占文

微信：Herr_Zhan
博客：www.mrzz.cc
邮箱：ulvpn@student.kit.edu
电话：+49 1625342038 （德国号码，如无法呼叫，请邮件或者微信联系）
地址：Sebastian-Kneipp-Str.15 76131 Karlsruhe Germany

教育背景

2013.09 - 2017.07 电子科技大学 通信学院 网络工程 GPA3.9/4.0 排名16/110(获保研)

2017.10 - 2018.06 KIT(卡尔斯鲁厄理工，德国精英大学) 预科 德语学习 DSH2.0

2018.10 - 2021.11 KIT(卡尔斯鲁厄理工，德国精英大学) 计算机学院 安全方向硕士

专业技能

- 熟悉C/C++及常见算法与数据结构
- 了解操作系统基本原理，Debian用户
- 熟悉计算机网络基本知识
- 了解渗透测试的基本流程
- 熟悉常见对称/非对称加密系统
- 理解RSA和DH原理和常见漏洞
- 熟悉常见数字签名原理和伪造手段
- 了解Nmap, Metasploit等工具的基本用法

实践经历

匿名代理 2020.07 - 2020.08

简介：一个小巧的SOCKS5代理工具

内容：设计了按字节混淆流量的加解密算法，使用随机函数生成256位长度密钥。在服务器端实现了监听端口请求、加解密、转发流量的功能；在客户端实现了监听本地地址，转发来自浏览器的网络请求。

代码仓库：https://git.scc.kit.edu/ulvpn/tinyproxy

密码学 2019.10 - 2020.02

简介：在EISS(欧洲系统安全研究所)参加的关于加密系统的实践项目，研究可能存在的缺陷并寻找攻击方法。

内容：针对传统对称Vigenere密码找到一种自相关系数，并结合统计概率应用到密钥破解；研究了块加密的PKCS7填充原理，并据此完成对AES-CBC的攻击获得明文；实现RSA中应用的模N大数幂乘的快速算法，并使用滑动窗口方法进一步提高运算速度；根据PKCS1的填充机制，通过迭代快速缩小RSA明文范围最终确定明文；研究了DH数字签名和校验机制，并根据校验漏洞伪造合法签名；实现64位密钥的2DES明文密文对Meet-in-the-Middle攻击获得密钥，并优化流程以减少存储要求实现Time-Memory-Tradeoff。

代码仓库：https://git.scc.kit.edu/ulvpn/crypto

渗透测试 2020.05 - 2020.07

简介：FZI(信息技术研究中心)开设的渗透测试实践，和两位德国队友一起完成了对FZI测试平台的Ubuntu18 和Windows10的渗透登录和提权操作。

内容：前期负责情报收集，寻找可能的漏洞，也参与制定攻击向量，渗透阶段和队友一起尝试对目标的攻击，比如通过GET参数实现对网页的LaTex注入、组合运用keepass2john和hashcat破解.kdbx文件的口令、利用Chrome80的JSCreate Side-effect Type Confusion漏洞实现对Windows10的登录，后期合作撰写报告并现场演示对一台机器的渗透。

渗透测试报告：https://git.scc.kit.edu/ulvpn/pentest-report/

语言能力

德语：DSH2.0 计算机专业德语听课、笔试、口试和Presentation。
英语：英文听课，流畅阅读技术书籍，可撰写报告。
日语：入门，简单日常会话。