第2章黑客常用的系统攻击方法

黑客

- 黑客类型 P31
  - 白帽黑客
  - 黑帽黑客
  - 脚本小子
  - 黑客活动家
  - 国家支持的黑客
  - 间谍黑客
  - 网络恐怖分子
- 黑客攻击入侵的过程P32
  1. 收集被攻击方的有关信息，分析被攻击方可能存在的漏洞。（收集信息）
  2. 建立模拟环境，进行模拟攻击，测试对方可能的反应。（模拟攻击）
  3. 利用适当的工具进行扫描。（目标扫描）
  4. 实施攻击（实施攻击）
- 入侵常用工具介绍P33
  - 扫描器：自动检测远程或本地主机安全性弱点的程序
  - 口令入侵：口令字典
  - 特洛伊木马
  - 网络嗅探器：获取的流量进行数据分析
  - 破坏装置：邮寄炸弹和病毒等

目标系统探测

- 常用网络探测方法P35
  - 基于ARP的端口入侵的检测
  - 基于安全日志的检测
  - 文件访问日志与关键文件保护
  - 进程监控
  - 注册表检验
  - 端口监控
  - 陷阱技术
- 网络扫描器P38
  - 定义P38
    - 网络安全扫描器是一种自动检测远程和本地主机安全性弱点的程序包
    - 扫描器大多采用客户端/服务器核心架构
  - 功能P38
    - 它通过与目标主机TCP/IP端口建立连接并请求某些服务（如TELNET、FTP等）获目标主机的应答，搜集目标主机相关信息（如匿名用户是否可以登陆服务从而发现目标主机某些内容的安全弱点。
  - 技术分类
    - 依查扫描P38
      - 定义
      - 目的
      - 常用扫描方法
    - 端口扫描P39
      - 定义
      - TCP端口扫描的四种方式
- 专用扫描器P40

口令攻击

- 攻击的三种方式P42
  1. 通过网络监听非法得到用户口令
  2. 在知道用户的账号后利用一些专门软件强行用户口令破解
  3. 利用系统管理员的失误
- 口令破解
  - 获得口令思路
    - 穷举尝试
    - 找到存放口令的文件并破解
    - 其它途径（网络嗅探、键盘记录器等）
  - 口令破解方式
    - 手工破解
    - 自动破解
- 口令攻击类型P43
  - 词典攻击
  - 强行攻击
    - 暴力破解（强行攻击），分布式暴力破解
  - 组合攻击
  - 其它攻击类型
    - 社会工程学
    - 偷窥
    - 搜索垃圾箱
    - 口令嗅探
      - 它通过个名为sniff.exe的可执行程序，实施发包进行网络感应操作
      - 默认它们的国内服务器被感染并自动与境外服务器进行连接
      - 利用的是网上用户对口令管理的弱点进行攻击。
      - 特点
        - 自带一些口令字典，对网上主机超级用户口令进行基于字典的猜测
        - 一旦破测口令成功，该程序植入7个与远程控制实现有关的程序，记录主动向国外的几个特定服务器联系，并可被远程控制
        - 可以实现大规模的自动化口令攻击，扫描流量很大，容易造成网络严重拥塞
    - 特洛伊木马
    - 重放

网络监听

- 定义P44
  - 也叫嗅探器、Sniffer,用网络上传输的数据编辑并进行分析的行为
- 使用范围P44
  - 只能用于连接同一网段的主机。常用获取用户密码
- 目的
  - 截获通信内容
- 手段
  - 对协议进行分析
- 工作原理
  - 以太网数据是以广播方式发送的，即将城网内的每台主机都在监听网内传输数据
  - 以太网硬件将监听到的数据帧所包含的MAC地址与自己的MAC地址相比较，如果相同，则接收该帧，否则丢掉它，这就是以太网的过滤规则。
  - 如果把网卡设置为“混杂模式”，它就能接收传输在网络上的每一个信息包。然后对数据包进行分析，获得到了网络中通信的数据。Sniffer就是抓这种数据来监测网络中流动着的数据。
- 用途
  - 把网络中的数据流转化成可读格式。（数据包转换为文件）
  - 进行性能分析以发现网络瓶颈。
  - 进行入侵检测以发现外界入侵者。
  - 生成网络活动日志和安全审计。
  - 进行故障分析以发现网络中潜在的问题。
- 意义（双刃剑）
  - 监视网络，快速进行网络故障定位
  - 口令失窃，敏感数据被截获
- 数据库安全审计技术P46
  - 日志审计技术
  - 代理审计技术
  - 网络监听审计技术
  - 网关审计技术

木马

- 定义
  - 是一种通过各种方法直接或者间接与远程计算机之间建立起连接，
  - 使远程计算机能够通过网络的制本地计算机的程序
  - 是具有伪装能力、隐蔽执行非法功能的恶意程序
- 组成P49
  - 通常有两个可行程序
    - 客户端，控控制端
    - 服务端，即被控制端一植入对方计算机程序为.exe
- 主要特点P53
  - 隐蔽性好
  - 通常只改写几个、几十个注册表加载点
  - 通常不感染系统文件
  - 通常不具备主动传播性
  - 利用网页挂马、木马下载器，欺骗下载等方式传播
  - 删除木马文件即可简单清除。
- 分类P50
  - 按照应用类型分为六类P50
    - 网络游戏类木马
    - 网银木马
    - 即时通讯软件木马
      - 发送消息型
      - 盗号型
      - 传播自身型
    - 网页点击类木马
    - 下载类木马
    - 代理类木马
  - 根据对计算机具体操作方式分为五类
    - 远程访问型木马：最广泛的，可以使远程控制者在本地机器上做任何事情，著名的BO，国产的冰河
    - 密码发送型木马：目的是找到所有的隐藏密码，在系统里自动使用25号端口发送电子邮件
    - 键盘记录型木马：非常简单，只记录登录者的键盘敲击，并在日志文件中做完整记录
    - 破坏型木马：以毁坏并且删除文件为目的，自动删除.ini和.exe文件，甚至格式化硬盘
    - FTP型木马：打开被控制计算机的21号端口，无需密码通过FTP匿名向受害人传和下载机密文件
  - 根据木马的网络连接方向分为两类
    - 正向连接型
    - 反向连接型
- 工作过程P56
  - 植入
  - 启动
  - 收集
  - 回报
- 隐藏方式P55
  - 在任务栏里隐藏
  - 在任务管理器里隐藏
  - 在端口隐藏
  - 隐蔽通信
  - 隐蔽加载方式
- 启动方式P57
  - 通过开始菜单
  - 通过Win.ini文件
  - 通过注册表启动
  - 通过Autoexec.bat文件和winstart.bat、config.sys文件
  - 通过System.ini文件
  - 通过某特定程序或文件启动
- 木马的防御P61
  - 基本防御思想：最佳胜于补救
  - 根本防御思想：防病胜于治病
  - 基本解决方法：进程服务注册表

拒绝服务攻击

- 概念P63
  - DoS--Denial of Service
- 定义P63
  - 攻击者想办法让目标机器停止提供服务，是黑客常用的攻击手段之一
- 不能合理解决的原因P63
  - 由网络协议本身的安全性缺陷造成的
- 攻击服务器实现效果P63
  - 迫使服务器的缓冲区满，不接收新的请求
  - 使用IP欺骗迫使服务器把合法用户的连接复位，影响合法用户的连接
- 目的P63
  - 让目标机器或网络无法提供正常的服务或资讯访问
  - 使目标系统服务系统停止响应甚至崩溃
- 简单的说
  - 是让攻击目标瞬痪的一种 损人不利己 的攻击手段
- 发生原因
  - 蓄意的：当未被授权的用户过量使用资源
  - 偶然的：当合法用户无意地操作而使得资源不可用时
- DoS攻击的原因P64
  - 软件的弱点
  - 错误配置
  - 重要请求导致过载
- 攻击手段P65
  - Ping of death
  - 泪滴(Tear drop)攻击
  - UDP洪水(UDP flood)
  - SYN洪水(SYN flood)
    - 四变遭受大规模SYN Flood攻击
  - Land(Land Attack)攻击
  - IP欺骗DoS攻击
- 分布式拒绝服务攻击(DDoS)
  - 定义P67
    - DDoS就是利用更多的傀儡机（肉鸡）来发起进攻，以比从前更大的规模来进攻受害者。
  - 体系结构P67图2.17
  - 攻击步骤P68
    - 搜集了解目标的情况；
    - 占领傀儡主机；
    - 实际攻击；

缓冲区溢出

- 定义P72
- 原理
  - 根本原因一C本质就是不安全的
  - 通过指针填充数据
  - 不好的编程习惯
- 类型P73
  - 栈溢出
  - 堆溢出