杨玉兰-王中英 windows入侵与防御 570.5-266

《万径寻踪：Windows入侵检测与防御编程（卷二）》是《万径寻踪：Windows入侵检测与防御编程（卷一）》的续篇，主要包括如下内容：

- 恶意行为防御篇：使用NDIS、WFP、内核回调、VT等技术应对各种恶意行为的检测和防御。
- 持久化防御篇：利用注册表过滤、COM钩子等技术应对恶意的持久化行为。
- 硬件与潜藏防御篇：利用硬件检测、VT技术、微过滤、磁盘过滤等技术应对硬件与rootkit、bootkit的恶意威胁。

联袂力荐

仲海啸 连云港市公安局网络安全保卫支队电子数据检验鉴定实验室教导员

陈　良 华为可信领域科学家，终端网络安全首席专家，终端奇点安全实验室主任，三届Pwn2Own世界冠军

姚纪卫 安芯网盾CTO，PCHunter作者

邵坚磊 前奇虎360安全技术委员会专家，现火绒高级终端安全研究员

段　钢 看雪学苑创始人

钱林松 武汉科锐逆向科技创始人，《C++反汇编逆向分析技术揭秘》作者

刘忠鑫 赛虎学院

扫一扫下载

本书资源

扫一扫查看

本书课程

水木书荟

www.shuimushuhui.com

图书详情　教学资源

会议资讯　图书出版

图书资源

书圈

ISBN 978-7-302-69514-1

定价：89.00元

万径寻踪

Windows入侵检测与防御编程

卷一

清华大学出版社

万径寻踪

Windows入侵检测与防御编程

卷一

谭文　周钰淇　郭艳君◎著

探寻网络攻击的惯用套路，揭秘激烈的攻防对抗，构筑系统安全的纵深防线。

清华大学出版社

作者简介

谭　文

某互联网企业安全技术专家，2002年毕业于西安交通大学信息工程专业，从事底层及安全相关开发二十余年。曾参与或带领团队开发DLP、防火墙、模拟器、反病毒软件、业务安全等诸多业内著名产品，亲手编写的代码在日活千万级的用户机器上稳定运行，守护着用户与系统的安全。著有《天书夜读：从汇编语言到Windows内核编程》《寒江独钓：Windows内核安全编程》《Windows内核编程》等多部技术专著。业余爱好射箭和剑道，为上海华剑馆弟子。

周钰淇

江苏省连云港市公安局网安支队四级警长，2018年获南京邮电大学信息安全专业硕士学位。长期从事网络安全工作，拥有丰富经验。曾任TrendMicro中国资深研发工程师，深度参与macOS平台EDR、XDR及SandBox项目研发。擅长安全系统开发及病毒恶意行为检测，擅长各类网络犯罪的追踪和取证技术。从警后曾获连云港市科技强警一等奖，连云港市五一创新能手称号和个人三等功一次。业余爱好空手道。

郭艳君

某互联网企业资深安全技术研发工程师，已从事安全行业相关工作近二十年。曾作为主要研究人员参与DLP、HIPS及XDR等多种业内著名安全产品研发，拥有极为丰富的开发经验。目前负责开发的RASP、HIPS等产品正守护着国内顶尖互联网企业的服务器的安全。业余爱好制作各种神奇电子产品。