拒绝服务攻击与防御技术

拒绝服务攻击（DOS）

简单的破坏性攻击，通常利用传输协议的缺陷、系统存在的漏洞、服务的漏洞，对系统发动大规模的进攻，消耗系统的各种软硬件资源，造成崩溃、瘫痪、宕机等。

- 有意与无意
  - 有意：为被授权的用户过量的使用资源
  - 无意：合法用户无意的操作使资源不可用：淘宝双11抢购
- 主要原因：网络协议本身的安全缺陷引起
- 可分配服务资源
  - 网络带宽
  - 文件系统空间容量
  - 开放的进程
  - 向内的连接等
- 实现思路分类
  - 滥用合理的服务请求
  - 制造高流量无用数据
  - 利用传输协议缺陷
  - 利用服务器程序的漏洞
- 漏洞利用方式分类
  - 特定资源消耗类
  - 暴力攻击类
- 发送速率变化方式
  - 固定速率
  - 可变速率
- 按产生的影响分类
  - 系统或程序崩溃类
  - 服务降级类
- 防御
  - 难点
    - 不容易确定攻击者的位置
    - 完全阻止是不可能的，但是适当的防范工作可以减少被攻击的机会
  - 方法
    - 有效完善的设计
    - 带宽限制
    - 及时给系统安装补丁
    - 运行尽可能少的服务
    - 只运行必要的通信
    - 封锁敌意IP

分布式拒绝服务攻击

- 定义
  - 借助C/S技术，将多个计算机联合作为攻击平台，对一个或者多个目标发动DOS攻击
  - 可以分别进行不同类型的攻击
- 组成
  - 客户端：控制台，发起攻击的主机
  - 服务器端：攻击服务，客户端发来的控制命令，它来完成
  - 守护程序：攻击器、攻击代理，它直接或者间接与攻击目标进行通信
- 过程
  - 探测扫描大量主机以寻找可入侵主机
  - 入侵有安全漏洞的主机并获取控制权
  - 在每台被入侵主机中安装攻击所用的客户进程或守护进程
  - 向安装有客户进程的主控端主机发出命令，由它们来控制代理主机上的守护进程进行协同入侵
- 被攻击后现象
  - 大量等待的TCP连接
  - 大量的无用数据包，源地址为假
  - 高流量无用数据
  - 无法及时处理正常请求
  - 死机
- 工具
  - TFN2K
  - Trinoo
  - Stacheldraht
  - 其他
- 检测
  - 核心方案：异常的网络交通流量
  - 检测异常
    - 大量的DNS PTR查询请求
    - 超出网络正常工作时的极限通讯流量
    - 特大型的ICMP和UDP数据包
    - 不属于正常连接通讯的TCP和UDP数据包
    - 数据段内容只包含文字和数字字符的数据包
- 防御
  - 优化网络和路由结构
  - 保护网络及主机系统安全
  - 安装入侵检测系统
    - 类型
      - 基于网络的IDS
      - 基于主机的IDS
    - 匹配
      - 样式匹配技术
      - 不规则探测系统
  - 与ISP服务商合作
  - 使用扫描工具

实现技术

- Ping of Death
  - 早期的计算机，当ICMP包大小超过64KB的时候，会出现溢出，倒是TCP/IP协议栈的崩溃
  - 防御：利用系统审计，当大于64KB，丢弃就行
- 泪滴 （Teardrop）
  - 分片攻击
  - 当一个大的数据需要传输的时候，要分片传输，TCP头部，就会有（分片识别号、偏移量、数据长度、标志位）
    - 正常的PSH，每一段长度相同，序号紧接着
      - PSH 1:1025
      - PSH 1025:2049
      - PSH 2049:3073
    - 异常的PSH，将无法重组，使协议栈崩溃
      - PSH 1:1025
      - PSH 100:2049
      - PSH 2049:3077
  - 防御：添加系统补丁，丢弃病态的分片数据包。
- IP欺骗DOS攻击
  - 利用RST位
  - 攻击流程
    - 假如一个合法用户1.1.1.1，与服务器建立了正常连接。
    - 攻击者伪装成为1.1.1.1，向服务器发送RST
    - 服务器认为1.1.1.1发送的连接有错误，清空缓存区建立好的连接
- UDP洪水：利用主机能自动回复的服务：UDP
  - chargen
  - echo
- SYN洪水
  - 发送大量伪造的TCP连接请求，使对方资源耗尽（CPU满负荷或内存不足）
  - 当一个客户端发送一个SYN的时候，服务器会放回SYN+ACK，假如此时客户端不在线，服务器会在一定时间内一直重发。成为SYN Timeout
  - 防御方法
    - 缩短SYN Timeout时间
    - 设置SYN Cookie：每一个请求连接的IP地址分配一个Cookie，如果短时间内受到某个IP重复SYN报文，以后从这个IP来的都丢弃
    - 负反馈策略：当SYN连接数达到一定的限制后，系统自动修改SYN Timeout、清空缓存区等一些参数。
    - 退让策略：当检测到被攻击，修改自己IP地址，或者修改DNS解析IP地址
    - 分布式DNS负载均衡
    - 防火墙
- Land攻击：发送大量源地址和目标地址相同的包，造成目标解析Land包时占用大量的系统资源
- Smurf攻击
  - 利用IP欺骗和ICMP回应包引起阻塞
  - 将源地址设置为被攻击主机的地址，而将目的地址设置为广播地址
- Fraggle攻击：与Smurf类似，但是使用的是UDP应答消息
- 电子邮件炸弹：大量的发送邮件
- 畸形消息攻击：利用目标主机或者特定服务存在的安全漏洞进行攻击
- Slashdot effect：合法的情况，服务器过载：双11
- WinNuke攻击
  - 带外输出攻击：端口
    - 139
    - 138
    - 137
    - 113
    - 53
  - 原理：制造特殊的报文，其指针字段与数据的实际位置不符，存在重合。Windows在处理这样数据会崩溃
    - URG 位 设置为 1