从基础到实践 基础内容完整覆盖 实践应用循序渐进

从必需到拓展 必需知识全面够用 拓展材料精心筛选

从入门到进阶 内容编排由浅入深 知识面广词汇量大

重点推荐

黑客攻击与防范技术

■ 宋超◎主编

北京理工大学出版社
BEIJING INSTITUTE OF TECHNOLOGY PRESS

黑客攻击与防范技术

主　编　宋　超
副主编　徐云晴　杨　骏
参　编　聂　飞　吴　明　王克垒　华　臻
　　陈晓筠　张锡明　谢茂南　潘亚宾

北京理工大学出版社
BEIJING INSTITUTE OF TECHNOLOGY PRESS

内容简介

本书是一本专注于黑客攻击和防范技术的教材，内容涵盖了黑客攻击的常见方法及系统加固的相关操作。本书以培养学生的职业能力为核心，以工作实践为主线，以项目为导向，采用任务驱动、场景教学的方式，面向企业信息安全工程师、系统维护工程师等岗位设置教材内容，建立以实际工作过程为框架的职业教育课程结构。

本书可以作为信息安全与管理、计算机网络技术专业的教材使用，也可以作为信息安全从业人员的参考用书。本书配有授课用交互式电子课件、微课视频、实验环境，也提供了链接，供下载使用。

图书在版编目（CIP）数据

黑客攻击与防范技术/宋超主编．—北京：北京理工大学出版社，2021.1
ISBN 978-7-5682-9451-5

Ⅰ.①黑…　Ⅱ.①宋…　Ⅲ.①黑客-网络防御-高等学校-教材　Ⅳ.①TP393.081

中国版本图书馆 CIP 数据核字（2021）第 005085 号

出版发行／北京理工大学出版社有限责任公司
社　　址／北京市海淀区中关村南大街 5 号
邮　　编／100081
电　　话／（010）68914775（总编室）
　　（010）82562903（教材售后服务热线）
　　（010）68948351（其他图书服务热线）
网　　址／http://www.bitpress.com.cn
经　　销／全国各地新华书店
印　　刷／唐山富达印务有限公司
开　　本／787 毫米×1092 毫米　1/16
印　　张／15
字　　数／352 千字
版　　次／2021 年 1 月第 1 版　2021 年 1 月第 1 次印刷
定　　价／62.00 元

责任编辑／王玲玲
文案编辑／王玲玲
责任校对／刘亚男
责任印制／施胜娟

前言 Preface

当前，信息技术产业欣欣向荣，处于空前繁荣的阶段，但是危害信息安全的事件不断发生，信息安全的形势非常严峻。敌对势力的破坏、黑客入侵、利用计算机实施犯罪、恶意软件侵扰、隐私泄露等，是我国信息安全面临的主要威胁和挑战。我国已经成为世界信息产业大国，但是还不是信息产业强国，在信息产业的基础性产品研制、生产方面还比较薄弱，例如，在计算机操作系统等基础软件和 CPU 等关键性集成电路方面，我国现在还部分依赖国外的产品，这就使得我国的信息安全基础不够牢固。

随着计算机和网络在军事、政治、金融、工业、商业等部门的广泛应用，社会对计算机和网络的依赖越来越强，如果计算机和网络系统的安全受到破坏，不仅会带来巨大的经济损失，还会引起社会的混乱。因此，确保以计算机和网络为主要基础设施的信息系统的安全已成为世人关注的社会问题和信息科学技术领域的研究热点。当前，我国正处在全面建成小康社会的决定性阶段，实现我国社会信息化并确保信息安全是我国全面建成小康社会的必要条件之一。而要实现我国社会信息化并确保信息安全的关键是人才，这就需要我们培养规模宏大、素质优良的信息安全人才队伍。

2014 年，习近平总书记在中央网络安全与信息化领导小组会议上指出：没有网络安全就没有国家安全，没有信息化就没有现代化。网络安全和信息化是事关国家安全和国家发展、事关广大人民群众工作和生活的重大战略问题，要从国际、国内大势出发，总体布局，统筹各方，创新发展，努力把我国建成网络强国。

“十四五”时期，我国将继续推动网络强国建设。网络强国涉及技术、应用、文化、安全、立法、监管等诸多方面，不仅要突破核心技术，还要提供更加安全可靠的软硬件支撑，加快建设高速、移动、安全、泛在的新一代信息基础设施。在不断推进新技术、新业务应用，繁荣发展互联网经济的同时，要强化网络和信息安全，而培育高素质人才队伍是实施网络强国战略的重要措施。

本书共有 8 个项目，分别为走进黑客世界、黑客实践之网络扫描、黑客实践之抓包分析、黑客实践之脚本编写、黑客实践之服务漏洞、黑客实践之网站漏洞、黑客实践之系统加固、黑客实践之赛题列举。本书由宋超担任主编，徐云晴、杨骏担任副主编，参加编写的还有聂飞、吴明、王克垒、华臻、陈晓筠、张锡明、谢茂南、潘亚宾。其中，宋超编写项目一至项目五，徐云晴编写项目六，杨骏编写项目七，其余编者编写项目八。

由于编者水平有限，书中难免出现疏漏和不妥之处，敬请广大读者批评改正，此外，本书在编写过程中参考了大量的书籍和互联网上的资源，在此向这些书籍和资源的作者表示感谢。

编者

目录 Contents

项目一　走进黑客世界

项目简介

本项目以 QQ 盗号、木马植入、网站入侵为例，阐述了黑客入侵的一般过程和基本步骤，其中网络扫描、抓取和分析数据包、制作攻击脚本等知识点会在后续项目中展开。另外，本项目也介绍了课程实验环境的搭建方法。

项目目标

技能目标

1. 能说出日常生活中遇到的威胁网络安全的事件。
2. 能说出黑客攻击的流程及使用的工具。
3. 能搭建本课程所需的实验环境。

知识目标

1. 理解网络空间安全的含义。
2. 了解 QQ 盗号、木马植入等黑客的行为。
3. 理解黑客攻击的流程及攻击“房产网”的过程。
4. 掌握 VMware Workstation 虚拟机搭建实验环境的方法。

工作任务

根据本项目要求，基于工作过程，以任务驱动的方式，将项目分成以下三个任务：

①走进网络空间安全。

②体验黑客入侵“房产网”。

③搭建网络攻防环境。

任务一　走进网络空间安全

（一）任务描述

本任务通过三个案例的实施（体验一个 QQ 盗号网站、体验一次电脑木马植入、体验网站万能密码），使学生感受到发生在身边的网络安全事件，同时理解黑客的含义。

（二）任务目标

1. 了解 QQ 盗号背后的原理。
2. 了解木马程序的危害。

3. 了解网站万能密码的结构。

知识准备

1. 网络空间安全的定义

网络空间英文名字是 Cyberspace。早在 1982 年，加拿大作家威廉·吉布森在其短篇科幻小说《燃烧的铬》中创造了 Cyberspace 一词，意指由计算机创建的虚拟信息空间。Cyberspace 在这里强调电脑爱好者在游戏机前体验到交感幻觉，体现了 Cyberspace 不仅是信息的简单聚合体，也包含了信息对人类思想认知的影响。此后，随着信息技术的快速发展和互联网的广泛应用，Cyberspace 的概念不断丰富和演化。2008 年，美国第 54 号总统令对 Cyberspace 进行了定义：Cyberspace 是信息环境中的一个整体域，它由独立且互相依存的信息基础设施和网络组成。其包括互联网、电信网、计算机系统、嵌入式处理器和控制器系统。除了美国之外，还有许多国家也对 Cyberspace 进行了定义和解释，但与美国的说法大同小异，通常把 Cyberspace 翻译成网络空间。

网络空间如图 1-1-1 所示，它既是人的生存环境，也是信息的生存环境，因此网络空间安全是人和信息对网络空间的基本要求。另外，网络空间是所有信息系统的集合，并且是复杂的巨系统。人在其中与信息相互作用、相互影响。

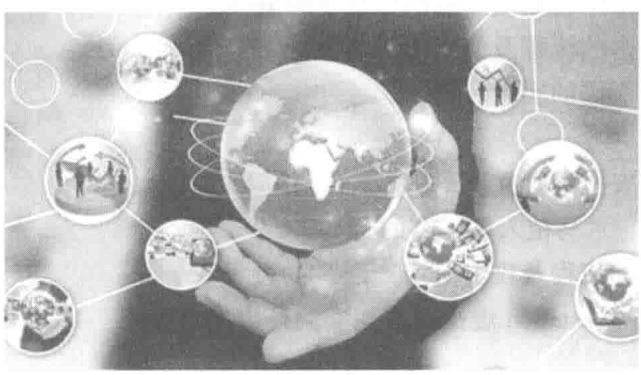


图 1-1-1　网络空间

因此，网络空间安全问题更加综合、更加复杂。网络安全的人才多种多样，包括立法人才、治理人才、战略人才、技术和理论研发人才、安全规划人才、宣传和教育人才、运维人才、防御人才等。

2017 年 6 月 1 日，《人民日报》刊文："网络空间是人类共同的活动空间。当前，互联网领域发展不平衡、规则不健全、秩序不合理等问题日益凸显，网络霸权主义、网络安全威胁等严重破坏全球互联网生态，国际网络空间亟待加强治理。全球互联网的健康发展，离不开世界各国的共同努力。我国作为互联网大国，一直致力于深化网络空间国际合作，自 2014 年起每年都召开世界互联网大会。习近平同志提出的'深化网络空间国际合作，携手构建网络空间命运共同体'主张，旗帜鲜明地表达了中国愿与各国携手构建网络空间命运共同体的积极态度。"

2. 网络空间安全事件和威胁

现代的人们生活在由网络组成的空间里，然而网络给大家带来便利的同时，网络安全事件却也频频发生，使人们不得不时刻保持警惕，见表 1-1-1 和表 1-1-2。从表中可以看出网络空间安全不仅是个人，更是政府和企业关注的重点。

表 1－1－1　2019 年国际网络安全事件（1—9 月）

时间	事件
2019 年 1 月 1 日	澳大利亚维多利亚州 3 万名政府雇员个人信息泄露
2019 年 1 月 16 日	俄克拉荷马州安全部门服务器泄露数百万政府文件
2019 年 1 月	云存储服务商 MEGA 泄露 87 GB 数据，含 7.7 亿个邮箱
2019 年 2 月	16 家网站 6.17 亿用户信息在暗网被售卖
2019 年 3 月 7 日	委内瑞拉两次大规模停电
2019 年 3 月 19 日	铝巨人 NorskHydro 遭受重大网络攻击，多家工厂关闭
2019 年 3 月 22 日	Facebook 被爆明文存储 6 亿用户密码，已被查看 900 万次
2019 年 3 月 22 日	亚特兰大市政府遭勒索软件袭击，重回纸质办公时代
2019 年 4 月 1 日	丰田服务器遭黑客入侵，威胁 310 万用户信息
2019 年 4 月	日本 Hoya 公司遭受网络攻击，计算机被用于挖掘加密货币
2019 年 6 月 10 日	佛罗里达州遭勒索攻击，政府工作停摆两周
2019 年 6 月 15 日	《纽约时报》宣称，美国已在俄罗斯电网中植入病毒
2019 年 6 月	世界最大飞机零件供应商 ASCO 遭受黑客攻击
2019 年 7 月 12 日	日本加密币交易所遭黑客攻击，损失资产 3 200 万美元
2019 年 7 月	美国银行第一资本遭黑客入侵，逾 1 亿用户信息泄露
2019 年 7 月	俄罗斯联邦安全局遭史上最大黑客攻击，7.5 TB 数据被盗
2019 年 7 月	南非电力公司遭勒索病毒攻击陷入瘫痪
2019 年 7 月	美国路易斯安那多学区遭网络攻击，宣布进入紧急状态
2019 年 8 月	首例“太空犯罪”：美国航天员被控从空间站入侵银行账户
2019 年 9 月 9 日	丰田纺织公司遭 BEC 攻击，损失 3 700 万美元
2019 年 9 月 19 日	全球 7.37 亿医疗数据泄露，波及 52 个国家超过 2 000 万人
2019 年 9 月	印度最大的核电站遭到网络攻击

表 1－1－2　2019 年国内十大网络安全事件

时间	事件
2019 年 1 月	超 2 亿中国求职者简历疑泄露，数据“裸奔”将近一周
2019 年 1 月 20 日凌晨	拼多多现优惠券漏洞，遭黑产团伙盗取数千万元
2019 年 2 月 16 日	京东金融 APP 被曝获取用户隐私
2019 年 2 月	抖音千万级账号遭撞库攻击，牟利百万，黑客被捕
2019 年 3 月 3 日	阿里云宕机，致大波互联网公司网站瘫痪
2019 年 3 月 13 日	境外黑客利用勒索病毒攻击部分政府和医院机构

续表

时间	事件
2019 年 3 月	华硕超百万用户可能感染恶意后门
2019 年 5 月	湖北首例入侵物联网系统案告破，十万设备受损
2019 年 5 月 26 日	易到用车服务器遭攻击，黑客勒索巨额比特币
2019 年 6 月	盗币 880 万元，广东警方打掉一个盗取游戏币的黑客团伙

目前网络空间面临的威胁如图 1 - 1 - 2 所示。

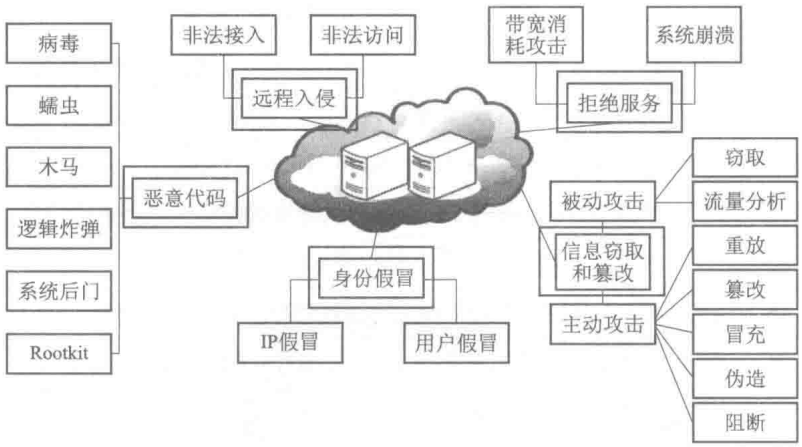


图 1 - 1 - 2　网络安全面临的威胁

恶意代码指的是经过存储介质和网络进行传播，从一台计算机系统到另外一台计算机系统，未经授权认证破坏计算机系统完整性的程序或代码。例如计算机病毒（Computer Virus），它是具有自我复制能力并会对系统造成巨大破坏的恶意代码，如表 1 - 1 - 3 和图 1 - 1 - 3 所示；蠕虫（Worms），它能自动完成自我复制，生命期短；特洛伊木马（Trojan Horse），它能与远程主机建立连接，使得远程主机能够控制本地主机；逻辑炸弹（Logic Bombs），特定逻辑条件满足时实施破坏；系统后门（Backdoor），它绕过安全性控制而获取对程序或系统的访问权；特殊类型恶意软件（Rootkit），隐藏自身及指定的文件、进程和网络链接；恶意脚本（Malicious Scripts），以制造危害或者损害系统功能为目的。

表 1 - 1 - 3　历史上著名的 5 个计算机病毒

年份	病毒名称	备注
1998 年	CIH 病毒	能够直接破坏计算机硬件，而不只是停留在软件层面，简单地说，它能够直接影响计算机主板 BIOS
2000 年	LOVE BUG	病毒的作用是不断复制和群发邮件
2003 年	冲击波病毒	计算机中了这个病毒，结果就是自动关机，并且这款病毒关机的时候会弹出倒计时，无论你使用什么手段，都没有办法结束掉
2006 年	熊猫烧香	这款病毒是国内草根计算机爱好者打造的一款蠕虫病毒，中毒用户不计其数。从可查阅的资料了解到全国数百万计算机中了这个病毒，这个病毒的变种数量接近 100 种

续表

年份	病毒名称	备注
2007 年	网游大盗	感染《魔兽世界》《完美世界》《征途》等多款知名网游，中毒之后会造成游戏账户和游戏装备丢失

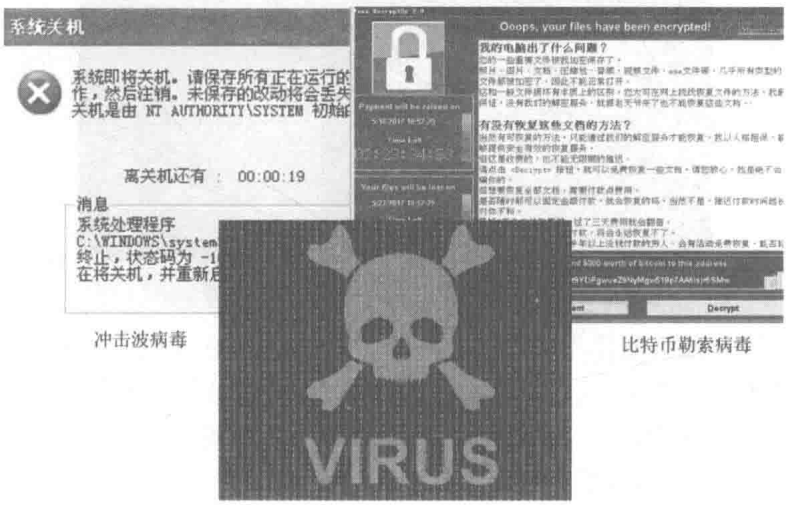


图 1－1－3　计算机病毒

远程入侵是有意违反安全服务和侵犯系统安全策略的智能行为。远程攻击分为非法接入和非法访问两种。

拒绝服务（图 1－1－4）让目标主机或系统停止提供服务或资源访问。资源包括磁盘空间、内存、进程及网络带宽等。拒绝服务一般分两种：一种是向服务器发送大量 IP 分组，导致正常用户请求服务的分组无法到达该服务器，其利用系统漏洞使得系统崩溃；第二种是利用 C 程序中存在的缓冲区溢出漏洞（图 1－1－5）进行攻击，发送精心编写的二进制代码，导致程序崩溃，系统停止服务。

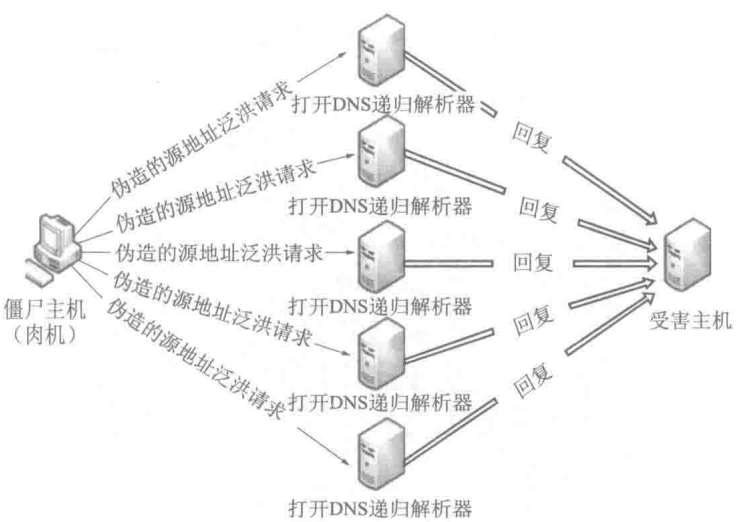


图 1－1－4　DNS 拒绝服务攻击

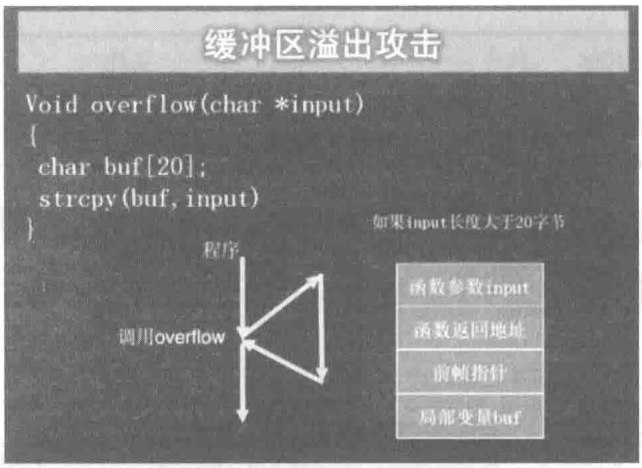


图1-1-5　缓冲区溢出攻击

身份假冒分为IP地址假冒和用户伪造两种。IP地址伪造（图1-1-6）即用不存在的或合法用户的IP地址，作为自己发送的IP分组的源IP地址，而网络的路由协议并不检查IP分组的源IP地址；用户伪造（图1-1-7）即身份信息使用一组特定的数据来表示，利用社会工程学方法或网络监听的方式窃取这些特定数据，利用这些数据欺骗远程系统，假冒合法用户。

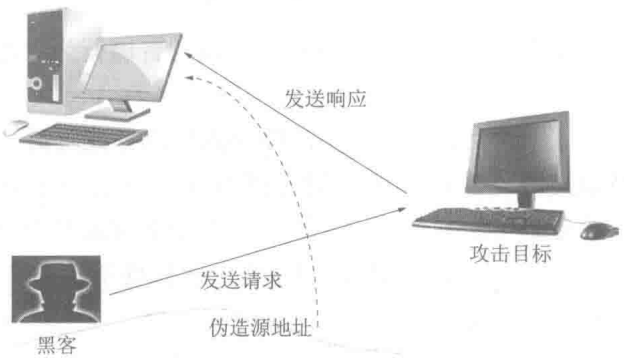


图1-1-6　IP地址伪造

图1-1-7　身份伪造

信息窃取和篡改分为主动攻击和被动攻击，如图 1－1－8 所示。

图 1－1－8　网络窃听

主动攻击有：重放，窃取到信息后，按照它之前的顺序重新传输；篡改，对窃取到的信息进行修改、延迟或重排，再发给接收方；冒充，先窃取到认证过程的全部信息，发现其中包含有效的认证信息流后重新发出这些信息；伪造，冒充合法身份在系统中插入虚假信息，并发给接收方；阻断，有意中断通信双方的网络传输过程，是针对可用性的一种攻击。

被动攻击有：在通信双方的物理线路上安装信号接收装置即可窃听通信内容；使用流量分析推测通信双方的位置和身份，观察信息的频率和长度。

3. 网络空间安全的目标

网络空间安全的目标是保证网络通信的保密性、完整性、不可抵赖性、可用性、可控性。

保密性：包括机密性，即隐私或机密的信息不会被泄露给未经授权的个体；隐私性，即个人仅可以控制和影响与之相关的信息。

完整性（图 1－1－9）：信息不被偶然或蓄意地删除、修改、伪造、乱序、重放、插入，目前的解决方法是依靠报文摘要算法和加密机制。

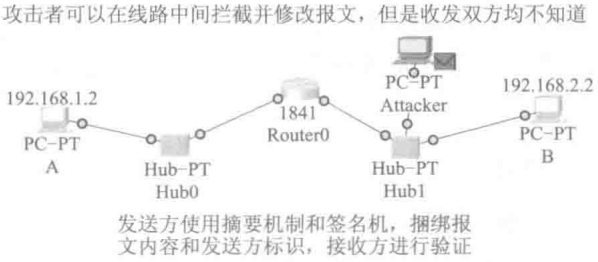
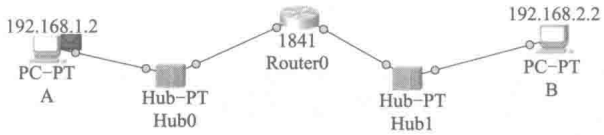


图 1－1－9　信息完整性

不可抵赖性（图 1－1－10）：通信的所有参与者都不能否认曾经完成的操作。目前的解决方法是依靠认证机制和数字签名技术。



A发数据包给B，B要赖说在收到的数据包里没有A发出的数据包，怎么办？

A对发出的数据进行数字签名，得到一串数字序列sig与数据发给B。

如果B要赖，法官只要对B收到的数据包验证有没有A的sig，从而判定B有没有说谎。

图 1－1－10　信息不可抵赖性

可用性（图 1－1－11）：信息被授权实体访问并按需使用，网络不能因病毒或拒绝服务而崩溃或阻塞。

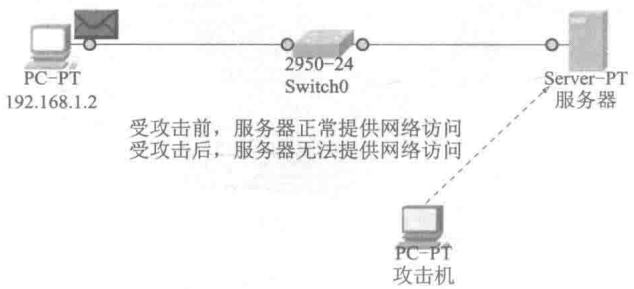


图 1－1－11　信息可用性

可控性（图 1－1－12）：仅允许实体以明确定义的方式对访问权限内的资源进行访问。

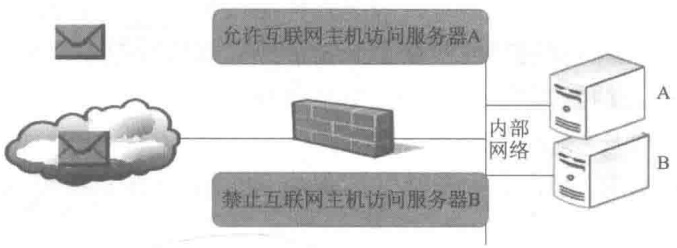


图 1－1－12　信息的可控性

4. 黑客的含义

黑客（Hacker）一般是精通网络、系统、外设及软硬件技术的程序员，他们崇尚 Free（自由、免费）的精神，将自己的心得与编写的工具和其他人分享；具有探索与创新的精神，喜欢探索软件程序奥秘；他们反传统，会找出系统漏洞，并策划相关的手段利用该漏洞进行攻击；具有合作的精神，需要数人或数十人的通力协作才能完成任务。

（三）任务实施

以下介绍三个网络安全事件。

案例一：体验一个 QQ 盗号网站

访问 http://192.168.244.135/qq，这是一个 QQ 网页登录界面，当输入 QQ 账号和密码时，如图 1－1－13 所示，网页中会跳出一个错误弹窗（图 1－1－14），而当单击弹窗上的“确定”按钮时，页面跳转到 QQ 登录的扫码界面。

整个过程看似很平常，但是就在这个过程中，你的 QQ 账号和密码就被记录到服务器端

图 1－1－13　在测试网站中输入密码

图 1－1－14　网页错误，跳转到 QQ 扫码界面

某个文件中了，如图 1－1－15 所示。

图 1－1－15　测试网站服务器记录的用户名和密码

小贴士：一些陌生的网站不要去访问，重要的个人信息不要轻易填写。

案例二：体验一次电脑木马植入

如图 1－1－16 所示，这是一个从网上下载的名为“冠状病毒的秘密”的压缩文件，从名字上看比较有吸引力，解压运行后，会发现是一张图片。

这时在另外一端黑客的电脑上出现图 1－1－17 所示的界面，表明查看“冠状病毒的秘密”图片的主机已经被控制，在黑客电脑端输入“shell”，就进入了被黑主机的命令行界面，于是在被黑主机不知情的情况下，黑客可以建立文件、建立用户、查看文件，甚至删除文件等，如图 1－1－18 和图 1－1－19所示。

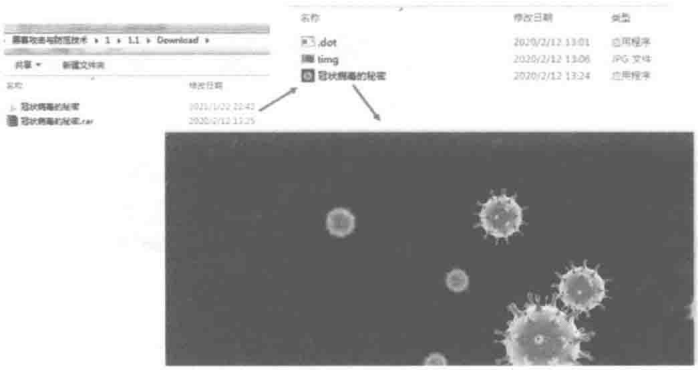


图 1－1－16　运行木马程序

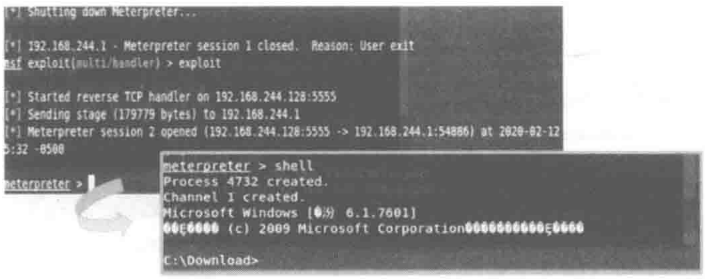


图 1－1－17　黑客进入系统

图 1－1－18　黑客建立文件

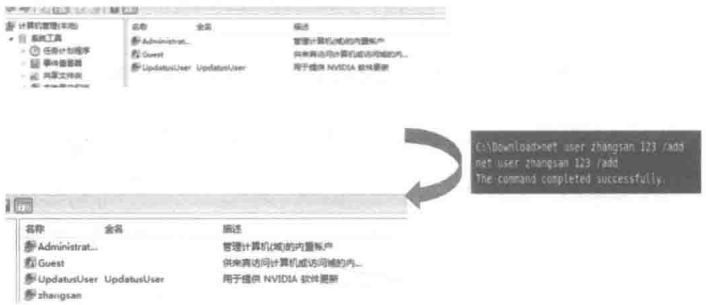


图 1－1－19　黑客添加用户

小贴士：请不要担心，目前杀毒软件足以对付大多数这样的木马。

案例三：体验网站万能密码的使用

如图 1－1－20 所示，这是一个简单的登录网站，当输入正确的用户名和密码时，跳转到登录成功的网页，否则，跳转到登录失败的网页。这种网站在日常生活中随处可见，但如图1－1－21 所示，在 username 输入框中随意输入字符，在 password 输入框中输入“any ' or ' 1 '='1”时，神奇的事情发生了，居然进入了登录成功的网页，这个密码称为万能密码，这是由于网站后台登录代码存在设计缺陷，这种缺陷称为 SQL 注入漏洞。

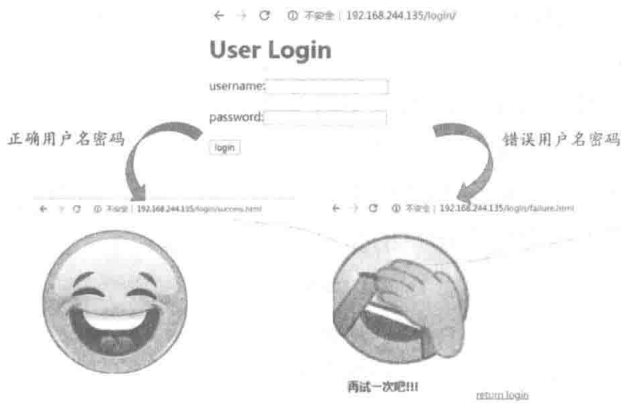


图 1－1－20　登录网页演示

图 1－1－21　万能密码登录

小贴士：一些漏洞网站除了存在着可利用的万能密码，还存在着万能用户名。

（四）任务评价

序号	一级指标	分值	得分	备注
1	认识 QQ 盗号	20		
2	认识电脑木马植入	20		
3	认识特殊网站的万能密码	20		
4	说出几件发生在身边的网络安全事件	30		