从基础到实践　基础知识全面覆盖 实践操作循序渐进

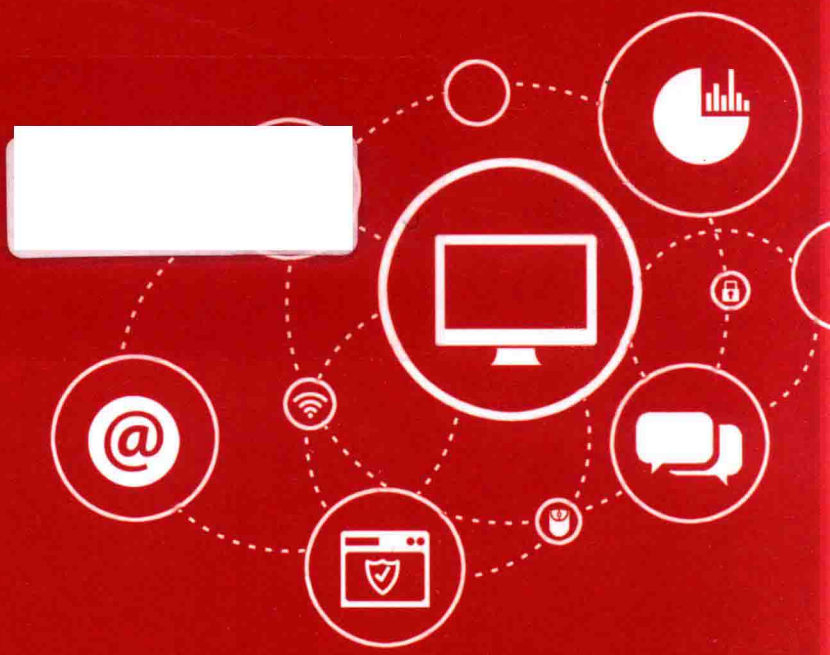
从理论到应用　理论讲解详尽具体 动手应用实操实练

从入门到进阶　内容编排由浅入深 进阶案例综合拓展

重点推荐

网络安全技术

■ 丛佩丽　陈震◎主编



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

网络安全技术

主　编　丛佩丽　陈　震
副主编　刘冬梅　沈　洋　金明日　姜源水

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

内 容 简 介

本书以网络攻击与防御为项目背景展开内容，介绍了网络时代的信息安全、Windows 安全防御、Linux 安全防御、Linux 安全工具使用、Windows 攻击技术、Web 渗透、密码学应用、计算机病毒与木马防护，体现了最新的网络渗透和防御技术。本书融入了作者多年的指导技能大赛和教学的经验，以项目实战的方式，深入浅出地阐述了各种安全技术，实用性和操作性强，注重培养实践操作能力。

本书适用于网络管理员和信息安全人员，以及所有准备从事网络安全管理的网络爱好者，并可作为计算机专业的教材、网络培训班的培训教材及参加信息安全大赛的参考教材。

图书在版编目（CIP）数据

网络安全技术/丛佩丽，陈震主编．—北京：北京理工大学出版社，2021.6
ISBN 978-7-5682-9176-7

Ⅰ.①网…　Ⅱ.①丛…②陈…　Ⅲ.①计算机网络-网络安全　Ⅳ.①TP393.08

中国版本图书馆 CIP 数据核字（2021）第 004966 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）68944723（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／涿州市新华印刷有限公司
开　　本／787 毫米×1092 毫米　1/16
印　　张／15.5
字　　数／364 千字
版　　次／2021 年 6 月第 1 版　2021 年 6 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

随着信息技术越来越广泛地应用于社会各个领域，国民经济和社会发展对信息安全保障的要求不断增强，日益突出的信息安全问题给国家政治、经济、文化和国防安全带来新的挑战。《国家网络空间安全战略》中提出，维护我国网络安全是协调推进全面建成小康社会、全面深化改革、全面依法治国、全面从严治党战略布局的重要举措，是实现“两个一百年”奋斗目标、实现中华民族伟大复兴中国梦的重要保障。

本书以“网络渗透与防御”为项目背景进行阐述，从信息安全管理员的视角进行系统防御和渗透实战，项目设计深入浅出、循序渐进，适合初学者的学习进阶。

本教材的特色有以下几点。

1. 紧跟行业技术发展，以网络渗透与防御为主线展开项目设计，依据全国职业技能大赛技能要求，根据课程内容特点采取项目导向的教学模式，每个项目与企业合作，共同进行项目的开发和设计。

2. 本书采用项目导向，任务驱动，教、学、做一体化的编写方式，除第 1 章外，其余各章均由知识目标、能力目标、项目拓扑、项目环境与要求和项目实战构成。每章中有若干实战，实战来自实际工作需求；实施操作步骤具体，学生按照正文步骤可以实现所有任务，在做中学，在学中做，边做边学，重点突出技能培养。

3. 本书融入了多个院校多名作者多年的技能大赛指导经验和教学经验，以项目实战的方式，深入浅出地阐述了各种安全技术，实用性和操作性强，注重培养实践操作能力，更好地适应信息安全管理员工作岗位。

全书共 8 章，主要内容包括信息安全定义、信息安全产品概述、网站安全检测；配置 Windows 安全防御、配置 Linux 安全防御、Linux 安全工具使用、通过扫描获取远程计算机相关信息实战、使用嗅探攻击窃取账号和口令实战、网络欺骗实战和拒绝服务攻击实战；利用网站漏洞进行 SQL 注入攻击实战、利用网站漏洞上传 WebShell 实战、XSS 漏洞挖掘和利用实战；口令破解 MD5、本地密码破解实战、云平台加密和密钥管理；计算机病毒概述、杀毒软件使用、宏病毒和网页病毒的防范、利用自解压文件携带木马程序、冰河木马实战、手机病毒等。

本书由辽宁机电职业技术学院丛佩丽和辽宁建筑职业学院陈震担任主编，铁岭师专高等专业学校刘冬梅、大连职业技术学院沈洋、辽宁轻工职业学院金明日和神州数码网络有限公司姜源水担任副主编。金明日和姜源水编写第 1 章，丛佩丽编写第 2 章和第 3 章，陈震编写

第4章、第5章和第7章，刘冬梅编写第6章，沈洋编写第8章。本书在编写过程中，得到了神州数码网络有限公司的工程师的大力帮助，在此表示诚挚的谢意。

本书适用于网络管理员和信息安全人员，以及所有准备从事网络安全管理的网络爱好者，并可作为计算机专业的教材、网络培训班的培训教材及参加信息安全大赛的参考教材。

由于作者的水平所限，本书在选材和内容安排上如有不妥之处，恳请读者批评指正！

编者

目　　录

第 1 章　网络时代的信息安全 …… 1
知识目标 …… 1
能力目标 …… 1
素养目标 …… 1
1.1　信息安全大事记 …… 1
1.1.1　信息泄露与网络攻击篇 …… 2
1.1.2　网络攻击对现实世界产生重大影响 …… 3
1.1.3　2018 年十大网络安全事件与趋势 …… 5
1.2　信息安全定义 …… 6
1.2.1　信息的概念 …… 6
1.2.2　信息安全的含义 …… 7
1.3　信息系统安全体系结构 …… 8
1.3.1　五类安全服务 …… 8
1.3.2　八类安全机制 …… 8
1.4　信息安全技术 …… 9
1.5　信息安全产品概述 …… 10
1.6　网站安全检测 …… 12
第 2 章　配置 Windows 安全防御 …… 13
知识目标 …… 13
能力目标 …… 13
素养目标 …… 13
项目环境与要求 …… 13
2.1　用户账号概述 …… 14
2.2　关闭多余系统服务 …… 18
2.3　账号安全配置 …… 21
2.4　利用 syskey 保护账户信息 …… 33
2.5　设置审核策略 …… 34
2.6　常用命令 …… 37
2.7　使用本地组策略编辑器对计算机进行安全配置 …… 47
2.8　通过过滤 ICMP 报文阻止 ICMP 攻击 …… 54
2.9　删除默认共享 …… 61
2.10　数据保密与安全 …… 66
第 3 章　配置 Linux 安全防御 …… 75

知识目标 …… 75
能力目标 …… 75
素养目标 …… 75
项目环境与要求 …… 75
3.1 使用 FinalShell 工具远程连接实验主机 …… 76
3.2 禁止 root 账户远程登录 …… 80
3.2.1 ssh_config 配置文件 …… 80
3.2.2 项目实施 …… 82
3.3 修改 SSH 服务端口 …… 84
3.4 修改 su 和 sudo 实现账户安全 …… 85
3.4.1 修改 su 实现账户安全 …… 85
3.4.2 使用 sudo 实现账户安全 …… 89
3.5 修改 root 密码 …… 91
3.6 防火墙高级配置 …… 94
3.6.1 防火墙概述 …… 94
3.6.2 防火墙的功能 …… 95
3.6.3 防火墙的种类 …… 95
3.6.4 Linux 内核的 Netfilter 架构 …… 96
3.6.5 Netfilter 的工作原理 …… 97
3.6.6 防火墙原理 …… 98
3.6.7 防火墙搭建任务一：实现全网互通 …… 101
3.6.8 防火墙搭建任务二：配置防火墙，实现允许服务通过 …… 110
3.6.9 防火墙搭建任务三：配置防火墙，实现端口转换 …… 118
第 4 章 Linux 安全工具使用 …… 125
知识目标 …… 125
能力目标 …… 125
素养目标 …… 125
项目环境与要求 …… 125
4.1 Linux 用户和组安全管理 …… 126
4.2 Linux 文件权限安全管理 …… 128
4.3 密码分析工具 …… 129
4.3.1 John the Ripper 简介 …… 129
4.3.2 使用 John the Ripper 破解 Linux 密码 …… 130
4.4 SSH 安全远程登录 …… 131
4.4.1 OpenSSH 简介 …… 131
4.4.2 SSH 安装 …… 132
4.4.3 SSH 案例应用 …… 133
4.5 Nmap 工具 …… 136
4.5.1 Nmap 简介 …… 136
4.5.2 Nmap 案例应用 …… 137

4.6　使用 Linux 审计工具 …… 138
4.6.1　Linux 审计重要性 …… 138
4.6.2　Linux 查看与分析日志 …… 138
第 5 章　Windows 攻击技术 …… 142
知识目标 …… 142
能力目标 …… 142
素养目标 …… 142
项目环境与要求 …… 142
5.1　信息收集与网络扫描 …… 143
5.1.1　网络扫描概述 …… 143
5.1.2　常用网络扫描工具 …… 144
5.1.3　通过扫描获取远程计算机相关信息实战 …… 144
5.2　网络嗅探 …… 153
5.2.1　网络嗅探概述 …… 153
5.2.2　网络嗅探原理 …… 153
5.2.3　常用网络嗅探器 …… 154
5.2.4　使用嗅探攻击窃取账号和口令 …… 155
5.3　网络欺骗 …… 158
5.3.1　网络欺骗概述 …… 158
5.3.2　网络欺骗种类与原理 …… 158
5.3.3　ARP 欺骗实战 …… 159
5.4　拒绝服务攻击 …… 161
5.4.1　拒绝服务攻击概述 …… 161
5.4.2　拒绝服务攻击原理 …… 162
5.4.3　拒绝服务攻击实战 …… 163
第 6 章　Web 渗透 …… 166
知识目标 …… 166
能力目标 …… 166
素养目标 …… 166
项目环境与要求 …… 166
6.1　Web 渗透概述 …… 167
6.2　SQL 注入 …… 168
6.2.1　SQL 原理 …… 168
6.2.2　常用 SQL 注入工具 …… 169
6.2.3　WebShell …… 172
6.2.4　提权 …… 174
6.3　XSS 攻击 …… 177
6.3.1　XSS 原理 …… 177
6.3.2　XSS 攻击方式 …… 177
6.3.3　XSS 安全防范 …… 178

6.4 实战练习 …… 179
6.4.1 利用网站漏洞进行 SQL 注入攻击 …… 179
6.4.2 利用网站漏洞上传 WebShell …… 183
6.4.3 XSS 漏洞挖掘和利用 …… 188
第 7 章 密码学应用 …… 192
知识目标 …… 192
能力目标 …… 192
素养目标 …… 192
项目环境与要求 …… 192
7.1 密码学概述 …… 192
7.2 口令破解 MD5 …… 193
7.3 本地密码破解实战 …… 195
7.4 云平台加密和密钥管理 …… 204
7.4.1 加密流程及术语 …… 204
7.4.2 客户端加密方式 …… 205
7.4.3 云服务端加密方式 …… 206
第 8 章 计算机病毒与木马防护 …… 207
知识目标 …… 207
能力目标 …… 207
素养目标 …… 207
项目环境与要求 …… 207
8.1 项目提出 …… 208
8.2 计算机病毒概述 …… 208
8.2.1 计算机病毒的起源 …… 208
8.2.2 计算机病毒的定义 …… 209
8.2.3 计算机病毒的分类 …… 209
8.2.4 计算机病毒的结构 …… 211
8.2.5 计算机病毒的危害 …… 212
8.2.6 常见的计算机病毒 …… 213
8.2.7 木马 …… 214
8.2.8 计算机病毒的检测与防范 …… 214
8.3 宏病毒和网页病毒的防范 …… 216
8.3.1 宏病毒 …… 216
8.3.2 网页病毒 …… 218
8.4 利用自解压文件携带木马程序 …… 219
8.5 典型木马案例 …… 221
8.6 第四代木马的防范 …… 235
8.7 手机病毒 …… 238
参考文献 …… 240

第 1 章

网络时代的信息安全

知识目标

1. 了解信息安全的概念。
2. 了解网络安全事件。
3. 掌握信息安全目标。

能力目标

1. 具备安全防御意识。
2. 具备应用安全策略的能力。
3. 能够掌握安全技术。

素养目标

1. 具有较强的安全意识。
2. 具备良好的职业道德和社会责任感。
3. 具有发现问题、分析问题和解决问题的能力。

在信息化飞速发展的今天，信息作为一种资源，它的普遍性、共享性、增值性、可处理性和多效用性，使其对人类具有特别重要的意义。随着现代通信技术的迅速发展和普及，互联网进入千家万户，计算机信息的应用与共享日益广泛和深入，信息技术已经成为一个国家的政治、军事、经济和文化等发展的决定性因素，但是信息系统或信息网络中的信息资源通常会受到各种类型的威胁、干扰和破坏，计算机信息安全问题已成为制约信息化发展的“瓶颈”，日渐成为人们必须面对的一个严峻问题，从大的方面来说，国家的政治、经济、军事、文化等领域的信息安全受到威胁；从小的方面来说，计算机信息安全问题也涉及人们的个人隐私和私有财产安全等。信息安全是任何国家、政府、部门、行业都必须十分重视的问题，是一个不容忽视的国家要求，也是保证国家安全和个人财产安全的必要途径。

信息是社会发展的重要战略资源。信息安全已成为亟待解决、影响国家大局和长远利益的重大关键问题，信息安全保障能力是21世纪综合国力、经济竞争实力和生存能力的重要组成部分，是世界各国奋力攀登的制高点。信息安全问题如果解决不好，将全方位地危及我国的政治、军事、经济、文化、社会生活的各个方面，使国家处于信息战和高度经济金融风险的威胁之中。

1.1 信息安全大事记

在生活中，经常可以看见下面的报道：

- ××计算机系统遭受到攻击，造成客户数据丢失；
- ××网站受到黑客攻击；
- 目前出现××计算机病毒，已扩散到各大洲；
- 手机越来越成为黑客攻击的对象；
- ARP病毒几乎使得网络瘫痪。

计算机网络在带给我们便利的同时，已经显现了它的脆弱性，网络安全性问题已经越来越重要。从20世纪90代年起，人们一路走来，经历了计算机安全、网络安全、信息安全、网络空间安全等各个时期不同的发展阶段。网络安全已经开始从信息技术的分支、支撑，逐渐上升到与之并行的地位。而未来是一个万物互联的时代，这种数字化世界的天然脆弱性，将会导致网络安全发生本质性的变化，不再只是信息网络系统的安全，而是业务的安全、经济的安全、人身的安全、社会的安全和国家的安全。

1.1.1 信息泄露与网络攻击篇

1. 信息泄露连续5年创历史纪录

自2013年斯诺登事件以来，全球信息泄露规模连年加剧。根据Gemalto发布的《数据泄露水平指数（Breach Level Index）》，仅2018年上半年，全球就发生了945起较大型的数据泄露事件，共计导致45亿条数据泄露，与2017年相比，数量增加了133%。

2. 2018年规模或影响较大的信息泄露事件

1月，印度媒体The Tribune声称以500卢比（约6英镑）的价格购买了对公民信息数据库Aadhaar的访问。该数据库包含10亿印度公民的个人信息。美国国土安全部承认，2.4万名现任雇员和前任员工个人信息由于黑客攻击而泄露。

2月，美国高端运动品牌安德玛的健康及饮食跟踪应用MyFitnessPal被黑客入侵，1.5亿用户账户信息泄露。

3月，安全研究人员披露，仅2018年前3个月，就发现了超过15.5亿份商业敏感文档在网上泄露，数据量高达12 PB，是巴拿马文档泄露事件的4 000倍。英国媒体披露Facebook超过5 000万名用户资料遭“剑桥分析”公司非法用来发送政治广告。

4月，加拿大零售集团HBC承认，其500万客户的信用卡和借记卡信息被黑客窃取，成为史上最大信用卡信息失窃案之一。Facebook承认，“剑桥分析”事件影响8 700万用户。同时，有恶意行为人使用Facebook的反向搜索和恢复功能，很可能恶意获取了20亿用户的账户基本信息。

5月，由于软件缺陷导致明文暴露证书，推特敦促其所有3.3亿用户更改口令。

6月，基因检测公司MyHeritage发布公告，称超过9 200万个账户信息被窃取。公告称，黑客入侵事件发生在2017年10月26日。国内安全专家发现一个被盗密码查询网站，包含14亿的邮箱口令，并且查询结果为明文。研究人员发现，数据统计公司Exactis包含3.4亿个人记录的数据库在网上可公开访问。该2 TB大的数据库包含上亿美国成年人的个人信息和数百万公司信息。谷歌Firebase平台2 271个数据库可公开访问，这些数据库中包括了1亿多条敏感信息记录，113 GB的数据量。

7 月，包括福特、通用、丰田、特斯拉等 100 多家公司的 157 GB 含有高度敏感信息的商业和技术文档数据可公开访问。

8 月，国内一家新媒体营销上市公司，非法劫持运营商流量赚取商业利益的案件被警方破获。百度、腾讯、阿里、今日头条等全国 96 家互联网公司用户数据被窃取，数量高达 30 亿条。国内某集团多家酒店 1.3 亿人身份信息、2.4 亿条开房记录和 1.23 亿条官网注册资料在暗网兜售，盗取数据的黑客 20 天后被警方抓获。

9 月，英国航空宣称被黑客攻击，38 万乘客的支付卡信息被盗。Facebook 官方公开承认，由于一个令牌访问漏洞，黑客可接管 5 000 万用户的账户，约 9 000 万用户受到影响，包括扎克伯格本人的账户。

10 月，在美国 2018 年中期选举之前，研究人员发现暗网上出售 20 个州的选民数据，数量达到 8 000 万之多。由于第三方供应商遭到黑客攻击，美国国防部至少 3 万名服务人员或雇员的个人和支付卡信息遭到泄露。香港国泰航空声称，包含有 940 万乘客的姓名、生日、电话、地址、身份证及护照号等敏感信息外泄。

11 月，万豪国际集团公布其酒店数据泄露事件，涉及约 5 亿客人的个人信息和开房记录。安全人员发现开源搜索引擎 Elasticsearch，至少有 3 个 IP 由于配置错误，可未授权访问，约 8 200 万美国公民的个人信息被暴露。

12 月，美国在线知识问答平台 Quora 官方发布通知，发现恶意第三方未经授权访问，约 1 亿用户数据泄露。谷歌承认 Google + 出现 API 漏洞，在 11 月的 6 天时间里，5 250 万用户的姓名、电子邮箱、职业和年龄及其他详细信息被访问。

（注：以上部分泄露事件由白帽汇安全研究院提供）

3. 2018 年的信息泄露事件的特点

①信息泄露事件自 2013 年开始，已经连续 5 年突破历史纪录，根本原因在于网络安全保障的意识、认知和能力均落后于信息网络技术及其应用的爆发式增长，两者之间出现极大裂痕。

②信息泄露事件常态化，不分行业、领域、国家。随着全球信息化程度的提高、全社会对网络和数字化技术的依赖，这一情况很有可能还会加剧。

③信息泄露给企业、个人带来的损失越来越大，可大幅度降低企业估值，令企业面临巨额赔偿，威胁个人财产和生活稳定等。

④信息泄露的途径主要为内部人员或第三方合作伙伴泄露，存在信息系统无法杜绝漏洞、机构本身的防护机制不健全、对数据的重要程度不敏感，以及对安全配置的疏忽大意等问题。

1.1.2　网络攻击对现实世界产生重大影响

从数字货币到勒索软件，从网络欺诈到舆论控制，从商业竞争到国家安全，随着数字化世界的到来，网络攻击对政治、经济、军事、国家、社会安全，甚至是人身安全的影响越来越大。据网络风险公司 RiskIQ 的统计，2017 年度全球网络犯罪造成 6 000 亿美元的损失，意味着每一分钟的损失约为 114 万美元。

1. 2018 年影响较大的网络攻击事件

1 月，东京交易所 Coincheck 价值 5.3 亿美元的加密货币 NEM 被黑客窃取，并尝试转移

到其他交易所。

2 月，韩国平昌冬奥会开幕式期间，服务器遭到身份不明的黑客入侵，导致主媒体中心的 IPTV（交互式网络电视）发生故障。奥组委关闭了内部网络服务器，导致官网彻底关闭，无法打印开幕式门票。

英国斯旺西大学计算机教授声称，英国国家医疗服务系统（NHS）每年因信息系统故障和漏洞导致的死亡事件在 100 ~ 900 例之间。

美国科罗拉多州交通部遭遇勒索软件两次攻击，致使该机构运转停滞数周，工资系统和供应商合约也受到了攻击的影响，员工被迫用纸笔处理事务。

3 月，代码共享平台 GitHub 遭遇反射放大（Memcached）拒绝服务攻击，峰值创纪录地达到 1.35 Tb/s。之后不到一周，Arbor 网络又声称美国一家服务提供商遭到了峰值 1.7 Tb/s 的 Memcached 攻击。

特朗普政府首次公开将 NotPetya 勒索软件，以及对美国电力、核能、商业、航空、制造业等基础设施的攻击，归咎于俄罗斯政府。

3 月，美国司法部起诉 9 名伊朗黑客，对 22 个国家的大学、私营公司和政府机构进行大规模网络攻击，窃取研究信息，其中被入侵的 320 所大学遭受了大约 34 亿美元的损失。

美国亚特兰大市政府受到勒索软件攻击，其所用 424 个软件程序中的 1/3 以上停止了服务或部分功能被禁用，影响核心城市服务，包括警署和法庭。在一份官员提交的预算简报中透露，该攻击可能是美国城市遭受的最严重网络攻击，这份预算提案包含了 950 万美元的服务恢复费用支出。

美国巴尔的摩市遭遇勒索软件攻击，导致 911 紧急调度服务的计算机辅助调度（CAD）功能掉线。CAD 系统是 911 派遣第一反应人员的工具，如果没有 CAD 系统，警察、消防员和救护车就不能第一时间派往事发地进行救助。掉线期间，911 操作人员仍能手动调度响应人员，但效率大幅降低。

3 月，区块链资产交易平台币安数十个用户账户被黑客控制，并通过买入、卖出操纵币价，专业人士估计黑客可能从中获利 7 亿美元。

5 月，一款名为 VPNFilter 的恶意软件感染了 Linksys、MikroTik、Netgear 和 TP - Link 等厂商的路由器，影响范围覆盖全球 54 个国家，超过 50 万台路由器和网络设备。

6 月，韩国最大虚拟货币交易平台 Bithumb 遭黑客入侵，价值约 350 亿韩元（3 000 万美元）的数字货币被盗。

7 月，美国参议员马可·卢比奥宣称，人工智能视频处理工具“Deep Fakes”是对国家安全的威胁，并将其与导弹、核武器相比。

美国阿拉斯加 Mat - Su 自治市遭遇勒索病毒，致使该市的网络电话和电子邮件全面瘫痪，工作人员只能使用原始的纸笔办公。

美国司法部副部长宣布，以阴谋干涉 2016 年美国大选的罪名起诉 12 名俄罗斯军官。

FBI 公共服务通告部发布统计报告，从 2013 年 10 月至 2018 年 5 月，全球披露的邮件欺诈事件造成的损失已达 120.5 亿美元。

一伙网络犯罪通过劫持 40 名受害者的手机 SIM 卡，共窃取了总额超过 500 万美元的加密货币。

币圈传出消息，区块链资产交易平台币安再次遭遇用户 API 被控，转走 7 000 多枚比特币，推论黑客可因此获得 8 000 万元。

8 月，安全公司 Securonix 披露，朝鲜黑客组织 Lazarus 通过侵入 SWIFT/ATM 系统，3 天内从印度最大的银行 Cosmos 盗走 9.4 亿卢比（约 1.35 亿美元）。

Email 安全公司 Valimail 发布的报告显示，全球虚假电子邮件的日发送量已高达 64 亿封。

9 月，美国政府正式指控朝鲜政府，称其是索尼影业黑客事件、WannaCry 勒索软件和孟加拉银行等一系列网络银行劫案背后主使。

日本数字货币交易所 Zaif 发布声明，被黑客盗走 3 种数字货币，分别为比特币、比特币现金和 MonaCoin，总价值约合 5 967 万美元。

10 月，网络安全公司 Group - IB 的研究报告披露，朝鲜黑客组织 Lazarus 从 2017 年开始，已经盗取了价值 5.7 亿美元的加密货币。

11 月，安全公司 Cylance 宣称，国家支持的黑客组织“白色军团”对巴基斯坦军队网络执行了名为“Operation Shaheen”的长期针对性攻击。

12 月，欧洲国际刑警宣布，在 3 个月的联合行动中，来自 30 个国家的执法机构共抓捕了 168 个“钱骡”。超过 300 家银行、20 个银行协会及其他机构总共报告了 26 376 起欺诈性钱骡交易，避免了 4 100 万美元的损失。

安全厂商 Upstream Security 发布的《全球汽车行业网络安全报告》预计，到 2023 年由于网络黑客攻击可导致汽车制造商损失 240 亿美元。

2. 2018 年的网络攻击呈现的特点

①针对加密货币的黑客攻击，无论是攻击数量还是造成的损失上，均呈爆发态势。依据有关统计，仅 2018 年上半年，损失已超过 17.3 亿美元。其主要原因为加密货币的火爆带来的巨大商业利益。

②勒索软件持续产生严重危害，发生多起影响企业生产、政府办公、城市运转的实际事故，反映出安全意识的普遍薄弱和基本防护手段的缺失，预示着网络安全给现实生活带来的重大隐患。

③电子邮件欺诈带来的损失史无前例。据 FBI 统计，2013—2016 年 5 月，商业欺诈邮件造成 53 亿美元的损失，但这一数字在 2018 年 5 月上升到了 120 亿美元。

④国家之间的网络对抗呈明显化趋势。美国政府已实施严格的商业禁令，并公开指责、诉讼他国黑客的攻击行为。如果说前两年国家支持的黑客行动还属于冷战时期，2018 年则进入了小规模冲突时期。

1.1.3　2018 年十大网络安全事件与趋势

①信息泄露连续 5 年创历史纪录，并且不分行业与领域。而随着网络世界向数字世界的演化，信息泄露将成为全球科技始终无法避免的“自然灾害”。

②随着加密货币的空前爆发带来的商业利益，吸引了大量的网络攻击，但这一安全态势在各国相继出台的限制措施下，以及币值的急剧萎缩，有可能得到缓解。

③勒索软件持续产生严重危害，反映出安全意识的普遍薄弱和基本防护手段的缺失，背

后则是黑色产业链的发达运转。勒索软件将会和过去的病毒、恶意软件一样，走向常态化、长期化。

④拒绝服务攻击的规模不断放大，已经出现万兆级别的攻击。不仅是因为联网设备的防护能力薄弱，各种攻击手法的层出不穷也是重要因素。在未来全球一体化的数字世界，可以预见会出现更大规模的攻击。

⑤电子邮件欺诈带来的损失史无前例，累计已达 120 亿美元。古老的骗局一而再再而三地卷土重来，其利用的是人们心理上的弱点与认知上的缺陷。针对这种攻击，人们注定无法完全免疫。

⑥人工智能技术是又一把安全的“双刃剑”。基于 AI 的防护技术还在尝试阶段，但显然坏人暂时取得领先。可篡改音/视频的 Deepfake 技术，被美国议员比喻成“核武器”。虽然目前并无重大危害事件出现，但其可能带来的社会恐慌或是对突发事件漠视，值得关注与保持警惕。

⑦网络安全被用于政治、经济、科技、军事等领域的博弈之中，攫取经济利益、盗取知识产权、攻击关键基础设施等行为层出不穷，并有着从试探性变成破坏性攻击的趋势，未来这一趋势还将越演越烈。

⑧漏洞受到业界的极大重视并成为重要战略资源。这种重视反而限制了漏洞公布的速度和数量，许多相关的破解活动和赛事陷入低潮。与此同时，如何减少漏洞的产生及如何进行客观的价值评价，成为各方面的关注重点。

⑨国内的经济发展受到中美贸易战、资本寒冬、供给侧改革等影响，但以国家、大型企业为主要用户的网络安全行业，所受的影响尚不明显。2018 年国内一级市场的融资规模可能会达到近年来的顶峰，但未来的注册制、科创板等股市改革措施将会给网络安全行业带来积极的推动。

⑩由公安部制定的《网络安全等级保护条例》即将实施。该条例将是继《网络安全法》之后又一最为重要的法规，是各机构部门、重点行业部署与开展安全工作的核心基础，必将极大地促进全社会对网络安全的重视，推动整个网络安全行业的全面发展。

1.2 信息安全定义

1.2.1 信息的概念

信息是对客观世界中各种事物的运动状态和变化的反映，是客观事物之间相互联系和相互作用的表征，表现的是客观事物运动状态和变化的实质内容。ISO/IEC 的 IT 安全管理指南（GMITS，即 ISO/IEC TR 13335）给出的信息（Information）解释是：信息是通过在数据上施加某些约定而赋予这些数据的特殊含义。

计算机的出现和逐步普及，使信息对整个社会的影响逐步提高到一种绝对重要的地位。信息量、信息传播的时速、信息处理的速度及应用信息的程度等，都以几何级数的方式在增长。

信息技术的发展对人们学习知识、掌握知识、运用知识提出了新的挑战。对每个人、每个企事业机构来说，信息是一种资产，包括计算机和网络中的数据，还包括专利、著作、文

件、商业机密、管理规章等。就像其他重要的固定资产一样，信息资产具有重要的价值，因而需要进行妥善保护。

知己知彼，百战不殆，要保证信息的安全，就需要熟悉所保护的信息及信息的存储、处理系统，熟悉信息安全所面临的威胁，以便做出正确的决策。

1.2.2　信息安全的含义

信息安全的实质就是要保护信息资源免受各种类型的危险，防止信息资源被故意的或偶然的非授权地泄露、更改、破坏，或使信息被非法系统辨别、控制和否认，即保证信息的完整性、可用性、保密性和可靠性。信息安全本身包括的范围很大，从国家军事政治等机密安全，到防范商业企业机密泄露、防范青少年不良信息的浏览、个人信息的泄露等。

信息安全包括软件安全和数据安全。软件安全是指软件的防复制、防篡改、防非法执行等。数据安全是指计算机中的数据不被非法读出、更改、删除等。

信息安全的含义包含如下方面：

1. 信息的可靠性

信息的可靠性是网络信息系统能够在规定条件下和规定时间内完成规定功能的特性。可靠性是系统安全的最基本要求之一，是所有网络信息系统的建设和运行的目标。

2. 信息的可用性

信息的可用性是网络信息可被授权实体访问并按需求使用的特性。即网络信息服务在需要时，允许授权用户或实体使用的特性，或者是网络部分受损或需要降级使用时，仍能为授权用户提供有效服务的特性。可用性是网络信息系统面向用户的安全性能。

3. 信息的保密性

信息的保密性是网络信息不被泄露给非授权的用户、实体或进程，或供其利用的特性。即，防止信息泄露给非授权个人或实体，信息只为授权者使用的特性。保密性是在可靠性和可用性基础之上，保障网络信息安全的重要手段。

4. 信息的完整性

信息的完整性是网络信息技术未经授权不能进行改变的特性。即网络信息在存储或传输过程中保持不被偶然或蓄意地删除、修改、伪造、乱序、重放、插入等破坏的特性。完整性是一种面向信息的安全性，它要求保持信息的原样，即信息的正确生成、正确存储和传输。

5. 信息的不可抵赖性

信息的不可抵赖性也称作不可否认性。在网络信息系统的信息交互过程中，确信参与者的真实同一性，即所有参与者都不可能否认或抵赖曾经完成的操作和承诺。利用信息源证据可以防止发信方不真实地否认已发送信息，利用递交/接收证据可以防止收信方事后否认已经接收的信息。

6. 信息的可控性

信息的可控性是对信息的传播及内容具有控制能力的特性。

除此以外，信息安全还包括鉴别、审计追踪、身份认证、授权和访问控制、安全协议、密钥管理的可靠性等。

1.3 信息系统安全体系结构

研究信息系统安全体系结构，就是将普遍性安全体系原理与自身信息系统的实际相结合，形成满足信息系统安全需求的安全体系结构。

1989 年 12 月，国际标准化组织 ISO 颁布了 ISO 7498 - 2 标准，该标准首次确定了 OSI 参考模型的计算机信息安全体系结构，并于 1995 年再次在技术上进行了修正。OSI 安全体系包括五类安全服务及八类安全机制。

1.3.1 五类安全服务

五类安全服务包括认证（鉴别）服务、访问控制服务、数据保密性服务、数据完整性服务和抗否认性服务。

①认证（鉴别）服务：提供对通信中对等实体和数据来源的认证（鉴别）。

②访问控制服务：用于防止未授权用户非法使用系统资源，包括用户身份认证和用户权限确认。

③数据保密性服务：为防止网络各系统之间交换的数据被截获或被非法存取而泄密，提供机密保护。同时，对有可能通过观察信息流就能推导出信息的情况进行防范。

④数据完整性服务：用于组织非法实体对交换数据的修改、插入、删除及在数据交换过程中的数据丢失。

⑤抗否认性服务：用于防止发送方在发送数据后否认发送和接收方在收到数据后否认收到或伪造数据的行为。

1.3.2 八类安全机制

八大类安全机制包括加密机制、数字签名机制、访问控制机制、数据完整性机制、认证机制、业务流填充机制、路由控制机制、公正机制。

①加密机制：是确保数据安全性的基本方法。在 OSI 安全体系结构中，应根据加密所在的层次及加密对象的不同，而采用不同的加密方法。

②数字签名机制：是确保数据安全性的基本方法。利用数字签名技术可进行用户的身份认证和消息认证，它具有解决收、发双方纠纷的能力。

③访问控制机制：从计算机系统的处理能力方面对信息提供保护。访问控制按照事先确定的规定决定主体对客体的访问是否合法。当主体访问一个不合法的客体时，会报警，并记录到日志中。

④数据完整性机制：破坏数据完整性的主要因素有数据在信道中传输时受信道干扰影响而产生错误、数据在传输和存储过程中被非法入侵者篡改、计算机病毒对程序和数据的传染