linux操作系统的加固方案

1.避免安装不必要的包

2.软件包即时更新，减少存在未知漏洞

3.服务器系统定期漏洞扫描

4.关闭不必要的服务降低对外暴漏的攻击面

5.减少外网直接ssh登录 限制尝试登录次数

6.减少人员使用root权限，使用sudo控制

7.记录shell执行命令

跳板机审计

8.linux二进制目录，定时任务文件变动监控

9.使用防火墙控制可信任网络监控

10.使用vpn构建虚拟内网 服务器 业务 后台走vpn才可以

11、所有账号口令定期修改，并满足3个字符以上复杂策略

12 业务系统上线前进行漏洞扫码，特别是主业务