“十二五”普通高等教育本科国家级规划教材

教育部“高等学校教学质量与教学改革工程”立项项目

孙建国 主编
张立国 汪家祥 夏松竹 编著

网络安全实验教程

（第3版）

计算机科学与技术专业实践系列教材

清华大学出版社

“十二五”普通高等教育本科国家级规划教材

计算机科学系列教材

教育部“高等学校教学质量与教学改革工程”立项项目

网络安全实验教程（第3版）

孙建国 主编
张立国 汪家祥 夏松竹 编著

清华大学出版社
北京

内容简介

本书基于网络安全体系结构，选择最新的网络安全实用软件和技术，在基本的网络安全实用技术和理论基础上，按照网络分析、远程控制技术、SSL-VPN 技术、防火墙技术、入侵检测技术和虚拟蜜网技术系统讲授网络安全实验内容。通过基础网络安全体系结构基本理论和方法的学习和实验训练，使学生建立网络信息安全的体系概念，了解网络协议、数据包结构、网络安全管理技术等在计算机系统中的重要性。

本书取材新颖，采用实例教学的组织形式，内容由浅入深、循序渐进。书中给出了大量设计实例及扩展方案，部分内容具有工程实践价值。本书适合作为高等学校计算机类、电子类和自动化类等相关专业的教材和参考书。

图书在版编目(CIP)数据

网络安全实验教程/孙建国主编. —3 版. —北京：清华大学出版社，2017
(计算机科学与技术专业实践系列教材)
ISBN 978-7-302-45618-6

Ⅰ. ①网…　Ⅱ. ①孙…　Ⅲ. ①网络安全－高等学校－教材　Ⅳ. ①TN915.08

中国版本图书馆 CIP 数据核字(2016)第 304761 号

责任编辑：张瑞庆
封面设计：傅瑞学
责任校对：李建庄
责任印制：李红英

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
课件下载：http://www.tup.com.cn，010-62795954

印 装 者：清华大学印刷厂
经　　销：全国新华书店
开　　本：185mm×260mm　　**印　　张**：18.75　　**字　　数**：456 千字
版　　次：2011 年 7 月第 1 版　2017 年 1 月第 3 版　　**印　　次**：2017 年 1 月第1 次印刷
印　　数：1～1000
定　　价：39.00 元

产品编号：072471-01

前　言

1. 写作背景

目前，我国高等教育的信息安全学科和专业方向设置问题受到非常大的关注。对于信息安全专业的本科生教育而言，其基本的培养方案、课程设置和教学大纲都需要根据新的形势发生变革，保密与信息安全专业方向也在积极地进行准备。

在新形势下，对于信息安全专业人才的培养标准是具有宽厚的理工基础，掌握信息科学和管理科学专业基础知识，系统掌握信息安全与保密专业知识，具有良好的学习能力、分析与解决问题能力、实践与创新能力。特别是在能力方面，要求本专业学生能够做到具有设计和开发信息安全与防范系统的基本能力，具有获取信息和运用知识解决实际问题的能力，具有良好的专业实践能力和基本的科研能力。

实践学时的设置不仅起到加深学生对理论课所学知识的理解的作用，还有助于培养学生形成理论与实践相结合解决实际问题的能力。对于实现当前的高等教育改革目标，提高毕业生综合素质具有重要的意义。但是，受实验设备所限，各课程的实验环节比较分散，分布在不同的实验平台或实验课程中，缺乏连贯性和整体性。网络安全课程实践环节的设立，是对计算机网络、现代密码学、信息系统安全、网络安全、软件安全和信息安全管理等专业核心课程的有效支撑。

本教材的编写思路是从网络安全的体系架构中，确定需要重点讲授和考核的内容，并针对具体内容选择最具代表性的实用型软件工具或主流技术，将基础实验和扩展实验相结合，既满足日常的实验教学活动，又能够促进学生创新实践能力的培养和提高。

2. 本书特点

本书兼顾高等学校理论教学与学生实践能力培养的需求，借鉴国外名校信息安全专业课程设置及相关课程内容安排，组织相关理论知识，设计实验用例，力争理论详尽、用例科学、指导到位。配合高等学校的计算机网络、现代密码学、信息系统安全、网络安全、软件安全和信息安全管理等课程的实践教学环节，突出实用性，所有实验可操作性强，与实践结合紧密。本书不仅介绍网络安全的核心理论和主要技术，更着重介绍在网络安全管理和实践过程中如何运用系统软件支撑和维护网络健康运行。

本书可以作为信息安全专业及相关专业计算机网络、现代密码学、信息系统安全、网络安全和信息安全管理等课程的实践教材，书中的全部实验示例都经过精心的设计和完全的调试，可以放心使用。

3. 内容安排

本书的内容安排如下：

- 第 1 章介绍网络安全的基本概念和发展历程，以及网络安全与信息安全的密切联系，并介绍网络安全实验的特点和基本要求。
- 第 2 章介绍网络安全的研究意义和研究内容，主要包括密码学、防火墙技术、网络入侵检测、数据备份与容灾、防病毒技术，并介绍网络身份认证技术。

- 第 3 章介绍网络分析实验的原理和技术，重点介绍基于 Sniffer Pro 嗅探软件的数据包捕获和网络监视等功能，并增加对多种网络协议进行嗅探分析的扩展实验环节。
- 第 4 章介绍远程控制软件 pcAnywhere 的安装和使用方法，讲解主控端、被控端的配置方法，并介绍远程文件控制的操作方式。
- 第 5 章介绍内存溢出的概念，并介绍针对内存溢出的漏洞攻击实验。
- 第 6 章介绍防火墙技术，并结合天网防火墙和瑞星防火墙，讲述防火墙的使用及配置方法。
- 第 7 章介绍入侵检测技术，重点讲述 Snort 入侵检测工具的使用方法。
- 第 8 章讨论常见的 Web 漏洞，并介绍针对 Web 漏洞扫描攻击实验。
- 第 9、10、11、12、13、14 章分别介绍主机探测及端口扫描实验、口令破解及安全加密电邮实验、自动化浏览器攻击实验、木马植入与防范实验、邮件钓鱼社会工程学实验、网络服务扫描实验。

4. 致谢

首先感谢哈尔滨工程大学计算机科学与技术学院、国家保密学院的各位老师和研究生的大力支持和热情帮助。以下同学参与了本书实验示例代码的编写和调试，以及原始资料的翻译和整理工作：曹翠玲、王文彬、李慧敏、寇亮等，感谢他们付出的辛勤劳动。感谢本教材的主审印桂生教授的热情帮助。

感谢评阅专家对本书提出的宝贵修改意见，这些意见对于完善和提高全书质量起到了关键的作用。

感谢清华大学出版社的张瑞庆编审，没有她的热情鼓励和无限耐心，本书是不可能完成的。

本书的编写得到国家自然科学基金（61472096，61202455）、省自然科学基金（F201306）、中央高校基础科研基金（HEUCF100609）的支持，在此一并致谢。

作者虽然从事信息安全实践教学多年，但是由于水平所限，书中难免存在缺点和错误，恳请读者提出宝贵意见，作者的联系方式为 sunjianguo@hrbeu.edu.cn。

作　者

2016 年 9 月

目　录

第 1 章　网络安全实验概述

1.1　引　　论

1.1.1　网络安全现状及发展

网络安全是指网络系统的软件、硬件及其存储的数据处于保护状态，网络系统不会由于偶然的或者恶意的冲击而受到破坏，网络系统能够连续可靠地运行。网络安全是一门涉及计算机科学、网络技术、通信技术、密码技术、信息安全技术、应用数学和信息论等多研究领域的综合性学科。概括地说，凡是涉及网络系统的保密性、完整性、可用性和可控性的相关技术和理论都是网络安全的研究内容。

1.1.1.1　网络安全问题

随着计算机技术和互联网技术的飞速发展，数字化信息已经成为社会发展的重要保证。例如，数字化城市、数字化国防的建设都需要大量网络信息支持。快速发展的各类网络将这些数字信息紧密地联系在一起，与之相伴的是随时可能发生的各类安全问题。

- 人为安全问题：信息泄漏、信息窃取、数据篡改、计算机病毒。
- 设备安全问题：自然灾害、设计缺陷、电磁辐射。

2016 年 6 月，国家计算机网络应急技术处理协调中心发布了《2015 年中国互联网网络安全报告》，报告对我国目前的网络安全状况进行了总体分析，总体状况概括为以下几点：

- 基础通信网络安全防护水平进一步提升。
- 我国域名系统防御拒绝服务攻击能力显著提升。
- 工业互联网面临的网络安全威胁加剧。
- 针对我国重要信息系统的高强度有组织攻击威胁形势严峻。
- 我国境内木马和僵尸网络控制端数量下降，首次出现境外木马和僵尸网络控制端数量多于国内的现象。
- 个人信息泄露事件频繁发生，个人信息泄露引发网络诈骗和勒索等“后遗症”。
- 移动互联网恶意程序数量大幅增长，大量移动恶意程序的传播渠道转移到网盘或广告平台等网站，应用软件供应链接安全问题凸显。
- DDoS 攻击仍然是我国互联网面临的严重安全威胁之一。
- 网络安全高危漏洞频现，网络设备安全漏洞风险依然较大，涉及重要行业和政府部门的高危漏洞事件持续增多，修复进度未跟上步伐，智能联网设备暴露出的安全漏洞问题严重。
- 网页仿冒和网页篡改事件暴涨，植入暗链是网页篡改的主要攻击方式。

1.1.1.2　网络安全技术

网络安全技术主要包括防火墙技术、入侵检测技术以及防病毒技术。这 3 种网络安全

技术还是针对数据、单一系统以及软硬件本身的安全保障。

首先，从用户角度来看，虽然安装了防火墙，但是仍避免不了蠕虫、垃圾邮件、病毒以及拒绝服务攻击等网络危害事件的发生。

其次，入侵检测产品在提前预警方面存在不足，对于危害程序和代码的精确定位以及系统全局管理能力还有很大的提升空间。

最后，虽然很多用户在系统终端上都安装了防病毒产品，但是内网安全问题仍然突出，尤其是安全策略的执行、外来非法侵入、补丁管理以及操作行为规范制订等方面。

目前来看，网络安全的防护重点将集中在信息语义范畴和网络行为。

1.1.1.3 网络安全发展趋势

在网络混合攻击时代，功能单一的防火墙系统无法满足业务的需要，防火墙技术必须具备多种安全功能，如基于应用协议层防御、低误报率检测、高可靠高性能平台和统一组件化管理技术等，由此 UTM(Unified Threat Management，统一威胁管理)技术应运而生。

UTM 在统一的产品管理平台下，集防火墙、VPN、网关防病毒、IPS 和防御拒绝服务攻击等众多产品功能于一体，实现了多种防御功能，向 UTM 方向演进将是防火墙的发展趋势。

UTM 设备应具备以下特点。

(1) 网络安全协议层防御。主要针对 IP 地址、端口等静态信息进行防护和控制，除了传统的访问控制外，还需对垃圾邮件、拒绝服务、黑客攻击等外部威胁进行综合检测和主动防御。

(2) 通过分类检测技术降低误报率。串联接入的网关设备一旦误报过高，将会严重影响系统的正常服务，给用户带来灾难性的后果。IPS 理念在 20 世纪 90 年代就被提出，但是目前 IPS 部署非常有限，影响其部署的一个重要问题就是误报率过高。分类检测技术可以大幅度降低误报率，针对不同的攻击类型，采取不同的检测技术，如防御拒绝服务攻击、防蠕虫和黑客攻击、防垃圾邮件攻击等，从而显著降低误报率。

(3) 高可靠性、高性能的硬件支撑平台。

(4) 一体化管理。UTM 设备具有能够统一控制和管理的平台，使用户能够有效地管理。设备平台可以实现标准化并具有可扩展性，用户可在统一的平台上进行组件管理，同时，一体化管理也能消除信息产品之间由于无法沟通而带来的信息孤岛，从而在应对各种各样攻击威胁的时候，更好地保障用户的网络安全。

1.1.1.4 网络威胁趋势分析

在信息网络普及的时代，信息安全威胁随时存在，且不断增加，信息网络安全性正逐步得到人们的重视。在当前复杂的网络应用环境下，信息网络所面临的安全形势异常严峻。来自中国电子商务研究中心的报告列举了如下严重的网络威胁。

(1) 垃圾邮件和网络欺骗。

社交网站成为网络安全的重灾区。2010 年，Koobface 蠕虫等安全问题对社交网站用户带来巨大威胁。从这些软件攻击过程来看，正逐步由攻击系统、窃取资料的被动方式转变为主动攻击模式。安全专家认为，恶意软件作者正在拓展攻击范围，把恶意软件植入社交网站

应用层内部，攻击者可以毫无限制地窃取用户的资料和登录密码。

思科公司在其2009年《年度安全报告》中揭示了社交媒体（尤其是社交网络）对网络安全的影响，并探讨了个体本身在为网络犯罪创造机会方面所起的关键作用。社交网络已经成为网络犯罪的导火索，网站成员过于信任社区伙伴，根本没有采取任何阻止恶意软件和计算机病毒的预防措施。这些不良用户行为以及系统、操作漏洞结合在一起具有不可估量的破坏性，将大幅增加网络安全风险。

2015年，我国发生多起危害严重的个人信息泄露事件。例如，某应用商店用户信息泄露事件、约10万条应届高考考生信息泄露事件、酒店入住信息泄露事件、某票务系统近600用户信息泄露事件等。此外，个人信息泄露事件频繁被媒体报道，反映出社会对此类问题的关注度不断提升。

（2）云计算为网络犯罪提供了新的技术。

云计算在2009年取得了长足的发展，但应该清醒地认识到：市场的快速发展会牺牲一定的安全性，攻击者今后将把更多的时间用于挖掘云计算服务提供商的API（应用编程接口）漏洞方面。

随着越来越多的IT功能通过云计算来提供，网络犯罪也顺应了这一趋势。网络攻击者和黑客也将效仿企业做法使用基于云计算的工具，以便更有效地部署远程攻击，甚至借此大幅拓展攻击范围。

云提供了许多工具，可以帮助黑客，特别是那些用偷来的信用卡和假的IP地址来获取资源的黑客，他们的活动难以追查。正如《计算机世界》中“云中的密码破解”文章中指出的那样，黑客可以利用基于云的计算资源，例如破解密码，这是一个强力的技术，破解一个中等长度和中等复杂程度的密码都需要很长的时间和大量的计算资源。文章指出了当破解密码时僵尸网络和云的关系：“对于一个黑客来说，可用于需要的计算的资源有两大来源，一个是消费者个人计算机组成的僵尸网络，另一个是由服务提供商提供的‘基础设施作为一种服务（iaas）’的云。任何一个都能够提供强大的计算能力，都可满足专用的计算需求”。对于云计算将被黑客利用这个严峻的问题，各大安全公司都把精力放在与云计算相关的安全服务上，提供加密、目录管理、反垃圾邮件和恶意程序扫描等各类解决方案。据悉，著名安全评测机构VB100号召安全行业联合起来，组成一个对抗恶意程序的共同体，分享技术和资源。

（3）智能手机安全问题愈发严重。

随着移动应用的不断增多，智能设备的受攻击范围也在不断扩大，移动安全所面临的问题将会越来越严重。目前，已经出现了手机蠕虫病毒和智能手机盗号木马病毒，虽然这些病毒不能自我传播，还需要依靠计算机来传播，但是可以预计到，具有自我传播能力的病毒势必出现，将严重威胁各类移动终端设备。针对安卓平台的窃取用户短信、通讯簿、微信聊天记录等信息的恶意程序将会爆发。安卓平台感染此类恶意程序后，大量涉及个人隐私的信息通过邮件发送到指定邮箱。

总体而言，安全专家认为，随着智能手机业务范围的拓展，用户利用手机来处理银行交易、社交网站和其他业务，黑客将越来越发关注这一攻击领域。

（4）搜索引擎成为黑客全新的赢利方式。

黑客不断寻找新的方法借助钓鱼网站吸引用户，利用搜索引擎优化技术展开攻击便是其中的一种方法。谷歌（Google）和必应（Bing）对实时搜索的支持也将吸引黑客进一步提升

相关技术。作为一种攻击渠道，搜索引擎是非常理想的选择，因为用户通常都非常信任搜索引擎，对于排在前几位的搜索结果更是没有任何怀疑，这就给了黑客可乘之机，从而对用户发动攻击。

(5)“僵尸网络”继续猖獗。

所谓僵尸，是指受恶意软件感染而被犯罪分子远程操控的个人计算机。犯罪分子通过网络将病毒植入成千上万台个人计算机，实现大范围的操控，犯罪分子使用这些计算机进行各种网络犯罪，如垃圾邮件发送、服务阻断攻击、网络钓鱼及非法主机攻击等，基本覆盖了所有网络犯罪行为。从当前的网络安全态势来看，愈来愈多的计算机皆受到感染，而被感染的时间也愈来愈长了。

2015 年 12 月 2 日，全国各执法机构在微软安全研究人员的协助下，成功地摧毁了由恶意软件 Win32/Dorkbot 组成的大型僵尸网络。该僵尸网络的影响非常广泛，已经感染了 190 多个国家的一百多万台个人计算机。Dorkbot 主要通过 USB 闪存、即时通信软件和社交网络进行传播。它不仅盗取用户凭证和个人信息、关闭安全保护软件，而且还会传播其他多种流行恶意软件，影响非常恶劣。

(6) 传统攻击方式再度兴起。

IBM X-Force 团队预计，大规模蠕虫攻击将再度兴起，与此同时，DDoS(分布式拒绝服务攻击)也将重新成为主流攻击方式，木马病毒仍将占据主要地位。

来自中国电子商务研究中心的报告显示，据 Websense 的卢纳德预计，电子邮件攻击也有重新抬头之势。研究人员已经发现，通过 PDF 等邮件附件发动的攻击开始增加。卢纳德说：“恶意邮件攻击在 2005 年至 2008 年期间已经销声匿迹。而现在不知出于何种原因，这种攻击方式又再度出现”。根据中国互联网协会组织的 2014 年第四季度中国反垃圾邮件状况调查报告显示，用户电子邮箱平均每周接收到的全部邮件数量为 35.0 封，平均每周接收到的垃圾邮件数量为 14.3 封，垃圾邮件占比是 41.0%。

从网络威胁方式来看，威胁方式的演进主要体现在以下几个方面。

(1) 实施网络攻击的主体发生了变化。

实施网络攻击的主要人群正由好奇心重、炫耀攻防能力的兴趣型黑客群，向更具犯罪思想的赢利型攻击人群过渡，针对终端系统漏洞实施“zero-day 攻击”和利用网络攻击获取经济利益逐步成为主要趋势。其中，以僵尸网络、间谍软件为手段的恶意代码攻击，以敲诈勒索为目的的分布式拒绝服务攻击，以网络仿冒、网址嫁接、网络劫持等方式进行的在线身份窃取等安全事件持续快速增加，而针对 P2P、IM 等新型网络应用的安全攻击也在迅速发展。

(2) 企业对安全威胁的认识发生了变化。

过去，企业信息网络安全的防护中心一直定位于网络边界及核心数据区，通过部署各种各样的安全设备来实现安全保障。但是，随着企业信息边界安全体系的基本完善，信息安全事件仍然层出不穷。企业内部人员安全管理不足、办公时间肆意上网、计算机使用不当等行为都使网络信息安全风险变得更为严重。

(3) 安全攻击的主要手段发生了变化。

安全攻击的手段多种多样，典型的手段包含拒绝服务攻击、非法接入、IP 欺骗、网络嗅探、木马攻击以及垃圾邮件等。随着攻击技术的发展，攻击手段正由单一攻击模式向多种攻击手段结合的复合性攻击发展。结合多种攻击手段的复合模式所带来的危害远远大于单一

模式的攻击，而且更加难以控制。

1.1.2 黑客及黑客入侵技术

1.1.2.1 黑客定义

黑客是计算机专业中的一个特殊的群体，随着计算机系统被攻击报道的逐渐增多，黑客越发成为业界的关注焦点。“黑客”是英文 hacker 一词的音译，是指计算机系统的非法入侵者。

在早期麻省理工学院的校园俚语中，“黑客”有“恶作剧”之意，尤指手法巧妙、技术高明的恶作剧；在日本《新黑客词典》中，黑客的定义是“喜欢探索软件程序奥秘，并从中增长了个人才干的人”。目前，黑客的准确界定为“以保护网络为目的，具有硬软件高级知识，有能力通过创新的方法剖析系统的技术精英，他们以侵入为手段找出网络漏洞，进而令互联网络趋于完善和安全。”一般认为，黑客起源于 20 世纪 50 年代麻省理工学院的实验室，他们热衷于解决难题。

20 世纪 60 年代至 70 年代，“黑客”富于褒义，专指那些独立思考、奉公守法的计算机爱好者，这些人智力超群，对计算机技术全身心投入，在他们看来，黑客活动意味着对计算机的最大潜力进行智力上的自由探索，为计算机技术的发展做出巨大贡献。正是这些黑客，倡导了一场个人计算机革命，倡导了现行的计算机开放式体系结构。现在黑客使用的入侵计算机系统的基本技巧，如破解口令（password cracking）、开天窗（trapdoor）、走后门（backdoor）、安放特洛伊木马（Trojan horse）等，都是在这一时期发明的。从事黑客活动的经历，成为后来许多计算机业巨子简历上不可或缺的一部分。例如，苹果公司创始人之一乔布斯就是一个典型的例子。

到了 20 世纪 80 年代至 90 年代，计算机越来越重要，大型数据库也越来越多，信息越来越集中在少数人的手里。黑客认为，信息应该共享而不应被少数人所垄断，于是将注意力转移到涉及各种机密的信息数据库上。而这时，计算机化空间已私有化，成为个人拥有的财产，社会不能再对黑客行为放任不管，必须采取行动，利用法律等手段来进行控制。黑客活动受到了打击。目前，许多政府机构已经邀请黑客为他们检验系统的安全性，甚至还请他们设计新的安保规程。

与黑客相对的是骇客，“骇客”是 cracker 的音译，就是“破坏者”的意思。骇客是贬义的，骇客做的事情更多的是破解商业软件、恶意入侵别人的网站并造成损失。利用网络漏洞破坏网络，他们具备广泛的计算机知识，但与黑客不同的是他们以破坏为目的。

黑客和骇客的基本差异在于，黑客是有建设性的，而骇客则专门搞破坏。对一个黑客来说，学会入侵和破解是必要的，但最主要的还是编程。对于一个骇客来说，他们只追求入侵的快感，不在乎技术，他们不会编程，不知道入侵的具体细节。还有一种情况是试图破解某系统或网络以提醒该系统所有者的系统安全漏洞，这群人往往被称为“白帽黑客”、“匿名客”（sneaker）或“红客”。许多这样的人是计算机安全公司的雇员，并在完全合法的情况下攻击某系统。

1.1.2.2 黑客活动

黑客的主要活动内容包括以下几个方面：

(1) 作为一个黑客,在找到系统漏洞并侵入的时候,往往都会很小心地避免造成损失,并且善意地提醒系统管理员,但是在这过程中会有许多因素都是未知的,没有人能肯定最终会是什么结果,因此,一个好的黑客不会随便攻击个人用户及站点。

(2) 编写一些有用的开源软件,这些软件都是免费的、公开的。

(3) 帮助别的黑客测试和调试软件。

(4) 黑客们都以探索漏洞与编写程序为乐,在黑客的圈子里,有许多其他事情可做,例如,维护和管理相关的黑客论坛、新闻组以及邮件列表,维持大的软件供应站点,推动 RFC 和其他技术标准,等等。

(5) 真正的黑客不会随意破解商业软件并将其广泛流传,也不会恶意侵入别人的网站并造成损失,黑客的所作所为应当更像是对于网络安全的监督。

1.1.2.3 黑客事件

历史上,发生过许多著名的黑客入侵事件。

1979 年,年仅 15 岁的凯文·米特尼克仅凭一台计算机和一部调制解调器闯入了北美空中防务指挥部的计算机主机。

1987 年,美联邦执法部门指控 16 岁的赫尔伯特·齐恩闯入美国电话电报公司的内部网络和中心交换系统。齐恩是美国 1986 年"计算机欺诈与滥用法案"生效后被判有罪的第一人。

1988 年,年仅 23 岁的大学生 Robert Morris 在 Internet 上释放了世界上首个"蠕虫"程序。Robert Morris 最初是把这个 99 行的程序放在互联网上进行试验,可结果却使得他的计算机被感染并迅速在互联网上蔓延。Robert Morris 也因此在 1990 年被判入狱。

1990 年,为了获得在美国洛杉矶地区 kiis-fm 电台第 102 个呼入者的奖励——保时捷跑车,Kevin Poulsen 控制了整个地区的电话系统,以确保他是第 102 个呼入者。最终,他如愿以偿获得跑车并为此入狱 3 年。

1995 年,来自俄罗斯的黑客 Vladimir Levin 成为历史上第一个通过入侵银行计算机系统来获利的黑客,他侵入美国花旗银行并盗走 1000 万美元。

1996 年,美国黑客 Timothy Lloyd 曾将一个 6 行的恶意软件放在了其雇主——Omega 工程公司(美国航天航空局和美国海军最大的供货商)的网络上,此事件导致 Omega 公司损失 1000 万美元。

1999 年,Melissa 病毒是世界上首个具有全球破坏力的病毒。David Smith 在编写此病毒的时候年仅 30 岁。Melissa 病毒使世界上 300 多家公司的计算机系统崩溃。整个病毒造成的损失接近 4 亿美元。David Smith 随后被判处 5 年徒刑。

2000 年,年仅 15 岁的 MafiaBoy(因为年龄太小没有公布其真实身份)在情人节期间成功侵入包括 eBay、Amazon 和 Yahoo 在内的大型网站服务器,并成功阻止了服务器向用户提供服务。他于 2000 年被捕。

2002 年 11 月,伦敦人 Gary McKinnon 在英国被指控非法侵入美国军方 90 多个计算机系统。

1994 年 4 月 20 日,中国 NCFC 工程通过美国 Sprint 公司连入 Internet 的 64K 国际专线开通,实现了与 Internet 的全功能连接,中国成为直接接入 Internet 的国家。从此,中国黑客开始了原始萌动。同年,中国第一部信息安全法规《中华人民共和国计算机信息系统安

全保护条例》颁布实施。1997 年,《中华人民共和国计算机信息网络国际联网管理暂行规定》颁布实施。

1998 年 6 月 16 日,上海某信息网的工作人员在例行检查时,发现网络遭到不速之客的袭击。同年 7 月 13 日,犯罪嫌疑人杨某被逮捕。这是我国第一例计算机黑客事件。

1999 年,中国黑客发展的历史上产生了一个高峰。这一年网络泡沫高度泛滥,黑客在这个浪潮中不可避免地泛起了泡沫。从 1999 年到 2000 年,中国黑客联盟、中国鹰派、中国红客联盟等一大批黑客网站兴起,带来了黑客普及教育。

2015 年 1 月 15 日,机锋论坛的 2300 万用户数据在网上疯传,引起公众的广泛关注。360 补天漏洞响应平台负责人赵武对此表示:“经调查,网上流传的 2300 万数据是机锋 2013 年的老数据,但是机锋论坛还有多个高危漏洞没有完全修复,其 2700 万最新用户数据也暴露在黑客的枪口下。”

2015 年 4 月,补天漏洞响应平台发布信息称:30 余个省份的社保、户籍查询、疾控中心等系统存在高危漏洞;仅社保类信息安全漏洞涉及的信息就达 5279.4 万条,包括身份证、社保参保信息、财务、薪酬和房屋等敏感信息。

2015 年 5 月 29 日,360 天眼实验室发布的报告,首次披露一种针对中国的国家级黑客攻击细节。该境外黑客组织被命名为“海莲花(OceanLocus)”,自 2012 年 4 月起,“海莲花”针对中国的海事机构、海域建设部门、科研院所和航运企业,使用木马病毒攻陷并控制政府人员、外包商、行业专家等目标人群的计算机,甚至操纵这些计算机自动发送相关情报,很明显这是一个有国外政府支持的 APT 行动。

2015 年 9 月 13 日,CNCERT/CC 接到报告称,使用非苹果公司官方渠道的 Xcode 开发工具开发 APP 时,非官方 Xcode 会向正常的 APP 植入恶意代码 XcodeGhost,且被植入恶意程序的苹果 APP 可以在 App Store 正常下载并安装使用,国内感染的用户达 2140 万,CNCERT/CC 已在 9 月 14 日发布预警通报,提醒开发者切勿使用非苹果官方渠道的 Xcode 工具,以维护广大用户的个人信息安全。

2015 年 12 月,CNCERT/CC 通报 Java 反序列化漏洞情况,该漏洞影响多块应用广泛的 Web 容器软件。远程攻击者利用漏洞可在目标系统上执行任意代码,危害较大的可以取得网站服务控制权。CNCERT/CC 对相关 Web 应用的分布情况和受漏洞影响进行了探测,发现境内主机 IP 中 Jboss、Weblogic、Jenkins 受到漏洞影响的未修复比例分别是 13.9%、50.4%、33.4%。

1.1.2.4 黑客入侵技术

黑客入侵一般分为信息收集、探测分析系统安全弱点和实施攻击 3 个步骤。

信息收集是为了了解所要攻击目标的详细信息,通常黑客会利用相关的网络协议或实用程序来收集,常用的工具如下。

- SNMP 协议:用来查阅网络系统路由器的路由表,从而了解目标主机所在网络的拓扑结构及其内部细节。
- TraceRoute 程序:能够用该程序获得到达目标主机所要经过的网络数和路由器数。
- Whois 协议:该协议的服务信息能提供所有有关的 DNS 域和相关的管理参数。
- DNS 服务器:该服务器提供了系统中可访问的主机的 IP 地址表和它们所对应的主

机名。

- Finger 协议：可以用 Finger 来获取一个指定主机上的所有用户的详细信息。
- Ping 实用程序：可以用来确定一个指定的主机的位置。

当收集到目标相关信息以后，黑客会利用探测分析系统寻找系统的安全漏洞或设计缺陷。黑客发现“补丁”程序的接口后会自己编写程序，通过该接口进入目标系统。还会使用 Talnet、FTP 等软件向目标主机申请服务，如果目标主机有应答就说明其开发了这些端口的服务。其次，使用一些公开的工具软件，如 Internet 安全扫描程序（Internet Security Scanner，ISS）、网络安全分析工具（SATAN）等来对网络进行扫描，确定安全漏洞或使用特洛伊木马来获取攻击目标系统的非法访问权。

在获得目标系统的非法访问权限后，黑客则会实施攻击，攻击可分为被动攻击与主动攻击。

- 被动攻击：攻击者只观察和分析某一个协议数据单元 PDU 而不干扰信息流，例如监听截获操作等。
- 主动攻击：攻击者对某个连接中通过的数据包进行各种处理，例如更改报文流、拒绝报文服务、伪造连接初始化等。

攻击程度包括以下等级：

- 只获得访问权（登录名和口令）。
- 获得访问权，并毁坏、侵蚀或改变数据。
- 获得访问权，并获得系统部分或整个系统控制权，拒绝拥有特权用户的访问。
- 未获得访问权，通过攻击程序引起网络持久性或暂时性的运行失败、重新启动、挂起或其他无法操作的状态。

1. 黑客攻击过程

黑客攻击过程包括以下步骤：

（1）隐藏自己的踪迹。通过清除日志、删除副本文件、进程隐藏、连接隐藏、使日志紊乱等方法销毁入侵痕迹，并在受攻击目标系统中为自己建立新的后门，以便继续访问该系统。

（2）在目标系统内安装探测软件，如特洛伊木马或其他一些远程控制程序，继续收集感兴趣的信息和敏感数据。黑客还可以目标系统为跳板向其他系统发起攻击。

（3）在被攻击目标系统上进一步获得特许访问权，开展对整个系统的攻击，毁坏重要数据乃至破坏整个网络系统。

2. 主要入侵方式

1）密码破解

密码破解包括字典攻击、伪造登录程序、密码探测程序、口令攻击、口令陷阱、网络踩点、协议栈指纹、会话劫持和非授权访问尝试等 9 种入侵方式。

- 字典攻击：是一种被动攻击，黑客获取系统的口令，然后利用字典进行匹配比较，字典攻击成功率较高。
- 伪造登录程序：是通过伪造登录界面来获得用户输入的账号和密码。
- 密码探测程序：能够反复模拟 NT 的编码过程，并与 Windows NT 系统的 SAM 密码数据库内的数据进行匹配。
- 口令攻击：通过网络监听非法得到用户口令，然后利用软件强行破解用户口令，获