网络监听及防御技术

- 共享式局域网监听
  - 基础知识
    - 使用集线器，公用一条总线，采用载波检测多路监听（CSMA/CD）机制进行传输控制
    - 集线器是一层设备只转发比特流，所以不知道哪一个端口转发到哪一个端口，所以传输信息的方式是广播
  - 监听原理
    - 正常网卡只响应
      - 与自己MAC地址匹配的数据帧
      - 全为F的广播帧
    - 混杂模式的网卡接受所有数据帧，被送到网络层
  - 实现方法
    - 链路层过滤
      - MAC地址
    - 网络层过滤
      - IP地址
    - 传输层
      - 判断本机端口是否打开
  - 过滤类型
    - 信息的过滤
      - 站过滤
      - 协议过滤
      - 服务过滤
      - 通用过滤
    - 时间的过滤
      - 捕获前过滤
      - 捕获后过滤
  - 相关库
    - Unix 的 Libpcap
    - Windows 的 Winpcap
- 工具
  - Wireshark
- 嗅探软件工作机制
  - 驱动程序支持
    - 网卡的混杂模式
  - 分组捕获过滤机制
    - 链路层网卡驱动程序上传数据帧有俩个去处
      - 正常协议栈
        - 非本地数据包丢弃
      - 分组过滤模块
        - 非本地数据包，由分组过滤模块决定丢弃还是上传
    - 类型
      - Unix
        - BSD 的 BPF（Berkeley Packet Filter）
        - SVR4 的 DLPI（Data Link Interface）
      - Linux
        - SOCK_PACKET
      - Windows
        - NPF
- 网卡的工作模式
  - 广播模式
    - 能接受网络中的广播信息
  - 组播模式
    - 能接受组播数据
  - 直接模式
    - 只匹配目的MAC地址的网卡才接受数据
  - 混杂模式
    - 能接受一切数据
- 硬件设备
  - 集线器
    - 物理层设备，目的就是端口扩展，带宽不变。
    - IEEE 802.3协议，随机选出某一端口的设备，让它占用全部带宽，与集线器的上联设备通信，本身不具备任何转发能力
  - 交换机
    - 数据链路层设备，简单的转发数据帧，基于MAC地址，具有流量控制能力
    - 每一个端口就是一个冲突域，独立的带宽。
- 监听的防御
  - 通用策略
    - 安全的网络拓扑结构
      - 网络分段
      - 划分VLAN
    - 数据加密技术
      - 数据通道加密
        - SSH
        - SSL
        - VPN
      - 数据内容加密
        - PGP
  - 共享网络下的防监听
    - 检测技术
      - 网络和主机响应时间测试
        - 原理
          - 混杂模式下的机器缺乏底层过滤机制，骤然增加目标地址不是本地的网络通讯流量会对该机器造成明显的影响。
        - 过程
          - 利用 ICMP Echo 请求及响应计算出需要检测机制的响应时间基准和平均值
          - 在得到这个数据后，立即向本地网络发送大量伪造数据包，与此同时再次发送测试数据包，以确定平均响应时间的变化值
          - 非监听的机器的响应时间变化量会很小，而监听的通常会有1~4个数量级的变化
      - ARP检测
        - 原理
          - 混杂模式下的网卡，对于ARP请求报文，照单全收，会做出响应，而正常的不匹配是不会收的。
        - 过程
          - 伪造ARP报文，发送到各个节点，有回应的通常运行着嗅探程序。
    - 帮助判断
      - 检测处于混杂模式的网卡
      - 网络通讯丢包率高
      - 网络带宽反常
  - 交换网络下的防监听
    - 不要把网络安全信任关系建立在单一的IP和MAC基础上，理想关系应该建立在IP-MAC对应关系的基础上。
    - 使用静态的ARP或者IP-MAC对应表代替动态的ARP或者IP-MAC对应表，禁止自动根更新，使用手动更新
    - 定期检查ARP请求，使用ARP监视工具，列入ARPWatch等监视并探测ARP欺骗
    - 制定良好的安全管理策略，加强用户安全意识
- 网络监听
  - 又名网络嗅探，在对方未察觉的情况下捕获其通信报文或通信内容技术
  - 双刃剑
    - 网络管理员可以很好的了解网络运行状况
    - 黑客可以有效收集信息的手段
  - 类型
    - 软件嗅探器
      - 易于使用
      - 功能有限，无法抓取网络上所有数据
      - 效率不高
    - 硬件嗅探器（协议分析仪）
      - 昂贵
- 网络传输技术
  - 广播式
    - 仅一条通信信道，由网络上的所有主机共享，信道上传输的分组可以被任何机器发送并被其他所有机器接受。
  - 点对点
    - 由一对，一对机器之间的多条连接构成，分组的传输是通过这些连接直接发往目标机器，因此不存在发送分组被多方接受的问题
- 交换式局域网监听
  - 定义与特点
    - 由交换机或者其他非广播式交换设备组件成的局域网
    - 根据MAC地址，转发到交换机的某个端口。
    - 端口间的帧传输彼此屏蔽，因此节点不担心自己发送的帧被发送到非目的节点中去。
  - 产生的原因
    - 预防嗅探器的入侵
    - 数据链路层维护了一个MAC与端口的映射表
  - 攻击方式
    - 溢出攻击
      - 交换机MAC地址表的溢出，回退到HUB的广播模式，向所有端口发送数据包，这样就可以实现监听了。
    - ARP欺骗
      - 计算机中维护了一个IP-MAC地址表。通过ARP报文，修改其内容，成为被攻击者和交换机之间的中间人，这样就可以收到所有的数据了。