6.2 通过Windows远程桌面入侵系统 .....	82
实战1: 使用“Windows”更新修复系统漏洞 .....	62	实战1: 开启Windows远程桌面功能 .....	82
实战2: 使用《360安全卫士》修复系统漏洞 .....	63	实战2: 使用远程桌面功能实现远程控制 .....	83
5.3 本地系统账户的安全防护 .....	64	6.3 使用RemotelyAnywhere入侵系统 .....	85
实战3: 启用本地Administrator账户 .....	64	实战3: 安装RemotelyAnywhere .....	85
实战4: 设置Administrator账户密码 .....	65	实战4: 连接入侵远程主机 .....	87
实战5: 删除不需要的本地用户账户 .....	67	实战5: 远程操控目标主机 .....	88
5.4 Microsoft账户的安全防护 .....	68	6.4 使用QuickIP实现远程控制入侵系统 .....	93
实战6: 注册并登录Microsoft账户 .....	68	实战6: 安装QuickIP工具 .....	93
实战7: 设置Microsoft账户登录密码 .....	70	实战7: 设置QuickIP服务端 .....	94
实战8: 设置Microsoft账户PIN密码 .....	71	实战8: 设置QuickIP客户端 .....	95
		实战9: 实现远程控制入侵 .....	96

6.5	远程控制入侵系统的安全防护策略 .....	97	实战10: 关闭Window远程桌面功能 .....	97	实战8: 避免进入钓鱼网站 .....	112	
	实战11: 开启拒绝系统入侵的防火墙 .....	98	实战12: 关闭远程注册表管理服务 .....	98	实战9: 使用网银安全证书 .....	115	
6.6	实战演练 .....	99	实战演练1——禁止访问计算机控制面板 .....	99	7.4 实战演练 .....	117	
	实战演练2——启用和关闭快速启动功能 .....	100	实战演练2——启用和关闭快速启动功能 .....	100	实战演练1——使用手机钱包给手机充话费 .....	117	
6.7	小试身手 .....	101	练习1: 开启系统的平板模式 .....	101	实战演练2——使用网银进行网上购物 .....	119	
	练习2: 设置默认打开应用程序 .....	101	练习2: 设置默认打开应用程序 .....	101	7.5 小试身手 .....	120	
<b>第7章 网络账号及密码的安全防护</b> .....				103	练习1: 启动系统中的BitLocker功能 .....	120	
7.1	QQ账号及密码的安全防护 .....	103	练习2: 使用BitLocker功能加密磁盘数据 .....	121	<b>第8章 浏览器的安全防护</b> .....		
	实战1: 盗取QQ账号与密码 .....	103	8.1 常见浏览器的攻击方式 .....				124
	实战2: 提升QQ账号的安全设置 .....	105	实战1: 修改浏览器的默认主页 .....	124	实战1: 修改浏览器的默认主页 .....	124	
	实战3: 找回被盗的QQ账号密码 .....	106	实战2: 恶意更改浏览器标题栏 .....	125	实战2: 恶意更改浏览器标题栏 .....	125	
7.2	微信账号及密码的安全防护 .....	107	实战3: 强行修改浏览器的右键菜单 .....	126	实战3: 强行修改浏览器的右键菜单 .....	126	
	实战4: 使用微信手机钱包转账 .....	107	实战4: 禁用浏览器的“源”菜单命令 .....	127	实战4: 禁用浏览器的“源”菜单命令 .....	127	
	实战5: 微信支付的安全设置 .....	109	实战5: 强行修改浏览器的首页按钮 .....	128	实战5: 强行修改浏览器的首页按钮 .....	128	
	实战6: 冻结微信账号以保护账号安全 .....	111	实战6: 删除桌面上的浏览器图标 .....	129	实战6: 删除桌面上的浏览器图标 .....	129	
7.3	网银账号及密码的安全防护 .....	112	8.2 IE浏览器的自我安全防护 .....	130	实战7: 提高IE的安全防护等级 .....	130	
	实战7: 网上挂失银行卡 .....	112	实战7: 提高IE的安全防护等级 .....	130	实战8: 清除浏览器中的表单信息 .....	132	
			实战8: 清除浏览器中的表单信息 .....	132	实战9: 清除浏览器的上网历史记录 .....	132	

实战10: 删除上网Cookie 信息 .....	133	实战2: 使用IPBook查看 .....	148
8.3 Microsoft Edge浏览器的 自我安全防护 .....	134	9.3 局域网的安全防护 .....	151
实战11: Microsoft Edge基本 操作 .....	134	实战3: 使用网络剪刀手切断 网络 .....	151
实战12: 在阅读视图模式下浏览 网页 .....	135	实战4: 局域网中的ARP攻击 .....	152
实战13: 使用InPrivate浏览网页 信息 .....	136	实战5: 监听局域网中的 数据包 .....	155
实战14: 启用SmartScreen筛选 功能 .....	137	实战6: 局域网中的网络欺骗 攻击 .....	157
8.4 使用工具保护浏览器的安全 .....	138	9.4 局域网安全的防护 .....	158
实战15: 使用IE伴侣快速修复 浏览器 .....	138	实战7: 使用“聚生网管” 管理局域网 .....	158
实战16: 使用IE修复专家修复 浏览器 .....	139	实战8: 使用“长角牛网络 监控机”保护局域网 .....	163
8.5 实战演练 .....	140	实战9: 使用“大势至局域网 安全卫士”保护局域网 .....	168
实战演练1——屏蔽浏览器网页广 告弹窗 .....	140	9.5 实战演练 .....	169
实战演练2——将计算机收藏夹 网址同步到手机 .....	141	实战演练1——设置局域网中宽带 连接方式 .....	169
8.6 小试身手 .....	144	实战演练2——诊断和修复网络 不通的问题 .....	172
练习1: 使用地址栏进行关键词 搜索 .....	144	9.6 小试身手 .....	172
练习2: 清除Microsoft Edge中的 浏览数据 .....	144	练习1: 取消计算机的开机锁屏 界面 .....	172
<b>第9章 有线局域网的安全防护</b> .....	146	练习2: 我用左手使用鼠标 怎么办? .....	173
9.1 局域网的安全介绍 .....	146	<b>第10章 无线局域网的安全防护</b> .....	174
9.1.1 局域网基础知识 .....	146	10.1 认识无线局域网 .....	174
9.1.2 局域网安全隐患 .....	146	10.1.1 无线局域网的优点 .....	174
9.2 查看局域网中的主机信息 .....	147	10.1.2 无线局域网的缺点 .....	174
实战1: 使用LanSee查看 .....	147	10.1.3 认识无线连接方式 .....	174
		10.2 组建无线局域网 .....	175
		实战1: 配置无线局域网 .....	175

实战2: 将计算机接入无线 局域网 .....	176	11.1 认识网站和网页 .....	194
实战3: 将手机接入无线局域网 ..	177	11.1.1 什么是网站 .....	194
10.3 无线局域网的安全设置 .....	178	11.1.2 网站的分类 .....	194
实战4: 设置路由器的管理员 密码 .....	178	11.1.3 什么是网页 .....	195
实战5: 设置无线网络WEP 密码 .....	178	11.2 网站攻击基础知识 .....	197
实战6: 设置无线网络WPA-PSK 密码 .....	180	11.2.1 网站攻击的原理 .....	198
实战7: 关闭路由器的SSID广播 功能 .....	181	11.2.2 网站攻击的特点 .....	198
实战8: 使用无线网络开启MAC 地址过滤功能 .....	182	11.3 网站攻击的常见方式 .....	198
10.4 无线路由器的安全防护 .....	183	实战1: 网站的DoS攻击 .....	198
实战9: 使用《360路由器卫士》 防护 .....	183	实战2: 网站的DDoS攻击 .....	199
实战10: 使用《路由优化大师》 防护 .....	186	实战3: 网站的SQL注入攻击 .....	201
10.5 实战演练 .....	190	11.4 网站系统的安全防护 .....	204
实战演练1——控制无线网中 设备的上网速度 .....	190	实战4: 网站硬件的安全防护 .....	204
实战演练2——通过向导设置 路由器并进行上网 .....	190	实战5: 网站软件的安全防护 .....	204
10.6 小试身手 .....	192	实战6: DDoS攻击的防御 措施 .....	205
练习1: 加密手机的WLAN热点 功能 .....	192	实战7: 设置网站的访问权限 .....	206
练习2: 通过修改WiFi名称隐藏 路由器 .....	193	11.5 实战演练 .....	207
<b>第11章 网站系统的安全防护</b> .....	194	实战演练1——检测网站的 安全性 .....	207
		实战演练2——查看网站的 流量 .....	208
		11.6 小试身手 .....	210
		练习1: 添加网站的网址到 收藏夹 .....	210
		练习2: 下载网站中的资料 资源 .....	211
		<b>第12章 电子邮箱与邮件的安全     防护</b> .....	213
		12.1 认识电子邮件病毒 .....	213
		12.1.1 电子邮件病毒的特征 .....	213
		12.1.2 识别电子邮件病毒 .....	214

12.2 获取电子邮箱密码的常用手段 .....	214	实战4: 禁止在登录前关机 .....	232
实战1: 盗取邮箱密码的常用方法 .....	214	实战5: 在超过登录时间后强制用户注销 .....	233
实战2: 使用“流光”盗取邮箱密码 .....	215	实战6: 登录时不显示用户名 .....	233
12.3 电子邮箱与邮件的安全防护策略 .....	216	实战7: 对备份和还原权限进行审核 .....	234
实战3: 重要邮箱的保护措施 .....	216	实战8: 设置本地账户共享与安全模式 .....	235
实战4: 找回被盗的邮箱密码 .....	217	实战9: 让Everyone权限应用于匿名用户 .....	235
实战5: 通过邮箱设置防止垃圾邮件 .....	217	13.3 通过设置组策略提高系统安全 .....	236
12.4 实战演练 .....	219	实战10: 设置账户锁定策略 .....	236
实战演练1——配置Outlook电子邮箱账户 .....	219	实战11: 设置账户密码策略 .....	237
实战演练2——通过账户设置来备份与恢复邮件 .....	220	实战12: 设置用户权限分配 .....	238
12.5 小试身手 .....	221	实战13: 更改系统默认的账户 .....	239
练习1: 通过向导备份电子邮件 .....	221	实战14: 禁止更改“开始”菜单 .....	240
练习2: 使用向导还原电子邮件 .....	222	实战15: 禁止更改桌面设置 .....	241
<b>第13章 操作系统的安全防护 .....</b>	<b>224</b>	13.4 使用入侵检测系统保护系统安全 .....	242
13.1 通过清理间谍软件保护系统安全 .....	224	实战16: 设置萨客嘶入侵检测系统 .....	242
实战1: 使用“反间谍专家”清理 .....	224	实战17: 使用萨客嘶入侵检测系统 .....	245
实战2: 使用“Windows清理助手”清理 .....	227	13.5 实战演练 .....	247
实战3: 使用Spybot-Search&Destroy清理 .....	230	实战演练1——一键锁定计算机 .....	247
13.2 通过本地安全设置保护系统安全 .....	232	实战演练2——禁用“添加或删除程序” .....	247
		13.6 小试身手 .....	248
		练习1: 使用Windows Defender .....	248

练习2: 管理鼠标的右键菜单	249	14.6 小试身手	265
<b>第14章 计算机安全的终极</b>		练习1: 设置虚拟内存的	
<b>防护</b>	250	大小	265
14.1 重装计算机操作系统	250	练习2: 系统的睡眠与唤醒	
14.1.1 什么情况下重装系统	250	模式	267
14.1.2 重装前应注意事项	250	<b>第15章 黑客后门入侵痕迹的</b>	
<b>实战1: 重装Windows 10操作</b>		<b>清理</b>	268
系统	251	15.1 黑客留下的“脚印”	268
14.2 备份计算机操作系统	254	15.1.1 日志的详细定义	268
<b>实战2: 使用系统工具备份</b>		15.1.2 为什么要清理日志	269
系统	254	15.2 分析系统日志信息	269
<b>实战3: 使用系统映像备份</b>		<b>实战1: 安装WebTrends日志分析</b>	
系统	255	工具	269
<b>实战4: 使用GHOST工具备份</b>		<b>实战2: 在WebTrends中创建日志</b>	
系统	257	站点	270
14.3 还原崩溃后的操作系统	258	<b>实战3: 使用WebTrends生成日志</b>	
<b>实战5: 使用系统工具还原</b>		报表	273
系统	258	15.3 清除服务器入侵日志	273
<b>实战6: 使用GHOST工具还原</b>		<b>实战4: 清除WWW日志和FTP日志</b>	
系统	259	信息	273
<b>实战7: 使用系统映像还原</b>		<b>实战5: 使用批处理清除日志</b>	
系统	260	信息	275
14.4 重置崩溃后的操作系统	261	15.4 实战演练	275
<b>实战8: 在可开机情况下重置</b>		<b>实战演练1——使用事件查看器</b>	
计算机	261	分析日志信息	275
<b>实战9: 在不可开机情况下重</b>		<b>实战演练2——利用SRVINSTW</b>	
置计算机	263	删除系统服务日志	277
14.5 实战演练	263	15.5 小试身手	278
<b>实战演练1——设置计算机系统</b>		练习1: 保存日志文件	278
启动密码	263	练习2: 将程序固定到	
<b>实战演练2——创建系统修复</b>		任务栏	279
备份光盘	264		

# 第1章 网络安全快速入门

随着信息时代的发展和网络的普及，越来越多的人走进了网络生活，然而人们在享受网络带来便利的同时，也时刻面临着黑客们残酷攻击的危险。本章介绍网络安全的相关技术信息，主要内容包括网络中的相关概念、网络通信的相关协议、IP地址、MAC地址、端口、系统进程等。

## 1.1 网络中的相关概念

在网络安全中，经常会接触到很多和网络有关的概念，如浏览器、URL、FTP、IP地址及域名等，理解这些概念，对保护网络安全有一定的帮助。

### 1.1.1 互联网与因特网

互联网是指将两台计算机或者是两台以上的计算机终端、客户端、服务端通过计算机信息技术的手段互相联系起来的结果。互联网在现实生活中应用很广泛，在互联网上人们可以聊天、玩游戏、查阅资料等。互联网是全球性的，这就意味着这个网络不管是谁发明了它，是属于全人类的。

因特网是一个把分布于世界各地的计算机用传输介质互相连接起来的网络，它是基于TCP/IP实现的。TCP/IP由很多协议组成，不同类型的协议又被放在不同的层，其中，位于应用层的协议就有很多，如FTP、SMTP、HTTP。

### 1.1.2 万维网与浏览器

万维网（World Wide Web，WWW）简称为3W，它是无数个网络站点和网页的集合，也是因特网提供的最主要的服务。万维网是由多媒体链接而形成的集合，通常我们上网看到的内容就是万维网的内容。如下图所示为使用万维网打开的百度首页。



**提示：**互联网、因特网、万维网三者的关系是由互联网包含因特网，因特网包含万维网。凡是由能彼此通信的设备组成的网络就叫互联网。所以，即使仅有两台计算机，不论用何种技术使其彼此通信，也叫互联网。

浏览器是将互联网上的文本文档（或其他类型的文件）翻译成网页，并让用户与这些文件交互的一种软件工具，主要用于查看网页的内容。目前最常用的浏览器有微软公司的Internet Explorer（通常称为IE浏览器），如下图所示是使用IE浏览器打开的页面。



### 1.1.3 URL地址与域名

URL (Uniform Resource Locator) 即统一资源定位器, 也就是网络地址, 是在因特网上用来描述信息资源, 并将因特网提供的服务统一编址的系统。简单来说, 通常在IE浏览器或Netscape浏览器中输入的网址就是URL的一种, 如百度网址http://www.baidu.com。

域名 (Domain Name) 类似于因特网上的门牌号, 是用于识别和定位互联网上计算机层次结构的字符标识, 与该计算机的因特网协议 (IP) 地址相对应。但相对于IP地址而言, 域名更便于使用者理解和记忆。URL和域名是两个不同的概念, 如http://www.sohu.com/是URL, 而www.sohu.com是域名, 如下图所示为使用URL打开的网页。



### 1.1.4 IP地址与MAC地址

IP地址用于在TCP/IP中标记每台计算机的地址, 通常使用十进制来表示, 如192.168.1.100, 但在计算机内部, IP地址是一个32位的二进制数值, 如11000000 10101000 00000001 00000110 (192.168.1.6)。

MAC地址与网络无关, 即无论将带有这个地址的硬件 (如网卡、集线器、路由器等) 接入到网络的何处, 都是相同的MAC地址, 它由厂商写在网卡的BIOS里。

MAC地址通常表示为12位十六进制数, 每2位十六进制数之间用冒号隔开, 如08:00:20:0A:8C:6D就是一个MAC地址, 其中前6位 (08:00:20) 代表网络硬件制造商的编号, 它由IEEE分配, 而后6位 (0A:8C:6D) 代表该制造商所制造的某个网络产品 (如网卡) 的系列号。每个网络制造商必须确保它所制造的每个以太网设备前3个字节都相同, 后3个字节不同, 这样, 就可以保证世界上每个以太网设备都具有唯一的MAC地址。

**提示:** IP地址与MAC地址的区别在于IP地址基于逻辑, 比较灵活, 不受硬件限制, 也容易记忆; MAC地址在一定程度上与硬件一致, 基于物理, 能够具体标识。这两种地址均有各自的长处, 使用时也因条件不同而采取不同的地址。

## 1.2 认识网络通信协议

“网络通信协议”是计算机网络的一个重要组成部分, 是不同网络之间通信、“交流”的公共语言。有了它, 使用不同系统的计算机或网络之间才可以彼此识别, 识别出不同的网络操作指令, 建立信任关系。

### 1.2.1 TCP/IP

TCP/IP包括两个子协议, 即TCP (Transmission Control Protocol, 传输控制协议) 和IP (Internet Protocol, 因特网协议)。在这两个子协议中又包括许多应用型的协议和服务, 使得TCP/IP的功能非常强大。

TCP/IP中除了包括TCP、IP两个协议外, 还包括许多子协议。它的核心协议包括用户数据报协议 (UDP)、地址解析协议 (ARP) 及因特网控制消息协议 (ICMP) 等。

## 1.2.2 IP

IP (Internet Protocol, 因特网协议) 可实现两个基本功能: 寻址和分段。IP可以根据数据报报头中包括的目的地址将数据报传送到目的地址。另外, IP使用4个关键技术提供服务: 服务类型、生存时间、选项和报头校验码。

IP的基本任务是通过互联网传送数据报, 各个IP数据报之间是相互独立的。IP从源运输实体取得数据, 通过它的数据链路层服务传给目的主机的IP层。在传送时, 高层协议将数据传给IP, IP再将数据封装为互联网数据报, 并交给数据链路层协议通过局域网传送。

## 1.2.3 ARP

ARP (Address Resolution Protocol, 地址解析协议) 基本功能就是通过目标设备的IP地址, 查询目标设备的MAC地址, 以保证通信的顺利进行。在局域网中, 网络中实际传输的是“帧”, 帧里面有目标主机的MAC地址。

在以太网中, 一个主机要和另一个主机进行直接通信, 必须要知道目标主机的MAC地址, 这个MAC地址就是通过地址解析协议获得的。所谓“地址解析”就是主机在发送数据帧前将目标IP地址转换成目标MAC地址的过程。

## 1.2.4 ICMP

ICMP (Internet Control Message Protocol, 因特网控制消息协议) 是TCP/IP中的子协议, 主要用于在IP主机、路由器之间传递控制消息。控制消息是指网络通不通、主机是否可达、路由是否可用等网络本身的消息。这些控制消息虽然并不传输用户数据, 但是对于用户数据的传递起着重要作用。

ICMP对于网络安全非常重要, 因为ICMP本身的特点, 决定了它非常容易

被用来攻击网络上的路由器和主机。例如, 可以利用操作系统规定的ICMP数据包最大尺寸不超过64KB这一规定, 向主机发起Ping of Death (死亡之Ping) 攻击。

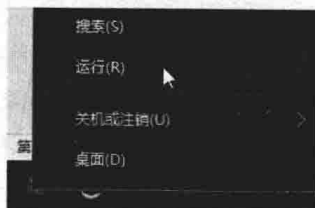
## 1.3 计算机基本信息的获取

一台计算机的基本信息包括IP地址、物理地址、端口信息、系统进程信息、注册表信息等各种系统信息, 用户要想提高计算机的安全系数, 必须要学会查看计算机基本信息的方法。

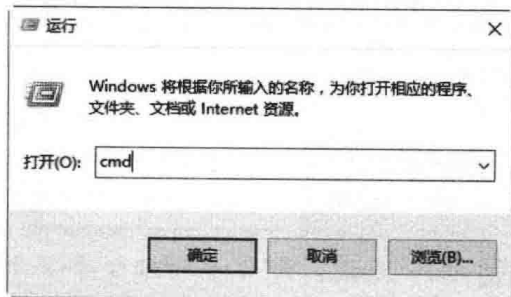
### 实战1: 获取本机的IP地址

在互联网中, 一台主机只有一个IP地址, 因此, 黑客要想攻击某台主机, 必须找到这台主机的IP地址, 然后才能进行入侵攻击, 可以说IP地址是黑客实施入侵攻击的一个关键。使用ipconfig命令可以获取本地计算机的IP地址, 具体的操作步骤如下。

**Step 01** 右击“开始”按钮, 在弹出的快捷菜单中执行“运行”命令, 如下图所示。



**Step 02** 打开“运行”对话框, 在“打开”文本框中输入cmd命令, 如下图所示。



**Step 03** 单击“确定”按钮, 打开“命令提示符”窗口, 在“命令提示符”窗口中输入



ipconfig, 按Enter键, 即可显示出本机的IP配置相关信息。

**提示:** 在“命令提示符”窗口中, 192.168.0.130表示本机在局域网中的IP地址。

### 实战2: 获取本机的物理地址

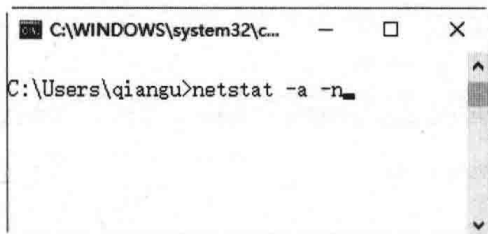
在“命令提示符”窗口中输入ipconfig /all命令, 然后按Enter键, 可以在显示的结果中看到物理地址: 00-23-24-DA-43-8B, 这就是本机的物理地址, 也是本机的网卡地址, 它是唯一的。



### 实战3: 查看系统开放的端口

经常查看系统开放端口的状态变化, 可以帮助计算机用户及时维护系统安全, 防止黑客通过端口入侵计算机。用户可以使用netstat命令查看自己系统端口状态。具体的操作步骤如下。

**Step 01** 打开“命令提示符”窗口, 在其中输入netstat -a -n命令, 如下图所示。



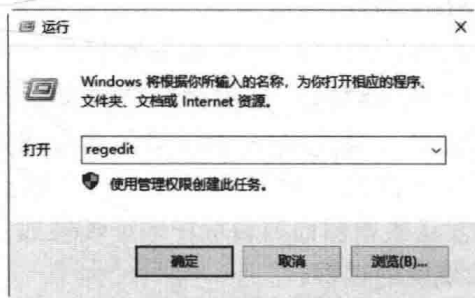
**Step 02** 按Enter键, 即可看到以数字显示的TCP和UCP连接的端口号及其状态, 如下图所示。



### 实战4: 查看系统注册表信息

注册表 (Registry) 是Microsoft Windows中的一个重要数据库, 用于存储系统和应用程序的设置信息。通过注册表, 用户可以添加、删除、修改系统内的软件配置信息或硬件驱动程序。查看Windows系统中注册表信息的操作步骤如下。

**Step 01** 在Windows操作系统中选择“开始”→“运行”选项, 打开“运行”对话框, 在其中输入命令regedit, 如下图所示。



**Step 02** 单击“确定”按钮, 即可打开“注册表编辑器”窗口, 在其中查看注册表信息, 如下图所示。

