# 《网络安全技术基础》实验指导

## 实验5 Linux安全策略设置

**一、实验目的和要求**

1. 了解操作系统安全的概念。
2. 熟悉Linux安全策略设置的工具和方法。
3. 了解Apache服务器和Ftp服务器安全配置。

**二、实验内容**

1. 查看并修改Linux相关配置文件，提高系统的安全性，并验证配置效果。
2. 查看并修改Apache服务器配置文件相关配置项，提高服务器的安全性，并验证配置效果。
3. 查看并修改Ftp服务器配置文件相关配置项，创建虚拟用户，提高服务器的安全性，并验证配置效果。

**三、实验步骤：**

1. 查看并修改Linux配置文件，提高系统的安全性：
   1. Linux引导程序安全设置：grub.conf；
   2. 防止使用组合键重启系统：/etc/inittab；
   3. 安全登录、注销：/etc/sudoers /etc/profile；
   4. 用户账号安全管理：/etc/login.defs；
   5. 资源使用的限制：/etc/security/limits.conf；
   6. 清除历史记录：/etc/profile histsize；
   7. 系统服务的访问控制：hosts.allow hosts.deny；
   8. 系统日志安全： syslog日志服务 /var/log。
2. 查看并修改Apache服务器配置文件相关配置项，提高服务器的安全性，并验证配置效果。
   1. 隐藏或伪装apache版本号；
   2. 禁止使用目录索引；
   3. 配置web目录的访问策略；
   4. Apache服务器的访问控制；
   5. 使用mod\_evasive来反驳DoS攻击；
   6. 建立安全的目录结构。
3. 查看并修改Ftp服务器配置文件相关配置项，创建虚拟用户，提高服务器的安全性，并验证配置效果。
   1. 修改配置文件，将ftp服务预设端口改为2121；
   2. 禁止匿名用户登录；
   3. 修改ftp默认主目录为/ftp文件夹，并将用户锁定在主目录内；
   4. 关闭ls -R命令，防止服务器被DoS攻击；
   5. 关闭ascii模式下载，防止被用于DoS攻击；
   6. 修改ssh配置文件，禁止root用户通过ssh登录；
   7. 配置TCP Wrappers ，对远程主机进行访问控制，仅允许特定网段使用ssh进行登录；
   8. 修改ssh配置文件，禁止使用空密码进行登录，设置最大尝试次数以防密码爆破；
   9. 使用虚拟用户访问ftp 服务器。