网络安全训练营

讲师：Cookie

- 国内知名互联网公司从业者，信息安全专家。
- 从事渗透测试、应急响应、安全运营、安全评估、信息安全体系建设等工作。
- 拥有丰富的实战经验：**HW**、国家级重要会议保障、大型攻防演练、**CTF**等。
- 拥有**CISP**、**PMP**、应急响应资质认证。

极客时间 训练营

云时代 · 掌握网络安全

六大主流方向 全体系安全技能全部get

Web安全 网络安全 信息安全 系统防护 攻防渗透 云安全

基础阶段

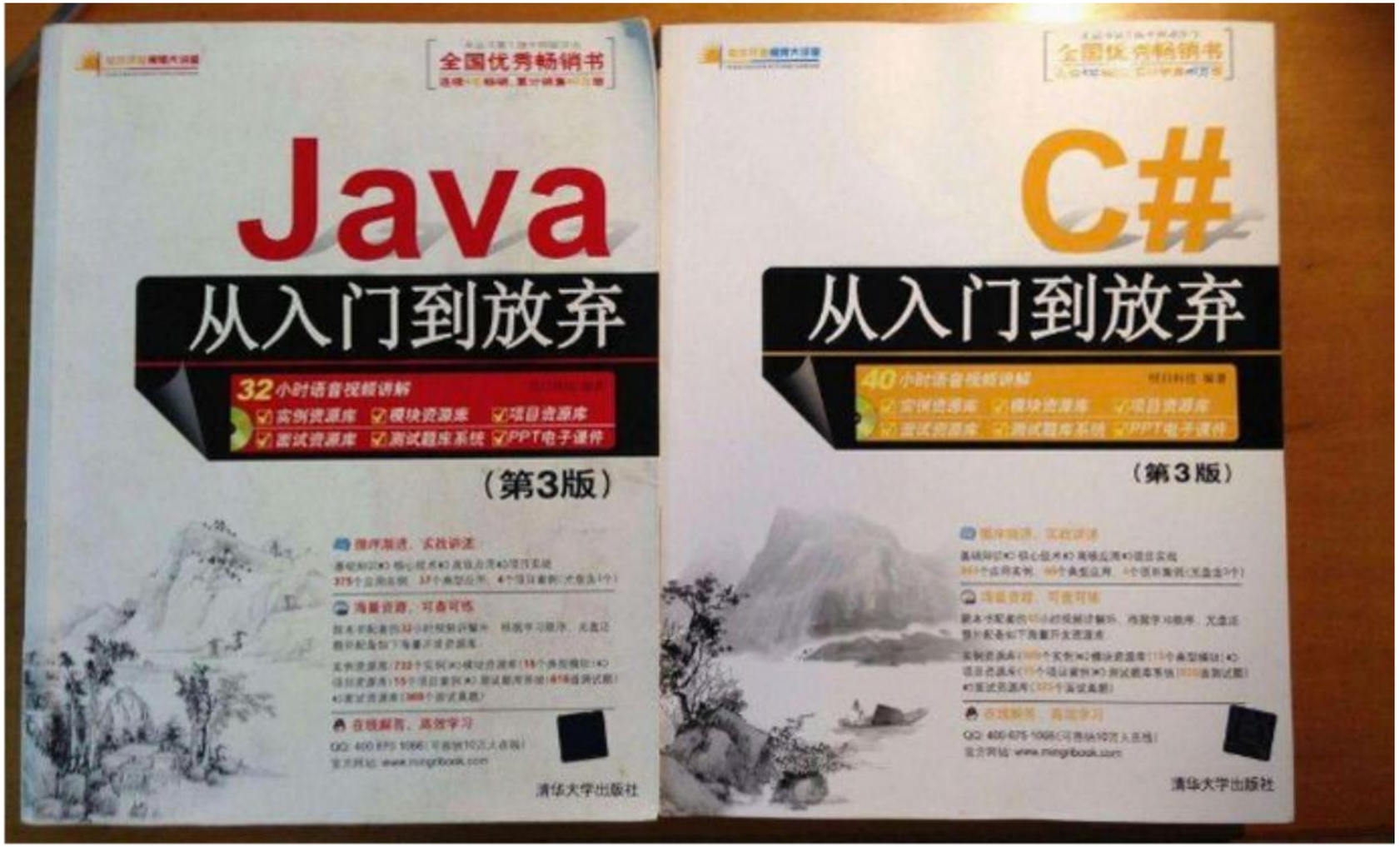
- 模块一：基础前置知识掌握
- 模块二：网络安全入门核心知识
- 模块三：信息安全基础
- 模块四：信息安全工具使用（渗透测试必备工具篇）
- 模块五：渗透测试
- 模块六：等级保护
- 模块七：风险评估

进阶阶段

- 模块八：安全巡检
- 模块九：信息安全工具使用（Kali之MSF渗透测试）
- 模块十：渗透测试进阶
- 模块十一：应急响应
- 模块十二：代码审计
- 模块十三：代码审计进阶
- 模块十四：Kubernetes安全
- 模块十五：安全开发

《网络安全法律法规》（解读）

责任要求\条文解读\合规建议


全国优秀畅销书
Java
从入门到放弃
32小时语音视频讲解
实例资源库 模块资源库 项目资源库
面试资源库 测试题库系统 PPT电子课件
（第3版）
清华大学出版社
全国优秀畅销书
C#
从入门到放弃
40小时语音视频讲解
实例资源库 模块资源库 项目资源库
面试资源库 测试题库系统 PPT电子课件
（第3版）
清华大学出版社


黑客渗透
从入门到入狱

目录

网络安全法

概述

《网络安全法》是我国第一部网络安全领域的法律，是保障网络安全的**基本法**，与《国家安全法》、《反恐怖主义法》、《刑法》、《保密法》、《治安管理处罚法》、《计算机信息系统安全保护条例》等现行法律法规共同构成中国关于网络安全管理的法律体系。

条文解读

第十二条 国

任何个人和 不得危害

网络安全， 、推翻社

会主义制度 民族仇

恨、民族歧 和社会秩

序，以及侵

解读：点明 为的网络

服务注意信


首页 → 国内新闻

分享到:

中国修订反间谍法 将对国家机关实施网络攻击等行为明确为间谍行为

2023年04月26日 15:06 来源：中国新闻网

A+ 大字体 A- 小字体

中新网北京4月26日电 (记者 黄钰钦)十四届全国人大常委会第二次会议26日表决通过修订后的反间谍法。新法完善了间谍行为的定义，将“投靠间谍组织及其代理人”、“针对国家机关、涉密单位或者关键信息基础设施等实施网络攻击等行为”明确为间谍行为。

修订后的反间谍法将于2023年7月1日起施行。现行反间谍法前身是1993年制定的国家安全法，主要规定国家安全机关履行的职责特别是反间谍方面的职责。2014年，反间谍法在原国家安全法的基础上修订出台。

条文解读

第三十七条　运营中收集和产生的个人信息和重要数据应当在境内存储。因业务需要，确需向境外提供的，应当按照国家网信部门会同国务院有关部门制定的办法进行安全评估；法律、行政法规另有规定的，依照其规定。

解读：个人信息和重要信息需境内存储。外企和有海外业务的国内企业应重点关注。

条文解读

第三十八条　关键信息基础设施的运营者应当自行或者委托网络安全服务机构对其网络的安全性和可能存在的风险每年至少进行一次检测评估，并将检测评估情况和改进措施报送相关负责关键信息基础设施安全保护工作的部门。

解读：每年至少一次的网络安全检测和风险评估。

条文解读

第四十条　网络运营者应当建立健全用户信息保护制度，对其收集的用户信息必须严格保密。

解读：进行用户信息保护。用户信息主要是指：用户使用产品或服务过程中收集的信息构成用户信息，包括IP地址、用户名和密码、上网时间、Cookie信息等。

条文解读

第四十一条　网络运营者收集、使用个人信息，应当遵循合法、正当、必要的原则，公开收集、使用规则，明示收集、使用信息的目的、方式和范围，并经被收集者同意。网络运营者不得收集与其提供的服务无关的个人信息，不得违反法律、行政法规的规定和双方的约定收集、使用个人信息，并应当依照法律、行政法规的规定和与用户的约定，处理其保存的个人信息。

解读：进行个人信息保护。个人信息指：以电子或者其他方式记录的能够单独或者与其他信息结合识别自然人个人身份的各种信息，包括但不限于自然人的姓名、出生日期、身份证件号码、个人生物识别信息、住址、电话号码。

总结

严处中介买卖交换个人信息
收集用户信息应取得同意

个人信息有了“保护伞”：

网络运营者不得泄露其收集的个人信息；中介买卖交换个人信息也算侵权；提供个人信息违法所得5000元以上可入刑。

网络产品、服务具有收集用户信息功能的，其提供者应向用户明示并取得同意；网络运营者不得泄露、篡改、毁损其收集的个人信息，未经被收集者同意，不得向他人提供个人信息；任何个人和组织不得窃取或者以其他非法方式获取个人信息，不得非法出售或者非法向他人提供个人信息；任何个人和组织应当对其使用网络的行为负责，不得设立用于实施诈骗，传授犯罪方法等。

总结

贩卖 50 条个人信息可入罪

对于刑法相关规定中“情节严重”的认定标准，司法解释明确规定了入罪情形，包括非法获取、出售或者提供行踪轨迹信息、通信内容、征信信息、财产信息50条以上的；非法获取、出售或提供住宿信息、通信记录、健康生理信息、交易信息等其他可能影响人身、财产安全的公民个人信息500条以上的。

数据安全法

概述

2021年6月10日，《数据安全法》由中华人民共和国第十三届全国人民代表大会常务委员会第二十九次会议通过，自2021年9月1日起施行。

数据安全法是总体国家安全观框架下，国家安全法律体系的重要组成部分。该法律在网络安全法的基础上，进一步明确了数据安全相关者的保护义务与职责，并与国家互联网信息办公室发布的《数据安全管理办法（征求意见稿）》相互照应。《数据安全法》的诞生，标志着数据安全上升到国家安全层面，意义重大。

条文解读

第二条　在中华人民共和国境内开展数据处理活动及其安全监管，适用本法。
在中华人民共和国境外开展数据处理活动，损害中华人民共和国国家安全、公共利益或者公民、组织合法权益的，依法追究法律责任。

解读：数据安全问题不仅在国内受到监管，境外势力威胁我国数据安全的恶意活动也将受到追究与惩罚。

条文解读

第三条　本法所称数据，是指任何以电子或者其他方式对信息的记录。
数据处理，包括数据的收集、存储、使用、加工、传输、提供、公开等。
数据安全，是指通过采取必要措施，确保数据处于有效保护和合法利用的状态，以及具备保障持续安全状态的能力。

解读：扩大了数据保护范围。

条文解读

第六条　各地区、各部门对本地区、本部门工作中收集和产生的数据及数据安全负责。工业、电信、交通、金融、自然资源、卫生健康、教育、科技等主管部门承担本行业、本领域数据安全监管职责。

公安机关、国家安全机关等依照本法和有关法律、行政法规的规定，在各自职责范围内承担数据安全监管职责。

国家网信部门依照本法和有关法律、行政法规的规定，负责统筹协调网络数据安全和相关监管工作。

解读：有监管才能有推进。

条文解读

第十八条　国家促进数据安全检测评估、认证等服务的发展，支持数据安全检测评估、认证等专业机构依法开展服务活动。
国家支持有关部门、行业组织、企业、教育和科研机构、有关专业机构等在数据安全风险评估、防范、处置等方面开展协作。

第三十条　重要数据的处理者应当按照规定对其数据处理活动定期开展风险评估，并向有关主管部门报送风险评估报告。
风险评估报告应当包括处理的重要数据的种类、数量，开展数据处理活动的情况，面临的数据安全风险及其应对措施等。

解读：网络安全行业的又一分支，热门发展方向。

条文解读

第十九条　国家建立健全数据交易管理制度，规范数据交易行为，培育数据交易市场。

解读：明确数据是可交易的，但是不能滥用。

条文解读

第二十一条　国家建立数据分类分级保护制度，根据数据在经济社会发展中的重要程度，以及一旦遭到篡改、破坏、泄露或者非法获取、非法利用，对国家安全、公共利益或者个人、组织合法权益造成的危害程度，对数据实行分类分级保护。国家数据安全工作协调机制统筹协调有关部门制定重要数据目录，加强对重要数据的保护。

关系国家安全、国民经济命脉、重要民生、重大公共利益等数据属于国家核心数据，实行更加严格的管理制度。

各地区、各部门应当按照数据分类分级保护制度，确定本地区、本部门以及相关行业、领域的重要数据具体目录，对列入目录的数据进行重点保护。

解读：数据安全的工作重点--分类分级。

条文解读

第二十七条　开展数据处理活动应当依照法律、法规的规定，建立健全全流程数据安全管理制度，组织开展数据安全教育培训，采取相应的技术措施和其他必要措施，保障数据安全。利用互联网等信息网络开展数据处理活动，应当在网络安全等级保护制度的基础上，履行上述数据安全保护义务。

重要数据的处理者应当明确数据安全负责人和管理机构，落实数据安全保护责任。

解读：数据安全要在满足等保的基础上进行。

总结

- 建立数据安全管理制度，落实数据全生命周期管控责任
- 通过数据分类分级，实现企业数据安全建设第一步
- 针对不同类别&级别的数据，实施具体保护措施
- 建立数据安全事件应急响应机制
- 组织开展数据安全培训教育

个人信息法

概述

数字时代的《个人信息保护法》，是保障个人信息权益乃至宪法性权利的基本法。

《个人信息保护法》第一条即开宗明义，为了保护个人信息权益，规范个人信息处理活动，促进个人信息合理利用，根据宪法，制定本法。其中在立法依据中“根据宪法”这四个字表明：我国将个人信息受保护的权利提升至更高高度，其来源于《宪法》：国家尊重和保障人权，公民的人格尊严不受侵犯，公民的通信自由和通信秘密受法律保护。

《个人信息保护法》于2021年8月20日正式出台，同年11月1日起施行。自此，我国终于形成了以《网络安全法》《数据安全法》《个人信息保护法》三法为核心的网络安全法律体系，为数字时代的网络安全、数据安全、个人信息权益保护提供了基础制度保障。

条文解读

第四条　个人信息是以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息，不包括匿名化处理后的信息。
个人信息的处理包括个人信息的收集、存储、使用、加工、传输、提供、公开、删除等。

第二十八条　敏感个人信息是一旦泄露或者非法使用，容易导致自然人的人格尊严受到侵害或者人身、财产安全受到危害的个人信息，包括生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等信息，以及不满十四周岁未成年人的个人信息。
只有在具有特定的目的和充分的必要性，并采取严格保护措施的情形下，个人信息处理者方可处理敏感个人信息。

解读：对个人信息和敏感个人信息进行了明确界定。

条文解读

第十四条　基于个人同意处理个人信息的，该同意应当由个人在充分知情的前提下自愿、明确作出。法律、行政法规规定处理个人信息应当取得个人单独同意或者书面同意的，从其规定。个人信息的处理目的、处理方式和处理的个人信息种类发生变更的，应当重新取得个人同意。

第十五条　基于个人同意处理个人信息的，个人有权撤回其同意。个人信息处理者应当提供便捷的撤回同意的方式。
个人撤回同意，不影响撤回前基于个人同意已进行的个人信息处理活动的效力。

第十六条　个人信息处理者不得以个人不同意处理其个人信息或者撤回同意为由，拒绝提供产品或者服务；处理个人信息属于提供产品或者服务所必需的除外。

解读：处理个人信息的核心原则是告知和同意。

条文解读

第三十一条　个人信息处理者处理不满十四周岁未成年人个人信息的，应当取得未成年人的父母或者其他监护人的同意。
个人信息处理者处理不满十四周岁未成年人个人信息的，应当制定专门的个人信息处理规则。

解读：重点保护未成年人信息。

条文解读 – 个人在个人信息处理活动中的权利

第四十四条　个人对其个人信息的处理享有知情权、决定权，有权限制或者拒绝他人对其个人信息进行处理；法律、行政法规另有规定的除外。

第四十五条　个人有权向个人信息处理者查阅、复制其个人信息；有本法第十八条第一款、第三十五条规定情形的除外。
个人请求查阅、复制其个人信息的，个人信息处理者应当及时提供。

第四十六条　个人发现其个人信息不准确或者不完整的，有权请求个人信息处理者更正、补充。

第四十七条　有下列情形之一的，个人信息处理者应当主动删除个人信息；个人信息处理者未删除的，个人有权请求删除：

。。。

第四十八条　个人有权要求个人信息处理者对其个人信息处理规则进行解释说明。

第四十九条　自然人死亡的，其近亲属为了自身的合法、正当利益，可以对死者的相关个人信息行使本章规定的查阅、复制、更正、删除等权利；死者生前另有安排的除外。

第五十条　个人信息处理者应当建立便捷的个人行使权利的申请受理和处理机制。拒绝个人行使权利的请求的，应当说明理由。
个人信息处理者拒绝个人行使权利的请求的，个人可以依法向人民法院提起诉讼。

总结

《个人信息保护法》正式实施，强化了对公民个人信息的系统保护。

之前，对于公民个人信息的保护虽然也写入了立法，但主要散落于《民法典》《刑法》《网络安全法》《消费者权益保护法》《电子商务法》《数据安全法》等法律中，且缺乏保护的基本原则。经由一部专门的法律“提纲挈领”，不仅集个人信息的法律保护之大成，便于公民个人“按图索骥”，保护合法权益，更凸显了立法对个人信息保护的重视程度，释放出依法维护个人信息安全的强烈讯号。尤其重要的是，《个人信息保护法》明确将“告知—同意”原则作为个人信息保护的基本规则，作为个人信息处理者处理用户信息的规范前提，赋予了公民对个人信息处理的知情权、决定权，也为界定“合法”与“违法”划出了分水岭。

THANKS