第八部分：系统安全与简单故障排查

一、基本安全理念

1.1 最小权限原则

- **不要用 root 执行一切**；
- 用户应只具备完成任务所需的最小权限。

1.2 使用 sudo 管理提权

- 使用 `sudo` 临时提权；
- 日志记录命令，便于追踪。

1.3 重要建议

- **及时更新系统**；
- **设置强密码**；
- **限制 SSH 登录用户或使用密钥**；
- **避免对外暴露不必要的服务或端口**；
- **使用日志监控系统活动**。

二、常用日志查看与排错

2.1 系统日志文件路径（默认在 `/var/log/`）

日志文件	说明
`/var/log/syslog`	系统级日志（默认推荐）
`/var/log/auth.log`	登录/认证日志（如 sudo, ssh）
`/var/log/dpkg.log`	安装/卸载软件记录
`/var/log/ufw.log`	防火墙日志（需启用）
`/var/log/nginx/`	Web 服务日志（如 Nginx）

2.2 日志查看命令

```
less /var/log/syslog
tail -f /var/log/auth.log
grep sshd /var/log/auth.log
```

三、用户登录安全与限制

3.1 查看当前登录用户

```
who
w
last
```

3.2 限制 root 登录（了解）

在 `/etc/ssh/sshd_config` 中添加或修改：

```
PermitRootLogin no
```

然后重启 SSH 服务：

```
sudo systemctl restart ssh
```

四、防火墙 ufw（简易防火墙）

4.1 安装与启用 ufw

```
sudo apt install ufw
sudo ufw enable
sudo ufw status
```

4.2 允许/拒绝端口

```
sudo ufw allow ssh
sudo ufw allow http
sudo ufw deny 23             # 禁用 telnet
sudo ufw delete allow 80     # 删除规则
```

五、系统更新与维护

5.1 安装安全更新

```
sudo apt update
sudo apt upgrade
```

5.2 自动更新设置（了解）

可以安装自动更新服务：

```
sudo apt install unattended-upgrades
```

并配置 `/etc/apt/apt.conf.d/50unattended-upgrades` 文件。

注意：正式对外提供服务的系统不要自动更新。

六、简单故障排查案例

6.1 SSH 无法登录

- 网络不通？→ `ping 服务器IP`
- 端口被防火墙拦截？→ `ufw status`
- SSH 服务是否运行？→ `systemctl status ssh`
- 查看日志：`tail /var/log/auth.log`

6.2 网站无法访问

- Nginx 是否运行？→ `systemctl status nginx`
- 端口是否监听？→ `ss -tuln | grep 80`
- 查看日志：`less /var/log/nginx/error.log`

6.3 软件无法安装

- 网络连通性；
- 源地址是否可达；
- 锁文件占用：

```
sudo rm /var/lib/dpkg/lock*
sudo dpkg --configure -a
```

本章练习任务

✅ 练习1：查看系统与安全日志

```
sudo less /var/log/syslog
sudo tail -f /var/log/auth.log
```

✅ 练习2：配置并启用防火墙

```
sudo apt install ufw
sudo ufw enable
sudo ufw allow ssh
sudo ufw allow http
sudo ufw status verbose
```

✅ 练习3：安全更新系统

```
sudo apt update
sudo apt upgrade
```

✅ 练习4：模拟故障排查流程

1. 停掉 SSH 服务

```
sudo systemctl stop ssh
```

2. 使用本机 ssh 登录失败，查看原因

```
ssh localhost
sudo systemctl status ssh
```

3. 重启 SSH 服务并重试

```
sudo systemctl start ssh
```

📦 课后拓展任务

1. 用 `last` 查看登录历史；
2. 查看系统启动时间：

```
who -b
```

3. 设置防火墙默认策略：

```
sudo ufw default deny incoming
sudo ufw default allow outgoing
```