暨南大学本科实验报告专用纸

课程名称 信息系统安全实验 成绩评定

实验项目名称 Linux恶意脚本 指导教师 林聪

实验项目编号 实验十五 实验项目类型 综合性 实验地点 B403

学生姓名 冯俊泰 学号 2018054582

学院 人工智能学院 系 专业 信息安全

实验时间 6 月 1 日 上 午～ 6 月 1 日 上 午 温度 ℃湿度

1. **实验目的**
2. 掌握linux下恶意脚本执行的原理
3. 了解一般恶意脚本的攻击方式
4. 掌握如何防治恶意脚本的攻击
5. **实验原理**

操作系统与外部最重要的接口就是shell。Shell是操作系统最外面的一层。Shell管理你与操作系统之间的交互：等待输入、向操作系统解释输入、并且处理各种各样的操作系统的输出结果。Shell基本上是一个命令解释器，类似于dos下的command.Com。它接受用户命令，然后调用相应的应用程序。本实验要求应用者了解一定的shell编程知识。

1. **实验解答过程及结果**

本练习单人为一组。

首先使用“快照X”恢复Linux系统环境。

1. 主机覆盖其它脚本文件

(1) 点击平台工具栏中“控制台”按钮，弹出终端，新建自己的工作目“jlcsstest”，然后新建三个shell脚本，“jlcssa.sh”“jlcssb.sh”“jlcssc.sh”如下图所示：



图1 显示脚本文件

(2) 在“jlcssa.sh”与“jlcssb.sh”中加入语句，如下图所示：

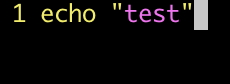


图2 脚本内容

(3) 在“jlcssc.sh”中添加如下语句实现功能，如下图所示：

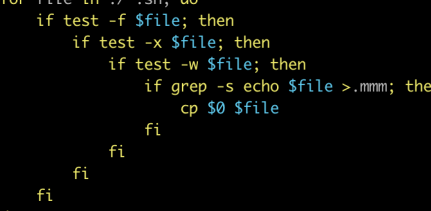


图3 脚本内容

(4) 改变三个文件的执行状态；如下图所示：



图4 改变文件执行状态

1. 查看三个文件的状态。如下图所示：



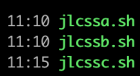


图5 查看文件状态

(6) 执行“jlcssc.sh”脚本，实现覆盖另两个脚本的功能，如下图所示：

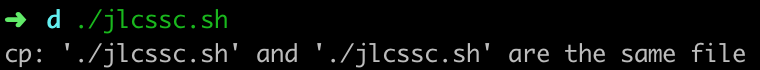


图6 执行jlcssc.sh

(7) 查看三个文件的状态。如下图所示：

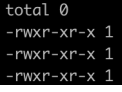
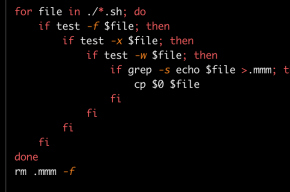
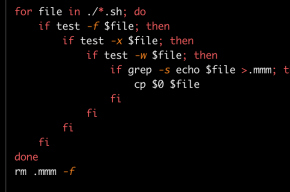


图7 查看文件状态

(8) 查看“jlcssa.sh”与“jlcssb.sh”中代码，和“jlcssc.sh”中相同，覆盖成功。



2. 插入其它脚本

(1) 在“jlcssa.sh”与“jlcssb.sh”清空原有代码，添加如下语句，如下图所示：

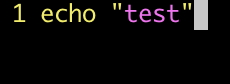


图8 脚本内容

(2) 在“jlcssc.sh”中添加如下语句实现功能，如下图所示：

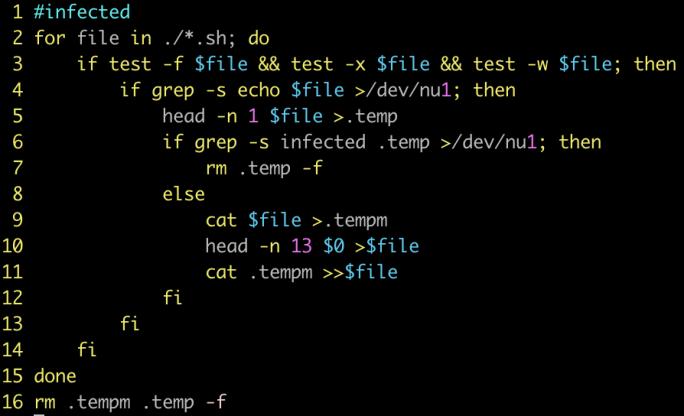


图9 脚本内容

(3) 改变三个文件的执行状态，如下图所示：



图10 改变文件状态

(4) 执行“jlcssc.sh”脚本，实现插入另两个脚本的功能，且此时状态。如下图所示：



图11 执行jlcssc.sh

(5) 查看“jlcssa.sh”与“jlcssb.sh”中代码，已插入“jlcssc.sh”中的代码，插入成功。

3. 恶意脚本

Shell基本都是明码，所以不难查处问题所在，一般shell得不到root权限，基本影响不会很大，但当得到root权限便可肆意删除、破坏系统。不过此类代码，只要使用者不轻易执行不明脚本，便使其无机可趁。

1. **实验总结**

学习了Linux恶意脚本的相关内容。