HZ BOOKS
华章教育

高等院校信息安全专业规划教材

信息安全攻防
实用教程

A Practical Guide to Information Security: Attack and Defense

马洪连 ◎ 主编
刘 旸 韩 瑜 孙 亮 ◎ 编著

机械工业出版社
China Machine Press

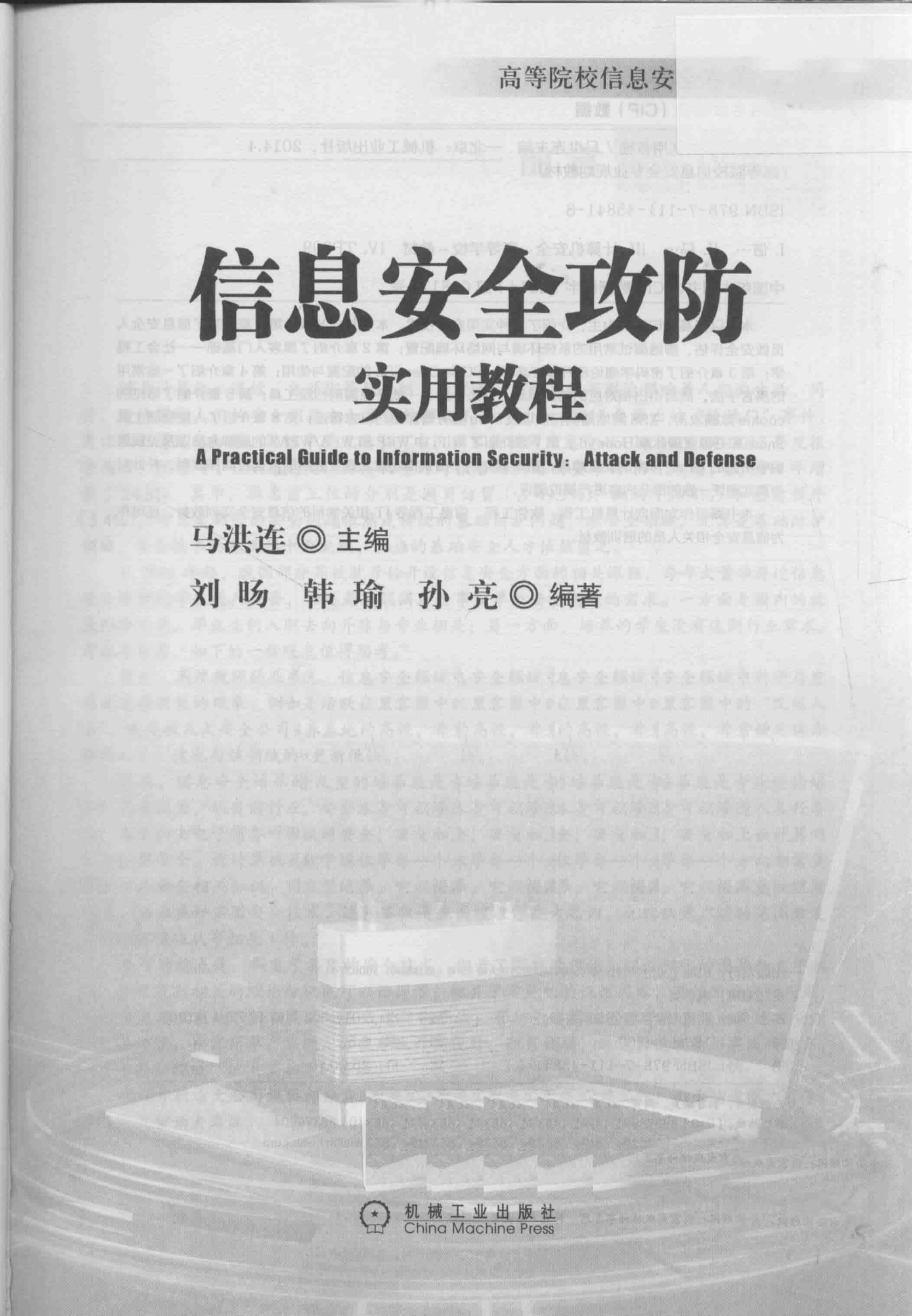
高等院校信息安

信息安全攻防
实用教程

A Practical Guide to Information Security: Attack and Defense

马洪连◎主编

刘旸　韩瑜　孙亮◎编著



机械工业出版社
China Machine Press

图书在版编目（CIP）数据

信息安全攻防实用教程 / 马洪连主编 . —北京：机械工业出版社，2014.4
（高等院校信息安全专业规划教材）

ISBN 978-7-111-45841-8

I. 信… II. 马… III. 计算机安全 – 高等学校 – 教材 IV. TP309

中国版本图书馆 CIP 数据核字（2014）第 028176 号

本书以提高意识理解为主，介绍了多种实用安全技术。本书共分 8 章，第 1 章介绍了信息安全人员做安全评估、渗透测试常用的系统环境与网络环境配置；第 2 章介绍了黑客入门基础——社会工程学；第 3 章介绍了密码学理论和开源工具 GnuPG 与 OpenSSL 的配置与使用；第 4 章介绍了一些常用的黑客手法，然后引出相对应的防护策略，并且介绍了一款开源漏洞扫描工具；第 5 章介绍了常见的 cookie 欺骗攻击、XSS 跨站漏洞扫描以及 Web 服务器加固与日志管理；第 6 章介绍了入侵检测工具 Snort 和开源蜜罐体系 Honeyd ；第 7 章介绍了 WiFi 中 WEP 和 WPA/WPA2 的破解方法以及无线路由中常见的 UPnP 带来的安全隐患；第 8 章介绍了国家推动信息安全战略的依据及测评流程，并针对与真实测评一致的部分内容进行模拟测评。

本书既可作为面向计算机工程、软件工程、信息工程等 IT 相关学科的信息安全实训教材，还可作为信息安全相关人员的培训教材。

出版发行：机械工业出版社（北京市西城区百万庄大街 22 号　邮政编码：100037）
责任编辑：朱秀英
印　　刷：北京市荣盛彩色印刷有限公司　　版　　次：2014 年 4 月第 1 版第 1 次印刷
开　　本：185mm × 260mm　1/16　　印　　张：8.5
书　　号：ISBN 978-7-111-45841-8　　定　　价：25.00 元

凡购本书，如有缺页、倒页、脱页，由本社发行部调换
客服热线：（010）88378991　88361066　　投稿热线：（010）88379604
购书热线：（010）68326294　88379649　68995259　　读者信箱：hzjsj@hzbook.com

前言

随着计算机、通信、自动化等领域的飞速发展，网络已经深刻地影响着人们的生活。同时，网络带给人们的安全问题也如噩梦般挥之不去。例如，2013 年爆出的“棱镜门”事件，更让人们清楚地知道，网络中毫无隐私可言。国家物联网应急中心 CNCERT/CC 2012 年度报告指出：2012 年，CNCERT/CC 共接收境内外报告的网络安全事件 19 124 起，较 2011 年增长了 24.5%，其中，排名前三位的分别是网页仿冒（占 49.5%）、漏洞（39.4%）和恶意程序（5.4%）。可见大部分的安全问题依然是传统的基础防护问题。在安全领域，尤其是基础防护领域，安全技术的普及仍十分欠缺，相应的基础安全人才依然匮乏。

从 2001 年起，我国部分高校就开始开设信息安全方面的相关课程，每年大量学习过信息安全课程的学生进入社会，但还是不能满足企事业单位安全岗位的需求。一方面是国内的就业形势所迫，毕业生的入职去向并非与专业相关；另一方面，培养的学生没有达到行业需求。考虑其原因，如下的一些观点值得思考。

首先，高校教师的业务能力与行业需求存在着不兼容的情况。信息安全领域中科研与应用存在着割裂的现象，例如，真正优秀的信息安全应用人才或是活跃在黑客圈中的“民间人士”，或是被几大安全公司高薪奉养的专业人员。而作为人才培养基地的高校，非常缺乏这方面的人才。这也与该领域的特殊性相关，安全领域技术的发展和更新很快。

其次，信息安全培养的针对性也存在争议。到底是专注普及型的培养还是专业型的培养？笔者认为，从目前行业情况来看，普及型培养的意义更大。安全本身可以渗透入各行各业：安全加上电子商务叫做电商安全，安全加上物联网叫做物联网安全，安全加上云计算叫做云计算安全。就计算机类学科来说，软件、网络、嵌入式、数字媒体等每一个方向都需要学习信息安全相关知识。同时普及型培养的可操作性要大于专业型培养，它以提高意识理解为主，辅以多种实用安全技术，这样不仅是在高校教师能力之内，也能从更广泛的范围激发学生的热情去从事相关工作。

本书的特点是：侧重于实用的安全技术，抛开了深奥的理论，以过程化的图片和文字叙述，即使没有相关的理论知识也可以读得懂；抛弃了常见的验证性内容，直接面向实际应用，使读者更加直观地了解相关的攻击或者防御手法；有利于计算机类的学生直接向普通安全测试人员迈进；内容简单、直观，方便学生开阔视野、积累经验，迅速拉近理论与实践的距离，使学生轻松摆脱“纸上谈兵”的窘境。

感谢中软吉大公司提供部分实验环境，感谢出版社编辑的辛苦工作！由于编者能力有限，不当之处望读者海涵。

编　者

2013 年 12 月

教学建议

本书内容按知识的重要性划分为重点内容（★）、熟悉内容（◎）和了解内容（◆），具体学时分配如下表。

教学章节	教学要求	学　时
第 1 章　准备	◎	2
第 2 章　社会工程学	★	1
第 3 章　加密与破解	★	3
第 4 章　主机攻防	★	4
第 5 章　Web 安全	★	3
第 6 章　入侵检测	◎	4
第 7 章　无线安全	◎	3
第 8 章　信息系统安全等级保护	◆	4
总学时		24

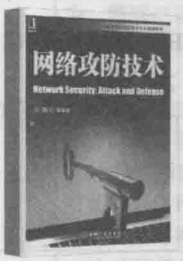
推荐阅读

信息安全导论

作者：何泾沙 ISBN：978-7-111-36272-2 定价：33.00元

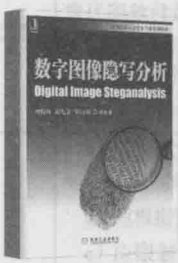
金融信息安全工程

作者：李改成 ISBN：978-7-111-28262-4 定价：35.00元



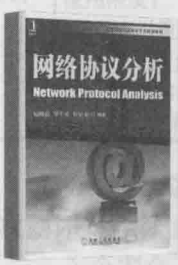
网络攻防技术

作者：吴灏 ISBN：978-7-111-27632-6 定价：29.00元



数字图像隐写分析

作者：刘粉林 刘九芬 罗向阳 ISBN：978-7-111-30517-07 定价：29.00元



网络协议分析

作者：寇晓蕤 罗军勇 蔡延荣 ISBN：978-7-111-26832-1 定价：33.00元

目录

Chapter

第1章 准备

1.1 概述

与所有传统行业一样，从事网络信息安全工作必须要遵守法律法规以及行业伦理。但是目前许多从业者是理工科出身，学校的专业课教学环节都是以技术培训为主并没有涉及太多行业性质的法律法规或者伦理课程。信息安全是一个经常涉及隐私、安全的行业，如果对这方面不了解，就可能违反法律法规或行业伦理，造成严重后果。因此，我们必须了解这方面的知识。

1.1.1 法律法规

读者首先应该清楚信息安全主要涉及的法律类型，其一般包括：民法、刑法、行政法规以及其他相关法律类型，如知识产权法、信息隐私法和隐私法等。法律法规既然是国家或地区制定的，那么在不同的国家和地区，这些法律法规也会不同。因此，我们分别从国内与国外两方面去了解和学习。

1. 国内法律法规

涉及信息安全的国家法律如下。

- 《中华人民共和国宪法》第三十五条、第四十条。
- 《中华人民共和国保守国家秘密法》共35条。
- 《中华人民共和国国家安全法》第十条、第十一条、第二十一条。
- 《中华人民共和国人民警察法》第六条、第十六条。
- 《中华人民共和国刑法》第二百一十九条、第二百二十一条、第二百二十二条、第二百八十二条、第二百八十五条、第二百八十六条、第二百八十七条、第二百八十八条、第三百六十三条、第三百六十四条、第三百六十五条、第三百六十六条、第三百六十七条。
- 《全国人民代表大会常务委员会关于维护互联网安全的决定》共7条。

- 《中华人民共和国电子签名法》共 36 条。
- 《中华人民共和国治安管理处罚法》第二十八条、第二十九条、第四十二条、第六十八条、第六十九条。

行政法规相关内容如下所示。

- 《中华人民共和国计算机信息系统安全保护条例》共 31 条。
- 《中华人民共和国计算机信息网络国际联网管理暂行规定》共 25 条。
- 《商用密码管理条例》共 27 条。
- 《中华人民共和国电信条例》第五十七条、第五十八条、第五十九条、第六十条、第六十一条、第六十二条、第六十三条、第六十四条、第六十五条、第六十六条。
- 《互联网信息服务管理办法》共 27 条。
- 《互联网上网服务营业场所管理条例》共 37 条。
- 《信息网络传播权保护条例》共 27 条。

国内相关职能部门规章和规范性文件大致如下。

（1）公安部

- 《计算机信息系统安全专用产品检测和销售许可证管理办法》
- 《计算机信息网络国际联网安全保护管理办法》
- 《金融机构计算机信息系统安全保护工作暂行规定》
- 《计算机病毒防治管理办法》
- 《互联网安全保护技术措施规定》

（2）工信部

- 《互联网电子公告服务管理规定》
- 《电信业务经营许可证管理办法》
- 《计算机信息系统集成资质管理办法（试行）》
- 《信息系统工程监理暂行规定》
- 《中国互联网络域名管理办法》
- 《非经营性互联网信息服务备案管理办法》
- 《互联网 IP 地址备案管理办法》
- 《电子认证服务管理办法》
- 《互联网电子邮件服务管理办法》
- 《中国互联网络信息中心域名争议解决办法》
- 《中国互联网络信息中心域名争议解决办法程序规则》

（3）国务院新闻办公室

- 《互联网新闻信息服务管理规定》

（4）国家密码管理局

- 《电子认证服务密码管理办法》
- 《商用密码科研管理规定》
- 《商用密码产品生产管理规定》
- 《商用密码产品销售管理规定》

（5）国家食品药品监督管理局

- 《互联网药品信息服务管理暂行规定》

- 《互联网药品交易服务审批暂行规定》

（6）卫生部

- 《互联网医疗卫生信息服务管理办法》

（7）中国银监会

- 《电子银行业务管理办法》
- 《电子银行安全评估指引》
- 《银行业金融机构信息系统风险管理指引》

（8）中国证监会

- 《网上证券委托暂行管理办法》
- 《证券期货业信息安全保障管理暂行办法》
- 《证券公司集中交易安全管理技术指引》

（9）国家保密局

- 《中华人民共和国保守国家秘密法实施办法》
- 《科学技术保密规定》
- 《计算机信息系统保密管理暂行规定》
- 《计算机信息系统国际联网保密管理规定》
- 《涉及国家秘密的通信、办公自动化和计算机信息系统审批暂行办法》
- 《涉及国家秘密的计算机信息系统集成资质管理办法（试行）》

（10）新闻出版广电总局

- 《电子出版物管理规定》
- 《关于对出版物使用互联网信息加强管理的通知》
- 《互联网出版管理暂行规定》
- 《互联网著作权行政保护办法》
- 《有线广播电视传输覆盖网安全管理办法》
- 《关于加强影视播放机构和互联网等信息网络播放 DV 片管理的通知》
- 《互联网等信息网络传播视听节目管理办法》

（11）教育部

- 《教育网站和网校暂行管理办法》
- 《高等学校计算机网络电子公告服务管理规定》

（12）铁道部（原）

- 《铁路计算机信息网络国际联网保密管理暂行规定》
- 《铁路计算机信息系统安全保护办法》

（13）其他部门

- 《中国金桥信息网公众多媒体信息服务管理办法》
- 《计算机信息网络国际联网出入口信道管理办法》
- 《中国公用计算机互联网国际联网管理办法》
- 《中国公众多媒体通信管理办法》
- 《专用网与公用网联网的暂行规定》
- 《中国教育和科研计算机网管理办法（试行）》

（14）地方性法律法规

- 《辽宁省计算机信息系统安全管理条例》
- 《湖南省信息化条例》
- 《重庆市计算机信息系统安全保护条例》

（15）司法解释

司法解释相当于对现有法律的一个补充，例如：

- 《关于审理扰乱电信市场管理秩序案件具体应用法律若干问题的解释》
- 《关于审理涉及计算机网络域名民事纠纷案件适用法律若干问题的解释》
- 《关于审理涉及计算机网络著作权纠纷案件适用法律若干问题的解释》
- 《最高人民法院关于审理非法出版物刑事案件具体应用法律若干问题的解释》
- 《最高人民法院关于审理涉及计算机网络著作权纠纷案件适用法律若干问题的解释》
- 《最高人民法院关于审理涉及计算机网络域名民事纠纷案件适用法律若干问题的解释》
- 《最高人民法院、最高人民检察院关于办理利用互联网、移动通信终端、声讯台制作、复制、出版、贩卖、传播淫秽电子信息刑事案件具体应用法律若干问题的解释》

以上这些信息安全法律法规或多或少所体现的我国信息安全的基本原则可以简单归纳为国家安全、单位安全和个人安全相结合的原则，等级保护的原则，保障信息权利的原则，救济原则，依法监管的原则，技术中立原则，权利与义务统一的原则。虽然我国信息安全的法律体系已初步形成，但还不够成熟。在这一体系中，部门规章、地方法规及规章等占了绝大多数，还没有一部信息安全的基本法。部门规章、地方法规及规章等效力层级较低，适用范围有限，相互之间可能产生冲突，也不能作为法院裁判的依据，直接影响了这些措施的效果。另外，我国现有信息安全相关法律法规普遍存在的问题是篇幅较小，规定得比较笼统，需要额外的司法解释补充。但是司法解释往往是不具备通用性和绝对的法理依据，在执行过程中也会出现争议。还有，针对行业性的信息安全法律法规还不健全，如电子商务、电子政务、网上支付、社交网络、云计算、物联网等。

2. 美国法律法规

美国历来将网络信息安全视作维护国家安全的重要内容。作为互联网诞生地的美国，是世界上第一个引入网络信息战概念和将网络信息安全应用于现实军事、文化和经济领域的国家，其网络信息安全法律规范体系较系统完善，且有连续性。美国坚持将网络信息安全保障体系作为系统工程来建设，其内容不仅涉及网络信息安全的技术保障，还包括相关的政策方针、法制建设、组织机构、管理体制以及人才培养和国际合作保障等。

1946 年出台的《原子能法》与 1947 年的《国家安全法》，是美国网络信息安全法律萌芽阶段的标志。自 1978 年以来，美国国会及政府各部门先后通过了 130 余项法律法规。1993 年，克林顿政府提出系统兴建涉及网络信息安全的《国家信息基础结构：行动纲领》，即信息高速公路（ISH）计划；1998 年颁布了《保护美国关键基础设施》总统令（PDD-63）。2000 年 1 月，美国政府发布《保卫美国的计算机空间——保护信息系统的国家计划》，同年，克林顿又提出《信息系统保护国家计划》，进一步强化了国家网络信息基础设施保护的概念，使“信息安全”成为国家安全战略的正式组成部分，正式进入国家安全战略框架。2001 年发布《信息时代的关键基础设施保护》（第 13231 号行政令）。2003 年 2 月，布什政府发表《国家网络安全战略》报告，正式将网络信息安全提升至国家安全的战略高度，从国家战略全局对网络信息的正常运行进行谋划，以确保国家和社会生活的安全与稳定。2010 年 2 月，美国众议院

通过《加强网络安全法案》，法案提出壮大高素质的网络安全队伍，增加联邦政府在网络安全领域的研发投入，提高全社会对网络安全的认识，积极参与制定形成国际网络安全技术标准等具体的安全保障措施等。2009 年 5 月，奥巴马办公室发布《网络空间安全政策评估》报告，对政府及军队当前网络信息安全状况进行评估并讨论了防御对策。

网络与信息自由正取代民主成为美国在全球扩展软实力、开展外交、影响他国的新的价值观。为此，美国进一步加强了海外网络安全，拟设立大使级网络安全职位，职责将包括在联合国协商网络政策，保障国外网络安全。2009 年 12 月 29 日，美国总统奥巴马签署第 13526 号行政命令《国家安全信息保密》，主张要在准确、合理的定密标准和常规、安全、有效的解密工作基础上，进一步强化对国家安全至关重要的网络信息的保护，要求进一步加强保密教育培训，明确培训的各项要求；进一步强化特别接触方案，并新增国土安全部长、司法部长等为方案的制定主体。

确保国家安全是美国压倒一切的首要任务。美国在互联网的管理上规章制度比较健全，联邦政府和各州地方政府通过立法，不论是战略层面还是策略层面，技术层面还是管理层面，都对网络实施有效监管。特别是自“9·11”事件后，为实施反恐的需要，美国国会通过《爱国者法案》，授权国家安全、司法部门和警方对涉及化学武器等恐怖行为、计算机欺诈及滥用等行为进行监听、有权查询电邮和其他种类的记录，可以监视公民网上交流情报机构，可以利用技术手段监控、跟踪乃至删改互联网上不利于美国国家利益的信息。而《国土安全法》则增加有关监控互联网和惩治黑客的条款。目前，美国有六大网络安全专职机构、130 多项法律法规。

现有主要法律法规包括：《计算机欺诈和滥用法》、《计算机安全法》、《国家信息基础设施保护法》、《1996 年通信净化法》、第 63 号总统令《克林顿政府对关键基础设施保护的政策》、第 13130 号行政令《国家基础设施保障委员会》、《爱国者法案》、《联邦信息安全管理法案》、第 7 号国家安全总统令《关键基础设施标识、优先级和保护》、13292 号行政令《涉密国家安全信息》。

3. 欧盟法律法规

欧盟信息安全立法的历史可以追溯到 1992 年，发展至今已经具有一定规模。1992 年的《信息安全框架决议》翻开了欧盟信息安全立法的崭新一页。该决议的目标在于给一般用户、行政管理部门和工商业界存储电子信息提供切实有效的安全保护，使之不危及公众的利益。随后，1995 年 1 月 17 日，《欧盟理事会关于合法拦截电子通信的决议》提出了网络环境下公权力行使与人权保护制衡的话题；1999 年 1 月 25 日，《欧洲议会和欧盟理事会关于采取通过打击全球互联网上的非法和有害内容以促进更安全使用互联网的多年度共同体行动计划的第 276/1999/EC 号决定》强调必须安全使用网络，为欧盟介入互联网管制，杜绝种族歧视、分裂主义等非法和有害信息提供法律依据。在 20 世纪末，“电子欧洲”的概念登上历史舞台之后，欧盟在 21 世纪之初掀起了一个信息安全立法的高潮。2003 年 2 月 18 日，欧盟理事会通过了“关于建立欧洲网络信息安全文化”的决议。从那时起，欧盟已经不满足于仅仅通过技术手段来保障网络与信息安全，而且考虑到要向所有利益相关者阐明网络信息安全的责任，通过合作与交流，提高全社会的网络安全意识。根据欧盟委员会 2006 年 5 月 31 日向欧盟理事会、欧洲议会、欧洲经济和社会委员会以及区域委员会递交的题为《关于建立欧洲信息安全社会的战略——对话、合作和授权》的通讯，欧盟于 2007 年 3 月 22 日正式通过了关于建立欧洲信息安全社会战略的决议。这意味着欧盟已经将区域的信息安全提升到社会形态的高度，要求在全社会实现网络和信息系统的可用性、保密性与完整性。欧盟信息安全法律框架并非一

蹴而就，它是在欧盟理事会、欧洲议会等官方机构和成员国的共同努力之下，根据信息技术的进步和经济社会的发展不断调整，经过了十几年的修正与完善，才具备了今天这样庞大的体系、全面的内容和明确的效力。

纵观欧盟信息安全法律框架，这是一个由欧盟一体化立法、成员国国内立法、综合立法和专项立法共同构建的多层次法律体系。它以保障整个欧盟的信息安全为目标，其结构、内容以及实施措施特点鲜明。而且与美国相比，欧洲各国对个人隐私的保护更为严格。主要法律法规包括：欧盟电子商务指令、欧洲理事会《网络犯罪公约》、欧盟委员会关于在视听和信息服务领域保护未成年儿童和维护人类尊严的绿皮书、建立欧洲网络与信息安全局的指令、德国《信息和通信服务规范法（草案）》、法国《费永修正案》、法国《互联网络宪章》（草案）、英国《三 R 互联网络安全规则》等。

4. 通用规则

经济合作和发展组织（Organization for Economic Cooperation and Development，OECD）在 1996 年提出了关于密码技术政策的一些指导方针。这些指导方针为国家提供了一些在制定国家密码技术政策时需要考虑的原则，具体内容如下：

1）加密方法应该是可信赖的，这样才会产生在信息和通信系统中使用它们的信心。

2）用户应该有权根据适用法律选择任何加密方法。

3）加密方法的开发目标应该满足个人、企业和政府的需求和责任。

4）加密方法的技术标准、类别和协议应该在国家或国际级别上开发和发布。

5）在国家加密技术政策和加密方法的实现与使用中，应该尊重个人隐私的基本权限，包括通信的保密性和个人数据的保护。

6）国家加密技术政策可以允许合法地访问加密数据的普通文本和加密密钥。这些政策应该在最大限度上尊重指导方针中所包含的其他原则。

7）不管是以合同形式或法律形式建立，都必须清楚地阐述提供加密服务和那些保存或访问加密密钥的个人或实体的责任。

8）各国政府应该相互合作以协调加密技术政策。作为这种努力的一部分，各国政府应该清除或避免创建加密政策名称，从而去除或避免不公平的贸易障碍。

1.1.2 行业伦理

法律终究是人制定的，因此一定存在不完善和漏洞。尤其是针对信息安全这种高科技犯罪，本身取证就存在困难和限制，攻击者往往更容易逃脱法律的惩罚。但要记住，不触犯法律不一定是对的，作为信息安全从业者，更应该遵守道德规范。

公认的道德规范有：

- 《注册信息安全员（CISM）职业道德规范》。
- 计算机道德协会（Computer Ethics Institute）：《计算机道德十戒》。
- 互联网体系结构委员会（IAB）：《道德和互联网（RFC 1087）》。
- 经贸合作开发组织（OECD）：《GASSP 通用可接受系统安全原则》。

其中，美国计算机道德协会制定的计算机道德十戒为：

- 你不应该用计算机伤害他人。
- 你不应该影响他人的计算机工作。
- 你不应该到他人的计算机文件里进行窥探。

- 你不应该到他人的计算机进行偷盗。
- 你不应该用计算机做假证。
- 你不应该复制或使用你没有购买的软件。
- 你不应该使用他人的计算机资源，除非你得到了准许或给予了补偿。
- 你不应该剽窃他人的精神产品。
- 你应该注意你正在写入的程序和你正在设计的系统的社会效应。
- 你应该始终注意，你使用计算机时是在进一步加强你对你的人类同胞的理解和尊敬。

1.1.3 技术风险

作为信息安全从业人员，由于工作需要，在许多时候容易游走于法律法规边缘，因此非常有必要做足技术准备来规避法律法规的风险。

通常来说，我们会选择代理服务器或跳板等技术手段隐藏自身的 IP 地址。但代理服务器一般会检查使用者的地理位置、用户使用的 ISP，甚至包括时区（一般是通过 JavaScript 来确定时区的，代理服务器与此无关）。因此，有经验的技术人员会立即更改服务器的配置，并禁止 JavaScript。然而，即使代理服务器看起来非常可靠，但谁知道它们暗地里会干些什么呢，说不定会收集用户的数据并交给黑客，或者很可能你正在使用的代理服务器就是黑客搭建的，而且也不能保证进出的连接信息不被 ISP 或通信公司收集。因此你应该了解的是，即使通过第三方代理服务器，甚至多个代理服务器也不是那么安全的，这也是 IP 网络的固有特性，你的 IP 总是被记录的，只不过是记录的深度有区别而已。或许当下还可以利用非 IP 网络隐藏自己的身份，例如，使用非实名的手机卡，通过 GPRS 或 3G 实施网络活动。然而，手机也不完全可靠。每部手机都有一个 Unique Number，在开机过程中，甚至在每次通话过程中（这要视服务提供商而定），它都会发送到基站。情报机关可以利用它定位失窃的手机、跟踪机主等。除非是经常地销毁手机，不然也很容易被发现。

可以说，没有技术是不存在风险的，也就是俗话说的“魔高一尺，道高一丈”。信息安全本身就是一个依靠计算机、通信等学科发展的技术，它只能是这些背景技术的跟随者，因此也只能为“魔”，不能为“道”。

本章实验环节，通过对主机、网络、系统等做一些简单的技术准备工作，不仅保护个人系统隐私，也能在一定程度上减少法律法规、伦理及技术的风险。但需要了解的是，我们所做的工作是非常基础的，并不算高深的技术手段，也不能逃脱高手的追踪。

1.2 实验环节

1.2.1 VMware 虚拟机

1. 实验目的

1）学会使用 VMware 软件。

2）利用 VMware 搭建单机多系统环境。

3）了解 VMware 中的网络类型。

2. 工具信息

VMware——VMware Workstation 是一个虚拟 PC 软件，可以让用户在一台机器上同时运

行两个或多个 Windows、DOS、Linux 操作系统。使用简单，功能强大。

3. 实验分组

每组 1 人。

4. 系统环境

Windows 系统。

5. 实验步骤

（1）使用 VMware 在 Windows 系统中安装 Linux 操作系统

1）首先按提示安装好 VMware 软件，这个过程没有什么需要特别说明的地方，一直单击“下一步”按钮即可。安装好后启动 VMware 软件，然后在“文件”→“新建”的扩展菜单中选中“虚拟机”一项，或者按快捷键 Ctrl+N，弹出新建虚拟机向导，如图 1-1 所示。

2）这里选择简单的“Typical”（或称标准）方式，单击 Next 按钮，如图 1-2 所示。

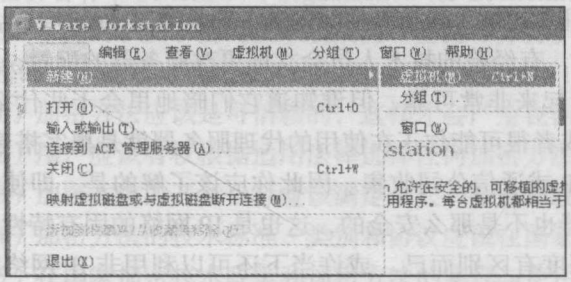


图 1-1　新建虚拟机

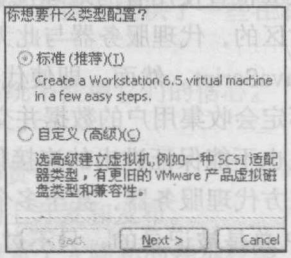


图 1-2　建立虚拟机的向导

3）按照向导提示，选择将要安装的系统光盘位置或镜像文件。在本例中我们选择用镜像文件进行虚拟机的安装，采用的例子为 Fedora 11 的 Linux 操作系统，单击“浏览”按钮选择要进行安装的对象。

这里要特别说明的是，VMware 6.5 引入了 Easy Install 特性，这个功能可以通过检测安装盘或镜像文件，来自动确定要安装的操作系统，然后进行从安装系统到安装 VMware Tools 一条龙的全自动无人值守安装，只需要在新建虚拟机向导里面输入一些安装选项就可以了。这样可以省去很多输入安装选项的时间，对系统管理员尤其有用。如图 1-3 所示为 VMware 能够自动识别出 Ubuntu 9.04 系统。

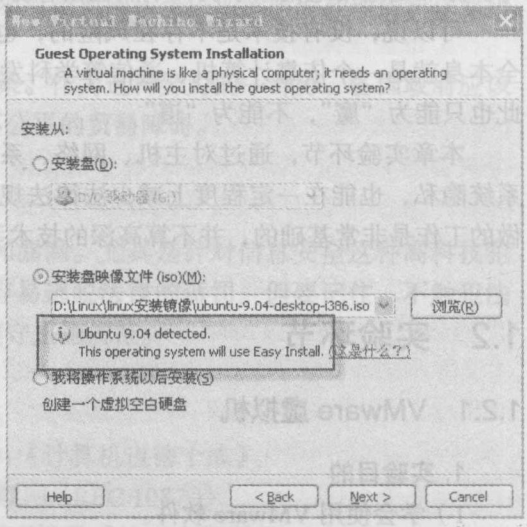


图 1-3　VMware 能够识别出来 Ubuntu 9.04 系统

不过很遗憾，本例中的 Fedora 11 系统 VMware 并不能进行自动识别，没关系，我们可以自行选择，选择好后单击 Next 按钮，如图 1-4 所示。

4）首先在单选按钮组中选择要安装的系统类型“Linux”，接着在版本选择中打开下拉列表框，在其中选择“Other Linux 2.6.x kernel”，然后单击 Next 按钮，如图 1-5 所示。

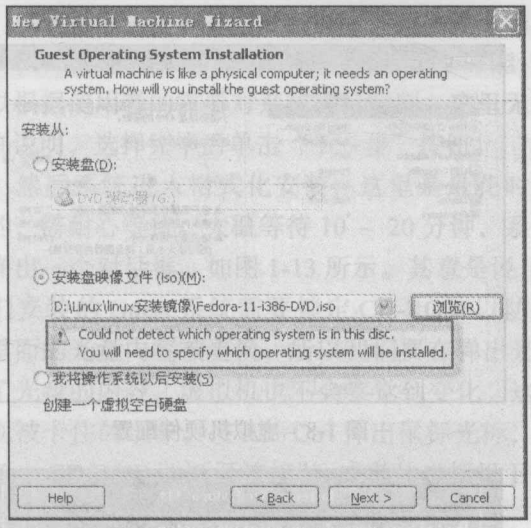


图 1-4 选择要安装的镜像文件

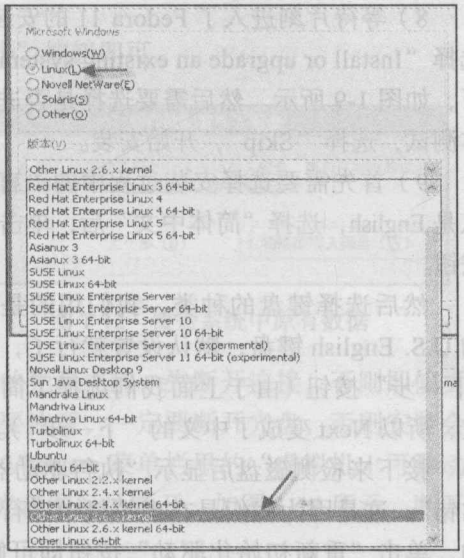


图 1-5 选择安装系统的类型和版本

5）给安装的虚拟机命名，默认值为“Other Linux 2.6.x kernel”，我们把其改为 Fedora 11。同时安装向导要我们选择创建虚拟机的位置，这里默认即可，当然也可以更改到其他位置，如图 1-6 所示。这也是 VMware 的强大之处，它不用我们改写硬盘分区格式，而是在一个文件中虚拟出一个新的分区来，而这一切对于用户来说都是透明的。单击 Next 按钮进行下一步。

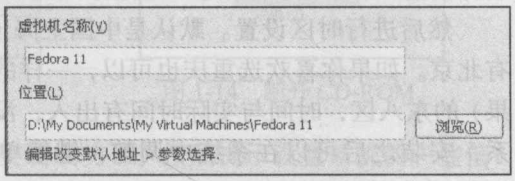


图 1-6 选择虚拟机的名称和位置

6）设定虚拟子系统所占磁盘的容量。这里设定的为最大值 8GB，即刚安装虚拟机后系统并不会占用 8GB（本例中选择 8GB）空间，虚拟的子系统被用户安装应用程序或新建文件和数据后，会变得越来越大，最大值不超过这里设定的值，也就是说这里的选择相当于虚拟机的硬盘容量大小。继续单击 Next 按钮，另外，VMware 还提供对划分给虚拟机空间的管理方式，可以以一个文件来存储虚拟机的磁盘，或者可以选择以每个文件（2GB）来存储。区别就是，当你需要把该虚拟机复制到另一台机器时，2GB 的文件显然要比 8GB 的文件容易移动。可以根据个人的情况进行选择。本实验选择结果如图 1-7 所示。

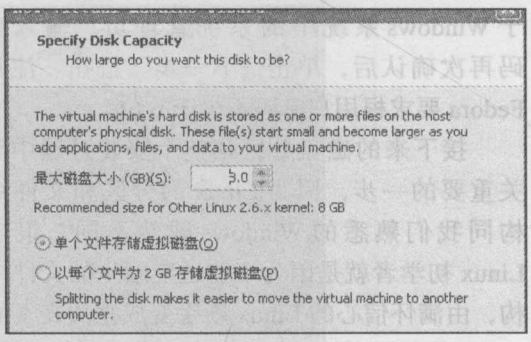


图 1-7 选择虚拟机磁盘大小

7）向导将我们前面的所有选择进行汇总，并进行显示。对信息进行确认，无误后，单击 Finish 按钮即可开始安装。注意，该确认信息的下方有一个“定制硬件”按钮，通过它我们可以对虚拟机的内存大小、光驱、软驱、网络适配器、USB 控制器、声卡、显卡以及处理器芯片个数进行设置，如图 1-8 所示。可以根据自己的实际需要和计算机配置情况进行选择，不过不用担心，这里的所有设置以后都可以在虚拟机的属性中进行更改。