《操作系统安全》

第三部分 内存安全保护

3.4 内存安全实验

中国科学院大学
网络空间安全学院
2018.3.23

中国科学院大学
University of Chinese Academy of Sciences

中国科学院信息工程研究所
INSTITUTE OF INFORMATION ENGINEERING,CAS

目录

缓冲区溢出与不可执行保护实验

- 实验目的
  - 理解掌握C栈帧结构
  - Shellcode构造
  - 加深理解缓冲器溢出攻击原理及防护措施
- 实验要求
  - 在关闭安全机制下，在Linux系统平台上实现缓冲区溢出攻击
  - 开启安全保护机制，运行一样的溢出攻击代码，比较实现现象

缓冲区溢出与不可执行保护实验

- 实验展示
  - 实验原理及平台介绍
  - 漏洞代码讲解及展示
  - Shellcode代码讲解及展示
  - 实验结果截图或录制视频
- 实验注意事项
  - 现在主流系统开启了溢出保护功能，实验前检查系统相关配置，找到控制开关

缓冲区溢出与不可执行保护实验

- 可选溢出实验内容
  - 格式化溢出
  - 堆溢出
  - ret2lic
  - ret2plt
  - ROP
  - ……

跨运行级别提权实验

- 实验目的
  - 理解跨运行级别提权攻击原理
- 实验要求
  - 跨运行权限执行代码或获取信息
- 实验内容（选择一个或多个）
  - 实现在ring-0（内核空间）运行级别上运行用户空间代码
  - 实现在ring-0（内核空间）运行级别上访问用户空间信息
  - 用户空间代码在ring-0下运行
  - 用户空间代码获取内核信息

跨运行级别提权实验

- 实验展示
  - 实验原理及平台介绍
  - 实现代码讲解及展示
  - 实现结果截图或录制视频
- 实验注意事项
  - 实验前检查实验环境，查看是否具备或开启SMEP和SMAP机制，有则关闭

Rootkit及检测实验

- 实验目的
  - 理解Rootkit实施原理
  - 掌握Rootkit检测技术
- 实验要求
  - 实现Rootkit隐藏内核模块检测技术
  - 实现Rootkit隐藏进程检测技术
  - 至少实现其中之一
  - Linux系统上实现
  - 可以使用工具

Rootkit及检测实验

- 实验展示
  - 实验原理及平台介绍
  - 实现代码讲解及展示
  - 实现结果截图或录制视频
- 实验注意事项
  - 实现代码不影响系统正常运行

Rootkit及检测实验

- 可选实验内容
  - 隐藏文件（检测）
  - 网络连接隐藏（检测）
  - 隐藏进程（检测）
  - 隐藏进程打开文件（检测）
  - 修改系统调用表（检测）
  - ……

提交材料要求

- 个人为单位，不分组（可以讨论）
- 提交word文档
  - 描述实验原理
  - 实验平台介绍及代码讲解
  - 实验现象和结果
  - 遇到的安全机制及规避
  - ……
- 2018年3月30日前提交（包含当天）
- PPT实验讲解（15-20分钟）
  - 自愿报名（2018年4月1日前，包含当天）
  - 选取4-6人（不足人数，随机选取）
- 提交作业及报名
  - 邮件：os_security@163.com

谢谢！