欺骗攻击及防御技术

计算机之间相互进行交流建立在两个前提之下

- 认证
  - 相互之间进行识别的一种鉴别过程，经过认证的过程，相互交流的计算机间会建立起相互信任的关系
- 信任
  - 信任和认证具有逆反关系，如果相互高度信任，那么交流就不会要求严格的验证，假如相互不信任，他们之间就会进行严格验证

欺骗

- 冒充身份通过认证骗取信任的攻击方式

ARP

- 定义
  - 将IP转化为MAC，链路层协议
- 包类型
  - 请求包
  - 应答包
- 基础知识
  - 在局域网（冲突域）中，数据帧是根据MAC寻址的
  - 内核必须知道目的端的硬件地址才能发送数据
- 缓存表
  - 每台主机、网关都有一个ARP缓存表
  - 类型
    - 动态
    - 静态
  - 命令
    - arp -a
    - 查看本机缓存表
- ARP协议请求过程
  - 局域网内通信
    - 192.168.1.2请求一个IP地址192.168.1.1
    - 查看本机ARP缓存表，有就直接发送
    - ARP缓存表中没有，广播ARP请求包，询问192.168.1.1的MAC地址，存入ARP缓存表中，发送包
  - 局域网间通信
    - 通常是不同网段的，首先检查ARP缓存表，假如没有，那么就直接丢给网关，由网关去决定，转发到路由器，或者是其他网段
- ARP欺骗原理
  - 利用ARP协议本身的缺陷进行的一种非法攻击
  - 容易被病毒、木马或者具有特殊目的的攻击者使用
  - 主机在接受到ARP应答报文时，不去确定是不是自己发送的，就直接替换到ARP缓存表中
- ARP欺骗危害
  - 同网段用户容易断网
  - 泄露敏感信息
  - 对信息进行篡改
  - 起到网管作用，让某特定用户不能上网
- 检测ARP欺骗攻击
  - 网络频繁掉线
  - 网速突然变慢
  - 使用arp -a命令发现网关的MAC地址与真实的网关MAC地址不同
  - 使用嗅探软件，发现有大量的ARP Reply包
- ARP欺骗的防护
  - MAC地址绑定
  - 静态ARP缓存表
  - 使用ARP服务器
  - 使用ARP防火墙
  - 及时发现正在进行ARP欺骗的主机，对其隔离

Web

- 又称中间人攻击
- 原理
  - 伪造站点，收集用户输入的数据，对数据进行相应的危害操作
- 流程
  - 改写web页面所有URL地址，使其指向自己伪造的Web页面
- 案例
  - 网络钓鱼
  - 伪造银行页面，收集用户账户密码，进行转账
- 防御
  - 习惯查看URL
  - 检查源代码，如果发生了URL重定向
  - 使用反钓鱼软件
  - 禁用脚本JavaScript，ActiveX
  - 确保应用有效和能适当的跟踪用户
  - 培养用户的安全意识

电子邮件

- 目的
  - 隐藏自己身份
  - 冒充别人
  - 社会工程的表现形式
- 组成部分
  - 用户代理
  - 传输代理
  - 投递代理
- 欺骗原理
  - 利用相似的电子邮件地址
  - 直接使用伪造的E-mail地址
  - 远程登录到SMTP端口发送邮件
- 欺骗防御
  - 邮件接收者
    - 配置邮件客户端，每次都能显示完整的电子邮件地址，而不只是别名
  - 邮件发送者
    - 保护好邮件客户端
  - 邮件服务器
    - 采用SMTP
  - 邮件加密
    - PGP

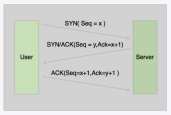
IP

基本的IP欺骗

- 简单的IP地址变化
  - 将自己的IP修改为别人的IP，伪造报文发给目的主机，由于IP是别人的，所以自己是收不到响应的，所以也称盲目飞行攻击
  - 无法建立完整的TCP，但可以使用UDP
- 源路由攻击
  - 源路由类型
    - 宽松的源站选择（LSR）
    - 严格的源站选择（SRS）
  - 攻击的类型
    - 插入到数据流的必经之路上
    - 保证数据包会经过一条给定的路线，而且作为一次欺骗，保证它经过攻击者的机器
  - 实现的基础
    - 源路由机制在TCP/IP协议组中，它允许用户在IP数据包包头的源路由选项字段设定接收方返回的数据包要经过的路径
    - 某些路由器对源路由包的反应是使用其中指定的路由，并使用其反向路由来传送应答数据，这就使一个入侵者可以假冒一个主机的名义通过一个特殊的路径来获取某些被保护的数据
- 利用Unix系统的信任关系
  - 基于IP地址信任的，而不是询问用户名和口令

TCP会话挟持

- 简介
  - 接管一个现存动态会话的过程，换句话说，攻击者通过会话挟持可以替代原来的合法用户，同时能够监视并掌握会话内容。此时，攻击者可以对受害者的回复进行记录，并在接下来的时间里对其进行响应，展开进一步的欺骗和攻击
- 结合了嗅探和欺骗技术



- 相关基础
  - TCP三次握手
  - 序列号机制
    - 32位计数器
    - 说明接收方下一步将要接收数据包的顺序
- 过程
  - 期望这个目标是一个被允许的TCP会话连接，检测数据列也是比较重要的问题，因为要猜测序列号，这就是嗅探之前通信的数据包，可能还需要ARP欺骗。
  - 发现攻击目标
    - 确认动态会话
      - 网络流通量越大，越不容易被发现
    - 猜测序列号
      - TCP区分正确的数据包和错误的数据包仅通过它们的SEQ/ACK序列号
      - 扰乱客户主机的SEQ/ACK，让服务器不信任客户机，从而伪装客户主机，使用正确的SEQ/ACK进行通信
    - 让客户机下线
      - DOS拒绝服务攻击
    - 接管会话
      - 通过发送数据建立一个账户，这样就可以进入系统

IP欺骗攻击的防御

- 防御地址变化欺骗
  - 限制用户修改网络配置
  - 出入口过滤
- 防范信任关系欺骗
  - 限制拥有信任关系的人员
  - 不允许通过外部网络使用信任关系
- 防范会话挟持
  - 进行加密
  - 使用安全协议
  - 限制保护措施

DNS

基本知识

- 域名解析，主机名字和IP地址转换
- DNS服务器里面有一个DNS缓存表
- 基于UDP使用53端口

解析过程

- 用户访问www.baidu.com
- 请求DNS服务器，假如本机设定的那个DNS服务器缓存表上有，就直接返回
- 如果没有就由该DNS服务器继续向上一级DNS服务器请求

欺骗实现

- 可以控制本地的域名服务器
  - 控制本地的域名服务器，在数据库中增加一个附加记录，例如example.com，将攻击目标的域名，指向攻击者的欺骗IP
  - 紧接着，攻击者向本机设定的DNS服务器（home.com）请求解析example.com，这时候，home.com的DNS服务器就会去问example.com的DNS服务器，请求得到后，刷新缓存替换成为攻击者修改过的地址
- 无法控制本地的域名服务器
  - 要点
    - 首先，黑客要冒充某个域名服务器的IP地址
    - 黑客要能预测目标域名服务器所发送DNS数据包的ID号（关键）
    - 在一段时间内，DNS服务器一般都采用一种可循的ID生成机制
  - 过程
    - 可以控制远端DNS服务器网段的某主机
      - 他只要在远程的DNS服务器网段上发送一个队攻击者本地域名的解析请求，通过嗅探得到数据包。（远程的DNS服务器转而请求本地的DNS服务器，从而拿到ID号）
    - 不可以控制远端DNS服务器网段的某主机
      - 向目标DNS服务器，请求某个不存在的域名地址进行解析
      - 攻击者冒充所请求的DNS服务器，向目标DNS服务器连续发送应答包，这些包中的ID号依次递增
      - 过一段时间，攻击者再次向目标DNS服务器发送针对该域名的解析请求，如果得到返回结果，就说明目标DNS的服务器接受了黑客的伪造应答。继而说明黑客猜测的ID在正确的区段中。否则可以继续尝试。
      - 假如拿到的ID号为666
      - 由攻击者本地主机发起，让远端DNS服务器，去请求其他的DNS服务器，假如请求www.baidu.com的DNS服务器
      - 此时攻击者，对远端的服务器，发送ID666www.baidu.com=1.1.1.1 ID667www.baidu.com=1.1.1.1 _应答包
      - 此时接收到的IP地址将会是1.1.1.1
  - 局限
    - DNS服务器存在缓存刷新时间问题
    - 不能替换缓存表已存在的记录

欺骗防御

- 使用最新版的DNS服务器软件
- 关闭DNS服务器的递归功能
- 限制区域传输范围
- 限制动态更新
- 采用分层的DNS体系结构