

# 第7章 网络安全介绍

- ❖ 为什么网络安全是必需的
- ❖ 定义安全的网络设计
- ❖ 对网络安全威胁进行分类
- ❖ 网络安全是怎样被破坏的
- ❖ 网络安全策略和安全轮图

# 为什么网络安全是必需的

- ❖ Internet是由成千上万的网络所组成，任何机构的网络都能被从世界上的任何一台计算机访问
- ❖ 计算机安全协会（CSI）最近的调查中显示，70%的被调查机构表示，他们的网络安全防卫系统曾经被破坏过，而且60%的事故来源于机构内部
- ❖ 由安全问题造成的损失是巨大的

# 定义安全的网络设计

- ❖ 当访问互联网络环境中的信息时，必须创建安全区域。用来分离这些区域的设备被称为防火墙。如图1-1。
- ❖ 由防火墙创建的三个区域：
  - 1.内部区域——互联网络的信任区域
  - 2.外部区域——互联网络中不被信任的区域
  - 3.停火区（DMZ）——一个或多个隔离的网络，它对于外部网络通常是可以访问的。

## 防火墙的基本职责：

- ❖ 不允许外部设备访问内部网络
- ❖ 允许外部设备有限度地访问停火区
- ❖ 允许内部设备访问外部网络
- ❖ 允许内部设备有限度地访问停火区

当然，在许多网络设计中可能会对这些规则的部分或全部内容存在例外的情况

# 网络安全威胁分类

- ❖ 无组织的威胁——这些威胁主要来自于没有经验的个人，他们采用从Internet上下载的简单易用的黑客工具。
- ❖ 有组织的威胁——发起这类威胁的人比脚本小子有着更深的动机和技术能力。
- ❖ 外部威胁——这类威胁来源于您的机构之外的个人或组织，他们没有获得访问您的计算机系统或网络的授权。
- ❖ 内部威胁——发起这类威胁的个人已经获得了访问网络的权利。



# 网络安全是如何被破坏的

网络攻击有三种类型：

- ❖ 侦查攻击——入侵者试图发现并定位系统、服务和弱点。
- ❖ 访问攻击——入侵者攻击网络或系统来提取数据、获取访问权限、或提升他们的个人访问权限。
- ❖ 拒绝服务攻击——入侵者使您的计算机系统遭到破坏或瘫痪，或拒绝您和其他授权用户访问您自己的网络、系统和服务。

# 网络安全策略和安全轮图

- ❖ 安全策略是对安全规则的正式声明，有权限访问一个公司的技术和信息资源的人必须遵守这些规则。
- ❖ 安全策略需要完成任务：
  - 1.明确公司需要达到的安全目标；
  - 2.用文档记录需要被保护的资源；
  - 3.通过当前的网络图和清单，识别网络基础设施。

安全策略是轴心，安全轮图(见图1-2)的四个步骤正式围绕它建立的：

❖ 步骤1：保证系统安全。实现对设备和/或系统的安全防护，目的是防止对网络系统的非授权访问：

a> “身份认证系统”，比如一次口令，允许经过认证和授权的用户进行访问；



- b> “加密”可以对数据流进行隐蔽；
- c> “防火墙”可以允许或拒绝特定的数据流，从而只允许合法的数据流和服务；
- d> “给漏洞打补丁”是指采用一些修复手段或措施来防止攻击者利用已知的漏洞；
- e> “物理安全”是非常重要的，但是在保护系统安全中经常被忽略。

- ❖ 步骤2：监视网络，防止对公司安全策略的违背行为和攻击。
- ❖ 步骤3：测试当前所采用的安全防卫措施的有效性。
- ❖ 步骤4：不断地完善公司的安全策略。收集并分析来自监视和测试阶段的信息，不断进行安全改进。

# 小结

- ❖ 计算机和网络在很多方面已经融入到我们的日常生活中。当我们使用网络进行工作的时候，理解数据流和安全是必要的。当需要考虑安全问题时，就必须拓宽我们自己的知识面。网络设计、所采用的应用程序、数据流和对安全威胁的理解，都是网络工作者应该了解的一些课题。

# 本章小结

- ❖ 当需要向一个不被信任的网络环境发送数据或接受数据时，防火墙应该是我们的安全解决方案的核心部分。