

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

(微视频+火力升级版)

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

214节同步微视频



超值
赠送

2

精美教学PPT课件



超值
赠送

3

黑客工具(107个)速查电子书



超值
赠送

4

常用黑客命令(160个)速查电子书



超值
赠送

5

常见故障维修电子书



超值
赠送

6

Windows 10系统使用和防护技巧电子书



超值
赠送

7

8大经典密码破解工具电子书



超值
赠送

8

加密与解密技术快速入门电子书



超值
赠送

9

网站入侵与黑客脚本编程电子书



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 与电脑安全

从新手到高手

(微视频+火力升级版)

网络安全技术联盟 编著

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,电脑系统漏洞的防护策略,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,电脑系统安全的防护策略,电脑系统账户的防护策略,磁盘数据安全的防护策略,文件密码数据的防护策略,网络账号及密码的防护策略,网页浏览器的防护策略,移动手机的安全防护策略,平板电脑的安全防护策略,网上银行的安全防护策略,手机钱包的安全防护策略,无线蓝牙设备的安全防护策略,无线网络安全的防护策略等内容。

本书赠送的微视频,读者可直接在书中扫码观看。另外,本书还赠送其他王牌资源,帮助读者掌握黑客防守方方面面的知识。由于赠送资源比较多,我们在本书前言部分对资源项做了详细说明。

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:微视频+火力升级版/网络安全技术联盟编著. —北京:清华大学出版社,2019

(从新手到高手)

ISBN 978-7-302-52590-5

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044611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

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:19.75

字 数:495千字

版 次:2019年6月第1版

印 次:2019年6月第1次印刷

定 价:69.80元

Preface

前言

随着手机、平板电脑的普及，无线网络的安全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、手机钱包等热点问题融入本书中。

本书特色

知识丰富全面：涵盖了所有黑客攻防知识点，由浅入深地介绍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便于读者在学习过程中直观、清晰地看到操作的过程及效果，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

本书除赠送214节同步微视频外，还赠送精美教学PPT课件，黑客工具（107个）速查电子书，常用黑客命令（160个）速查电子书，常见故障维修电子书，Windows 10系统使用和防护技巧电子书，8大经典密码破解工具电子书，加密与解密技术快速入门电子书，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至zhangmin2@tup.tsinghua.edu.cn获取PPT课件和电子书。



PPT课件



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，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组织编写，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、皮素芹等人参与了编写工作。在编写过程中，虽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。若您在学习过程中遇到困难或疑问，或有何建议，可通过电子邮件至zhangmin2@tup.tsinghua.edu.cn与我们联系。

编者

Contents

目 录

第1章 电脑安全快速入门	1	2.1.1 什么是系统漏洞	12
1.1 IP地址与MAC地址	1	2.1.2 系统漏洞产生的原因	12
1.1.1 认识IP地址	1	2.2 系统漏洞评分标准——CVSS	12
1.1.2 认识MAC地址	2	2.2.1 CVSS简介	12
1.1.3 查看IP地址	2	2.2.2 CVSS计算方法	13
1.1.4 查看MAC地址	2	2.3 RPC服务远程漏洞的防护策略	13
1.2 什么是端口	3	2.3.1 什么是RPC服务远程漏洞	14
1.2.1 认识端口	3	2.3.2 RPC服务远程漏洞入侵演示	16
1.2.2 查看系统的开放端口	3	2.3.3 RPC服务远程漏洞的防御	17
1.2.3 关闭不必要的端口	4	2.4 WebDAV漏洞的防护策略	18
1.2.4 启动需要开启的端口	4	2.4.1 什么是WebDAV缓冲区溢出漏洞	18
1.3 黑客常用的DOS命令	5	2.4.2 WebDAV缓冲区溢出漏洞入侵演示	18
1.3.1 cd命令	5	2.4.3 WebDAV缓冲区溢出漏洞的防御	19
1.3.2 dir命令	6	2.5 系统漏洞的防护策略	21
1.3.3 ping命令	7	2.5.1 使用“Windows更新”及时更新系统	21
1.3.4 net命令	8	2.5.2 使用《360安全卫士》下载并安装补丁	22
1.3.5 netstat命令	8	2.6 实战演练	23
1.3.6 tracert命令	9	实战演练1——使用系统工具整理磁盘碎片	23
1.4 实战演练	9	实战演练2——关闭开机时的多余启动项	25
实战演练1——自定义“命令提示符”窗口的显示效果	9		
实战演练2——使用shutdown命令实现定时关机	10		
1.5 小试身手	11		
练习1：快速锁定Windows桌面	11		
练习2：隐藏桌面搜索框	11		
第2章 电脑系统漏洞的防护策略	12		
2.1 系统漏洞概述	12		

2.7 小试身手	25	实战演练2——启用和关闭快速启动功能	46
练习1: 怎样用左手操作键盘	25	3.7 小试身手	47
练习2: 将应用程序固定到任务栏	26	练习1: 开启系统“上帝模式”	47
第3章 系统入侵与远程控制的防护策略	27	练习2: 开启系统“平板模式”	47
3.1 通过账号入侵系统的常用手段	27	第4章 电脑木马的防护策略	48
3.1.1 使用DOS命令创建隐藏账号	27	4.1 什么是电脑木马	48
3.1.2 在注册表中创建隐藏账号	28	4.1.1 常见的木马类型	48
3.2 抢救被账号入侵的系统	30	4.1.2 木马常用的入侵方法	49
3.2.1 揪出黑客创建的隐藏账号	30	4.2 木马常用的伪装手段	50
3.2.2 批量关闭系统危险端口	31	4.2.1 伪装成可执行文件	50
3.3 通过远程控制工具入侵系统	32	4.2.2 伪装成自解压文件	52
3.3.1 什么是远程控制	32	4.2.3 将木马伪装成图片	54
3.3.2 通过Windows远程桌面实现远程控制	33	4.2.4 将木马伪装成网页	54
3.4 使用RemotelyAnywhere工具入侵系统	35	4.3 木马的自我保护	56
3.4.1 安装RemotelyAnywhere	35	4.3.1 给木马加壳	56
3.4.2 连接入侵远程主机	37	4.3.2 给木马加花指令	58
3.4.3 远程操控目标主机	38	4.3.3 修改木马的入口点	58
3.5 远程控制的防护策略	43	4.4 木马常见的启动方式	59
3.5.1 关闭Windows远程桌面功能	43	4.4.1 利用注册表启动	59
3.5.2 开启系统的防火墙	43	4.4.2 利用系统文件启动	59
3.5.3 关闭远程注册表管理服务	44	4.4.3 利用系统启动组启动	60
3.6 实战演练	45	4.4.4 利用系统服务启动	60
实战演练1——禁止访问控制面板	45	4.4.5 利用系统组策略启动	61
		4.5 查询系统中的木马	62
		4.5.1 通过启动文件检测木马	62
		4.5.2 通过进程检测木马	62
		4.5.3 通过网络连接检测木马	64
		4.6 使用木马清除软件清除木马	65
		4.6.1 使用金山《贝壳木马专杀》软件清除木马	65
		4.6.2 使用木马间谍清除工具清除木马	66
		4.7 实战演练	68
		实战演练1——在任务管理器中结束木马进程	68

实战演练2——使用Windows Defender保护系统	70	6.1 系统安全之清理间谍软件	91
4.8 小试身手	71	6.1.1 使用“事件查看器”清理	91
练习1: 删除上网缓存文件	71	6.1.2 使用《反间谍专家》清理	93
练习2: 清除系统临时文件	72	6.1.3 使用《Windows清理助手》清理	96
第5章 电脑病毒的防护策略	74	6.1.4 使用Spybot-Search&Destroy清理	98
5.1 认识电脑病毒	74	6.2 重装Windows 10操作系统	100
5.1.1 电脑病毒的特征和种类	74	6.2.1 什么情况下重装系统	100
5.1.2 电脑病毒的工作流程	75	6.2.2 重装前应注意事项	100
5.1.3 电脑中毒的途径	75	6.2.3 使用安装光盘重装Windows 10	101
5.1.4 电脑中病毒后的表现	75	6.3 系统安全提前准备之备份	104
5.2 查杀电脑病毒	75	6.3.1 使用系统工具备份系统	104
5.2.1 安装杀毒软件	76	6.3.2 使用系统映像备份系统	105
5.2.2 升级病毒库	76	6.3.3 使用Ghost工具备份系统	107
5.2.3 设置定期杀毒	78	6.4 系统崩溃后的修复之还原	108
5.2.4 快速查杀病毒	78	6.4.1 使用系统工具还原系统	108
5.2.5 自定义查杀病毒	80	6.4.2 使用Ghost工具还原系统	109
5.2.6 查杀宏病毒	80	6.4.3 使用系统映像还原系统	110
5.2.7 自定义《360杀毒》软件设置	81	6.5 系统崩溃后的修复之重置	111
5.3 使用病毒专杀工具查杀病毒	82	6.5.1 在可开机情况下重置电脑	111
5.3.1 查杀异鬼病毒	82	6.5.2 在不可开机情况下重置电脑	112
5.3.2 查杀CAD病毒	83	6.6 实战演练	113
5.3.3 查杀顽固病毒	84	实战演练1——设置系统启动密码	113
5.3.4 查杀U盘病毒	85		
5.4 实战演练	87		
实战演练1——在Word中预防宏病毒	87		
实战演练2——在安全模式下查杀病毒	88		
5.5 小试身手	89		
练习1: 使用命令修复系统错误	89		
练习2: 设置默认打开应用程序	89		
第6章 电脑系统安全的防护策略	91		

实战演练2——设置虚拟内存的大小	114
6.7 小试身手	115
练习1: 制作系统备份光盘	115
练习2: 给系统盘“瘦身”	116
第7章 电脑系统账户的防护策略	118
7.1 了解Windows 10的账户类型	118
7.1.1 认识本地账户	118
7.1.2 认识Microsoft账户	118
7.1.3 本地账户和Microsoft账户的切换	118
7.2 破解管理员账户的方法	120
7.2.1 强制清除管理员账户密码	120
7.2.2 绕过密码自动登录操作系统	121
7.3 本地系统账户的防护策略	121
7.3.1 启用本地账户	122
7.3.2 更改账户类型	123
7.3.3 设置账户密码	123
7.3.4 设置账户名称	126
7.3.5 删除用户账户	127
7.3.6 创建密码恢复盘	128
7.4 Microsoft账户的防护策略	129
7.4.1 注册并登录Microsoft账户	129
7.4.2 设置账户登录密码	130
7.4.3 设置PIN密码	131
7.4.4 使用图片密码	133
7.5 别样的系统账户数据防护策略	134
7.5.1 更改系统管理员账户名称	134
7.5.2 通过伪造陷阱账户保护管理员账户	135

7.5.3 限制Guest账户的操作权限	137
7.6 通过组策略提升系统账户密码的安全	138
7.6.1 设置账户密码的复杂性	138
7.6.2 开启账户锁定功能	139
7.6.3 利用组策略设置用户权限	141
7.7 实战演练	141
实战演练1——禁止Guest账户在本系统登录	141
实战演练2——找回Microsoft账户的登录密码	142
7.8 小试身手	143
练习1: 取消Windows开机密码	143
练习2: 设置屏幕保护密码	144
第8章 磁盘数据安全的防护策略	146
8.1 数据丢失的原因和注意事项	146
8.1.1 数据丢失的原因	146
8.1.2 发现数据丢失后的注意事项	146
8.2 备份磁盘各类数据	146
8.2.1 分区表数据的备份	147
8.2.2 驱动程序的修复与备份	147
8.2.3 磁盘文件数据的备份	149
8.3 还原磁盘各类数据	151
8.3.1 还原分区表数据	151
8.3.2 还原驱动程序数据	152
8.3.3 还原磁盘文件数据	153
8.4 恢复丢失的磁盘数据	155
8.4.1 从回收站中还原	155

8.4.2	清空回收站后的恢复	156	9.4	实战演练	183
8.4.3	使用EasyRecovery恢复数据	157		实战演练1——使用命令隐藏数据	183
8.4.4	使用FinalRecovery恢复数据	159		实战演练2——显示文件的扩展名	184
8.4.5	使用FinalData恢复数据	160	9.5	小试身手	185
8.4.6	使用《DataExplore数据恢复大师》恢复数据	162		练习1：限制编辑Word文档	185
8.5	实战演练	166		练习2：将文档上传至OneDrive	186
	实战演练1——恢复丢失的磁盘簇	166			
	实战演练2——格式化硬盘后的数据恢复	166			
8.6	小试身手	168			
	练习1：隐藏/显示磁盘文件或文件夹	168			
	练习2：添加常用文件夹到“开始”菜单	169			
第9章 文件密码数据的防护策略			第10章 网络账号及密码的防护策略		
		171			187
9.1	破解文件密码的常用方式	171	10.1	QQ账号及密码的防护策略	187
9.1.1	破解Word文档密码	171	10.1.1	盗取QQ密码的方法	187
9.1.2	破解Excel文件密码	172	10.1.2	使用盗号软件盗取QQ账号与密码	187
9.1.3	破解PDF文件密码	173	10.1.3	提升QQ账号的安全设置	189
9.1.4	破解压缩文件密码	174	10.1.4	使用《金山密保》来保护QQ号码	190
9.2	各类文件密码的防护策略	175	10.2	邮箱账号及密码的防护策略	191
9.2.1	加密Word文档	175	10.2.1	盗取邮箱密码的常用方法	191
9.2.2	加密/解密Excel文件	176	10.2.2	使用《流光》盗取邮箱密码	191
9.2.3	加密PDF文件	178	10.2.3	重要邮箱的保护措施	192
9.2.4	加密压缩文件	179	10.2.4	找回被盗的邮箱密码	193
9.2.5	加密文件或文件夹	180	10.2.5	通过邮箱设置防止垃圾邮件	194
9.3	使用BitLocker加密磁盘或U盘数据	181	10.3	网游账号及密码的防护策略	194
9.3.1	启动BitLocker	181	10.3.1	使用盗号木马盗取账号的防护	195
9.3.2	为磁盘进行加密	182	10.3.2	使用远程控制方式盗取账号的防护	195

10.3.3	利用系统漏洞盗取账号的防护	197
10.4	实战演练	198
	实战演练1——找回被盗的QQ	
	账号密码	198
	实战演练2——将收到的“邮件炸弹”标记为垃圾邮件	199
10.5	小试身手	200
	练习1: 通过向导备份电子邮件	200
	练习2: 使用向导还原电子邮件	201
第11章 网页浏览器的防护策略		
11.1	认识网页恶意代码	203
11.1.1	恶意代码概述	203
11.1.2	恶意代码的特征	203
11.1.3	恶意代码的传播方式	203
11.2	常见网页恶意代码及攻击方法	203
11.2.1	启动时自动弹出对话框和网页	203
11.2.2	利用恶意代码禁用注册表	204
11.3	网页恶意代码的预防和清除	205
11.3.1	网页恶意代码的预防	205
11.3.2	网页恶意代码的清除	205
11.4	常见网页浏览器的攻击方式	207
11.4.1	修改默认主页	207
11.4.2	恶意更改浏览器标题栏	207

11.4.3	强行修改网页浏览器的右键菜单	208
11.4.4	禁用网页浏览器的“源”菜单命令	209
11.4.5	强行修改浏览器的首页按钮	211
11.4.6	删除桌面上的浏览器图标	212
11.5	网页浏览器的自我防护技巧	213
11.5.1	提高IE的安全防护等级	213
11.5.2	清除浏览器中的表单	214
11.5.3	清除浏览器的上网历史记录	214
11.5.4	删除Cookie信息	215
11.6	使用其他工具保护网页浏览器的安全	216
11.6.1	使用《IE修复专家》	216
11.6.2	使用《IE修复免疫专家》	216
11.6.3	使用《IE伴侣》	221
11.7	实战演练	225
	实战演练1——查看加密网页的源码	225
	实战演练2——屏蔽浏览器窗口中的广告	226
11.8	小试身手	226
	练习1: 使用地址栏进行关键词搜索	226
	练习2: 清除Microsoft Edge中的浏览数据	227

第12章 移动手机的安全防护策略	
12.1	手机的攻击手法

12.1.1	通过网络下载	228
12.1.2	利用红外线或蓝牙 传输	228
12.1.3	短信与乱码传播	229
12.1.4	利用手机BUG传播	229
12.2	手机的防护策略	229
12.2.1	关闭手机蓝牙功能	230
12.2.2	保证手机下载应用 程序的安全性	230
12.2.3	关闭乱码电话，删除 怪异短信	230
12.2.4	安装手机卫士软件	231
12.2.5	经常备份手机中的个人 资料	231
12.3	实战演练	232
	实战演练1——使用手机交流 工作问题	232
	实战演练2——使用《手机管家》 查杀手机病毒	232
12.4	小试身手	233
	练习1：使用手机QQ传输 文件	233
	练习2：使用手机邮箱发送办公 文档	233

第13章 平板电脑的安全防护

	策略	235
13.1	平板电脑的攻击手法	235
13.2	平板电脑的防护策略	235
13.2.1	自动升级iPad固件	235
13.2.2	重装iPad系统	237
13.2.3	为视频加锁	238
13.2.4	开启“查找我的iPad” 功能	239
13.2.5	远程锁定iPad	240
13.3	实战演练	241

	实战演练1——给丢失的iPad发 信息	241
	实战演练2——丢失的iPad 在哪	242
13.4	小试身手	242
	练习1：修复iPad的白苹果 现象	242
	练习2：远程清除iPad中的 信息	243

第14章 网上银行的安全防护

	策略	244
14.1	开通个人网上银行	244
14.1.1	开通个人网上银行的 步骤	244
14.1.2	注册网上个人银行	244
14.1.3	自助登录网上银行	245
14.2	账户信息与资金管理	246
14.2.1	账户信息管理	246
14.2.2	网上支付缴费	248
14.2.3	网上转账汇款	248
14.3	网银安全的防护策略	249
14.3.1	网上挂失银行卡	249
14.3.2	避免进入钓鱼网站	249
14.3.3	使用网银安全证书	252
14.3.4	使用过程中的安全	254
14.4	实战演练	255
	实战演练1——如何网上申请 信用卡	255
	实战演练2——使用网银进行 网上购物	256
14.5	小试身手	258
	练习1：设置手机短信认证的 最低限额	258
	练习2：开通银行账户余额变动 提醒	258

第15章 手机钱包的安全防护

策略 260

- 15.1 手机钱包的攻击手法 260
 - 15.1.1 手机病毒 260
 - 15.1.2 盗取手机 260
- 15.2 手机钱包的防护策略 260
 - 15.2.1 手机盗号病毒的防范 ... 260
 - 15.2.2 手机丢失后手机钱包的
防范 261
 - 15.2.3 强健手机钱包的支付
密码 261
 - 15.2.4 微信手机钱包的安全
设置 262
- 15.3 实战演练 263
 - 实战演练1——手机钱包如何
开通 263
 - 实战演练2——手机钱包如何
充值 263
- 15.4 小试身手 264
 - 练习1: 使用微信手机钱包
转账 264
 - 练习2: 使用手机钱包给手机
充值 265

第16章 无线蓝牙设备的安全防护

策略 267

- 16.1 了解蓝牙 267
 - 16.1.1 什么是蓝牙 267
 - 16.1.2 蓝牙适配器的选择 268
- 16.2 蓝牙设备的配对操作 269
 - 16.2.1 蓝牙（驱动）工具
安装 269
 - 16.2.2 启用蓝牙适配器 270
 - 16.2.3 搜索开启蓝牙功能的
设备 271
 - 16.2.4 使用蓝牙适配器进行设备
间配对 272

- 16.3 蓝牙基本Hacking技术 273
 - 16.3.1 识别及激活蓝牙设备 ... 273
 - 16.3.2 查看蓝牙设备相关
内容 273
 - 16.3.3 扫描蓝牙设备 274
 - 16.3.4 蓝牙攻击技术 276
- 16.4 蓝牙DoS攻击技术 277
 - 16.4.1 关于蓝牙DoS攻击 277
 - 16.4.2 蓝牙DoS攻击演示 277
- 16.5 安全防护及改进 279
- 16.6 实战演练 280
 - 实战演练1——蓝牙bluebugging
攻击技术 280
 - 实战演练2——蓝牙DoS测试
问题 283
- 16.7 小试身手 284
 - 练习1: 修改蓝牙设备地址 284
 - 练习2: 使用耳机建立通信 284

第17章 无线网络安全的防护

策略 286

- 17.1 组建无线网络 286
 - 17.1.1 搭建无线局域网环境 ... 286
 - 17.1.2 配置无线局域网 286
 - 17.1.3 将电脑接入无线网 287
 - 17.1.4 将手机接入WiFi 288
- 17.2 电脑和手机共享无线上网 289
 - 17.2.1 手机共享电脑的网络 ... 289
 - 17.2.2 电脑共享手机的网络 ... 290
- 17.3 无线网络的安全策略 291
 - 17.3.1 设置管理员密码 291
 - 17.3.2 无线网络WEP加密 291
 - 17.3.3 WPA-PSK安全加密
算法 292
 - 17.3.4 禁用SSID广播 294
 - 17.3.5 媒体访问控制地址
过滤 295

17.4 无线路由器的安全管理工具 ...	296	17.6 小试身手	304
17.4.1 《360路由器卫士》	296	练习1：加密手机的WLAN热点	
17.4.2 《路由优化大师》	298	功能	304
17.5 实战演练	302	练习2：通过修改WiFi名称隐藏	
实战演练1——控制无线网中		路由器	304
设备的上网速度	302		
实战演练2——诊断和修复网络			
不通的问题	303		

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及学习一些计算机安全方面的知识。本章介绍一些电脑安全方面的基础知识，主要内容包括IP地址、MAC地址、端口及黑客常用DOS命令的应用等。

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，可以说找到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，分别是网络号和主机号。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、E 5类，其中A、B、C类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。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。只有这些部分协同工作，在互联网中计算机才能相互访问。

- 子网掩码：子网掩码是与IP地址结合使用的一种技术。其主要作用有两个：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，每两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。

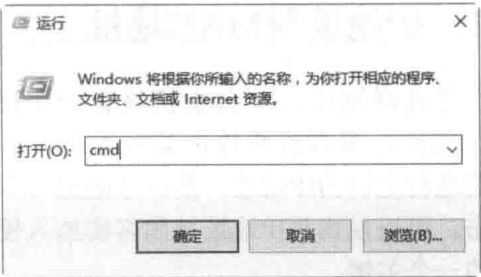
1.1.3 查看IP地址

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。

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查看到MAC地址。

果中看到一个物理地址：00-23-24-DA-43-8B，这就是用户计算机的网卡地址，它是唯一的。



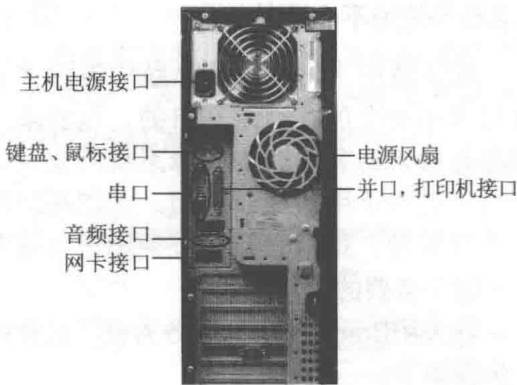
1.2 什么是端口

“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（256×256-1）。

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。

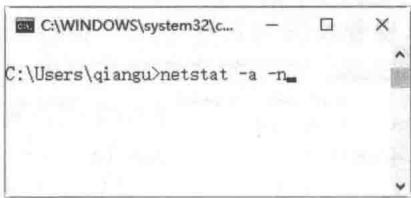
在网络技术中，端口又有几种含义：其中，一种是物理意义上的端口，如集线器、交换机、路由器等连接设备，用于连接其他的网络设备的接口，常见的有RJ-45端口、Serial端口等；另一种是逻辑意义上的端口，一般指协议TCP/IP中的端口，范围是0~65 535（256×256-1）。



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计算机。用户可以使用netstat命令查看自己系统的端口状态，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UCP连接的端口号及其状态。



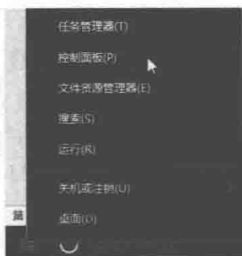


1.2.3 关闭不必要的端口

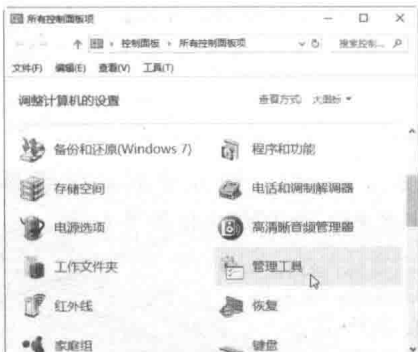
默认情况下，计算机系统中有许多没有用或不安全的端口是开启的，这些端口很容易被黑客利用。为保障系统的安全，可以将这些不用的端口关闭。关闭端口的方式有多种，这里介绍通过关闭无用服务来关闭不必要的端口。

以关闭Branch Cache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。



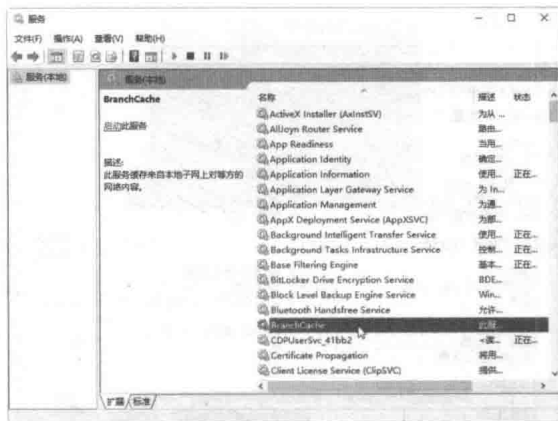
Step 02 打开“控制面板”窗口，双击“管理工具”图标。



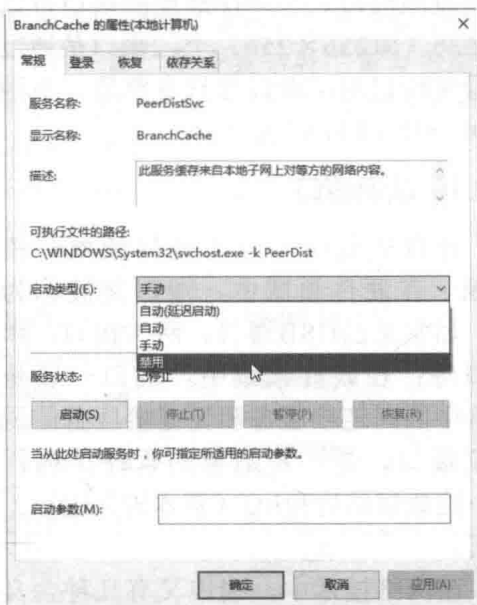
Step 03 打开“管理工具”窗口，双击“服务”图标。



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。



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。这里以右边上述停止的Branch Cache服务端口为例。

Step 01 在“Branch Cache的属性”对话框中单击“启动类型”右侧的下拉按钮，在弹出的下拉列表中选择“自动”。