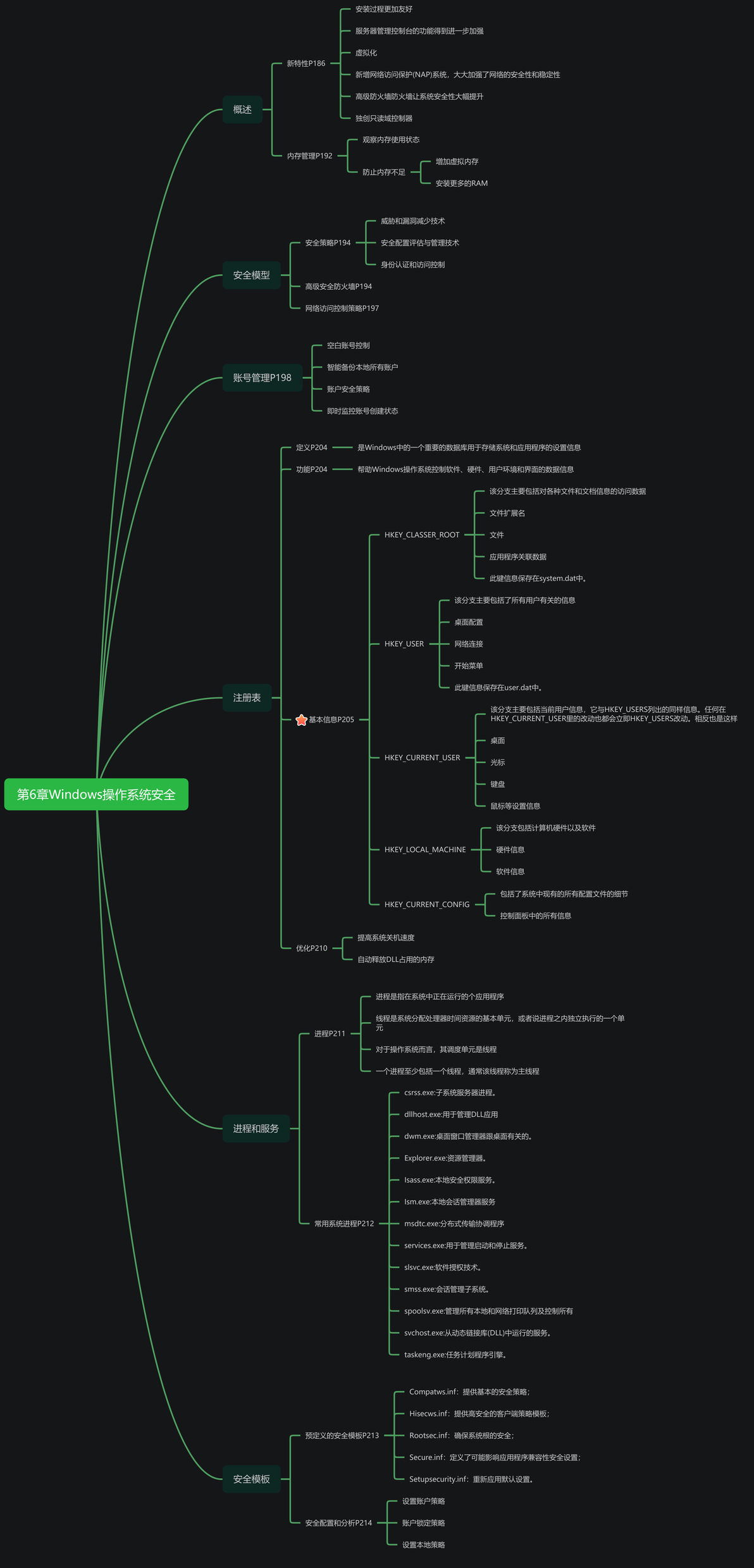
第6章Windows操作系统安全
概述
新特性P186
安装过程更加友好
服务器管理控制台的功能得到进一步加强
虚拟化
新增网络访问保护(NAP)系统，大大加强了网络的安全性和稳定性
高级防火墙防火墙让系统安全性大幅提升
独创只读域控制器
内存管理P192
观察内存使用状态
防止内存不足
增加虚拟内存
安装更多的RAM
安全模型
安全策略P194
威胁和漏洞减少技术
安全配置评估与管理技术
身份认证和访问控制
高级安全防火墙P194
网络访问控制策略P197
账号管理P198
空白账号控制
智能备份本地所有账户
账户安全策略
即时监控账号创建状态
注册表
定义P204
是Windows中的一个重要的数据库用于存储系统和应用程序的设置信息
功能P204
帮助Windows操作系统控制软件、硬件、用户环境和界面的数据信息
基本信息P205
HKEY_CLASSER_ROOT
该分支主要包括对各种文件和文档信息的访问数据
文件扩展名
文件
应用程序关联数据
此键信息保存在system.dat中。
HKEY_USER
该分支主要包括了所有用户有关的信息
桌面配置
网络连接
开始菜单
此键信息保存在user.dat中。
HKEY_CURRENT_USER
该分支主要包括当前用户信息，它与HKEY_USERS列出的同样信息。任何在HKEY_CURRENT_USER里的改动也都会立即HKEY_USERS改动。相反也是这样
桌面
光标
键盘
鼠标等设置信息
HKEY_LOCAL_MACHINE
该分支包括计算机硬件以及软件
硬件信息
软件信息
HKEY_CURRENT_CONFIG
包括了系统中现有的所有配置文件的细节
控制面板中的所有信息
优化P210
提高系统关机速度
自动释放DLL占用的内存
进程和服务
进程P211
进程是指在系统中正在运行的个应用程序
线程是系统分配处理器时间资源的基本单元，或者说进程之内独立执行的一个单元
对于操作系统而言，其调度单元是线程
一个进程至少包括一个线程，通常该线程称为主线程
常用系统进程P212
csrss.exe:子系统服务器进程。
dllhost.exe:用于管理DLL应用
dwm.exe:桌面窗口管理器跟桌面有关的。
Explorer.exe:资源管理器。
lsass.exe:本地安全权限服务。
lsm.exe:本地会话管理器服务
msdtc.exe:分布式传输协调程序
services.exe:用于管理启动和停止服务。
slsvc.exe:软件授权技术。
smss.exe:会话管理子系统。
spoolsv.exe:管理所有本地和网络打印队列及控制所有
svchost.exe:从动态链接库(DLL)中运行的服务。
taskeng.exe:任务计划程序引擎。
安全模板
预定义的安全模板P213
Compatws.inf：提供基本的安全策略；
Hisecws.inf：提供高安全的客户端策略模板；
Rootsec.inf：确保系统根的安全；
Secure.inf：定义了可能影响应用程序兼容性安全设置；
Setupsecurity.inf：重新应用默认设置。
安全配置和分析P214
设置账户策略
账户锁定策略
设置本地策略