软考-信息安全-操作系统安全保护 原创

kgd529501683 2022-08-07 00:10:12 博主文章分类：安全

文章标签 安全 unix 系统安全 linux 文章分类 运维 阅读数 485

文章目录

19.1 操作系统安全概述

- 操作系统负责计算系统的资源管理，支撑和控制各种应用程序运行，为用户提供计算机系统管理接口。
- 操作系统是构成网络信息系统的核心关键组件，其安全可靠程度决定了计算机系统的安全性和可靠性。

19.1.1 操作系统安全概念

- 一般来说，操作系统的安全是指满足安全策略要求，具有相应的安全机制及安全功能，符合特定的安全标准。
- 在一定的约束条件下，能够抵御常见的网络安全威胁，保障自身的安全运行及资源安全。
- 国家相关标准《信息安全技术 操作系统安全技术要求（GB/T 20272-2019）》根据安全功能和安全保障要求，将操作系统分成五个安全等级，具体如下：
    - 用户自主保护级
    - 系统审计保护级
    - 安全标记保护级
    - 结构化保护级
    - 访问验证保护级
- 操作系统的安全可控目标分为两个层面：
    - 第一个层面：
        - 是指给定一个操作系统，用户能够实现对操作系统的**可理解，可修改，可检测，可修复，可保护。**
    - 第二个层面：
        - 商业用户能够自己主导操作系统的产品化，**不受恶意的商业利益绑架或遭受知识产权专利陷阱，操作系统不能被利用危及国家安全。**

19.1.2 操作系统安全需求

- 操作系统的安全目标是能够防范网络安全威胁，保障操作系统的安全运行及计算机系统资源的安全性。
    - 通常情况下，操作系统的安全需求主要包括以下几个方面：
        - 1）标识和鉴别
            - 能够唯一标识系统中的用户，并进行身份真实性鉴别。
        - 2）访问控制
            - 按照系统安全策略，对用户的操作进行资源访问控制，防止用户对计算机资源的非法访问（窃取，篡改和破坏）。
        - 3）系统资源安全
            - 能够保护系统中信息及数据的完整性，保密性，可用性。
        - 4）网络安全
            - 能够进行网络访问控制，保证网络通信数据安全及网络服务的可用性。
        - 5）抗攻击
            - 具有系统运行监督机制，防御恶意代码攻击。
        - 6）自身安全
            - 操作系统具有自身安全保护机制，确保系统安全和完整性，具有可信恢复能力。

19.1.3 操作系统安全机制

- 操作系统的安全保障集成多种安全机制，主要包括硬件安全，标识与鉴别，访问控制，最小特权管理，安全审计，可信路径，系统安全增强等。
- **1.硬件安全**

- 是操作系统安全的基础保障机制，包括硬件安全可靠性，存储保护，I/O保护，CPU安全，物理环境安全等。

- **2.标识与鉴别**
  - 又称为认证机制，用于操作系统的用户及相关活动主体的身份标识，并给用户和相应的活动主体分配唯一的标识符。
  - 标识符具有唯一性，能够防止伪造。
  - 而鉴别则指证实，用户或活动主体的真实身份的过程。
- **3.访问控制**
  - 用于操作系统的资源管理控制，防止资源滥用。常见的访问控制又自主和强制。
- **4.最小特权管理**
  - 是指系统中某些用户或进程具有超级权限的操作能力。
  - 例如：UNIX/Linux等多用户操作系统的用户root具有所有特权，普通用户不具有任何特权。
  - 特权管理方式虽然便于系统维护和配置，但不利于系统的安全性。
  - 一旦特权用户的口令丢失或被冒充，将会对系统造成极大的损失。
  - 超级用户的误操作也是系统极大的安全隐患。
  - 必须建立并实行最小特权管理机制。
  - 最小特权管理就是-**操作系统不分配用户超过执行任务所需的权限，防止权限滥用，减少系统的安全风险。**
- **5.可信路径**
  - 是指操作系统的本地用户和远程用户进行初始登录或鉴别时，操作系统安全系统与用户之间建立的安全通信路径。
  - 可信路径保护通信数据免遭修改，泄露，防止特洛伊木马模仿登录过程，窃取用户的口令。
- **6.安全审计**
  - 就是操作系统对系统中有关安全的活动进行记录，检查及审核，其主要目的就是核实系统安全策略执行的合规性，以追踪违反安全策略的用户及活动主体，确认系统安全故障。
- **7.系统安全增强**
  - 又称为安全加固，通过优化操作系统的配置或增加安全组件，以提升操作系统的抗攻击能力。

19.1.4 操作系统安全技术

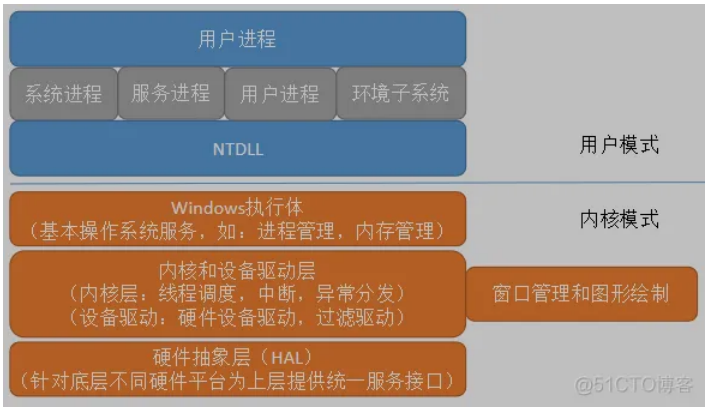
- 操作系统是复杂的系统软件，其安全机制的实现综合集成了多种安全技术，主要包括硬件容灾备份技术，可信计算技术，身份认证技术，访问控制技术，加密技术，安全审计和监测技术，系统安全增强技术，特权管理技术，形式化分析技术，安全渗透技术，隐蔽信道分析，安全补丁，防火墙，入侵检测，安全沙箱，攻击欺骗，地址空间随机化和系统恢复等技术，这些技术不同程度地应用在操作系统的安全机制构建，安全功能实现，安全保障，安全测评以及安全运行等各个方面。

19.2 Windows操作系统安全分析与防护

19.2.1 Windows系统架构

- Windows XP的结构是层次结构和客户机/服务器结构的混合体。
  - 系统划分为三层，最底层是硬件抽象层，它为上面的一层提供硬件结构的接口，有了这一层就可以使系统方便地移植。
  - 第二层是内核层，它为底层提供执行，中断，异常处理和同步的支持。
  - 第三层是由一系列实现基本系统服务的模块组成的，例如虚拟内存管理，对象管理，进程和线程管理，I/O管理，进程间通信和安全参考监督器。

文章目录



- Windows 2000系统在安全设计上有专门的安全子系统，安全子系统主要由本地安全授权（LSA），安全管理账户（SAM）和安全参考监视器（SRM）等组成。
    - LSA提供了许多服务程序，保障用户获得存取系统的许可权，它产生令牌，执行本地安全管理，提供交互式登录认证服务，控制安全审查策略和SRM产生的审查记录信息。
    - SAM对SAM数据库进行维护，该数据库包含所有组和用户的信息。并为用户赋予一个安全标识符（SID）。
    - SRM是负责访问控制和审查策略。

19.2.2 Windows安全机制

- **1.Windows认证机制**
    - 系统提供两种基本的认证类型，即本地认证和网络认证。
    - 身份认证技术有：KerberosV5 ，公钥证书和NTLM
- **2.Windows访问控制机制**
    - Windows的安全性达到了橘皮书C2级，实现了用户级自主访问控制。
- **3.Windows审计/日志机制**
    - 有三种类型日志，分别为系统日志，应用程序日志和安全日志。
- **4.Windows协议过滤和防火墙**
    - Windows自带防火墙
- **5.Windows文件加密系统**
    - 微软研究开发了加密的文件系统EFS。
- **6.抗攻击机制**
    - 常见针对缓冲区溢出，恶意代码攻击等微软增加了抗攻击的安全机制。
        - 堆栈保护（Stack Protection）
        - 安全结构例外处理（SafeSEH）
        - 数据执行保护（DEP）
        - 地址随机化（ASLR）
        - 补丁保护（PatchGuard）
        - 驱动程序签名（Driver Signing）
    - Windows 10提供减少攻击面规则配置。
        - 总结下来有阻止office相关创建子进程，代码注入其他进程，js执行，vbs执行，混淆脚本，调用Win32API，阻止不受信任的可执行文件，防勒索软件，阻止身份凭据窃取，阻止PsExec和WMI命令创建进程，其中PsEexec和WMI都可以远程执行代码。阻止USB运行不受信任，未签名的进程，阻止利用WMI事件订阅进行持久性攻击。

19.2.3 Windows系统安全分析

- **1.Windows口令**
- **2.Windows恶意代码**
- **3.Windows应用软件漏洞**
- **4.Windows系统程序漏洞**
- **5.Windows注册表安全**
- **6.Windows文件共享安全**
- **7.Windows物理临近攻击**

文章目录

- 使用WinPE（例如：微PE工具箱等）之类的系统重装辅助工具，重新引导系统，查看NTFS文件系统。

19.2.4 Windows系统安全增强技术方法与流程

- Windows系统的安全增强是指通过一些安全措施来提高系统的安全防护能力。
- 系统安全增强方法如下：
  - 1）安全漏洞打补丁（Patch）
  - 2）停止服务和卸载软件
  - 3）升级或更换程序
  - 4）修改配置或权限
  - 5）去除特洛伊等恶意程序（清除后门）
  - 6）安装专用的安全工具软件
- Windows系统安全增强是一件繁琐的事情，其基本步骤如下：
  - 1）确认系统安全增强的安全目标和系统的业务用途
  - 2）安装最小化的操作系统
  - 3）安装最新系统补丁
  - 4）（按需）配置安装的系统服务
  - 5）配置安全策略
    - 密码复杂度
    - 账户锁定阈值
    - 账户锁定时间
    - 账户锁定计数器。
  - 6）禁用NetBIOS
  - 7）账户安全配置
    - 禁用默认账号
    - 定期检查账户，尽早发现可以账户
    - 锁定Guest账户
  - 8）文件系统安全配置
    - 删除不必要的程序例如：cmd.exe
    - 启用加密文件系统
    - 设置文件共享口令
    - 修改系统默认安装目录名
  - 9）配置TCP/IP筛选和ICF
    - 配置Windows自带的功能TCP/IP工具和自带的防火墙
  - 10）禁用光盘或软盘启动
  - 11）使用屏幕保护口令
  - 12）设置应用软件安全
    - 及时安装应用软件安全补丁
    - 修改应用软件安全的默认设置
    - 限制应用软件的使用范围
  - 13）安装第三方防护软件

19.2.5 Windows 2000系统安全增强实例

- **1.系统启动安全增强**
  - 配置系统引导的时候只允许C盘启动，或者设置系统引导前要输入密码。
- **2.账号与口令管理安全增强**
  - 1）停掉guest账号
  - 2）限制不必要的用户数量
  - 3）把系统administrator账号改名
  - 4）创建一个陷阱账号
    - 设置最低权限账号，密码复杂度设置很高，账号名称为administrator
  - 5）设置安全复杂的口令
  - 6）设置屏幕保护口令
  - 7）不让系统显示上次登录的用户名

文章目录

- 8）开启口令安全策略
- 9）开启账号策略

- **3.安装最新系统补丁**
- **4.网络安全增强**
  - 禁止建立空连接，关闭默认共享，关闭不必要的网络服务和网络端口。
- **5.安装第三方防护软件**

19.2.6 Windows系统典型安全工具与参考规范

- 远程安全登录管理工具OpenSSH
- 系统身份认证增强工具Kerberos
- 恶意代码查杀Clam AV，火绒，360
- 系统安全检查工具Nmap，Sysinternals（工具集成）
- 系统安全监测工具netstat
- 针对Windows系统进行安全管理问题可根据国内外安全组织制定的安全标准规范，作为Windows操作系统配置的安全基线。
  - CIS（Center for Internet Security）
  - SANS TOP20
  - NIST SP 800-70
  - 《信息安全技术 政务计算机终端核心配置规范》（GB/T 30278-2013）

19.3 Unix/Linux操作系统安全分析与防护

19.3.1 Unix/Linux系统架构

- 分为三层硬件层，系统内核和应用层

19.3.2 Unix/Linux安全机制

- **1.Unix/Linux认证**
  - 1）基于口令的认证方式
  - 2）终端认证
  - 3）主机信任机制
  - 4）第三方认证
- **2.Unix/Linux访问控制**
  - 普通的Unix/Linux系统一般通过文件访问控制列表ACL来实现系统资源的控制，就是我们常说的通过“9bit”位来实现
- **3.Unix/Linux审计机制**

19.3.3 Unix/Linux系统安全分析

- **1.Unix/Linux账号和口令安全**
- **2.Unix/Linux可信主机文件安全**
- **3.Unix/Linux应用软件漏洞**
- **4.Unix/Linux的SUID文件安全**
- **5.Unix/Linux的恶意代码**
- **6.Unix/Linux文件系统安全**
- **7.Unix/Linux网络服务安全**
- **8.Unix/Linux系统程序漏洞**

19.3.4 Unix/Linux系统安全增强方法和流程

- **1.Unix/Linux系统安全增强方法**
  - 安全漏洞打补丁
  - 停止不必要服务
  - 升级或更换软件包
  - 修改系统配置
  - 安装专用的安全工具软件
- **2.Unix/Linux系统安全增强基本流程**
  - 1）确认系统的安全目标
  - 2）安装最小化Unix/Linux系统

文章目录

- 3）利用Unix/Linux系统自身的安全机制
- 4）使用SSH替换Telnet
- 5）利用系统安全测试工具
- 6）根据系统安全测试
- 7）定期安全监控，包括进程监控，用户监控，网络连接监控，日志分析等。

19.3.5 Unix/Linux系统安全增强技术

- 1.安装系统补丁软件包
- 2.最小化系统网络服务
- 3.设置系统开机保护口令
- 4.弱口令检查
- 5.禁用默认账号
- 6.用SSH增强网络服务安全
- 7.利用tcp_wrapper增强访问控制
- 8.构筑Unix/Linux主机防火墙（iptables）
- 9.使用Tripwire或MD5Sum完整性检查工具
- 10.检测LKM后门
- 11.系统安全监测

19.3.6 Linux安全增强配置参考

- 1.禁止访问重要文件
- 2.禁止不必要的SUID程序
- 3.为LILO增加开机口令（可能现在已经不适用了）
- 4.设置口令最小长度和最短使用时间
- 5.限制远程访问
- 6.用户超时注销
- 7.注销时删除命令记录

19.3.7 Unix/Linux安全模块应用参考

- Linux安全模块（LSM）为Linux内核提供了一个轻量级的，通用目的的访问控制框架，使得很多不同的访问控制模型可以作为可加载模块来实现。
- 目前采取上述提到的安全模块采取的方式来增强Linux安全的主要有插件式身份验证模块框架（Pluggable Authentication Modules，PAM），SELinux等。

19.3.8 Unix/Linux系统典型安全工具与参考规范

- 这里几乎跟上面描述Windows章节一模一样。

19.4 国产操作系统安全分析与防护

19.4.1 国产操作系统概况

- 有以中科方德，中标麒麟，北京凝思，普华，深度等代表的操作系统厂商
- 华为鸿蒙，阿里飞天云操作系统

19.4.2 国产操作系统安全分析

- 1.Linux内核的安全风险
- 2.自主研发系统组件的安全
- 3.依赖第三方系统组件的安全
- 4.系统安全配置的安全
- 5.硬件的安全

19.4.3 国产操作系统安全增强措施

- 标准参考：《信息安全技术 操作系统安全技术要求（GB/T 20272-2019）》
- 1.中科方德方舟安全操作系统
  - 1）基于三权分立的管理机制
    - 根据管理员在系统运行过程中的职责范围和最小特权原则，将普通操作系统中超级管理员的权限分配给系统管理员，安全管理员，审计管理员，并形成相互制约关系，防止管理员的恶意或偶然操作引起系统安全问题。
  - 2）强化的身份标识与认证机制

文章目录

- 为系统中的所有用户提供身份标识和认证机制，用户的身份标识在系统的整个生命周期内可以唯一地标识用户的身份，采用强化的口令管理及基于数字证书认证机制，实现对用户身份的真实性鉴别。

  - 3）综合应用多种安全策略，提高系统的安全性
  - 4）基于内核层的安全审计
  - 5）支持各类通用软件，具有良好的软硬件兼容性

- 2.中标麒麟安全操作系统
- 3.中标麒麟可信操作系统

  - 提供基于三权分立机制的多项安全功能（身份鉴别，访问控制，数据保护，安全标记，可信路径，安全审计等）和统一的安全控制中心
  - 支持国内外可信计算规范（TCM/TPCM,TPM2.0)
  - 支持国家密码管理部门发布的SM2，SM3，SM4等国密算法，兼容主流的软硬件和自主CPU平台。
  - 提供可持续的安全保障，防止软硬件被篡改和信息被窃取，系统免受攻击。

迷茫的人生，需要不断努力，才能看清远方模糊的志向！

文章目录

上一篇：PMP-6.项目进度管理-6.6控制进度

下一篇：PMP-6.项目进度管理-6.5制定进度计划

相关文章

操作系统学习笔记：保护

保护是指一种控制程序、进程或用户对计算机系统资源进行访问的机制。操作系统中的进程必须加以保护，使其免受其他进程活...

操作系统 访问矩阵 访问控制 访问权限

操作系统修炼指南——保护模式

环境搭建000 实验环境搭建保护模式001 保护模式 002 段寄存器 003 段选择子与段描述符结构 00

导航 OS 保护模式 分页 环境搭建

如何保护你的linux操作系统

如何保护你的linux操作系统 如何保护你的linux操作系统 导读 在现在这个世道中，Linux操作系统的安全是十分重要的。但是，你...

linux linux操作系统 访问控制

操作系统--实模式到保护模式

操作系统--实模式到保护模式一.实模式到保护模式(上)A.在这里需要从计算机的历史谈起1.远古时期的程序开发:是直接操作物理...

保护模式 实模式 make

操作系统之实模式和保护模式(简图)

操作系统之实模式和保护模式分段机制和分页机制

其他

操作系统-保护模式中的特权级

一.保护模式中的特权级(上)A.保护模式小结a.使用选择子访问段描述符表时，索引值的合法性检测1.当索引值越界时，引发+异常...

特权级 CPL DPL 选择子

软考-信息安全-操作系统安全保护

19.1 操作系统安全概述 操作系统负责计算系统的资源管理，支撑和控制各种应用程序运行，为用户提供计算机系统管理接口。

安全 unix 系统安全 linux

操作系统-从保护模式返回实模式

Q.从上节课可以引出一个小问题，下面的语句是否有Bug的存在在进入保护模式后,在第一处使用了栈段选择址对ss赋值，然后使…

保护模式 实模式 转换 高速缓冲

操作系统--进阶操作系统

一.操作系统A.由此我们可以的得出一个疑问，什么是操作系统?1.在我们日常生活中Windows,UNIX,Linux,MasOS,Android,ios等…

BIOS 操作系统 流程

【操作系统】操作系统原理

一、参考资料王道计算机考研 操作系统_哔哩哔哩_bilibili【王道论坛】版权所有，官方发布！本版为2018年第一次录制，后续版…

操作系统 迭代 参考资料 ide

操作系统-操作系统引论

计算机系统由硬件和软件两部分组成，操作系统(OS,Operating System)是配置在计算机硬件上的第一层软件，是对硬件系统…

操作系统 引论

【操作系统】操作系统引论

管理者OS是各类资源的管理者，计算机系统

操作系统 批处理系统 计算机系统 时间片

【操作系统】操作系统接口

令其他命令键盘终端处理程序命令解释程序的作用工作流程系统调用基本概念1.运行在不同的系统状态2.通过软中断进入3.返回…

操作系统 系统调用 程序接口 文件操作

操作系统概论——操作系统

操作系统是接口，并管软硬件资源主要功能：处理及，内存，文件，设备电子器，十五处理，分时处理OS/369和OS/390操作系…

批处理 批处理系统 计算逻辑

操作系统-保护模式中的特权级(中)

Q:如何在不同特权级代码段之间跳转执行？A.一种新的描述符，门描述符1.通过门描述符在不同的特权级的代码间进行跳转2.根…

调用门 选择子 特权级

【自制操作系统04】从实模式到保护模式

通过前三章的努力，我们成功将控制权转交给了 loader.asm 这个程序。具体说就是 bios 通过加载并跳转到 0x7c00（IMB大叔们…

描述符 保护模式 实模式 描述符表 寄存器

读懂操作系统(x64)之堆栈帧（过程调用）

前言 上一节内容我们对在32位操作系统下堆栈帧进行了详细的分析，本节我们继续来看看在位操作系统下对于过程调用在处理机…

寄存器 堆栈 局部变量

数据结构中的堆栈和操作系统中的堆栈

在面试的时候我们经常被问到堆和栈相关的问题，悲催的是还傻傻分不清面试官要问的是哪个堆栈。 是的，堆和栈有两层含义，…

数据结构 堆栈 堆和栈 数组 编译器

操作系统开发之——进入保护模式

依旧直接贴代码： %macro Descriptor 3 dw %2 & 0FFFFh ; 段界限 1 (2 字节) dw %1 & 0FFFFh ; 段基址 1 (2 字节) db (%1 >> 1…

属性值 保护模式 ide 代码段 数据段

hadoop固态硬盘 hadoop磁盘块的意义和作用

HDFS的概念 1、数据块 HDFS跟磁盘一样也有块的概念，磁盘上块的大小一般为512字节，而文件系统的块则一般是磁盘块…

hadoop固态硬盘 hadoop HDFS 数据

文章目录

cookie jquery 存放对象 jquery cookie用法

一个轻量级的cookie 插件，可以读取、写入、删除 cookie。 jquery.cookie.js 的配置 首先包含jQuery的库文件，在后面包含 jque…

cookie jquery 存放对象 有效时间 jquery 默认值

hive在root安装时为什么时anonymous hive的安装模式

一、安装三种模式hive的安装一共有三种方式:内嵌模式、本地模式、远程模式 内嵌模式内嵌模式使用的是内嵌的Derby数据库…

大数据 hive bc mysql

java 开发数据库面试题 java数据库系统开发

这篇文档是为了给开发者提供访问和修改oracle数据库的帮助。 通过一个简单的例子(jdbc 应用程序) 来阐述如何实施这此任…

java 开发数据库面试题 数据库 oracle java jdbc

java map减少if java map.clear

关于Map集合中常用的方法：

java map减少if java 数据库 System 键值对

文章目录