

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（绝招篇）

网络安全技术联盟 编著



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 8 | 加密与解密技术快速入门电子书 |
|  超值赠送 2 | 精美教学PPT课件 |  超值赠送 9 | 网站入侵与黑客脚本编程电子书 |
|  超值赠送 3 | 黑客工具（107个）速查电子书 |  超值赠送 10 | 黑客命令全方位详解电子书 |
|  超值赠送 4 | 常用黑客命令（160个）电子书 |  超值赠送 11 | CDlinux 系统文件包 |
|  超值赠送 5 | 常见故障维修电子书 |  超值赠送 12 | Kali 虚拟机镜像文件 |
|  超值赠送 6 | Windows 10 系统使用和防护技巧电子书 |  超值赠送 13 | 无线密码的字典文件 |
|  超值赠送 7 | 8大经典密码破解工具电子书 | | |



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(绝招篇)

网络安全技术联盟 编著

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，以利于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 13 章，包括黑客攻防与网络安全快速入门、Windows 中的 DOS 窗口与 DOS 命令、网络踩点侦察与系统漏洞扫描、缓冲区溢出攻击与网络渗透入侵、目标系统的扫描与网络数据的嗅探、Windows 系统远程控制与网络欺骗、黑客信息的追踪与代理服务器的应用、木马病毒的防御与查杀软件的使用、网络流氓软件与间谍软件的清理、可移动 U 盘的安全防护与病毒查杀、磁盘数据的备份与恢复技巧、无线网络的组建与安全分析、无线路由器及密码的安全防护等内容。

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，帮助读者全面地掌握黑客攻防知识。赠送资源较多，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教学参考书。

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. 绝招篇 / 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 978-7-302-53369-6

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163551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：宋 林

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：16.25 字 数：375千字

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

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，还融入了目前市场上流行的无线攻防等热点知识。

本书特色

- 知识丰富全面：知识讲解由浅入深，涵盖了常见黑客攻防知识点，使读者能循序渐进地掌握黑客攻防方面的技术。
- 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示意图。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）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、CDlinux 系统文件包、Kali 虚拟机镜像文件、无线密码的字典文件。读者可扫描右侧二维码，或发邮箱至 zhangmin@tup.tsinghua.edu.cn 获取相关资源。

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教学参考书。

写作团队

本书由长期研究网络安全技术的网络安全技术联盟编著，另外还有王秀英、王英英、刘玉萍、刘尧等人参加编写工作。在编写过程中，编者尽所能地将最好的讲解呈现给读者，但难免有疏漏和不妥之处，敬请不吝指正。



Contents

目录

第1章 黑客攻防与网络安全快速入门.....1	
1.1 怎样从零开始学黑客.....1	
1.1.1 计算机原理很重要.....1	
1.1.2 了解黑客相关术语.....2	
1.1.3 掌握黑客技术应学习的编程技术有哪些.....3	
1.1.4 学习的耐心很重要.....3	
1.1.5 黑客技术未来方向在哪里.....3	
1.2 网络安全中的相关概念.....3	
1.2.1 互联网与因特网.....3	
1.2.2 万维网与浏览器.....4	
1.2.3 URL 地址与域名.....4	
1.2.4 IP 与 MAC 地址.....4	
1.3 认识网络通信中的协议.....5	
1.3.1 HTTP.....5	
1.3.2 TCP/IP.....5	
1.3.3 IP.....5	
1.3.4 ARP.....5	
1.3.5 ICMP.....5	
1.4 实战演练.....6	
实战演练 1——获取本机的 IP 地址.....6	
实战演练 2——获取本机的 MAC 地址.....6	
1.5 小试身手.....6	
练习 1: 显示系统文件的扩展名.....6	
练习 2: 快速锁定 Windows 桌面.....7	

第2章 Windows中的DOS窗口与DOS命令.....8	
2.1 认识Windows 10系统中DOS窗口.....8	
绝招 1: 使用菜单的形式进入 DOS 窗口.....8	
绝招 2: 通过“运行”对话框进入 DOS 窗口.....8	
绝招 3: 通过 IE 浏览器访问 DOS 窗口.....9	
绝招 4: 编辑“命令提示符”窗口中的代码.....9	
绝招 5: 自定义“命令提示符”窗口的风格.....10	
2.2 黑客常用DOS命令应用绝招.....12	
绝招 6: cd 命令的应用.....12	
绝招 7: dir 命令的应用.....13	
绝招 8: ping 命令的应用.....14	
绝招 9: net 命令的应用.....15	
绝招 10: netstat 命令的应用.....16	
绝招 11: tracert 命令的应用.....17	
绝招 12: Tasklist 命令的应用.....17	
绝招 13: SFC 命令的应用.....18	
2.3 实战演练.....19	
实战演练 1——使用命令代码清除系统垃圾文件.....19	
实战演练 2——使用 shutdown 命令实现定时关机.....19	

2.4 小试身手.....20	第4章 缓冲区溢出攻击与网络 渗透入侵.....40
练习 1: 通过滑动鼠标关闭 计算机.....20	4.1 什么是缓冲区溢出攻击.....40
练习 2: 设置计算机的锁屏界面.....20	4.1.1 缓冲区溢出概述.....40
第3章 网络踩点侦察与系统漏洞 扫描.....22	4.1.2 缓冲区溢出简单实例.....40
3.1 网络踩点侦察.....22	4.2 RPC服务远程溢出漏洞攻击.....42
绝招 1: 侦察对方是否存在.....22	绝招 1: RPC 服务远程溢出漏洞入 侵演示.....42
绝招 2: 侦察对方的操作系统.....23	绝招 2: RPC 服务远程溢出漏洞的 防御.....43
绝招 3: 确定可能开放的端口 服务.....24	4.3 WebDAV缓冲区溢出攻击.....44
绝招 4: 查询 WHOIS 和 DNS.....25	绝招 3: WebDAV 缓冲区溢出漏洞 入侵演示.....44
绝招 5: 侦察对方的网络结构.....27	绝招 4: WebDAV 缓冲区溢出漏洞 的防御.....46
绝招 6: 快速确定漏洞范围.....28	4.4 防止缓冲区溢出攻击的方法.....47
3.2 防御网络侦察的对策.....31	绝招 5: 防范缓冲区溢出的根本 方法.....47
绝招 7: 实体层次防御对策.....31	绝招 6: 普通用户防范缓冲区溢出 的方法.....49
绝招 8: 能量层次防御对策.....32	绝招 7: 通过加密 CMD 防范缓冲 区溢出攻击.....49
绝招 9: 信息层次防御对策.....32	4.5 网络渗透入侵系统的手段与防御.....50
3.3 堵塞系统漏洞.....33	绝招 8: 通过注册表创建隐藏账号 入侵.....50
绝招 10: 使用 Windows 更新修复 系统漏洞.....33	绝招 9: 通过 DOS 命令创建隐藏 账号入侵.....52
绝招 11: 使用《360 安全卫士》 修补系统漏洞.....34	绝招 10: 通过设置组策略找出创建 的隐藏账号.....53
绝招 12: 使用《腾讯电脑管家》 修复系统漏洞.....35	4.6 实战演练.....55
3.4 实战演练.....36	实战演练 1——扫描并批量关闭 系统危险端口.....55
实战演练 1——阻止更新驱动 程序.....36	实战演练 2——通过 IP 安全策略 关闭危险端口.....56
实战演练 2——探测目标主机的弱 口令.....37	4.7 小试身手.....57
3.5 小试身手.....38	
练习 1: CPU 高危漏洞“裂谷”.....38	
练习 2: 蓝牙协议中的 BlueBorne 漏洞.....39	

练习 1: 怎样用左手操作鼠标.....	57
练习 2: 将应用程序固定到任务栏.....	57
第5章 目标系统的扫描与网络数据的嗅探.....	59
5.1 扫描目标系统的端口信息.....	59
绝招 1: 使用 ScanPort 扫描端口.....	59
绝招 2: 使用“Nmap 扫描器”扫描端口.....	60
绝招 3: 使用“极速端口扫描器”扫描端口.....	62
绝招 4: 使用“S-GUI Ver 扫描器”扫描端口.....	63
5.2 扫描目标系统的其他信息.....	65
绝招 5: 扫描目标主机的 IPC\$ 用户列表.....	65
绝招 6: 扫描指定地址范围内的目标主机.....	66
绝招 7: 扫描目标主机的系统进程信息.....	67
5.3 嗅探网络中的数据信息.....	69
绝招 8: 嗅探网络中的 TCP/IP 数据包.....	69
绝招 9: 嗅探网络中的上下行数据包.....	70
绝招 10: 嗅探网络中流过网卡的数据.....	71
5.4 实战演练.....	73
实战演练 1——使用“流光扫描器”扫描端口.....	73
实战演练 2——关闭系统中无用的端口.....	74
5.5 小试身手.....	75
练习 1: 设置默认应用程序.....	75
练习 2: 快速找到文件的路径.....	76
第6章 Windows系统远程控制与网络欺骗.....	78
6.1 通过Windows远程桌面实现远程控制.....	78
绝招 1: 开启 Windows 远程桌面功能.....	78
绝招 2: 使用远程桌面功能实现远程控制.....	78
6.2 使用Symantec pcAnywhere实现远程控制.....	80
绝招 3: 安装 Symantec pcAnywhere 工具.....	80
绝招 4: 配置 Symantec pcAnywhere 的性能.....	82
绝招 5: 开始进行远程控制.....	85
6.3 防范远程控制的方法与技巧.....	86
绝招 6: 开启系统自带 Windows 防火墙.....	86
绝招 7: 关闭 Windows 远程桌面功能.....	87
绝招 8: 关闭远程注册表管理服务.....	87
6.4 形形色色的网络欺骗攻击.....	88
绝招 9: 网络中的 ARP 欺骗攻击.....	88
绝招 10: 网络中的 DNS 欺骗攻击.....	91
绝招 11: 局域网中的主机欺骗.....	92
绝招 12: 钓鱼网站的欺骗技术.....	93
6.5 网络欺骗攻击的防护技巧.....	96
绝招 13: 使用绿盾 ARP 防火墙防御 ARP 攻击.....	96
绝招 14: 通过 AntiARP-DNS 防御 DNS 欺骗.....	97
6.6 实战演练.....	99
实战演练 1——查看系统中的 ARP 缓存表.....	99

实战演练 2——在“网络邻居”中隐藏自己.....	100	绝招 2: 使用“网络神偷”木马攻击.....	119
6.7 小试身手.....	100	绝招 3: 使用 VBS 脚本病毒攻击.....	121
练习 1: 禁用计算机的开机启动项.....	100	绝招 4: 使用邮箱病毒攻击.....	122
练习 2: 清理系统盘中的垃圾文件.....	101	8.2 使用木马清除软件清除木马.....	123
第7章 黑客信息的追踪与代理服务器的应用	103	绝招 5: 使用《木马清理王》清除木马.....	123
7.1 黑客信息的追踪.....	103	绝招 6: 使用《贝壳木马专杀》清除木马.....	124
绝招 1: 使用网站定位 IP 物理地址.....	103	绝招 7: 使用 Spyware Doctor 清除木马.....	125
绝招 2: 使用网络追踪器追踪信息.....	104	8.3 使用《360杀毒》软件查杀病毒.....	128
7.2 网络代理服务器的应用.....	106	绝招 8: 安装《360 杀毒》软件.....	128
绝招 3: 利用《代理猎手》查找代理服务器.....	106	绝招 9: 升级《360 杀毒》的病毒库.....	129
绝招 4: 使用 SocksCap 设置动态代理.....	110	绝招 10: 快速查杀计算机中的病毒.....	130
绝招 5: 使用 MultiProxy 自动设置代理.....	113	绝招 11: 自定义查杀计算机病毒.....	131
7.3 实战演练.....	115	8.4 使用病毒专杀工具查杀病毒.....	132
实战演练 1——获取网络代理服务器.....	115	绝招 12: 查杀异鬼病毒.....	132
实战演练 2——在 IE 中设置代理服务器.....	115	绝招 13: 查杀 CAD 病毒.....	133
7.4 小试身手.....	116	绝招 14: 查杀 Office 宏病毒.....	134
练习 1: 调出常用桌面图标.....	116	绝招 15: 查杀 QQ 木马病毒.....	134
练习 2: 开启计算机的平板模式.....	116	8.5 实战演练.....	136
第8章 木马病毒的防御与杀毒软件的使用	117	实战演练 1——在 Word 中预防宏病毒.....	136
8.1 常见木马病毒的攻击方法.....	117	实战演练 2——在安全模式下查杀病毒.....	136
绝招 1: 使用“广外女生”木马攻击.....	117	8.6 小试身手.....	137
		练习 1: 禁止计算机进入睡眠状态.....	137
		练习 2: 救活假死的新建文件夹.....	138

第9章 网络流氓软件与间谍软件的清理.....140

- 9.1 感染恶意或间谍软件后的症状.....140
- 9.2 恶意软件的清理.....140
 - 绝招 1: 使用《360 安全卫士》清理.....140
 - 绝招 2: 使用《金山清理专家》清理.....142
 - 绝招 3: 使用《恶意软件清理助手》清理.....142
 - 绝招 4: 使用《恶意软件查杀助理》清理.....143
- 9.3 间谍软件的清理.....144
 - 绝招 5: 使用《反间谍专家》清理.....144
 - 绝招 6: 使用《Windows 清理助手》清理.....147
 - 绝招 7: 使用 SpyBot-Search& Destroy 清理.....150
 - 绝招 8: 使用《微软反间谍专家》清理.....152
- 9.4 实战演练.....153
 - 实战演练 1——删除上网缓存文件.....153
 - 实战演练 2——删除系统临时文件.....154
- 9.5 小试身手.....155
 - 练习 1: 屏蔽网页广告弹出窗口.....155
 - 练习 2: 阻止流氓软件自动运行.....156

第10章 可移动U盘的安全防护与病毒查杀.....157

- 10.1 U盘病毒概述.....157
 - 10.1.1 了解 U 盘病毒.....157
 - 10.1.2 常见 U 盘病毒.....157

- 10.2 U盘的安全防护技巧.....158
 - 绝招 1: 使用组策略关闭“自动播放”功能.....158
 - 绝招 2: 通过注册表关闭“自动播放”功能.....159
 - 绝招 3: 设置服务关闭“自动播放”功能.....159
- 10.3 U盘病毒的查杀.....160
 - 绝招 4: 使用 WinRAR 查杀.....160
 - 绝招 5: 使用 USBKiller 查杀.....161
 - 绝招 6: 使用 USBCleaner 查杀.....164
 - 绝招 7: 使用 Autorun 病毒防御者查杀.....167
- 10.4 U盘数据的加密.....169
 - 绝招 8: 启动 BitLocker 功能.....169
 - 绝招 9: 为 U 盘进行加密.....170
- 10.5 实战演练.....172
 - 实战演练 1——U 盘病毒的手动删除.....172
 - 实战演练 2——禁止计算机使用 U 盘.....172
- 10.6 小试身手.....173
 - 练习 1: 限制编辑 Word 文档.....173
 - 练习 2: 保护 U 盘中的办公文档.....174

第11章 磁盘数据的备份与恢复技巧.....176

- 11.1 备份各类磁盘数据.....176
 - 绝招 1: 备份分区表数据.....176
 - 绝招 2: 备份引导区数据.....177
 - 绝招 3: 备份驱动程序.....178
 - 绝招 4: 备份电子邮件.....180
 - 绝招 5: 备份磁盘文件数据.....181
- 11.2 恢复各类磁盘数据.....183
 - 绝招 6: 恢复分区表数据.....184
 - 绝招 7: 恢复引导区数据.....184

绝招 8: 恢复驱动程序数据.....185

绝招 9: 恢复丢失的电子邮件.....186

绝招 10: 恢复丢失的磁盘文件
数据.....187

11.3 使用数据恢复工具恢复丢失的
数据.....189

绝招 11: 使用 EasyRecovery 恢复
数据.....189

绝招 12: 使用 FinalRecovery 恢复
数据.....191

绝招 13: 使用 FinalData 恢复
数据.....192

绝招 14: 使用《数据恢复大师》
恢复数据.....194

11.4 实战演练.....198

实战演练 1——格式化硬盘后的
恢复.....198

实战演练 2——还原已删除的
文件.....200

11.5 小试身手.....200

练习 1: 从回收站中还原数据.....200

练习 2: 清空回收站后的恢复.....201

第12章 无线网络的组建与

安全分析.....204

12.1 认识无线网络及相关概念.....204

12.1.1 狭义无线网络.....204

12.1.2 广义无线网络.....206

12.1.3 认识无线网卡.....208

12.1.4 认识无线路由器.....209

12.1.5 无线网络中的术语.....209

12.2 组建无线网络并实现上网.....210

绝招 1: 搭建无线网环境.....210

绝招 2: 配置无线局域网.....210

绝招 3: 将计算机接入无线网.....211

绝招 4: 将手机接入无线网.....212

12.3 无线网络的安全分析.....213

绝招 5: 快速配置 Wireshark.....214

绝招 6: 首选项的设置.....216

绝招 7: 捕获选项的设置.....217

绝招 8: 分析捕获的数据包.....220

绝招 9: 统计捕获的数据包.....221

12.4 实战演练.....222

实战演练 1——筛选出无线网络中的
握手信息.....222

实战演练 2——快速定位身份验证
信息数据包.....223

12.5 小试身手.....223

练习 1: 诊断和修复网络不通的
问题.....223

练习 2: 控制无线网中设备的
上网速度.....224

第13章 无线路由器及密码的安全

防护.....225

13.1 无线路由器的基本设置.....225

绝招 1: 通过设置向导快速
上网.....225

绝招 2: 网络参数与无线设置.....226

绝招 3: 安全设置与家长控制.....228

绝招 4: 上网控制与路由功能.....229

绝招 5: 路由器系统工具的
设置.....229

13.2 无线路由器的密码破解.....231

绝招 6: 破解无线路由器的 WEP
密码.....231

绝招 7: 破解无线路由器的 WPA
密码.....232

绝招 8: 破解无线路由器的 WPS
密码.....234

13.3 无线路由器的安全防护技巧.....235

绝招 9: 强化管理员密码.....235

绝招 10: 无线网络 WEP 加密.....235

绝招 11: WPA-PSK 安全加密.....236

绝招 12: MAC 地址过滤的设置	237	实战演练 2——在 Windows 10 系统 创建 AP 热点	245
13.4 无线路由器的安全管理	238	13.6 小试身手	247
绝招 13: 使用《360 路由器卫士》 管理	238	练习 1: 开启并加密手机 WLAN 热点	247
绝招 14: 使用《路由优化大师》 管理	241	练习 2: 关闭无线路由器的广播 功能	248
13.5 实战演练	245		
实战演练 1——在 Linux 系统中 查看无线网卡信息	245		

第1章 黑客攻防与网络安全 快速入门

真正的黑客并不只是攻击，而是通过攻击来研究漏洞，从而大大提高系统的安全性。本章介绍黑客攻防与网络安全的相关基础知识，主要内容包括怎样从零开始学黑客攻防技术以及网络安全中的相关概念等。

1.1 怎样从零开始学黑客

很多学生对黑客技术很感兴趣，但是对于怎样从零开始学习黑客知识还是很茫然。例如，不知道要掌握黑客技术应该学哪些知识，哪些知识是必学的，要掌握黑客编程技术应该学习哪些程序开发语言，学会之后要干什么？本节就来介绍怎样从零开始学黑客技术。

1.1.1 计算机原理很重要

在学习黑客知识之前，计算机原理是一定要学习的，从中可以了解很多未来会用到的知识，如计算机的工作流程、数据和指令的存储机制等。这些都是非常重要的知识，如果这些都不懂，那还谈什么黑客技术呢？

1. 计算机的工作原理

用户预先要把指挥计算机如何进行操作的指令序列（称为程序）和原始数据通过输入设备输送到计算机内存储器（简称内存）中。这些指令中的每一条指令中都会明确规定计算机从哪个地址取数，进行什么操作，然后送到什么地址等。

计算机在运行时，先从内存中取出第一条指令，通过控制器的译码，按指令的要求，从存储器中取出数据进行指定的运算和逻辑操作等加工，然后再按地址把结果送到内存中去。接下来，再取出第二条

指令，在控制器的指挥下完成规定操作。依此进行下去，直至遇到停止指令。

程序与数据一样存储，按程序编排的顺序，一步一步地取出指令，自动完成指令规定的操作是计算机最基本的工作原理。这一原理最初是由美籍匈牙利数学家冯·诺依曼（John von Neumann）于1945年提出来的，故称为冯·诺依曼原理。

2. 计算机的系统架构

计算机系统由硬件系统和软件系统两部分组成。冯·诺依曼奠定了现代计算机的基本结构，这一结构又称冯·诺依曼结构，其特点如下：

- （1）使用单一的处理部件来完成计算、存储以及通信的工作。
- （2）存储单元是定长的线性组织。
- （3）存储空间的单元是直接寻址的。
- （4）使用低级机器语言，指令通过操作码来完成简单的操作。
- （5）对计算进行集中的顺序控制。
- （6）计算机硬件系统由运算器、存储器、控制器、输入设备、输出设备五大部件组成，并规定了它们的基本功能。
- （7）采用二进制形式表示数据和指令。
- （8）在执行程序和处理数据时必须将程序和数据从外存储器装入主存储器中，然后才能使计算机在工作时自动地从存储器中取出指令并加以执行。

1.1.2 了解黑客相关术语

在黑客领域中，有一些常用术语，如渗透、DDoS、旁注、WebShell、注入等，需要初学者了解，如果连这些术语都不知道，那真是个黑客“菜鸟”了！下面介绍黑客领域中的相关术语。

1. 肉鸡

所谓“肉鸡”是一种比喻，是指那些能够随意被黑客操控的计算机，对方可以是 Windows 系统，可以是 UNIX/Linux 系统，可以是一般的个人计算机，也可以是大型的服务器，能够像操作自己的计算机那样来操作它们，而不被对方所发觉。

2. 木马

木马是那些表面上伪装成了正常的程序，可是当这些程序被运行时，就会获取系统的整个操控权限。有很多黑客就是热衷于运用木马程序来操控别人的计算机，如灰鸽子、黑洞、PcShare 等。

3. 网页木马

网页木马表面上伪装成一般的网页文件或是将木马代码直接插入到正常的网页文件中，当有人访问网页时，网页木马就会运用对方系统的漏洞主动将配置好的木马客户端下载到对方的计算机上主动运行，从而控制目标计算机。

4. 挂马

挂马就是在别人的网站文件里面放入网页木马或者是将木马代码潜入到对方正常的网页文件里，以使阅读者中马。

5. 后门

后门是指一种绕过安全性操控而获取对程序或系统控制权的办法。在软件的开发阶段，程序员常会在软件内创建后门以便能够修正程序中的缺陷。如果后门被其

他人知道，或是在软件发布之前没有删除，那么它就成了安全隐患。一般大多数的特洛伊木马（Trojan Horse）程序都能够被入侵者用于制造后门。

6. Rootkit

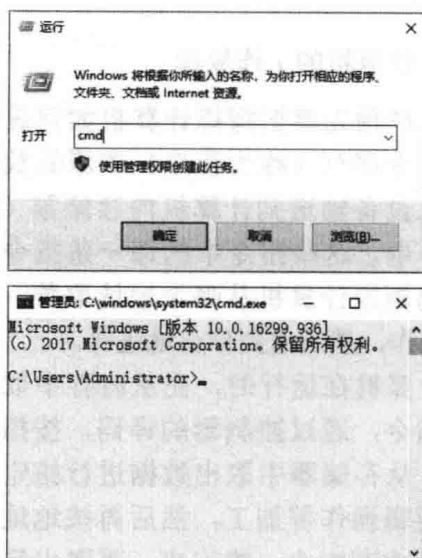
Rootkit 是入侵者用来隐藏自己的行踪和保留 root 控制权限的程序工具。一般，入侵者通过入侵的方式获得 root 拜访权限进入系统后，再通过对方系统内存在的安全漏洞获得系统的 root 权限。最后，入侵者就会在对方的系统中安装 Rootkit，以达到自己长久操控对方计算机的目的。

7. 弱口令

所谓弱口令是指密码与用户名相同，密码为空的用户名与密码组合，也包括那些密码强度不够，容易被猜解的组合，类似 123、abc 这样的口令（密码）。

8. Shell

Shell 指的是一种指令执行环境，如按 Windows+R 组合键，打开“运行”对话框，在“打开”文本框中输入 cmd，单击“确定”按钮，就会弹出一个用于执行指令的窗口，这个就是 Windows 的 Shell 执行环境，也被称为“命令提示符”窗口，如下图所示。



9. 溢出

确切地讲，所谓“溢出”应该是“缓冲区溢出”。简单的解释就是程序对接收的输入数据没有履行有效的检测而导致过错，后果可能是造成程序崩溃或者是履行入侵者的指令。大致分为两类：堆溢出和栈溢出。

10. 免杀

免杀是通过加壳、加密、修正特征码、加花指令等技能来修正程序，使其逃过杀毒软件的查杀。

11. 加壳

加壳是运用特别的算法，将 exe 可执行程序或者 dll 动态链接库文件的编码进行改变（如实现压缩、加密），以达到缩小文件体积或者加密程序编码，甚至是躲过杀毒软件查杀的目的。目前较常用的加壳工具有 UPX、ASPack、PePack、PECompact、UPack、免疫 007、木马彩衣等。

12. 花指令

花指令是几条汇编指令，让汇编语句进行一些跳转，使得杀毒软件不能正常判断病毒文件的结构。通俗来讲，就是杀毒软件是从头到脚按顺序来查找病毒，如果把病毒的头和脚颠倒位置，杀毒软件就找不到病毒了。

1.1.3 掌握黑客技术应学习的编程技术有哪些

很多黑客初学者会遇到一个问题，那就是黑客需要学习编程知识吗？答案是肯定的，那么需要学习哪些编程知识呢？其实这与个人的爱好与发展方向有关，如果是要对网站进行安全漏洞检测，就应该学会 HTML、PHP、数据库等编程语言；如果对程序开发有兴趣的话，可以学 Java、C++、Python 等开发性语言。不过，每种语

言都有它的优点和缺点，需要通过自己的筛选进行选择学习。

1.1.4 学习的耐心很重要

学黑客技术的人很多，失败的人也很多，这是因为一些初学者一旦遇到解决不了的问题，就放弃了；或者三天打鱼两天晒网，刚开始有热情，到了后面就没兴趣了。所以只有真正热爱黑客技术的人，才能坚持下来，这就需要学习的耐心了。

1.1.5 黑客技术未来方向在哪里

黑客技术真正的未来在于安全方面，因为只有安全才对社会的发展有意义，那些对社会有意义的东西才能长久的生存下来。为此，现在的黑客一般都会转型做网络安全，因为网络安全研究的是攻防兼备，这是社会发展的必然趋势。

1.2 网络安全中的相关概念

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，理解了这些概念，对网络安全有一定的帮助。

1.2.1 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的，它总是属于全人类的。

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。因特网是基于 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。

1.2.2 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 Internet 提供的最主要的服务。它是由多媒体链接而形成的集合，通常人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：互联网包含因特网，因特网包含万维网。凡是能彼此通信的设备组成的网络就叫互联网。所以，即使仅有两台机器，不论用何种技术使其彼此通信，也都叫互联网。

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为微软公司的 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。



1.2.3 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 或 Netscape 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。



1.2.4 IP与MAC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）。

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，它由厂商写在网络硬件的 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 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 6 个字节都相同，后 6 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。

1.3 认识网络通信中的协议

“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。

1.3.1 HTTP

HTTP (HyperText Transfer Protocol, 超文本传输协议) 是用于从 WWW 服务器传输超文本到本地浏览器的传送协议。它可以使浏览器更加高效显示网页内容。该协议不仅能保证计算机正确快速地传输超文本文档，还能确定传输文档中的哪些内容首先显示（如文本先于图形）等。

1.3.2 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, 网际协议)。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。

1.3.3 IP

IP, 即互联网协议 (Internet Protocol), IP 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含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。

1.3.4 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”, 帧里面是有目标主机的 MAC 地址的。

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。

1.3.5 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包含用户

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，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。

1.4 实战演练

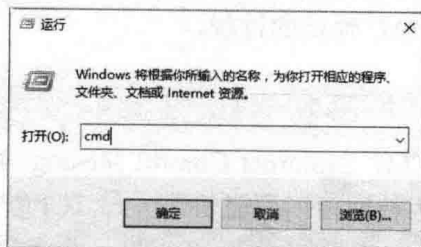
实战演练1——获取本机的IP地址

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选择“运行”菜单命令，如下图所示。



Step 02 打开“运行”对话框，在“打开”文本框中输入 cmd，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 命令，按 Enter 键，即可显示出本机的 IP 配置相关信息，如下图所示。



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。

实战演练2——获取本机的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 MAC 地址：00-23-24-DA-43-8B，这是本机的物理地址，也是本机的网卡地址，它是唯一的，如下图所示。



1.5 小试身手

练习1：显示系统文件的扩展名

Windows 10 系统默认情况下并不显示文件的扩展名，用户可以通过设置显示文件的扩展名。具体的操作步骤如下。