8. 攻击和对策

8.1 IDS:入侵检测系统

分组过滤:
- 对TCP/IP头部进行检查
- 不检查会话间的相关性

IDS: intrusion detection system
- 深入分组检查: 检查分组的内容 (e.g., 检查分组中的特征串 已知攻击数据库的病毒和攻击串
- 检查分组间的相关性，判断是否是有害的分组
  - 端口扫描
  - 网络映射
  - DoS 攻击

multiple IDSs: 在不同的地点进行不同类型的检查

8.2 Internet 安全威胁与对策

映射:
- 在攻击之前: “踩点” – 发现在网络上实现了哪些服务
- 使用ping来判断哪些主机在网络上有地址
- 端口扫描：试图顺序地在每一个端口上建立TCP连接 (看看发生了什么)
- nmap (http://www.insecure.org/nmap/) mapper:“network exploration and security auditing”

对策:
- 记录进入到网络中的通信流量
- 发现可疑的行为 (IP addresses, 端口被依次扫描)

分组嗅探:
- 广播式介质
- 混杂模式的NIC获取所有的信道上的分组
- 可获取所有未加密的数据 (e.g. passwords)
- e.g.: C 嗅探B的分组

对策:
- 机构中的所有主机都运行能够监测软件，周期性地检查是否有 网卡运行于混杂模式
- 每一个主机一个独立的网段 (交换式以太网而不是使用集线器)

IP Spoofing欺骗:
- 可以有应用进程直接产生 “raw” IP分组, 而且可以在IP源地址部分直接放置任何地址
- 接收端无法判断源地址是不是具有欺骗性的
- e.g. C 伪装成B

对策：入口过滤
- 路由器对那些具有非法源地址的分组不进行转发(e.g., 数据报的源地址不是路由器所在的网络地址)
- 很好，但是入口过滤不能够在全网范围内安装

Denial of service (DOS):
- 产生的大量分组淹没了接收端
- Distributed DOS (DDOS): 多个相互协作的源站淹没了接收端
- e.g., C 以及远程的主机SYN-attack A

对策:
- 在到达主机之前过滤掉这些泛洪的分组 (e.g., SYN): throw out good with bad
- 回溯到源主机(most likely an innocent, compromised machine)

总结：
    基本原理
        加密 (对称和公开)
        报文完整性
        端节点的认证（鉴别）
    在多种安全场景中使用
        安全电子邮件
        安全传输层 (SSL)
        IP sec
        802.11
    运行中的安全性: firewalls and IDS