

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 与电脑安全

从新手到高手（超值版）

网络安全技术联盟 编著



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 1000分钟精品教学视频
-  超值赠送 2 教学用PPT课件
-  超值赠送 3 黑客防守工具包
-  超值赠送 4 107个黑客工具速查手册

-  超值赠送 5 160个常用黑客命令速查手册
-  超值赠送 6 180页常见故障维修手册
-  超值赠送 7 191页Windows 10系统使用和防护技巧



清华大学出版社

从新手到高手155

黑客攻防 与电脑安全

(超值版)

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17章,包括电脑安全快速入门、系统漏洞与安全的防护策略、系统入侵与远程控制的防护策略、电脑木马的防护策略、电脑病毒的防护策略、系统安全的终极防护策略、文件密码数据的防护策略、磁盘数据安全的防护策略、系统账户数据的防护策略、网络账号及密码的防护策略、网页浏览器的防护策略、移动手机的防护策略、平板电脑的防护策略、网上银行的防护策略、手机钱包的防护策略、无线蓝牙设备的防护策略、无线网络安全防护策略等内容。

另外,本书还赠送海量王牌资源,包括1000分钟精品教学视频、107个黑客工具速查手册、160个常用黑客命令速查手册、180页常见故障维修手册、191页Windows 10系统使用和防护技巧、教学用PPT课件以及随书攻防工具包,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,也可作为大、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

黑客攻防与电脑安全从新手到高手:超值版/网络安全技术联盟编著. —北京:清华大学出版社,2017
(从新手到高手)

ISBN 978-7-302-47371-8

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(2017)第124150号

责任编辑:张 敏

封面设计:杨玉兰

责任校对:徐俊伟

责任印制:沈 露

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

质量反馈:010-62772015, 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:20 字 数:503千字

版 次:2017年9月第1版 印 次:2017年9月第1次印刷

印 数:1~4000

定 价:59.80元

产品编号:074521-01

Preface

前言

随着手机、平板电脑的普及，无线网络的防范就变得尤为重要，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、移动端攻防、手机钱包等热点融入本书中。

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知识点，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1000分钟精品教学视频、107个黑客工具速查手册、160个常用黑客命令速查手册、180页常见故障维修手册、191页Windows 10系统使用和防护技巧，读者可扫描二维码获取海量王牌资源，也可联系QQ群223145261获得更多赠送资源（包括黑客防守工具包），掌握黑客防守方方面面的知识。

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，也可作为大、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编著，另外还有王莉、方秦、程木香、李小威、刘辉、刘尧、任志杰、王朵朵、王猛、王婷婷、张芳、张桐嘉、王英英、王维维、肖品等人也参与了编写工作。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，可联系QQ群223145261和作者QQ625948078，获得作者的在线指导和本书海量资源。

编者

Contents

目 录

第1章 电脑安全快速入门	1	2.1.3 常见系统漏洞类型	13
1.1 IP地址与MAC地址	1	2.2 RPC服务远程漏洞的防护策略	15
1.1.1 认识IP地址	1	2.2.1 什么是RPC服务远程漏洞	15
1.1.2 认识MAC地址	2	2.2.2 RPC服务远程漏洞入侵演示	18
1.1.3 查看IP地址	2	2.2.3 RPC服务远程漏洞的防御	18
1.1.4 查看MAC地址	3	2.3 WebDAV漏洞的防护策略	20
1.2 什么是端口	3	2.3.1 什么是WebDAV缓冲区溢出漏洞	20
1.2.1 认识端口	3	2.3.2 WebDAV缓冲区溢出漏洞入侵演示	20
1.2.2 查看系统的开放端口	3	2.3.3 WebDAV缓冲区溢出漏洞的防御	21
1.2.3 关闭不必要的端口	4	2.4 系统漏洞的防护策略	23
1.2.4 启动需要开启的端口	5	2.4.1 使用“Windows更新”及时更新系统	23
1.3 黑客常用的DOS命令	6	2.4.2 使用360安全卫士下载并安装补丁	24
1.3.1 cd命令	6	2.4.3 使用瑞星安全助手修复系统漏洞	25
1.3.2 dir命令	7	2.5 系统安全的防护策略	26
1.3.3 ping命令	7	2.5.1 使用任务管理器管理进程	26
1.3.4 net命令	9	2.5.2 卸载流氓软件	28
1.3.5 netstat命令	9	2.5.3 查杀恶意软件	29
1.3.6 tracert命令	10	2.5.4 删除上网缓存文件	30
1.4 实战演练	11	2.5.5 删除系统临时文件	31
实战演练1——使用netstat命令快速查找对方IP地址	11		
实战演练2——使用代码检查指定端口开放状态	12		
1.5 小试身手	12		
第2章 系统漏洞与安全的防护策略	13		
2.1 了解系统漏洞	13		
2.1.1 什么是系统漏洞	13		
2.1.2 系统漏洞产生的原因	13		

2.5.6 使用Windows Defender 保护系统	32	3.6 实战演练	59
2.6 实战演练	33	实战演练1——禁止访问控制 面板	59
实战演练1——使用系统工具 整理碎片	33	实战演练2——启用和关闭快 速启动功能	60
实战演练2——关闭开机时多 余的启动项目	35	3.7 小试身手	60
2.7 小试身手	35	第4章 电脑木马的防护策略	61
第3章 系统入侵与远程控制的 防护策略	36	4.1 什么是电脑木马	61
3.1 通过账号入侵系统的常用手段 ...	36	4.1.1 常见的木马类型	61
3.1.1 使用DOS命令创建隐 藏账号入侵系统	36	4.1.2 木马常用的入侵方法	61
3.1.2 在注册表中创建隐藏 账号入侵系统	37	4.2 木马常用的伪装手段	62
3.1.3 使用MT工具创建复制 账号入侵系统	39	4.2.1 伪装成可执行文件	63
3.2 抢救被账号入侵的系统	41	4.2.2 伪装成自解压文件	65
3.2.1 揪出黑客创建的隐藏 账号	41	4.2.3 将木马伪装成图片	67
3.2.2 批量关闭危险端口	42	4.3 木马的自我保护	67
3.3 通过远程控制工具入侵系统	43	4.3.1 给木马加壳	67
3.3.1 什么是远程控制	43	4.3.2 给木马加花指令	69
3.3.2 通过Windows远程桌面 实现远程控制	43	4.3.3 修改木马的入口点	70
3.4 使用RemotelyAnywhere工具入 侵系统	46	4.4 常见的木马启动方式	71
3.4.1 安装RemotelyAnywhere	46	4.4.1 利用注册表启动	71
3.4.2 连接入侵远程主机	48	4.4.2 利用系统文件启动	71
3.4.3 远程操控目标主机	49	4.4.3 利用系统启动组启动	71
3.5 远程控制的防护策略	54	4.4.4 利用系统服务启动	72
3.5.1 关闭Window远程桌面 功能	54	4.5 查询系统中的木马	72
3.5.2 开启系统的防火墙	54	4.5.1 通过启动文件检测木马 ..	72
3.5.3 使用天网防火墙防护 系统	55	4.5.2 通过进程检测木马	73
3.5.4 关闭远程注册表管理 服务	58	4.5.3 通过网络连接检测木马 ..	74
		4.6 使用木马清除软件清除木马 ...	75
		4.6.1 使用木马清除大师清除 木马	75
		4.6.2 使用木马清除专家清除 木马	77
		4.6.3 金山贝壳木马专杀清除 木马	80
		4.6.4 使用木马间谍清除工具 清除木马	82
		4.7 实战演练	84
		实战演练1——将木马伪装成 网页	84

实战演练2——在组策略中启动 木马	86	6.4 系统安全提前准备之备份	111
4.8 小试身手	87	6.4.1 使用系统工具备份 系统	111
第5章 电脑病毒的防护策略	88	6.4.2 使用系统映像备份 系统	112
5.1 认识电脑病毒	88	6.4.3 使用Ghost工具备份 系统	113
5.1.1 电脑病毒的特征和种类 ..	88	6.4.4 制作系统备份光盘	115
5.1.2 电脑病毒的工作流程	89	6.5 系统崩溃后的修复之还原	115
5.1.3 电脑中毒的途径	89	6.5.1 使用系统工具还原 系统	116
5.1.4 电脑中病毒后的表现	89	6.5.2 使用Ghost工具还原 系统	117
5.2 Windows系统病毒	89	6.5.3 使用系统映像还原 系统	118
5.2.1 PE文件病毒	90	6.6 系统崩溃后的修复之重置	119
5.2.2 VBS脚本病毒	90	6.6.1 使用命令修复系统	119
5.2.3 宏病毒	92	6.6.2 重置电脑系统	120
5.3 电子邮件病毒	93	6.7 实战演练	122
5.3.1 邮件病毒的特点	93	实战演练1——设置系统启动 密码	122
5.3.2 识别“邮件病毒”	93	实战演练2——设置虚拟内存 ..	123
5.3.3 编制邮箱病毒	93	6.8 小试身手	124
5.4 查杀电脑病毒	95	第7章 文件密码数据的防护 策略	125
5.4.1 安装杀毒软件	95	7.1 黑客常用破解文件密码的 方式	125
5.4.2 升级病毒库	96	7.1.1 利用Word Password Recovery 破解Word文档密码	125
5.4.3 设置定期杀毒	98	7.1.2 利用AOXPPR破解Word 文件密码	126
5.4.4 快速查杀病毒	98	7.1.3 利用Excel Password Recovery 破解Excel文档密码	127
5.4.5 自定义查杀病毒	100	7.1.4 利用APDFPR破解PDF 文件密码	128
5.4.6 查杀宏病毒	100	7.1.5 利用ARCHPR破解压缩 文件密码	130
5.4.7 自定义360杀毒设置	101	7.2 各类文件密码的防护策略	131
5.5 实战演练	102		
实战演练1——在Word 2016中预 防宏病毒	102		
实战演练2——在安全模式下 查杀病毒	103		
5.6 小试身手	104		
第6章 系统安全的终极防护 策略	105		
6.1 什么情况下重装系统	105		
6.2 重装前应注意事项	105		
6.3 常见系统的重装	106		
6.3.1 重装Windows 7	106		
6.3.2 重装Windows 10	108		

7.2.1	利用Word自身功能给Word文件加密	131	8.3.5	磁盘文件数据丢失后的补救	157
7.2.2	利用Excel自身功能给Excel文件加密	132	8.4	恢复丢失的数据	159
7.2.3	利用Adobe Acrobat Professional加密PDF文件	134	8.4.1	从回收站中还原	159
7.2.4	利用PDF文件加密器给PDF文件加密	136	8.4.2	清空回收站后的恢复	159
7.2.5	利用WinRAR的自加密功能加密压缩文件	137	8.4.3	使用Easy Recovery恢复数据	161
7.2.6	给文件或文件夹进行加密	138	8.4.4	使用Final Recovery恢复数据	163
7.3	使用BitLocker加密磁盘或U盘数据	139	8.4.5	使用Final Data恢复数据	164
7.3.1	启动BitLocker	139	8.4.6	使用“数据恢复大师Data Explore”恢复数据	166
7.3.2	为磁盘进行加密	140	8.4.7	格式化硬盘后的恢复	170
7.4	实战演练	141	8.5	实战演练	172
	实战演练1——利用命令隐藏数据	141		实战演练1——恢复丢失的磁盘簇	172
	实战演练2——显示文件的扩展名	142		实战演练2——还原已删除或重命名的文件	173
7.5	小试身手	143	8.6	小试身手	173
第8章 磁盘数据安全的终极防护策略			第9章 系统账户数据的防护策略		
8.1	数据丢失的原因	144	9.1	了解Windows 10的账户类型	174
8.1.1	数据丢失的原因	144	9.1.1	认识本地账户	174
8.1.2	发现数据丢失后的操作	144	9.1.2	认识Microsoft账户	174
8.2	备份磁盘各类数据	144	9.1.3	本地账户和Microsoft账户的切换	174
8.2.1	分区表数据的防护策略	145	9.2	破解管理员账户的方法	176
8.2.2	引导区数据的防护策略	145	9.2.1	强制清除管理员账户的密码	176
8.2.3	驱动程序的防护策略	147	9.2.2	绕过密码自动登录操作系统	177
8.2.4	电子邮件的防护策略	149	9.3	本地系统账户的防护策略	178
8.2.5	磁盘文件数据的防护策略	150	9.3.1	启用本地账户	178
8.3	各类数据丢失后的补救策略	153	9.3.2	更改账户类型	179
8.3.1	分区表数据丢失后的补救	153	9.3.3	设置账户密码	180
8.3.2	引导区数据丢失后的补救	153	9.3.4	设置账户名称	182
8.3.3	驱动程序数据丢失后的补救	154	9.3.5	删除用户账户	183
8.3.4	电子邮件丢失后补救	155	9.3.6	设置屏幕保护密码	184

9.3.7	创建密码恢复盘	186	10.2.2	使用流光盗取邮箱 密码	209
9.4	Microsoft账户的防护策略	187	10.2.3	重要邮箱的保护措施 ..	210
9.4.1	注册并登录Microsoft 账户	187	10.2.4	找回被盗的邮箱密码 ..	210
9.4.2	设置账户登录密码	189	10.2.5	通过邮箱设置防止 垃圾邮件	211
9.4.3	设置PIN码	189	10.3	网游账号及密码的防护策略	212
9.4.4	使用图片密码	191	10.3.1	使用盗号木马盗取 账号的防护	212
9.5	别样的系统账户数据防护 策略	192	10.3.2	使用远程控制方式 盗取账号的防护	213
9.5.1	更改系统管理员账户 名称	192	10.3.3	利用系统漏洞盗取 账号的防护	215
9.5.2	通过伪造陷阱账户保护管 理员账户	193	10.4	实战演练	216
9.5.3	限制Guest账户的操作 权限	196		实战演练1——找回被盗的 QQ账号密码	216
9.6	通过组策略提升系统账户 密码的安全	197		实战演练2——将收到的“邮 件炸弹”标记为垃圾邮件	217
9.6.1	设置账户密码的复杂性 ..	197	10.5	小试身手	218
9.6.2	开启账户锁定功能	198			
9.6.3	利用组策略设置用户 权限	200	第11章	网页浏览器的防护策略 ..	219
9.7	实战演练	201	11.1	认识网页恶意代码	219
	实战演练1——禁止Guest账户在本 系统登录	201	11.1.1	恶意代码概述	219
	实战演练2——找回Microsoft账户 的登录密码	201	11.1.2	恶意代码的特征	219
9.8	小试身手	203	11.1.3	恶意代码的传播方式 ..	219
			11.2	常见恶意网页代码及攻击 方法	219
第10章	网络账号及密码的 防护策略	204	11.2.1	启动时自动弹出对 话框和网页	219
10.1	QQ账号及密码的防护策略	204	11.2.2	利用恶意代码禁用 注册表	220
10.1.1	盗取QQ密码的方法 ..	204	11.3	恶意网页代码的预防和清除 ..	221
10.1.2	使用盗号软件盗取QQ账 号与密码	204	11.3.1	恶意网页代码的预防 ..	221
10.1.3	提升QQ安全设置	206	11.3.2	恶意网页代码的清除 ..	221
10.1.4	使用金山密保来保护 QQ号码	207	11.4	常见浏览器的攻击方式	223
10.2	邮箱账号及密码的防护策略	208	11.4.1	修改默认主页	223
10.2.1	盗取邮箱密码的 常用方法	208	11.4.2	恶意更改浏览器标 题栏	223
			11.4.3	强行修改浏览器的 右键菜单	224

11.4.4 禁用浏览器的【源】 菜单命令	226	12.2.5 经常备份手机中的 个人资料	248
11.4.5 强行修改浏览器的 首页按钮	227	12.3 实战演练	248
11.4.6 删除桌面上的浏览器 图标	228	实战演练1——使用手机交流 工作问题	248
11.5 网页浏览器的自我防护技巧 ..	229	实战演练2——iPad的白苹果 现象	249
11.5.1 提高IE的安全防护 等级	229	12.4 小试身手	249
11.5.2 清除浏览器中的表单 ..	230	第13章 平板电脑的防护策略 ..	250
11.5.3 清除浏览器的上网历 史记录	231	13.1 平板电脑的攻击手法	250
11.5.4 删除Cookie信息	231	13.2 平板电脑的防护策略	250
11.6 使用网上工具保护网页浏览器 的安全	232	13.2.1 自动升级固件	250
11.6.1 使用IE修复专家	232	13.2.2 重装系统	252
11.6.2 IE修复免疫专家	233	13.2.3 为视频加锁	252
11.6.3 IE伴侣	238	13.2.4 开启“查找我的iPad” 功能	254
11.7 实战演练	241	13.2.5 远程锁定iPad	255
实战演练1——查看加密网页 的源码	241	13.2.6 远程清除iPad中的信息 ..	256
实战演练2——屏蔽浏览器 窗口中的广告	242	13.3 实战演练	256
11.8 小试身手	243	实战演练1——给丢失的iPad 发信息	256
第12章 移动手机的防护策略 ..	244	实战演练2——丢失的iPad 在哪	257
12.1 手机的攻击手法	244	13.4 小试身手	257
12.1.1 通过网络下载	244	第14章 网上银行的防护策略 ..	258
12.1.2 利用红外线或蓝牙 传输	244	14.1 开通个人网上银行	258
12.1.3 短信与乱码传播	245	14.1.1 开通个人网上银行步骤 ..	258
12.1.4 利用手机BUG传播	245	14.1.2 注册与登录网上个人银行 ..	258
12.1.5 手机炸弹攻击	245	14.1.3 自助登录网上银行	259
12.2 移动手机的防护策略	246	14.2 账户信息与资金管理	260
12.2.1 关闭手机蓝牙功能	246	14.2.1 账户信息管理	260
12.2.2 保证手机下载的应用 程序的安全性	247	14.2.2 网上支付缴费	262
12.2.3 关闭乱码电话, 删除 怪异短信	247	14.2.3 网上转账汇款	262
12.2.4 安装手机卫士软件	248	14.2.4 网上定期存款	263
		14.3 网银安全的防护策略	263
		14.3.1 网上挂失银行卡	263
		14.3.2 避免进入钓鱼网站	264
		14.3.3 使用网银安全证书	266

14.3.4 使用过程中的安全	269	16.3.2 查看蓝牙设备相关内容 ..	286
14.4 实战演练	269	16.3.3 扫描蓝牙设备	286
实战演练1——如何在网上		16.3.4 蓝牙攻击技术	288
申请信用卡	269	16.3.5 修改蓝牙设备地址	290
实战演练2——使用网银进行		16.4 蓝牙DoS攻击技术	290
网上购物	270	16.4.1 关于蓝牙DoS	290
14.5 小试身手	273	16.4.2 蓝牙DoS攻击演示	290
第15章 手机钱包的防护策略 ...	274	16.5 安全防护及改进	292
15.1 手机钱包的攻击手法	274	16.6 实战演练	294
15.1.1 手机病毒	274	实战演练1——蓝牙bluebuging	
15.1.2 盗取手机	274	攻击技术	294
15.2 手机钱包的防护策略	274	实战演练2——蓝牙DoS测试	
15.2.1 手机盗号病毒的防范 ..	274	问题	297
15.2.2 手机丢失后的手机		16.7 小试身手	297
钱包的防范	275	第17章 无线网络安全防护策略 ...	298
15.2.3 强化手机钱包的支付		17.1 组建无线网络	298
密码	275	17.1.1 搭建无线局域网环境 ..	298
15.3 实战演练	276	17.1.2 配置无线局域网	298
实战演练1——手机钱包		17.1.3 将电脑接入无线网	299
如何开通	276	17.1.4 将手机接入WiFi	300
实战演练2——手机钱包		17.2 电脑和手机共享无线上网	301
如何充值	276	17.2.1 手机共享电脑的网络 ..	301
15.4 小试身手	276	17.2.2 电脑共享手机的网络 ..	302
第16章 无线蓝牙设备的防护策略 ...	277	17.2.3 加密手机的WLAN热	
16.1 了解蓝牙	277	点功能	303
16.1.1 什么是蓝牙	277	17.3 无线网络的安全策略	303
16.1.2 蓝牙技术体系及相关术语 ..	278	17.3.1 设置管理员密码	303
16.1.3 蓝牙适配器的选择	280	17.3.2 修改WiFi名称	304
16.2 蓝牙设备的配对操作	281	17.3.3 无线网络WEP加密	304
16.2.1 蓝牙(驱动)工具安装 ..	281	17.3.4 WPA-PSK安全加密算法 ..	305
16.2.2 启用蓝牙适配器	282	17.3.5 禁用SSID广播	306
16.2.3 搜索开启蓝牙功能的设备 ..	283	17.3.6 媒体访问控制(MAC)	
16.2.4 使用蓝牙适配器进行		地址过滤	307
设备间配对	284	17.4 实战演练	308
16.2.5 使用耳机建立通信		实战演练1——控制无线网中	
并查看效果	284	设备的上网速度	308
16.3 蓝牙基本Hacking技术	285	实战演练2——诊断和修复网	
16.3.1 识别及激活蓝牙设备 ..	285	络不通的问题	309
		17.5 小试身手	309

第1章 电脑安全快速入门

作为计算机或网络终端设备的用户，要想使自己的设备不受或少受黑客的攻击，就必须了解一些黑客常用的入侵技能以及学习一些计算机安全方面的基础知识，本章将介绍有关这方面的知识，如什么是端口、IP地址以及黑客常用的攻击命令等。

1.1 IP地址与MAC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。

1.1.1 认识IP地址

IP地址用于在TCP/IP通信协议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）。

一个完整的IP地址由两部分组成，分别是网络号部分和主机号部分。网络号表示其所属的网络段编号，主机号则表示该网段中该主机的地址编号。

按照网络规模的大小，IP地址可以分为A、B、C、D、E5类，其中A、B、C类是3种主要的类型地址，D类专供多目传送地址，E类用于扩展备用地址。

- A类IP地址。一个A类IP地址由1个字节的网络地址和3个字节的主机地址组成，网络地址的最高位必须是“0”，地址范围从1.0.0.0 ~ 126.0.0.0。
- B类IP地址。一个B类IP地址由2个字节的网络地址和2个字节的主机地址组成，网络地址的最高

位必须是“10”，地址范围从128.0.0.0~191.255.255.255。

- C类IP地址。一个C类IP地址由3个字节的网络地址和1个字节的主机地址组成，网络地址的最高位必须是“110”。地址范围从192.0.0.0~223.255.255.255。
- D类IP地址。用于多点广播（Multicast）。D类IP地址第一个字节以“10”开始，它是一个专门保留的地址。它并不指向特定的网络，目前这一类地址被用在多点广播（Multicast）中。多点广播地址用来一次寻址一组计算机，它标识共享同一协议的一组计算机。
- E类IP地址。以“10”开始，为将来使用保留，全“0”（0.0.0.0）IP地址对应于当前主机；全“1”的IP地址（255.255.255.255）是当前子网的广播地址。

具体来讲，一个完整的IP地址信息应该包括IP地址、子网掩码、默认网关和DNS等4部分。只有这4部分协同工作，才能与互联网中的计算机相互访问。

- 子网掩码：子网掩码是与IP地址结合使用的一种技术。主要作用有两个：一是用于确定IP地址中的网络号和主机号；二是用于将一个大的IP网络划分为若干小的子网络。

- 默认网关：默认网关意为一台主机如果找不到可用的网关，就把数据包发送给默认指定的网关，由这个网关来处理数据包。
- DNS：DNS服务用于将用户的域名请求转换为IP地址。

1.1.2 认识MAC地址

MAC地址是在媒体接入层上使用的地址，也称为物理地址、硬件地址或链路地址，由网络设备制造商生产时写在硬件内部。MAC地址与网络无关，也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，MAC地址都是相同的，它由厂商写在网卡的BIOS里。

MAC地址通常表示为12个十六进制数，每2个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3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。

知识链接

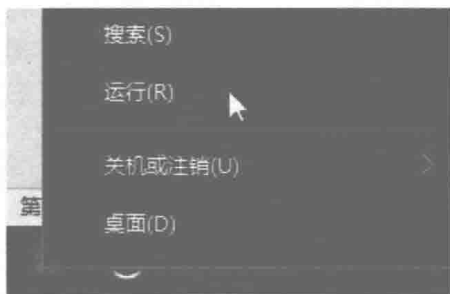
IP地址与MAC地址的区别在于：IP地址基于逻辑，比较灵活，不受硬件限制，也容易记忆。MAC地址在一定程度上与硬件一致，基于物理，能够具体标识。这两种地址均有各自的长处，使用时也因条件不同而采取不同的地址。

1.1.3 查看IP地址

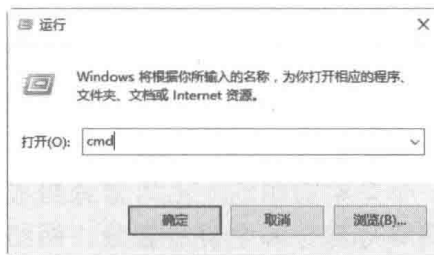
计算机的IP地址一旦被分配，可以说是固定不变的，因此，查询出计算机的IP地址，在一定程度上就实现了黑客入侵的前提工作。使用ipconfig命令可以获取本地计算机的IP地址和物理地址。

具体的操作步骤如下。

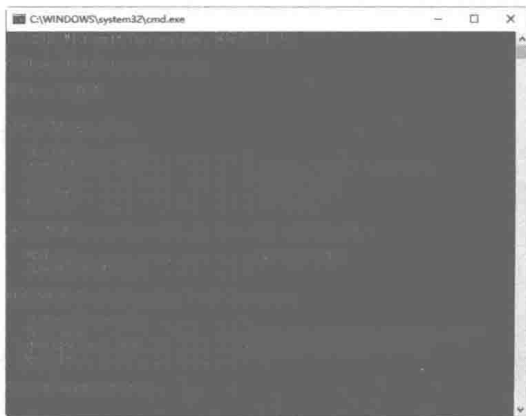
Step 01 右击【开始】按钮，在弹出的快捷菜单中执行【运行】命令。



Step 02 打开【运行】对话框，在【打开】后面的文本框中输入cmd命令。



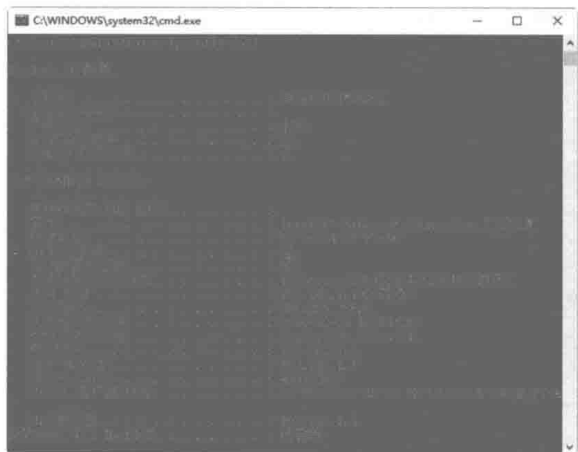
Step 03 单击【确定】按钮，打开【命令提示符】窗口，在【命令提示符】窗口中输入ipconfig，按Enter键，即可显示出本机的IP配置相关的信息。



 **提示：**在【命令提示符】窗口中，192.168.0.102表示本机在局域网中的IP地址。

1.1.4 查看MAC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一个物理地址：6C-0B-84-3E-F7-AB，这就是用户自己的计算机的网卡地址，它是唯一的。

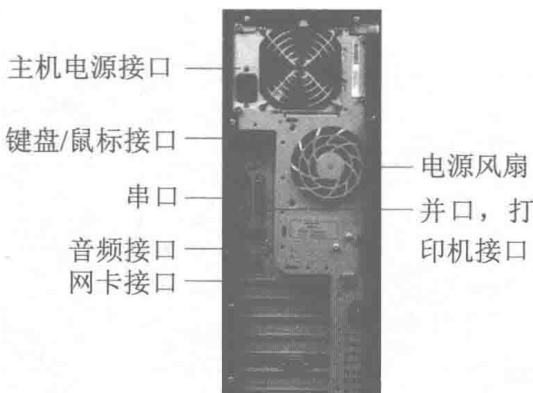


1.2 什么是端口

“端口”可以认为是计算机与外界通信交流的出口。一个IP地址的端口可以有65 536（即 256×256 ）个，端口是通过端口号来标记的，端口号只有整数，范围是0~65 535（ $256 \times 256 - 1$ ）。

1.2.1 认识端口

计算机领域可分为硬件领域和软件领域，在硬件领域中，端口又被称作为接口，如常见的USB端口、网卡接口、串行端口等；在软件领域中，端口一般是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（基本输入输出）缓冲区。



在网络技术中，端口又有几种含义：其中，一种是物理意义上的端口，如集线器、交换机、路由器等连接设备，用于连接其他的网络设备的接口，常见的有RJ-45端口、Serial端口等；另一种是逻辑意义上的端口，一般指TCP/IP协议中的端口，范围是0~65 535（ $256 \times 256 - 1$ ）。

1.2.2 查看系统的开放端口

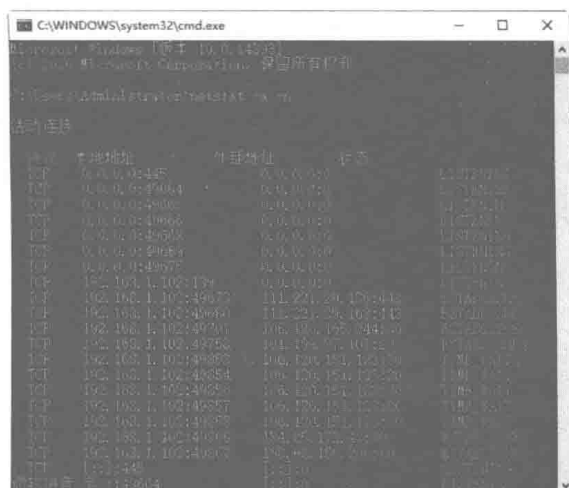
经常查看系统开放端口的状态变化，可以帮助计算机用户及时提高系统安全，防止黑客通过端口入侵电脑，用户可以使用netstat命令查看自己系统的端口的状态。

具体操作步骤如下。

Step 01 打开【命令提示符】窗口，在其中输入netstat -a -n命令。



Step 02 按Enter键，即可看到以数字显示的TCP和UDP连接的端口号及其状态。

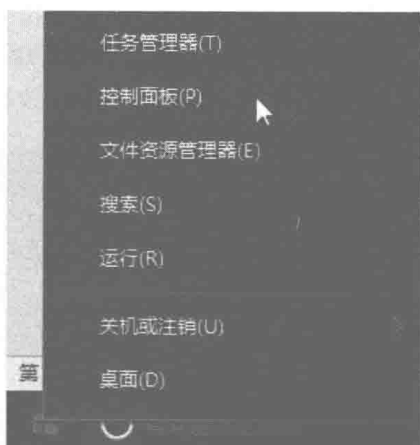


1.2.3 关闭不必要的端口

默认情况下, 计算机系统中有许多没有用或不安全的端口是开启的, 这些端口很容易被黑客利用。为保障系统的安全, 可以将这些不用的端口关闭。关闭端口的方式有多种, 这里介绍通过关闭无用服务来关闭不必要的端口。

以关闭Remote Desktop Help Session Manager (Windows远程协助服务) 为例, 具体操作步骤如下。

Step 01 右击【开始】按钮, 在弹出的快捷菜单中执行【控制面板】命令。



Step 02 打开【控制面板】窗口, 双击【管理工具】图标。

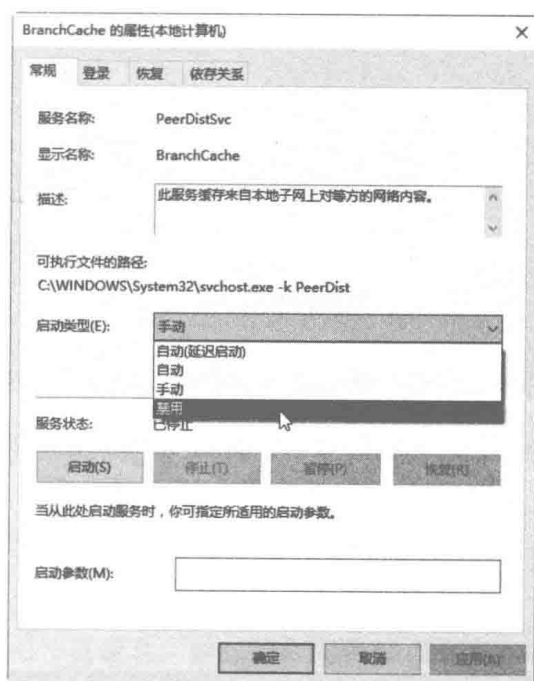
Step 03 打开【管理工具】窗口, 双击【服务】图标。



Step 04 打开【服务】窗口, 找到Branch Cache服务项。



Step 05 双击该服务项, 弹出【Branch Cache的属性】对话框, 在【启动类型】下拉列表中选择【禁用】选项, 然后单击【确定】按钮禁用该服务项的端口。



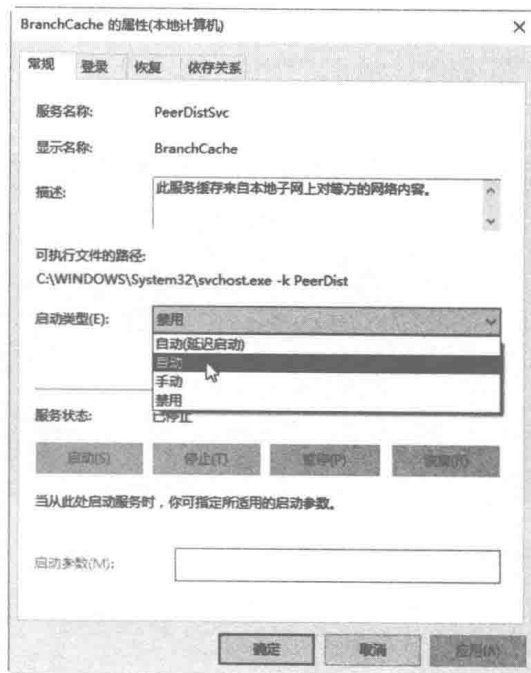
Step 02 单击【应用】按钮，激活“服务状态”下的【启动】按钮。



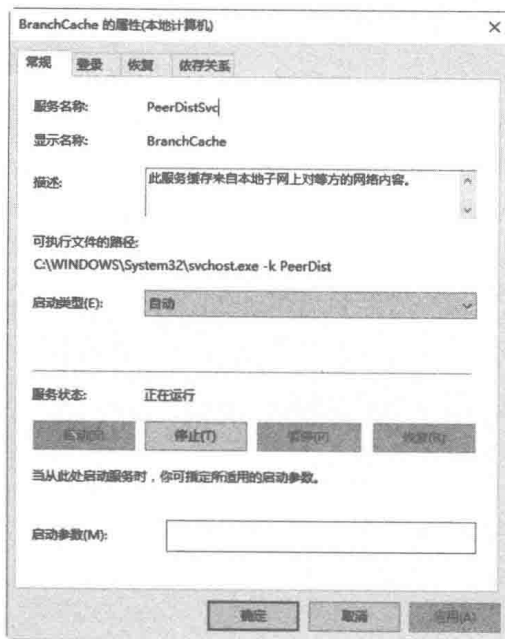
1.2.4 启动需要开启的端口

开启端口的操作与关闭端口的操作类似，下面具体介绍通过启动服务的方式开启端口的具体操作步骤。

Step 01 这里以上述停止的Branch Cache服务端口为例。在【Branch Cache的属性】对话框中单击【启动类型】右侧的下拉按钮，在打开的下拉菜单中选择【自动】。



Step 03 单击【启动】按钮，即可启动该项服务，再次单击【应用】按钮，在【Branch Cache的属性】对话框中可以看到该服务的【服务状态】已经变为【正在运行】。



Step 04 单击【确定】按钮，返回【服务】窗口，此时即可发现Branch Cache服务的【状态】变为【正在运行】，这样就可以成功开启Branch Cache服务对应的端口。



1.3 黑客常用的DOS命令

熟练掌握一些DOS命令是一名黑客的基本功，下面就来介绍黑客常用的一些DOS命令，了解这样命令可以帮助计算机用户追踪黑客的踪迹，从而提高个人计算机的安全性。

1.3.1 cd命令

cd（Change Directory）命令的作用是改变当前目录，该命令用于切换路径目录。

cd命令主要有以下3种使用方法。

（1）cd path：path是路径，例如输入cd c:\命令后按Enter键或输入cd Windows命令，即可分别切换到C:\和C:\Windows目录下。

（2）cd..：cd后面的两个“.”表示返回上一级目录，例如当前的目录为C:\Windows，如果输入cd..命令，按Enter键即可返回上一级目录，即C:\。

（3）cd\：表示当前无论在哪个子目录下，通过该命令可立即返回到根目录下。

下面将介绍使用cd命令进入C:\Windows\system32子目录，并退回根目录的具体操作步骤。

Step 01 在【命令提示符】窗口中输入cd c:\命令，按Enter键，即可将目录切换为C:\。



Step 02 如果想进入C:\Windows\system32目录中，则需在上面的【命令提示符】窗口中输入cd Windows\system32命令，按Enter键即可将目录切换为C:\Windows\system32。



Step 03 如果想返回上一级目录，则可以在【命令提示符】窗口中输入cd..命令，按Enter键即可。



Step 04 如果想返回到根目录，则可以在【命令提示符】窗口中输入cd\命令，按Enter键即可。