威盛中国芯 htc 成长数字营 创新课堂系列丛书

中国儿童青少年计算机表演赛辅导用书

北京市中小学校本选修课教材

青少年信息安全实践

威盛中国芯 htc 成长数字营活动办公室 组织编写

贾志勇 编著

科学出版社

创新课堂系列丛书
中国儿童青少年计算机表演赛辅导用书
北京市中小学校本选修课教材

信息安全实践

威盛中国芯 hTC 成长数字营活动办公室　组织编写
贾志勇　编著

科学出版社
北京

内 容 简 介

本书围绕信息安全进行系统介绍，将网络攻防由浅入深进行展开，全书共分为8章，系统讲解了网络扫描与嗅探、密码破解技术、网络欺骗技术、漏洞利用技术、拒绝服务攻击技术、恶意代码技术、Web攻击技术、安全防护技术等知识。通过本书学习到的不仅是信息安全的攻防技术，还有信息时代网络伦理道德的加深。

本书是威盛中国芯·HTC·成长数字营创新课堂系列丛书之一，也是中国儿童青少年威盛中国芯·HTC·计算机表演赛配套辅导用书。内容针对比赛与课堂教学，也可作为中小学信息技术等相关课程的教材和参考书。

图书在版编目(CIP)数据

青少年信息安全实践 / 贾志勇编著. —北京：科学出版社，2016.1
（威盛中国芯 HTC 成长数字营创新课堂系列丛书）
中国儿童青少年计算机表演赛辅助用书. 北京市中小学校本选修课教材
ISBN 978-7-03-046599-3
Ⅰ.①青… Ⅱ.①贾… Ⅲ.①计算机安全-信息安全-中小学-教材
Ⅳ.①G634.671
中国版本图书馆CIP数据核字（2015）第290600号

责任编辑：于海云 / 责任校对：郭瑞芝
责任印制：霍 兵 / 封面设计：迷底书装

科学出版社出版
北京东黄城根北街16号
邮政编码：100717
http://www.sciencep.com
安泰印刷厂印刷
科学出版社发行 各地新华书店经销
*
2016年1月第 一 版 开本：787×1092 1/16
2016年1月第一次印刷 印张：8 1/2
字数：201 000
定价：28.00元
（如有印装质量问题，我社负责调换）

编写委员会

丛书序

党的十八大报告明确把“信息化水平大幅提升”纳入全面建成小康社会的目标之一，大力推进信息化已成为事关国民经济和社会发展全局的重要举措。教育信息化是国家信息化的重要组成部分和战略重点，具有基础性、战略性、全局性地位。二十多年来，教育信息化得到了迅速发展，教育信息化日益被普及推广，对教育的改革和发展起到了重要推动作用。

威盛中国芯 HTC 成长数字营（以下简称“数字营”）是一个致力于推动教育信息化的公益项目，数字营目前主要有创新课堂、教育扶贫、未来教室三大项目。其中，创新课堂项目主要以提供信息技术创新应用课程、开展相关教师培训为核心，丰富教师的教学内容，拓展教师的教学思路。

随着信息技术的迅速发展，相关的教学内容也在不断更新，教师面临着新技术、新内容、新教学方法等多方面的问题。创新课堂系列丛书正是根据信息技术发展的需要，由一批相关领域的专家、学者，以及工作于教学第一线的教师共同编写而成的。本套丛书将目前国内外前沿的、具有实用价值和创新性的内容进行了科学、系统的整理和创新，作为对学校现有课程的延伸和补充，帮助教师提升自身的专业能力。

本套丛书及相关课程的开发主要结合了现代教育和社会热点，根据循序渐进的教学规律划分成若干阶段，并以趣味性的课堂设计引领学生进入课程学习。目前，丛书主要涉及信息技术的相关领域，包含《虚拟机器人设计与实践》、《手机应用开发》、《数字故事创作》、《网络信息搜索》、《创客进行时——用 Arduino 去创造》、《青少年信息安全实践》等。

本套丛书具有较广的适用面，已经纳入北京市中小学校本选修课教材，可作为中国儿童青少年计算机表演赛等信息技术普及教育活动的辅导用书。

相信本套丛书的出版有助于进一步推动信息技术课程的研究和改革，对培养适应信息时代的高素质人才，提高青少年信息素养起到积极的作用。热忱欢迎全国教育界同行和关注青少年信息技术教育的广大有识之士对我们的工作提出宝贵意见和建议！

威盛中国芯·HTC·成长数字营活动办公室

2015 年 6 月

序　言

信息安全已随着网络的普及而与所有人息息相关，从保障国家军事政治机密安全，到防范商业企业机密泄露和个人网银安全，再到防范青少年对不良信息的浏览等，信息安全应是所有人重视的领域。

“网络空间安全”于2015年6月获批成为“国家一级学科”，凸显了国家的网络信息安全人才培养的重视，但网络安全人才来源的缺乏是大家都普遍面对的问题，通过高考考入信息安全相关专业的学生，绝大多数在中学时期并没有接受过网络安全方面的系统训练，选择网络安全相关专业有很大的盲目性。相对于“育人”来讲，“选人”是更需要解决的问题，解决之道就是在中学，甚至小学对同学们进行系统的，有计划的培训，让信息安全进入课堂，让同学们从小就开始接触网络安全知识，应用网络安全知识，激发对网络安全的兴趣，理解网络安全的意义。在人人初步了解网络安全的基础上，让有天赋的同学脱颖而出，可以在进入大学之前就显露其才华，可以被更有效识别出来，进入大学相关专业培养。

市面上信息安全的书籍很多，但适合中小学生的信息安全教育的却凤毛麟角，相对于对某个细分领域的深入研讨，更需要给同学们展现网络安全的全貌以及可以快速动手就进行简单尝试的教程，而一直致力于信息化人才培养的中国儿童青少年威盛中国芯HTC计算机表演赛，也十分关注青少年信息安全教育的发展，并借此契机邀请贾志勇老师编撰《青少年信息安全实践》一书填补了这个空白。

贾志勇老师有多年中学信息化、信息安全教育经验，所编著的该书，涵盖了TCP/IP协议基础知识、密码学基础知识，对网络欺骗、拒绝服务攻击、Web攻击、恶意代码技术都做了介绍，最后还简单介绍了网络防护技术，除了深入浅出对网络攻防原理做介绍，还对实验方法进行介绍，方便同学们亲自动手试一试，兴趣的产生往往就是从“动手试一试”开始的。

网络信息安全人才的培养是一项艰巨、长期的任务，在面向中小学生的网络安全培训材料上我们才刚刚开始，期待有更多更好的培训材料不断涌现出来。

谭晓生

2015 年 9 月

前　言

1984年，邓小平观看小学生操作简易电子计算机，提出“计算机的普及要从娃娃做起”。之后随着互联网的迅速的发展，网络安全也逐渐成为了社会的关键词。到2015年，网络安全已经被提升到前所未有的高度，“没有网络安全就没有国家安全，没有信息化就没有现代化。”这一论述，把网络安全上升到了国家安全的层面，列于和国家信息化同等重要的位置。

当今世界信息化、网络化飞速发展，网络安全领域已经成为众多计算机高手施展才华的舞台。他们被大多数人称为“黑客”。在信息安全的世界里，“黑客”一词是由英语Hacker音译出来的，这个英文单词本身并没有明显的褒义或贬义，其本意类似于汉语对话中常提到的捉刀者、枪手、能手之类词语。“黑客”泛指擅长IT技术的人群、计算机科学家。黑客们往往精通各种编程语言和各类操作系统，同时对于数学的掌握也是必不可少的，运行计算机程序其实就是运算、离散数学、线性代数、微积分等知识的综合应用。

但随着计算机和网络的发展。“黑客”也逐渐分为了两个方向。当他们利用公共通信网路，如互联网和电话系统，在未经许可的情况下，载入对方系统的被称为“黑帽黑客”（black hat，另称cracker），这种“黑客”往往会利用漏洞攻击用户窃取资料，是一种违法行为；另一种是调试和分析计算机安全系统，这类人群被称为“白帽黑客”（white hat）。

“白帽黑客”的代表人物有很多，而王琦就是其中之一。王琦在网络安全圈早已鼎鼎有名，人称“大牛蛙”。他曾是微软中国安全响应中心技术负责人，建立了微软在美国总部以外的第一个安全响应中心。而且他还成功发现了这个世界上最难发现的最危险漏洞，并将这个漏洞报告给厂商修复，让其他“黑帽黑客”没有可乘之机，从而让互联网变得更安全。而本书宗旨就是让每个学习者都能成为像王琦这种对国家、企

业网络信息安全有帮助的“白帽黑客”。

网络安全和信息化对一个国家很多领域都是牵一发而动全身的，要认清我们面临的形势和任务，充分认识做好工作的重要性和紧迫性，因势而谋，应势而动，顺势而为。建设网络强国，要把人才资源汇聚起来，建设一支政治强、业务精、作风好的强大队伍；要培养造就世界水平的科学家、网络科技领军人才、卓越工程师的高水平创新团队。“把关键技术掌握在自己手里”是网络信息安全的保障，希望对网络安全感兴趣的初学者认真阅读，深入钻研，为我们国家的强盛贡献力量。

编者

2015 年 9 月

目　录

丛书序

序言

前言

第一章　网络扫描与嗅探 …… 1

第二章　密码破解技术 …… 18

第三章　网络欺骗技术 …… 37

第四章　漏洞利用技术 …… 51

第五章　拒绝服务攻击技术 …… 63

第六章　恶意代码技术 …… 78

第七章　Web 攻击技术 …… 95

第八章　安全防护技术 …… 109

附　录 …… 121

第一章　网络扫描与嗅探

每年我们国家的互联网应急中心（CNCERT/CC）都会对过去一年里所有的网络安全事件进行统计，像我们熟知的计算机病毒、网络诈骗，还有同学们可能没有听过的拒绝服务攻击、Web 攻击技术等都是重点调查的对象。

大家千万不能小瞧这些安全事件，就是这些事件造成了现在网络上的各种隐私泄露和经济损失的恶果。人们使用网络越多，安全问题就变得越严重。在这一章中我们将为大家介绍网络攻防技术的基础技术——网络扫描与嗅探。

1.1 基础知识

1.1.1 数据传输过程

计算机网络就像是一个看不见的“天网”一样，只要有一方连入 Internet 上，就算是再远我们都能够找到。这个几乎让人察觉不到的巨大的“天网”实际上具有十分复杂的结构和运行机制。下面我们就来学习一下数据在 Internet 中是怎样传输的。

（1）数据是在什么中传输的？

我们使用水管将水引导流到别的地方，而数据的传输也需要一个有方向的管道。目前最先进的传输技术就是光纤，使用了这种技术的数据将会变成光信号，以世界上最快的速度到达任何想去的地方，如图 1-1 所示。

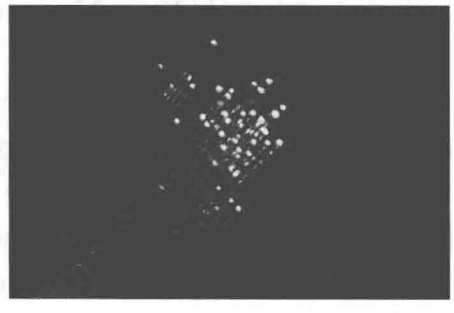

图 1-1

（2）数据怎样找到自己的目的地？

世界上的每一个地方都有自己不同的邮政编码，而 Internet 上的计算机也有自己的地址编码，也就是我们常说的 IP 地址。

（3）数据传输的过程中经过了什么？

如图 1-2 所示，就像人们在生活中寄出一封信一样，数据在发送之前也是要被装进“信封”、贴上“邮票”再“寄出”的。Internet 的结构十分复杂，可以简单地分成五层，即 TCP 协议，数据每经过一层就会被包裹上一层“信封”，而且每一个“信封”都有不同的作用。TCP 协议模型如图 1-3 所示。

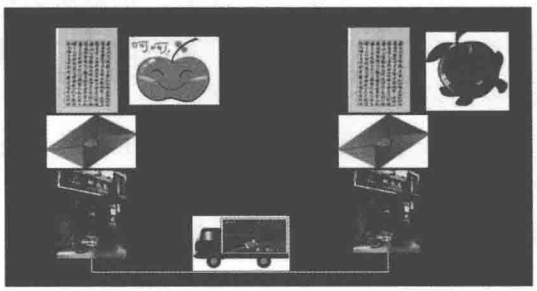

图 1-2

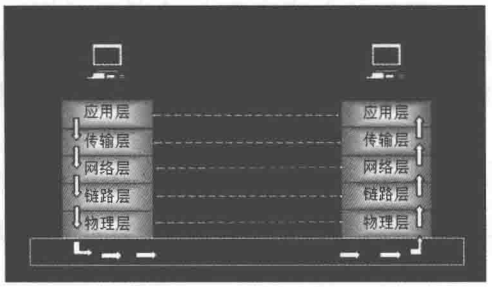

图 1-3

1.1.2 IP 地址

IP 地址是指互联网协议地址（Internet Protocol Address，又称网际协议地址），是 IP Address 的缩写。IP 地址是 IP 协议提供的一种统一的地址格式，它为互联网上的每一个网络和每一台主机分配一个逻辑地址，以此来屏蔽物理地址的差异。常见的 IP 地址分为 IPv4 与 IPv6 两大类。

1. 详细介绍

IP 地址被用来给 Internet 上的每台电脑编一个号。大家日常见到的情况是每台联网的 PC 上都需要有 IP 地址，才能正常通信。我们可以把 PC 比作“一部电话”，那么“IP 地址”就相当于“电话号码”，而 Internet 中的路由器，就相当于电信局里的“程控式交换机”。

IP 地址是一个 32 位的二进制数，通常被分割为 4 个 8 位二进制数（也就是 4 个字节）。IP 地址通常用“点分十进制”表示成 a.b.c.d 的形式，其中，a、b、c、d 都是 0 ~ 255 之间的十进制整数。例如：点分十进制 IP 地址 100.4.5.6，实际上是以下 32 位二进制数：01100100.00000100.00000101.00000110。

IP 地址编址方案如下：将 IP 地址空间划分为 A、B、C、D、E 五类，其中 A、B、C 是基本类，D、E 类作为多播和保留使用。

IPv4 就是有 4 段数字，每一段最大不超过 255。由于互联网的蓬勃发展，IP 位址的需求量越来越大，使得 IP 位址的发放趋于严格。各项资料显示，全球 IPv4 位址可能在 2005 年至 2010 年间全部发完（实际情况是在 2011 年 2 月 3 日 IPv4 位地址发完）。

地址空间的不足必将妨碍互联网的进一步发展。为了扩大地址空间，有关机构通过 IPv6 重新定义地址空间。IPv6 采用 128 位地址长度。在 IPv6 的设计过程中，除了一劳永逸地解决了地址短缺问题以外，还考虑了在 IPv4 中解决不好的其他问题。

2. IP 地址的分配

TCP/IP 协议需要针对不同的网络进行不同的设置，且每个节点一般需要一个“IP 地址”、一个“子网掩码”、一个“默认网关”。不过，可以通过动态主机配置协议（DHCP）给客户端自动分配一个 IP 地址，既避免了出错，也简化了 TCP/IP 协议的设置。

3. IP 地址分类

最初设计互联网络时，为了便于寻址以及构造层次化网络，每个 IP 地址包括两个标识码（ID），即网络 ID 和主机 ID。同一个物理网络上的所有主机都使用同一个网络 ID，网络上的一个主机（包括网络上工作站、服务器和路由器等）有一个主机 ID 与其对应。Internet 委员会定义了 5 种 IP 地址类型以适合不同容量的网络，即 A 类 ~ E 类。

其中 A、B、C3 类（如表 1-1 所示）由 InternetNIC 在全球范围内统一分配，D、E 类为特殊地址。

表 1-1

类别	最大网络数	IP 地址范围	最大主机数	私有 IP 地址范围
A	126	0.0.0.0 ~ 127.255.255.255	16777214	10.0.0.0 ~ 10.255.255.255
B	16384	128.0.0.0 ~ 191.255.255.255	65534	172.16.0.0 ~ 172.31.255.255
C	2097152	192.0.0.0 ~ 223.255.255.255	254	192.168.0.0 ~ 192.168.255.255

4. 特殊的网址

（1）每一个字节都为 0 的地址（0.0.0.0）对应于当前主机。

（2）IP 地址中的每一个字节都为 1 的 IP 地址（255.255.255.255）是当前子网的广播地址。

（3）IP 地址中凡是以 11110 开头的 E 类 IP 地址都保留用于将来或实验使用。

（4）IP 地址中不能以十进制 127 作为开头，该类地址中数字 127.0.0.1 ~ 127.255.255.255 用于回路测试，例如：127.0.0.1 可以代表本机 IP 地

址，用 http://127.0.0.1 就可以测试本机中配置的 Web 服务器。

（5）网络 ID 的第一个 8 位组也不能全置为 0，全 0 表示本地网络。

5. 实用操作——查任意人 IP

1）主动查对方的 IP

查任意人 IP 地址的基本思路是：若想知道对方的地址，只需设法让对方访问自己的 IP 地址就可以了。一旦对方来访问，也就建立了一个 SOCKET 连接，就可以轻松地捕获他（她）的 IP 地址。当然前提是他得在线。

（1）申请一个转向域名，如 126com 等，并在网上做一个主页（无论怎么简单都可以，目的只是为了查 IP 地址）。

（2）在你想查别人 IP 的时候，到你申请域名的地方，将链接转到你的 IP。

（3）打开查 IP 地址的软件。

（4）联系那个你想查其 IP 地址的人，想办法让他登录你的网站看看，给他这个转向域名。

（5）当他输入此网址以后，域名会自动指向你的 IP，此时你就能知道对方的 IP 了。

（6）当你查到对方的 IP 地址后，再将转向的地址改为你网站的地址，这样可达到隐藏自己的目的。

2）被动查对方 IP

如今的互联网上真的不大安全，总有一些不怀好意的人拿着“扫描器”扫来扫去。如果你想查那个扫描你电脑的人的 IP，可用下面两种方法。

一种做法是用“天网”软件，用软件默认的规则即可。如果有人扫描你的电脑，那么在“日志”中就可以看到那个扫描你的人的 IP 地址了，他扫描你电脑用的哪个端口也可从中看出。

另外一种做法是用“黑客陷阱”软件，这些软件可以欺骗对方你的某些端口已经打开，让他误以为你已经中了木马，当他与你的电脑产生连接时，他的 IP 就记录在这些软件中了。以“小猪快跑”为例，在该软件中有个非常不错的功能：“自定义密码欺骗端口设置”，你可以用它来自定义开启 10 个端口以监听扫描。

1.1.3 Ping 命令

Ping 命令是我们在判断网络故障常用的命令，但你真正明白这个命令运行后会发生什么，以及出现的各种信息说明了什么吗？其实熟练掌握 Ping 命令的各种技巧可以帮助你解决很多网络故障。下面我们就来详细了解一下 Ping 命令。

它是用来检查网络是否通畅或者网络连接速度的命令。作为一个与网络联系密切的管理员或者黑客来说，Ping 命令是第一个必须掌握的 DOS 命令。它的原

理是这样的：网络上的机器都有唯一确定的 IP 地址，我们给目标 IP 地址发送一个数据包，对方就要返回一个同样大小的数据包。根据返回的数据包我们可以确定目标主机的存在，从而初步判断目标主机的操作系统等信息。下面就来看看它的一些常用的操作。先看帮助，在 DOS 窗口中键入：ping /？回车，出现如图 1-4 所示的帮助画面。

```
D:\>ping /?

Usage: ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS]
            [-r count] [-s count] [[-j host-list] | [-k host-list]]
            [-w timeout] target_name

Options:
    -t             Ping the specified host until stopped.
                   To see statistics and continue - type Control-Break;
                   To stop - type Control-C.
    -a             Resolve addresses to hostnames.
    -n count       Number of echo requests to send.
    -l size        Send buffer size.
    -f             Set Don't Fragment flag in packet.
    -i TTL         Time To Live.
    -v TOS         Type Of Service.
    -r count       Record route for count hops.
    -s count       Timestamp for count hops.
    -j host-list   Loose source route along host-list.
    -k host-list   Strict source route along host-list.
    -w timeout     Timeout in milliseconds to wait for each reply.
```

图 1-4

在此，我们只要掌握一些基本的有用参数就可以了。

-t 表示不间断地向目标 IP 发送数据包，直到我们强迫其停止。试想，如果你使用 100M 的宽带接入，而目标 IP 是 56K 的小“猫”，那么要不了多久，目标 IP 就因为承受不了这么多的数据而掉线，那么，一次攻击就这么简单地实现了。

-l 定义发送数据包的大小，默认为 32 字节，可以利用它最大定义 65 500 字节。结合上面介绍的 -t 参数一起使用，会有更好的效果。

-n 定义向目标 IP 发送数据包的次数，默认为 3 次。如果网络速度比较慢，3 次对我们来说也浪费了不少时间，因为现在我们的目的仅仅是判断目标 IP 是否存在，那么就定义为一次。说明一下，如果 -t 参数和 -n 参数一起使用，Ping 命令就以位于后面的参数为标准，比如 Ping IP -t -n 3，虽然使用了 -t 参数，但并不是一直 Ping 下去，而是只 Ping 3 次。另外，Ping 命令不一定非得 Ping IP，也可以直接 Ping 主机域名，这样就可以得到主机的 IP 了。

下面我们举个例子来说明具体用法，如图 1-5 所示。这里 time=2ms 表示从发出数据包到接收到返回数据包所用的时间是 2 毫秒，从这里可以判断网络连接速度的快慢。从 TTL 的返回值可以初步判断被 Ping 主机的操作系统，之所以

```
D:\>ping 192.168.0.7 -l 65500 -t

Pinging 192.168.0.7 with 65500 bytes of data:

Reply from 192.168.0.7: bytes=65500 time=2ms TTL=32
Reply from 192.168.0.7: bytes=65500 time=2ms TTL=32
Reply from 192.168.0.7: bytes=65500 time=2ms TTL=32
Reply from 192.168.0.7: bytes=65500 time=2ms TTL=32
Reply from 192.168.0.7: bytes=65500 time=2ms TTL=32
Reply from 192.168.0.7: bytes=65500 time=2ms TTL=32
Reply from 192.168.0.7: bytes=65500 time=2ms TTL=32
```

图 1-5

说“初步判断”是因为这个值是可以修改的。这里 TTL=32 表示操作系统可能是 Windows 98。

1.1.4 IPConfig

IPConfig 实用程序可用于显示当前的 TCP/IP 配置的设置值。这些信息一般用来检验人工配置的 TCP/IP 设置是否正确。但是，如果你的电脑和所在的局域网使用了动态主机配置协议（Dynamic Host Configuration Protocol，DHCP，Windows NT 下一种把较少的 IP 地址分配给较多主机使用的协议，类似于拨号上网的动态 IP 分配），这个程序所显示的信息也许更加实用。

1. 常用选项

当使用 ipconfig 命令时不带任何参数选项，那么它显示每个已经配置了的接口的 IP 地址、子网掩码和缺省网关值。

参数简介（也可以在 DOS 方式下输入 ipconfig /？进行参数查询）如下。

- ipconfig /all：显示本机 TCP/IP 配置的详细信息。
- ipconfig /release：DHCP 客户端手工释放 IP 地址。
- ipconfig /renew：DHCP 客户端手工向服务器刷新请求。
- ipconfig /flushdns：清除本地 DNS 缓存内容。
- ipconfig /displaydns：显示本地 DNS 内容。
- ipconfig /registerdns：DNS 客户端手工向服务器进行注册。
- ipconfig /showclassid：显示网络适配器的 DHCP 类别信息。
- ipconfig /setclassid：设置网络适配器的 DHCP 类别。

2. 举例说明

在 RUN（运行）窗口中输入 CMD，打开 DOS 窗口。

在盘符提示符中输入 ipconfig /all 后回车。

显示如下（若想查自己或网络中存在的网络信息就用这种方法）：

Windows IP Configuration【Windows IP 配置】（中文意思，下同）

Host Name.....: PCNAME【域中计算机名、主机名】

Primary Dns Suffix.....:【主 DNS 后缀】

Node Type.....: Unknown【节点类型】

IP Routing Enabled.....: No【IP 路由服务是否启用】

WINS Proxy Enabled.....: No【WINS 代理服务是否启用】

Ethernet adapter:【本地连接】

Connection-specific DNS Suffix :【连接特定的 DNS 后缀】