Linux服务器安全加固

Table of Contents

[1 Linux服务器安全介绍 2](#__RefHeading___Toc281_3060272606)

[1.1 操作系统的基本安全概念 2](#__RefHeading___Toc283_3060272606)

[1.1.1 计算机安全性 2](#__RefHeading___Toc285_3060272606)

[1.1.2 安全威胁 2](#__RefHeading___Toc287_3060272606)

[1.1.3 信息安全原则 3](#__RefHeading___Toc289_3060272606)

[1.1.4 安全性与可用性 3](#__RefHeading___Toc291_3060272606)

[1.1.5 防御层次 4](#__RefHeading___Toc293_3060272606)

[1.1.6 访问控制模型 4](#__RefHeading___Toc295_3060272606)

# Linux服务器安全介绍

关于Linux服务器安全，主要介绍的内容包括：

* 了解操作系统的基本安全概念，机制和工具
* 执行基本的系统锁定
* 本地帐户安全性管理
* 处理特权提升
* 保护基本网络服务
* 了解Linux内核安全模块
* 使用AppArmor和SELinux保护系统

本节介绍通用计算机安全概念和设计原理。 任何技术加密算法，身份验证机制和安全协议形式的组件，有助于实施那些安全性原则将得到审查。 最后，说明Linux发行版本如何实现安全性以及跟Linxu相关的安全认证。

## 操作系统的基本安全概念

### 计算机安全性

也称为网络安全性或IT安全性，是保护计算机系统免遭盗窃或损坏其硬件，软件或信息，以及防止其提供的服务受到破坏或误导。

<https://en.wikipedia.org/wiki/Computer_security>

### 安全威胁

通过未经授权的访问，破坏，披露，数据修改和/或拒绝服务可能对IS产生不利影响的任何情况或事件。

计算机安全的一些常见安全威胁包括：

* 物理损坏–更改或破坏物理设备，导致系统无法运行或不可靠。
* 欺骗–以伪造数据伪造数据，从而获得非法访问或验证的身份，从而以另一用户身份呈现给系统或服务。
* 信息披露–通常通过数据泄露的方式向未经授权的各方披露，发布，传输或复制受限制的访问信息。
* 拒绝服务–导致系统或服务暂时或永久停止提供预期的服务水平。
* 特权提升–通过使用软件系统漏洞或系统错误配置，可以访问系统中更高级别的特权。

### 信息安全原则

防止未经授权访问、使用、披露或修改信息是信息安全的主要目标。 信息保证通过授予信息或数据的机密性，完整性和身份验证来提供对信息的信任。

* 机密性–保护信息不泄露给未授权方。
* 完整性–维护并确保数据的准确性和完整性。
* 可用性–随时保持数据可用。
* 真实性–确保数据来自声称是发起者的人。
* 不可否认性–将行为或变更与唯一的个人或实体相关联的能力。

### 安全性与可用性

安全当然需要权衡。

每当您被告知密码不够长或由于使用新设备而被迫重新登录时，安全性和可用性之间的平衡就会显示出来。 这很痛苦，但是更安全。



在身份验证方面，我们今天遇到的通常以以下三种方式中的一种（或多种）实现：

* 您知道的一些信息（例如密码）
* 您拥有的东西（智能卡）
* 您是某物（指纹）

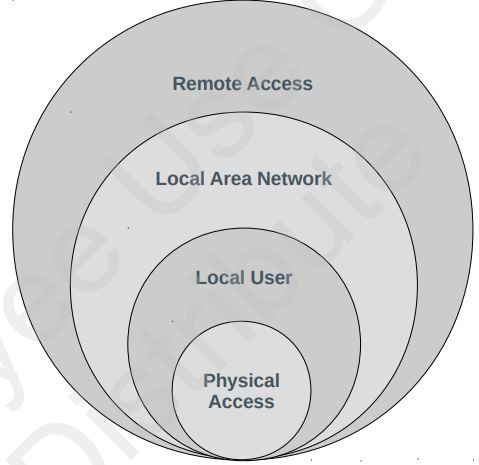
许多系统使用用户名/密码对进行访问控制，这在很大程度上是因为大多数系统的接口通常都是某种键盘。 某些智能手机使用PIN或指纹，而银行ATM则结合使用您拥有的东西（卡）和您知道的东西（PIN）。

确定适当的安全级别时，需要考虑以下事项：

* 数据的价值（创建或丢失数据的成本（有形或无形）
* 保护数据的成本
* 可用性权衡

### 防御层次

防御层次是一种信息保证概念，其中建立了多层安全控制。



* 物理安全性：指人们物理上访问计算机系统的能力。 物理访问为黑客入侵开辟了各种途径。 其中一些对策是：物理访问受锁定的服务器机房，登录表，摄像机监控，安全启动，硬件加密引擎，文件加密等限制。
* 本地安全性：本地安全性从计算机运行所在位置的物理环境开始。 在安全性符合您的期望和需求的地方安装计算机。 本地安全性的主要目标是使用户彼此分开，因此任何用户都不能承担他人的权限或身份。 一些对策是：强制或自由访问控制，身份管理或基于角色的访问控制，jail root等。
* 网络安全性：网络安全性对于防止网络外部发起的攻击非常重要。 在进行实际身份验证之前发生的是网络安全，而在此之后发生的一切是本地安全。 一些对策是：使用防火墙，VPN，限制服务远程访问配置等

### 访问控制模型

可以通过不同的访问控制模型来限制对信息系统的访问，其中最著名的是：

* 任意访问控制(Discretionary Access Control )–根据对象所属的主题和/或组的身份限制对对象的访问的手段。 具有特定访问权限的主题可以将此权限传递给其他主题。 Linux文件系统权限是DAC的一个很好的例子。
* 强制访问控制(Mandatory Acess Control)–采用分层方法，以系统管理员设置占优的方式强制控制对资源（数据，文件等）的访问。 用户无法直接更改这些设置，即使对于root用户也是如此。 到目前为止，这是Linux系统中最安全的访问控制方法。 SELinux和AppArmor是MAC的很好例子
* 基于角色的访问控制(Role Based Access Control)– RBAC系统上的访问基于系统所属组织内用户的工作职能。 将权限分配给角色，将角色应用于用户或用户组。

在计算机安全方面，访问控制提供身份验证，授权和计费（AAA），标识和访问批准的基本服务。身份验证涉及识别，会计需要审核。

* 身份证明Identification：是指声明或以其他方式表明声称证明某人或事物的身份的主张的行为，通常在认证之前进行。
* 认证Authentication：确认实体声称为真的单条数据（数据）的属性真相的行为。与身份验证相反，身份验证是指陈述或以其他方式表明声称证明某人或事物的身份的主张的行为，而身份验证则是实际确认该身份的过程。
* 授权Authorization：授权是指定对通常与信息安全和计算机安全有关的资源的访问权限，尤其是对访问控制的访问权限。更正式地说，“授权”是定义访问策略。
* 记帐Accounting：记帐是在访问网络资源时跟踪用户活动的过程，包括在网络上花费的时间，在那里访问的服务以及会话期间传输的数据量。会计数据用于趋势分析，容量计划，计费，审计和成本分配。
* 审核Audit：是对系统或应用程序进行的手动或系统的，可衡量的技术评估

### 安全方法

安全方法应包括以下方面的识别：

* 要保护的资产：资产是支持信息相关活动的任何数据，设备或环境的其他组件。资产通常包括硬件（例如服务器和交换机），软件（例如关键任务应用程序和支持系统）和机密信息。应保护资产免遭非法访问，使用，披露，更改，破坏和/或盗窃，从而对组织造成损失。进行风险分析时，重要的是权衡要花费多少钱来保护每项资产与损失资产的成本。同样重要的是要考虑到每次损失的可能性。还必须考虑无形成本。
* 威胁可能性：威胁可能性是威胁事件可能发生的概率。
* 安全机制–成本与收益：成本效益分析可以弥合安全经理与信息技术（IT）经理之间的沟通鸿沟。 IT经理希望知道他们在安全方面的投资已将风险降低到可接受的水平，并且安全经理希望确保其设计是最安全的。

### 系统安全设计原则

在系统设计阶段应用一些良好实践可能会导致系统更安全。 应遵循以下系统安全设计原则：

* 尽可能使用数据加密。 有几种通过加密保护数据的方法：加密硬盘分区，创建作为容器的加密文件，加密主目录，加密单个ASCII文本文件。
* 最少的软件包安装。 不存在的东西将无法使用。 未安装的二进制文件无法执行。 最少减少软件占用空间。
* 服务隔离-在单独的系统上运行不同的服务：只要有可能，服务器应专用于仅服务一个服务或应用程序。
* 系统指纹和备份：如果怀疑对系统进行了攻击，那么没有什么比备份，系统指纹可以检测到修改，完成工作后提供的舒适度更高了。