**Chapter 9. Security 安全性**

【理解】安全性概念

安全性是衡量系统向合法用户提供服务的同时，阻止非授权使用的能力。

三个特点（**CIA**）：Confidentiality（机密）、Integrity（完整）、Availability（可用）

支持CIA的其他特征：Authentication（认证）、Nonrepudiation（不可否认）、Authorization（授权）

【了解】性一般场景。

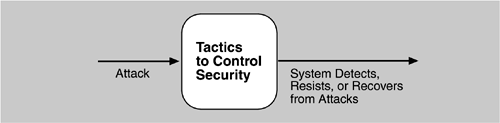
|  |  |
| --- | --- |
| **Portion of  Scenario** | **Possible Values** |
| 源 | 先前已经识别/当前未知的人或其他系统。人类攻击者可能来自组织外部/内部。 |
| 刺激 | 刺激就是攻击或试图违反安全性。未经授权的人或系统试图显示信息、改变和/或删除信息、访问系统服务或降低系统服务的可用性 |
| 制品 | 系统服务；系统内的数据；系统的一个或多个组成部分；系统生成或使用的数据 |
| 环境 | 系统在线/离线;连接到网络/从网络断开;连接有防火墙/直接连接到网络上;完全运行/部分运行/不运行 |
| 响应 | 交易以这样的方式进行   * 保护数据或服务，阻止未经授权的访问 * 未经授权不得操作数据或服务 * 用户需要通过认证 * 用户不能否认参与了交易 * 数据，资源和系统服务可供合法使用   系统跟踪活动   * 记录访问或修改 * 记录尝试访问数据，资源或服务的行为 * 有明显攻击行为时通知相应的实体（人员或系统） |
| 相应度量 | 以下一项或多项：   * 当特定组件或数据受到损害时，系统会收到多大程度的危害 * 在检测到攻击之前经历了多长时间 * 抵挡了多少攻击 * 从攻击中恢复中需要多长时间 * 有多少数据容易收到特定攻击 |

Example: 来自远端的心怀不轨的员工试图在正常操作期间修改报表，系统维护审计追踪，并在一天内恢复正确的数据。

【掌握】安全性战术

目标：考虑安全性的一种方法是考虑物理安全性。

这引出了四种策略：检测（detect），抵抗（resist），反击（react）和恢复（recover）。



**安全性战术：**



1. Detect Attacks 检测攻击

* 检测入侵
* 检测拒绝的服务
* 验证邮件完整性
* 检测消息延迟

1. 抵挡攻击Resist Attacks

* 识别参与者：识别系统一切外部输入的来源
* 验证参与者：确保参与者（用户或远程计算机）实际上是谁
* 授权参与者：确保通过身份验证的参与者有权访问和修改数据或服务
* 限制访问：限制对内存，网络连接或访问点等资源的访问。
* 限制曝光：通过尽可能少的接入点来使系统的攻击面到达最小
* 加密数据：对数据和通信应用进行某种形式的加密。
* 单独实体：可以通过连接到不同网络的不同服务器上的物理分离，虚拟机的使用或用“air gap”来实现
* 更改默认设置：强制用户更改默认分配的设置

1. React to Attacks 进行反击

* 撤消访问：限制对敏感资源的访问。即使是合法用户和使用，对于有攻击嫌疑的行为也要限制。
* 锁定计算机：如果重复尝试访问资源失败，则限制对资源的访问。
* 通知参与者：在怀疑或检测到攻击时通知操作员，其他人员或协作系统。

1. Recover From Attacks 从攻击中恢复

除了恢复失败资源的可用性策略之外，还有Audit（审计）。

Audit：记录用户和系统操作及其影响，以帮助跟踪攻击者的操作并识别他们。

【掌握】安全性设计清单

* 采用合适的架构模式和策略。
* 建立安全模型/公式。
* 条例Regulations
* 协议/算法
* 确定哪些系统职责需要安全。 确保它们已被分配：

识别，验证和授权参与者

授予或拒绝访问数据或服务

记录尝试访问或修改数据或服务

加密数据

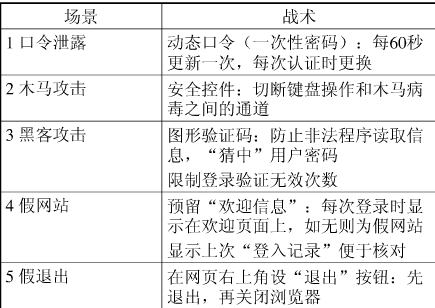
识别DOS攻击

从攻击中恢复

验证校验和（checksums）和哈希值

Study case(随便看看):

银行信息系统的安全策略



移动支付可靠吗？缺乏有力认证手段