Chapter 1

概论

1 信息系统的脆弱性主要体现在以下几个方面：

1. 物理因素，物理设备的自然、人为破坏。
2. 网络因素，信息系统软件复杂度越来越高。
3. 系统因素，信息系统软件复杂度越来越高
4. 应用因素，不正确的操作和人为的蓄意破坏。
5. 管理因素，管理制度、法律不健全。

2 信息安全的目标： 对网络中的硬件、软件和系统中的数据进行保护，不受偶然或者恶意的因素影响而遭到破坏、更改、泄漏，使系统能稳定可靠正常地运行，使信息服务不中断。

3 信息安全关注的几点问题:

1. 密码理论与技术
2. 安全协议理论与技术
3. 安全体系结理论与技术
4. 信息对抗理论与技术
5. 网络安全与安全产品

4 互联网络的特点:

1. 无中心网，再生能力强
2. 可实现移动通信、多媒体通信等多种服务
3. 互联网一般分为外部网和内部网
4. 互联网的用户主体是个人

5 P2DR 模型

- Policy 安全策略
- Protection 防护
- Detection 检测
- Response 响应

6 PDRR 模型

- Protection 防护
- Detection 检测
- Response 响应
- Recovery 恢复

7 ISO 开方系统互联安全体系的五类安全服务

1. 鉴别服务
2. 访问控制服务
3. 数据机密性服务
4. 数据完整性服务
5. 抵抗性

Chapter 2

防火墙

1 什么是防火墙 防火墙是一种协助确保信息安全的设施，**依照特定的规则**，允许或是禁止传输的数据通过。

2 防火墙放置位置 位于信任内部网络和不可信任的外界网络之间，如网关, 防火墙主机上的一些特定的应用程序。

3 防火墙的特性

1. 内部网络和外部网络之间的所有网络数据都必须经过防火墙
2. 只有符合安全策略的数据流才能通过防火墙
3. 防火墙自身应具有非常强的抗攻击免疫力

4 防火墙的功能

1. 防火墙是网络安全的屏障
2. 防火墙可以强化网络安全策略
3. 防火墙可以对网络存取和访问进行监控审计
4. 防火墙可以防范内部消息的外泄

5 防火墙网络层的性质指标

1. 吞吐量指标
2. 时延指标
3. 丢包率指标
4. 背靠背缓冲指标

6 防火墙常见的功能指标

1. 服务平台支持
2. LAN 口支持
3. 协议支持
4. VPN 支持
5. ...

7 防火墙核心技术

1. 包过滤技术, 在**网络层**截获网络数据包，根据防火墙的规则表，来检测攻击行为，在网络层提供较低级别的安全防护和控制
2. 应用网关技术, 又被成为代理技术，位于应用层上，所以主要采用协议代理服务。应用代理防火墙壁分组过滤防火墙提供更高层次的安全性，但这丧失对应用程序的透明性。
3. 状态检测技术，采用一种基于连接的状态监测机制，将属于同一连接的所有包作为一个整体的数据流看待，构成连接状态表，通过规则表与状态的共同配置，对表中的各个连接状态因素加以识别。**是一种动态的判定方法**。**（前两种为静态）**Steps:
   - 检查是否属于一个已建立的连接
   - 若已建立，则根据连接状态表的策略对数据包实施丢弃、拒绝或是转发。
   - 若未建立连接，会检查数据包是否与他配置的规则集匹配。

8 防火墙分类

1. 个人防火墙
2. 分布式防火墙
3. 分层式防火墙

9 防火墙的体系结构, 部署位置

基本概念:

1. 堡垒主机，一种被强化的可以防御攻击的计算机，作为进入内部网络的一个检查点。堡垒主机是网络中**最容易受到侵害**的主机。**包过滤路由器和应用代理服务器均可视为堡垒主机**。
2. 非军事区，也成为“隔离区”，他是为了解决安装防火墙后，外部网络不能访问内部网络服务器的问题，而设立的一个非安全系统与安全系统之间的缓冲区。

体系结构分类:

1. 筛选路由器体系结构。
2. 单宿主堡垒主机，由包过滤路由器和堡垒主机构成。外部路由器配置把所有进来的数据发送到堡垒主机上，所有出去的数据包也经过堡垒主机（代理）。实现了网络层安全（包过滤）和应用层安全（代理服务）。缺点: 可通过重新配置路由器，使数据绕过堡垒主机。
3. 双宿主堡垒主机，与单宿主堡垒主机的区别在于，双宿主堡垒主机有两块网卡，一块连接内部网络，一块连接包过滤路由器，但是主机两个端口之间直接转发信息的功能被关闭。在应用层提供代理服务
4. 屏蔽子网体系结构：由两个包过滤路由器和一个堡垒主机构成，支持网络层和应用层的安全功能。在定义非军事区 (DMZ)，即屏蔽子网后。存在内部防火墙和外部防火墙。攻击者要通过外部防火墙，堡垒主机和内部防火墙三道防线，才能到达内部网络。

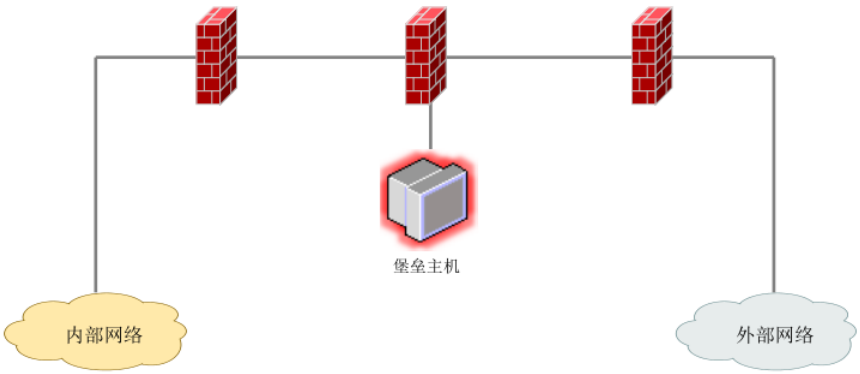

Figure 2.1:

10 常见产品

1. Firewall
2. PIX
3. AXENT Raptor
4. NetScreen
5. 天融信网络卫士
6. 东软 NetEye 4032 防火墙