

网络犯罪全景透视

——计算机犯罪取证手册

作者 [美]德博拉·利特尔约翰·欣德
埃德·蒂特尔（技术编辑）
译者 高卓

目 录

前言

第一章 扑面而来的网络犯罪问题

概述

危机的量化数据

定义网络犯罪

从笼统到具体

司法辖区问题的重要性

区分利用网络的犯罪和依赖网络的犯罪

收集网络犯罪统计数据

犯罪报告系统

全国报告系统犯罪分类

接近网络犯罪的有效定义

美国联邦和各州的法律法规

国际法：联合国的网络犯罪定义

网络犯罪分类

划分网络犯罪类别

暴力或潜在暴力网络犯罪类

非暴力网络犯罪类别

网络犯罪执法的重点

打击网络犯罪

确定参与反网络犯罪斗争的人员

教育反网络犯罪斗士

教育立法者和司法专业人员

教育信息技术专业人员

教育并调动公众

积极投身打击网络犯罪的斗争

利用同伴压力打击网络犯罪

利用技术打击网络犯罪

开发打击网络犯罪的新方法

总结

常见问题解答

参考文献

第二章 网络犯罪历史回顾

概述

独立计算机时代的犯罪

共享的不仅仅是时间

黑客一词的演变

早期电话飞客、黑客和快客

攻击电话网

著名电话飞客

大西洋彼岸的电话飞客

各色“匣子”

从电话飞客到黑客

以局域网为生：早期的计算机网络黑客

BBS 助长犯罪活动泛滥

在线服务为网络犯罪大开方便之门

ARPANet：网络西部莽原

苏联卫星催生 ARPA

ARPA 转向研究计算机技术

网络应用迅猛发展

互联网继续扩展

80 年代的 ARPANet

90 年代的互联网

蠕虫开始肆虐，安全成为忧患

网络犯罪伴随互联网的商业化愈演愈烈

今天的网络犯罪

新技术产生了新的脆弱性

网络犯罪分子为什么喜欢宽带

网络犯罪分子为什么喜欢无线连接

网络犯罪分子为什么喜欢移动计算

网络犯罪分子为什么喜欢尖端网络和电子邮件技术

网络犯罪分子为什么喜欢电子商务和网上银行

网络犯罪分子为什么喜欢即时信息传递

网络犯罪分子为什么喜欢新操作系统和应用项目

网络犯罪分子为什么喜欢标准化

规划未来：如何应对明天的网络犯罪

总结

常见问题解答

参考文献

第三章 了解图景中的人物

概述

了解网络犯罪分子

网络犯罪分子剖析

罪犯剖析工作原理

重新审视有关网络犯罪分子的神话和错误概念

典型网络犯罪分子概貌

了解犯罪分子的动机

- 统计分析的局限性
- 网络犯罪分子分类
 - 罪犯将互联网用作犯罪工具
 - 罪犯偶尔利用互联网犯罪
 - 在网上犯罪的现实生活守法者
- 了解网络罪行受害者
 - 网络罪行受害者分类
 - 把受害者团结到反犯罪的队伍中来
- 了解网络犯罪调查员
 - 优秀网络犯罪调查员的素质
 - 从技能水平角度给网络犯罪调查员分类
 - 充实和训练网络犯罪调查员
 - 促进合作：CEO 在场景中扮演的角色
- 总结
- 常见问题解答
- 参考文献
- 第四章 计算机基本原理
 - 概述
 - 了解计算机硬件
 - 观察计算机内部
 - 数字计算机的组件
 - 主板的作用
 - 处理器和存储器的作用
 - 存储介质的作用
 - 这个问题为什么对调查人员关系重大？
 - 计算机的语言
 - 在数字世界中徜徉
 - 数字基础
 - 了解二进制计数系统
 - 二进制与十进制的转换
 - 二进制与十六进制的转换
 - 文本转换为二进制
 - 非文本文件编码
 - 这个问题为什么对调查人员关系重大？
 - 了解计算机操作系统
 - 了解操作系统软件的作用
 - 多任务和多重处理的类型区别
 - 多任务
 - 多重处理
 - 专有操作系统与开放源码操作系统的区别
 - 常用操作系统概述
 - 了解 DOS
 - Windows 1.x-3.x
 - Windows 9x (95、95b、95c、98、98SE 和 ME)

- Windows NT
- Windows 2000
- Windows XP
- Linux/UNIX
- 其他操作系统
- 了解文件系统
 - FAT12
 - FAT16
 - VFAT
 - FAT32
 - NTFS
 - 其他文件系统
- 总结
- 常见问题解答
- 参考文献
- 第五章 网络基本原理
 - 概述
 - 了解计算机网络通信
 - 通过网络传输比特和字节
 - 数字信号和模拟信号
 - 多路复用的工作原理
 - 方向因素
 - 分时因素
 - 信号干扰
 - 数据包、片段、数据报和帧
 - 访问控制方法
 - 网络类型和拓扑
 - 这个问题为什么对调查人员关系重大?
 - 了解联网模型和标准
 - OSI 联网模型
 - 国防部联网模型
 - 物理 / 数据连通层标准
 - 这个问题为什么对调查人员关系重大?
 - 了解网络硬件
 - 网络接口卡的作用
 - 网络媒体的作用
 - 网络连通装置的作用
 - 这个问题为什么对调查人员关系重大?
 - 了解网络软件
 - 了解客户机 / 服务器计算
 - 服务器软件
 - 客户机软件
 - 网络文件系统和文件共享协议
 - 有关（联网）协议的一个问题

了解互联网上使用的 TCP/IP 协议

使用标准化协议的必要性

TCP/IP 简史

互联网协议和 IP 寻址

路由工作原理

传送层协议

MAC 地址

名字解析

TCP/IP 公用程序

网络监测工具

这个问题为什么对调查人员关系重大？

总结

常见问题解答

参考文献

第六章 网络入侵和攻击

概述

了解网络入侵和攻击

入侵和攻击

辨别直接攻击和分布式攻击

自动攻击

意外“攻击”

防范有意内部安全破坏

防范未经授权外部入侵

制定防火墙疏漏预防计划

拥有内部访问权的外部入侵者

确定“攻击事实”

攻击类型的识别和分类

识别入侵 / 攻击前活动

端口扫描

地址哄骗

IP 哄骗

ARP 哄骗

DNS 哄骗

放置特洛伊木马

放置追踪装置和软件

放置数据包捕捉软件和协议分析器软件

预防和反应

口令破解

蛮力攻击

利用保存的口令

监听口令

口令解密软件

社会工程

预防和反应

- 口令的总体保护措施
- 保护网络不受社会工程是侵扰
- 恶意利用技术
 - 协议利用
 - 利用 TCP/IP 的拒绝服务攻击
 - 源路由攻击
 - 其他协议利用
 - 应用软件利用
 - 错误利用
 - 邮件炸弹
 - 浏览器利用
 - Web 服务器利用
 - 缓冲区溢出
 - 操作系统利用
 - WinNuke 带外攻击
 - Windows 注册表攻击
 - 其他 Windows 利用
 - UNIX 利用
 - 路由器利用
 - 预防和反应
- 特洛伊、病毒和蠕虫攻击
 - 特洛伊
 - 病毒
 - 蠕虫
 - 预防和反应
- 技术水平低下的黑客攻击
 - 脚本小子现象
 - “即点即用”黑客
 - 预防和反应
- 总结
- 常见问题解答
- 参考文献
- 第七章 预防网络犯罪
 - 概述
 - 了解网络安全概念
 - 安全规划基本原理
 - 安全的定义
 - 多层次安全的重要性
 - 入侵三角形
 - 消除入侵机会
 - 业内行话：安全术语
 - 物理安全的重要性
 - 保护服务器
 - 确保工作站安全

- 保护网络装置
- 密码学基本概念
 - 加密安全的目的
 - 认证身份
 - 提供数据保密性
 - 确保数据完整性
 - 基本加密概念
 - 通过代码和密码混杂文本
 - 什么是加密？
 - 通过密码算法确保数据安全
 - 信息安全中的加密应用
 - 什么是隐蔽术？
 - 现代破解密码的方法
 - 网络罪犯对加密和隐蔽术的利用
- 基于硬件和软件的安全方案
 - 实施基于硬件的安全措施
 - 基于硬件的防火墙
 - 认证装置
 - 实施基于软件的安全措施
 - 加密软件
 - 数字证书
 - 公钥基础设施
 - 基于软件的防火墙
- 防火墙
 - 防火墙分层过滤
 - 数据包过滤
 - 电路过滤
 - 应用过滤
 - 一体化入侵检测
- 组建事件响应小组
- 制定和实施安全政策
 - 安全以政策为根基
 - 什么是安全政策？
 - 这个问题为什么对调查人员关系重大？
- 评估安全需要
 - 机构安全计划的组成部分
 - 定义各方面责任
 - 分析风险因素
 - 评估威胁和威胁级别
 - 分析机构和网络的脆弱性
 - 分析机构因素
 - 考虑法律因素
 - 分析成本因素
 - 评估安全解决方案

遵守安全标准

政府安全等级

借鉴政策样板

定义各方面具体政策

口令政策

其他方面的政策

形成政策文件

确定范围和优先重点

政策制定指南

政策文件结构

网络用户安全教育

政策的执行

政策的传播

政策的反复评估和修订

总结

常见问题解答

参考文献

第八章 确保系统安全

概述

什么是系统安全？

安全心态

系统安全要素

实施宽带安全措施

宽带安全问题

配备防病毒软件

定义强用户口令

设置访问许可

禁用文件和打印共享

使用 NAT

配备防火墙

禁用不需要的服务

配置系统审计

实施浏览器和电子邮件安全措施

危险代码的类型

JavaScript

ActiveX

Java

改善浏览器和电子邮件客户软件的安全状态

限制编程语言

时时更新安全补丁

了解 Cookie

确保 Web 浏览器软件安全

确保微软 Internet Explorer 安全

确保 Netscape Navigator 安全

- 确保 Opera 安全
- 实施 Web 服务器安全措施
 - DMZ 与要塞
 - 隔离 Web 服务器
 - Web 服务器封闭
 - 管理访问控制
 - 处理目录和数据结构
 - 脚本脆弱性
 - 记录活动
 - 备份
 - 保持完整性
 - 欺骗性 Web 服务器
- 了解微软操作系统及其安全特性
 - 微软的普遍性安全问题
 - NetBIOS
 - 流行的自动化功能
 - IRDP 脆弱性
 - 网卡捆绑
 - 确保 Windows 9x 机安全
 - 确保 Windows NT 4.0 网络安全
 - 确保 Windows 2000 网络安全
 - Windows .NET: Windows 安全的未来
- 了解 UNIX/Linux 操作系统及其安全特性
- 了解 Macintosh 操作系统及其安全特性
- 了解主机系统的安全特性
- 了解无线网络的安全特性
- 总结
- 常见问题解答
- 参考文献

第九章 网络犯罪检测技术

- 概述
- 安全审计和日志文件
 - Windows 平台的审计
 - UNIX 和 Linux 平台的审计
- 防火墙日志、报告、警报和预警
- 电子邮件标题
- 追踪域名和 IP 地址
- 商用入侵检测系统
 - 入侵检测系统的特点
 - 商用 IDS 供应商
- IP 哄骗和其他反检测手段
- 蜜罐、蜜网和其他“网络圈套”
- 总结
- 常见问题解答

参考文献

第十章 收集和保存数字证据

概述

证据对于刑事案件的意义

证据的定义

证据的可接受性

计算机犯罪取证检查标准

收集数字证据

第一反应人员的角色

调查人员的角色

犯罪现场技术员的角色

保存数字证据

保存易失数据

硬盘成像

硬盘成像简史

成像软件

独立成像工具

成像技术在计算机犯罪取证中的作用

“快照”工具和文件拷贝

特殊考虑

环境因素

保留时间和日期戳

保存个人数字助理和袖珍电脑中的数据

恢复数字证据

恢复“被删除”和“被抹擦”数据

解密加密数据

寻找隐藏数据

数据隐藏在哪儿？

检测隐蔽数据

替换数据流

隐藏文件的方法

回收站

定位被遗忘数据

Web 缓存和 URL 历史

临时文件

交换文件和页面文件

从备份恢复数据

挫败数据恢复技术

覆盖硬盘

消磁或退磁

物理销毁硬盘

记录证据的文件

证据标签记和标记

证据日志

- 有关证据分析的文件
- 证据保管链文件
- 有关计算机犯罪取证的资源
 - 计算机犯罪取证培训和证书
 - 计算机犯罪取证设备和软件
 - 计算机犯罪取证服务
 - 计算机犯罪取证信息
- 了解相关法律问题
 - 搜查和没收数字证据
 - 美国宪法问题
 - 有关搜查证的要求
 - 无证搜查
 - 没收数字证据
 - 有关没收的法律
 - 有关隐私权的法律
 - 《美国爱国法案》的影响
- 总结
- 常见问题解答
- 参考文献
- 第十一章 网络犯罪立案起诉
 - 概述
 - 起诉过程复杂化的主要因素
 - 定义罪行的困难
 - 法律团体
 - 法律类型
 - 法律级别
 - 基本刑事司法理论
 - 违法元素
 - 举证水平和举证责任
 - 司法辖区问题
 - 司法辖区定义
 - 与司法辖区相关的成文法律
 - 与司法辖区相关的案例法律
 - 国际问题
 - 实际操作问题
- 证据的特性
- 人的因素
 - 执法人员的“态度”
 - 高科技生活方式
 - 天生对头？
- 排除障碍，惩治罪犯
- 调查程序
 - 调查工具
 - 调查步骤

确定各方人员的责任
网络犯罪案件作证
 审理程序
 证据证人作证
 专家证人作证
 提供直接证词
 复主诘问花招
 笔记本
总结
常见问题解答
参考文献
后记
附录 在全球范围内开展与网络犯罪的斗争