《计算环境安全》知识点串讲

第一篇 操作系统安全

第 1 节 Windows 操作系统安全

1.标识

1.1 主体：用户账号、组账号、计算机、服务。

1.2 方法：SID 具有唯一性（编码），用户名相同则 SID 不同。

2.身份鉴别

2.1 分类：本地鉴别和远程鉴别。

2.2 信息文件：SAM 仅对 System 有权限。

2.3 远程：安全性的高低，NTLM>LM>SMB。

3.访问控制

3.1 用户的角色分配：RBAC（基于角色的访问控制）

3.2 权限管理和分配：CL

3.3 文件的访问控制：ACL

3.4 网络访问控制：ACL

4.保密性

4.1 EFS 加密文件系统

4.2 BitLocker

4.3 四层加密实现：物理层、分卷层、文件系统层、应用层。层次越低安全性越高，层次越高可移植性越高。

5.完整性：操作完整性、系统完整性等。

6.审计：系统审计、应用审计、安全审计、IE 审计。

7.备份恢复：系统还原的方式、OS 镜像文件、集群的方式。

8.补丁升级：WSUS 的部署。

9.系统的配置：

9.1 IPC 进程共享对于操作系统关闭后重启无效。

9.2 远程访问 CD-ROM 等外设禁用。

9.3 匿名禁用。

9.4 不安全服务的关闭的正确流程。

第 2 节 Linux 操作系统安全

1.标识

1.1 用户（UID）、用户组（GID）

1.2 用户可以在一个组中，也可以在多个组中。

1.3 Root 最高权限的用户

1.4 系统中任何用户、程序、设备都是用文件表达。
2.身份鉴别
2.1 方式：**本地**和**远程**
2.2 文件：password（用户描述、早期密码散列）、shadow（当前密码散列、密码策略信息）
3.访问控制
3.1 权限分类：读、写、执行、S（特殊）。
3.2 权限表达模式位（见 PPT）。Rwx rwx rwx 表达方式。
3.3 关于权限二进制标准（见 PPT）
3.4 关于 S 位和 X 位的表达：小写 s 代表不可删除可以执行，大写 S 代表不可删除不可以执行。
4.保密性：eCryptFS
5.完整性：linux 普通版本包括系统完整，SElinux 包括强制的完整。
6.审计：**链接时间**、**系统**日志和**应用**日志。
7.备份
8.补丁升级。
9.配置
9.1 可以部署在多个分区。
9.2 SSH、ETC 目录下、防火墙的远程访问均需要配置。
9.3 Banner 信息的修改，SSH 和 ETC 信任主机访问。
9.4 账号安全：多余、空口令、ID=0 等需要做好配置。
9.5 远程访问：SSH 代替 TELNET。
9.6 服务禁用：初始化部署时是服务梳理和禁用的最佳时间。
9.7 权限掩码：保障权限的唯一性和确定性。
9.8 防护软件：IPTABLES。

第二篇 数据库和应用安全

第 1 节 数据库安全

1. 关系数据库的特点：结构化、独立性、完整性约束。
2. 结构化查询语句的分类：事务控制>数据控制>数据操纵。
3. 数据库的**安全机制**

3.1 标识和鉴别：采用**用户名**和**密码**的方式实现。则同其他的用户名和密码的管理要求。
3.2 访问控制：
1）权限类型：**数据**权限、**模式**权限（用户）、**系统**权限。
2）权限表现形式
— 基于 RBAC 角色访问控制权限。
— 基于 Clark-Wilson 动态访问控制权限（体现是事务机制）。

3.3 数据保密性
1）传输保密：VPN（SSL/TLS）
2）存储保密
— OS 层加密（EFS\BITLOCKER\ECRYPTFS）
— DBMS 内核层加密（DBMS，转码处理比较少）
— DBMS 外层加密（应用层加解密系统、采用加密系统）
3）其他保密
— 视图机制，基于“知必所需”的原则
— 数据库的统计规则（F(X)=ABC），应用在大数据安全
3.4 完整性
1）基于**约束条件**的完整性
— **实体**完整性（主键唯一不为空）
— **参照**完整性（外键与主键的关系确定性表达）
— **自定义**完整性（例如，密码不能低于 10 位）
2）基于 Clark-Wilson 事务处理过程的完整性
a.输入进行数据分类（约束和非约束）
b.约束性数据进行完整性校验（值）
c.进行一个转化处理过程（TP）
算法证明（证据 A+B=C）。
*日志（事务日志）****。*
d.转化结果进行一个校验（理论值和执行值一致）
3.5 数据库审计：**数据**级审计、**用户**级审计、**系统**级审计。
3.6 备份恢复场景：**事务**故障、**系统**故障、**介质**故障。
3.7 数据库的补丁升级。
4. 数据库运行的安全
4.1 基于 IATF 运行安全：多层的防护体系，体现“深度防御”思想。
4.2 基于事件（PPDR）运行安全：事前检查、事中监控、事后审计。
事中监控：基于网络监控、基于本地的日志进行监控。

第 3 节 应用安全

1.应用安全的基础
1.1 应用安全的基础建立在**物理**、**网络**、**系统**的安全之上。
1.2 应用安全总体关注：**鉴别**、**访问控制**、**保密性**、**完整性**、**抗抵赖**。
2.Web 应用安全措施
2.1 Web 程序的安全：通过软件的安全开发来实现。
2.2 HTTP 协议的安全：
1）**HTTP**：请求、响应简单；无连接和状态；信息泄露；弱认证。
2）解决措施：采用 SSL\TLS 来解决，HTTPS 的方式。

2.3 支撑软件的安全
1）**身份鉴别**：采用白名单的方式来实现。
2）**目录安全**：最小化目录访问权限，修改默认路径。
3）**日志安全**：日志记录及保护。
4）**传输安全**：采用 VPN 的方式。
5）**其他安全**：连接数、重定向的页面定制。
2.4 终端**浏览**的安全
1）采用**安全浏览器**
2）采用高级别安全访问
3）采用**白名单**的方式进行**脚本控制**
4）Cookies 信息及隐私保护。
2.其他应用安全
2.1 电子邮件安全：
1）采用安全协议：PGP\SMIME\PEM。
2）进行安全配置：鉴别、反向验证、关闭开放式转发、安全浏览。
2.2 FTP 的安全：FTPS（ftp+ssl/tls）的方式进行解决。
2.3 远程管理安全：SSH 等。
2.4 域名的安全：域名系统服务商采用加固及白名单方式，高级 DNS 采用可靠的第三方服务。
2.5 办公软件的安全：**防宏病毒、加密保护、PDF 发布**。
2.6 即时通信的安全。

第三篇 恶意代码

1.恶意代码的分类：
— **病毒**：破坏为目的，载体为破坏对象，传播。
— **木马**：监控窃取信息为目的，载体为隐藏对象，传播。
— **蠕虫**：消耗资源为目的，无载体，传播。
2.恶意代码的传播方式：信息流是恶意代码传播的渠道和路径。
3.恶意代码的防护技术
— 特征检测：漏报率高、误报率低。
— 行为检测：误报率高、漏报率低。
— **沙箱**技术：检测环境。
4.恶意代码分析技术
— 静态分析：漏报率低、误报率高。
— 动态分析：漏报率高、误报率低。
5.恶意代码清除技术
— 文件清除

— 进程退出
— 嵌入式系统等。

6. 互联网恶意代码防护技术
— 蜜罐
— 蜜网
— 云查杀

（End）
（END）

温馨提示：为了减少学习的负担和聚焦核心，知识点总结写的是关键的精要的要点，并非是知识点的全文，请根据你的理解程度和需要，结合教材和其他可信文献进行理解和掌握全面，以免产生以偏概全的问题。