[toc]

共享网络和交换网络

- 共享式网络
    - 通过网络的所有数据包发往每一个主机
    - 最常见的是通过HUB连接起来的子网
- 交换式网络
    - 通过交换机连接网络
    - 由交换机构造一个MAC地址-端口映射表
    - 发送包的时候只发到特定的端口上

> ==如何监听？==
>
> - 端口镜像
> - arp欺骗

交换技术

- 二层交换技术
- 三层交换技术
    - 二层交换 + 三层转发
- 四层交换技术

> - 包过滤
> - 服务质量(QOS)
> - 服务器负载均衡
> - 主机备用连接
> - 统计

负载均衡

- 路由模式
- 桥接模式

> ==路由和桥接的区别==

- 服务直接返回模式
    - 应答的数据包不再经过负载均衡设备
    - 适合数据量大的服务

网络监听

- 如何防范

    - 加密
    - 确保以太网的整体安全性
- 检测手段
    - 反应时间
    - DNS测试
    - 利用ping
    - 利用arp数据包

检测处于混杂模式的节点

- 检测手段
    - 根据操作系统的特征
    - 根据网络和主机的性能

口令破解

- 攻击类型
    - 字典攻击
    - 暴力攻击
    - 组合攻击
- 口令破解器
- 注册码

拒绝服务攻击概述

- DoS(Denial of Service)
    - 阻止或拒绝合法使用者存取网络服务器的一种破坏性攻击方式
- 实现方式
    - 资源消耗
    - 服务中止
    - 物理破坏