网络安全 – 拒绝服务攻击

第4章 拒绝服务攻击

- 4.1 拒绝服务攻击概述
- 4.2 拒绝服务攻击分类
- 4.3 服务端口攻击
- 4.4 电子邮件轰炸
- 4.5 分布式拒绝服务攻击DDoS

反弹技术

拒绝服务攻击概述

- DoS定义
  - 拒绝服务攻击DoS（Denial of Service）是阻止或拒绝合法使用者存取网络服务器的一种破坏性攻击方式

这种攻击往往是针对TCP／IP协议中的某个弱点，或者系统存在的某些漏洞，对目标系统发起的大规模进攻使服务器充斥大量要求回复的信息，消耗网络带宽或系统资源，导致目标网络或系统不胜负荷以至于瘫痪而无法向合法的用户提供正常的服务

拒绝服务攻击概述

- 从某种程度上可以说，**DoS**攻击永远不会消失。
- 而且从技术上，目前还没有根本的解决办法。

拒绝服务攻击概述

- DoS攻击思想及方法
  - 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。这也即是DoS攻击实施的基本思想
- DoS攻击的实现方式
  - 资源消耗、服务中止、物理破坏等

拒绝服务攻击分类

- 攻击模式
  - 消耗资源
    - 网络带宽、存储空间、 CPU时间等
  - 破坏或改变配置信息
  - 物理破坏或者改变网络部件
  - 利用服务程序中的处理错误使服务失效
- 发起方式
  - 传统的拒绝服务攻击
  - 分布式拒绝服务攻击（Distributed Denial of Service ）

拒绝服务攻击分类

- 攻击模式
  - 消耗资源
    - 针对网络连接的拒绝服务攻击
      - ping 、flooding、SYN flooding
      - ping、finger广播包
      - 广播风暴（SMURF攻击）
    - 消耗磁盘空间
      - Email
      - ERROR-LOG
      - FTP站点的incoming目录
      - 制造垃圾文件

拒绝服务攻击分类

- 攻击模式
  - 消耗资源
    - 消耗CPU资源和内存资源

```
main()
{
        Fork();
        main();
}
```

拒绝服务攻击分类

- 攻击模式
  - 破坏或更改配置信息
    - 修改服务用户群(deny)
    - 删除口令文件

拒绝服务攻击分类

- 攻击模式
  - 物理破坏或改变网络部件
    - 计算机、路由器、网络配线室、网络主干段、电源、冷却设备、其它的网络关键设备
  - 利用服务程序中的处理错误使服务失效
    - LAND

拒绝服务攻击分类

- 攻击模式
  - 拒绝服务攻击分析
  - 加强管理
    - 机房管理
    - 设备分离
    - 定时检查各种配置
    - 定时检查关键资源的使用情况
    - 定时检查升级包

服务端口攻击

- SYN Flooding
- Smurf攻击
- 利用处理程序错误的拒绝服务攻击

4.3 服务端口攻击

- SYN Flooding

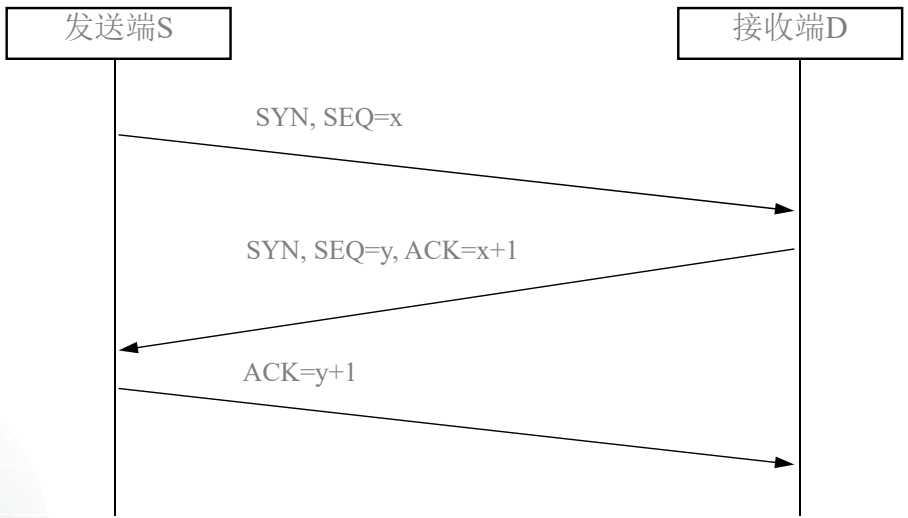


图4-1 TCP连接的三次握手

服务端口攻击

- SYN Flooding

```
192.168.0.210 -> 192.168.0.255 NBT Datagram Service Type=17 Source=ROOTDC[20]
192.168.0.247 -> 192.168.0.255 NBT Datagram Service Type=17 Source=TSC[0]
? -> (broadcast) ETHER Type=886F (Unknown), size = 1510 bytes
192.168.0.200 -> (broadcast) ARP C Who is 192.168.0.102, 192.168.0.102 ?
```

```
127.0.0.178 -> lab183.lab.net TCP D=124 S=1352 Syn Seq=674711609 Len=0 Win=65535
127.0.0.178 -> lab183.lab.net TCP D=125 S=1352 Syn Seq=674711609 Len=0 Win=65535
127.0.0.178 -> lab183.lab.net TCP D=126 S=1352 Syn Seq=674711609 Len=0 Win=65535
127.0.0.178 -> lab183.lab.net TCP D=128 S=1352 Syn Seq=674711609 Len=0 Win=65535
127.0.0.178 -> lab183.lab.net TCP D=130 S=1352 Syn Seq=674711609 Len=0 Win=65535
127.0.0.178 -> lab183.lab.net TCP D=131 S=1352 Syn Seq=674711609 Len=0 Win=65535
127.0.0.178 -> lab183.lab.net TCP D=133 S=1352 Syn Seq=674711609 Len=0 Win=65535
127.0.0.178 -> lab183.lab.net TCP D=135 S=1352 Syn Seq=674711609 Len=0 Win=65535
……
……
```

服务端口攻击

- SYN Flooding
  - 同步包风暴拒绝服务攻击具有以下特点
    - 针对TCP/IP协议的薄弱环节进行攻击
    - 发动攻击时，只要很少的数据流量就可以产生显著的效果
    - 攻击来源无法定位
    - 在服务端无法区分TCP连接请求是否合法
  - 同步包风暴攻击的本质是利用TCP/IP协议集的设计弱点和缺陷
  - 只有对现有的TCP/IP协议集进行重大改变才能修正这些缺陷
  - 目前还没有一个完整的解决方案，但是可以采取一些措施尽量降低这种攻击发生的可能性

服务端口攻击

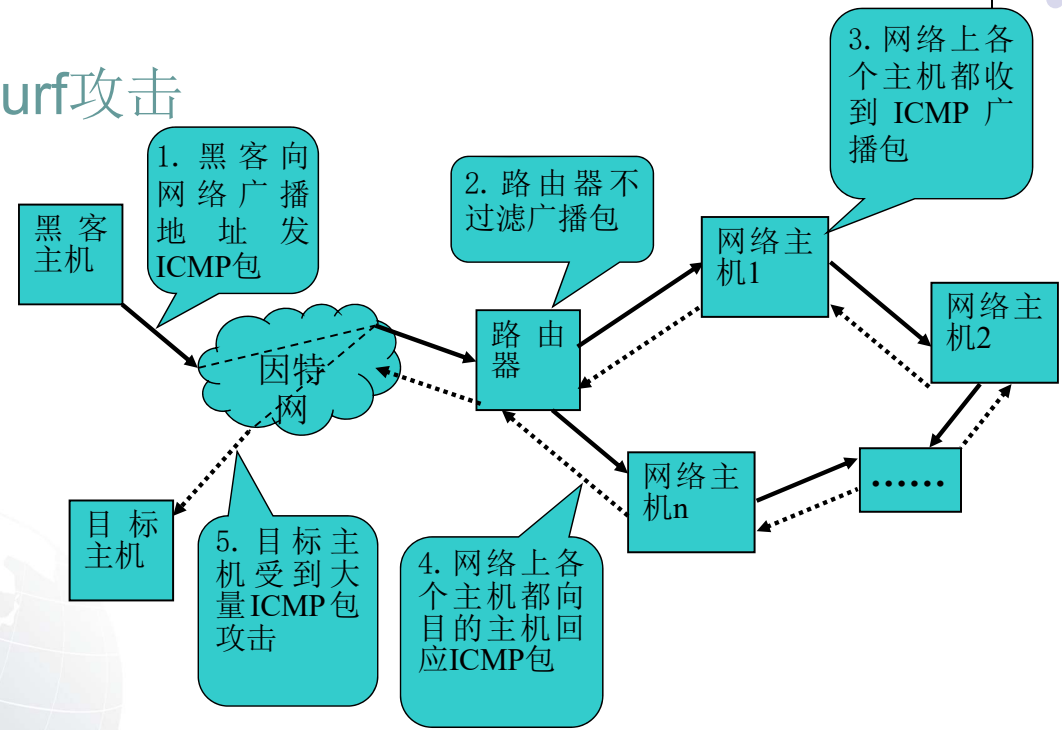
- SYN Flooding
  - 应对
    - 优化系统配置
    - 优化路由器配置
    - 使用防火墙
    - 主动监视
    - 完善基础设施

服务端口攻击

- Smurf攻击
  - 这种攻击方法结合使用了IP欺骗和ICMP回复方法使大量网络数据充斥目标系统，引起目标系统拒绝为正常请求进行服务

服务端口攻击

- Smurf攻击



（图中实线部分表示攻击者发出的ICMP包，虚线部分表示对目的攻击的ICMP包）

服务端口攻击

- Smurf攻击
  - 应对
    - 实际发起攻击的网络
      - 过滤掉源地址为其他网络的数据包
    - 被攻击者利用的中间网络
      - 配置路由器禁止IP广播包
    - 被攻击的目标
      - 与ISP协商，由ISP暂时阻止这些流量

服务端口攻击

- 错误处理
  - Ping of Death

```
C:\>ping -l 65507 -n 1 192.168.1.107
Bad value for option -l, valid range is from 0 to 65500.
```

服务端口攻击

- 错误处理
  - Teardrop攻击

举个例子来说明这个漏洞：

第一个碎片：mf=1 offset=0 payload=20

第二个碎片：mf=0 offset=10 payload=9

fp-〉len=19-20=-1；

那么memcpy将拷贝过多的数据导致崩溃。

服务端口攻击

- 错误处理
  - Winnuke攻击
    - Windows : NetBIOS : 139
    - OOB
    - 蓝屏

```
send (sock,&c,1,MSG_OOB);
```

服务端口攻击

- 错误处理
  - Land攻击
    - 攻击者将一个包的源地址和目的地址都设置为目标主机的地址，然后将该包通过IP欺骗的方式发送给被攻击主机，这种包可以造成被攻击主机因试图与自己建立连接而陷入死循环，从而很大程度地降低了系统性能
    - 对Land攻击反应不同，许多UNIX实现将崩溃，而Windows会变的极其缓慢（大约持续五分钟）
    - 127.0.0.1

电子邮件轰炸

- 在很短时间内收到大量无用的电子邮件
- SMTP端口 (25)

telnet smtp.ercist.net smtp

Trying 2.4.6.8…

Connected to smtp.ercist.net.

Escape character is '^]'.

220 smtp.ercist.net ESMTP

hello yahoo.com

250 smtp.ercist.net

mail from: abc@ercist.net

250 Ok

rcpt to: def@university.net

250 Ok

data

354 End data with <CR><LF>.<CR><LF>

垃圾邮件内容

250 Ok: queued as 96FE61C57EA7B

quit

电子邮件轰炸

- 邮件列表炸弹
  - KaBoom!
  - 这种攻击有两个特点
    - 真正的匿名，发送邮件的是邮件列表
    - 难以避免这种攻击，除非被攻击者更换电子邮件地址，或者向邮件列表申请退出
- 病毒发送电子邮件炸弹

电子邮件轰炸

- 应对
  - 配置路由器和防火墙，识别邮件炸弹的源头，不使其通过
  - 提高系统记账能力，对事件进行追踪

分布式拒绝服务攻击DDoS

- 分布式拒绝服务DDoS（Distributed Denial of Service）攻击是对传统DoS攻击的发展
- 攻击者首先侵入并控制一些计算机，然后控制这些计算机同时向一个特定的目标发起拒绝服务攻击

分布式拒绝服务攻击DDoS

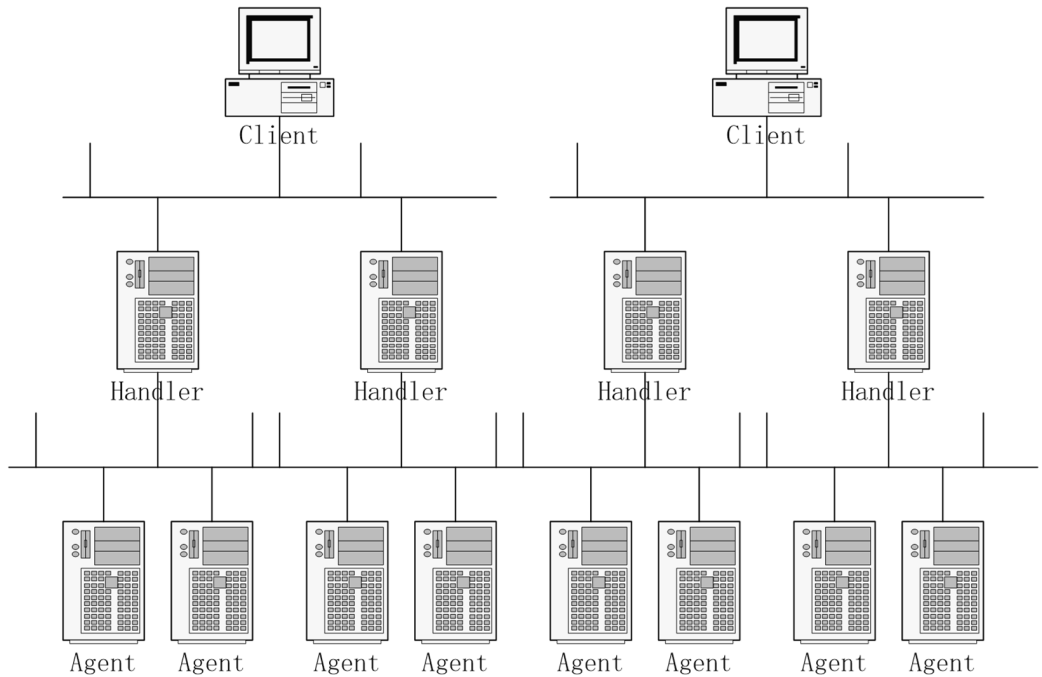
- 传统的拒绝服务攻击的缺点
  - 受网络资源的限制
  - 隐蔽性差
- DDoS克服了这两个致命弱点
  - 突破了传统攻击方式从本地攻击的局限性和不安全性
  - 其隐蔽性和分布性很难被识别和防御

分布式拒绝服务攻击DDoS

- 被DDoS攻击时可能的现象
  - 被攻击主机上有大量等待的TCP连接
  - 端口随意
  - 大量源地址为假的无用的数据包
  - 高流量的无用数据造成网络拥塞
  - 利用缺陷，反复发出服务请求，使受害主机无法及时处理正常请求
  - 严重时会造成死机

分布式拒绝服务攻击DDoS

- DDoS的三级控制结构



4.5 分布式拒绝服务攻击DDoS

- DDoS工具
  - Trinoo
    - UDP
  - TFN（Tribe Flooding Network）
  - Stacheldraht
  - TFN2K（Tribe Flooding Network 2000）
    - 多点攻击、加密传输、完整性检查、随机选择底层协议和攻击手段、IP地址欺骗、哑代理、隐藏身份等特点
  - Trinity v3

分布式拒绝服务攻击DDoS

- 应对
  - 在数据流中搜寻特征字符串
  - 利用攻击数据包的某些特征
  - 监视本地主机端口的使用
  - 对通信数据量进行统计

DDoS新技术 - 反弹技术

反弹技术就是利用反弹服务器实现攻击的技术

所谓反弹服务器（Reflector）是指当收到一个请求数据报后就会产生一个回应数据报的主机

例如，所有的Web服务器、DNS服务器和路由服务器都是反弹服务器。攻击者可以利用这些回应的数据报对目标机器发动DDoS攻击

反弹技术原理

反弹服务器攻击过程和传统的DDoS攻击过程相似，如前面所述的4个步骤中

只是第4步改为：攻击者锁定大量的可以作为反弹服务器的服务器群，攻击命令发出后，代理守护进程向已锁定的反弹服务器群发送大量的欺骗请求数据包，其原地址为受害服务器或目标服务器

传统DDoS第4步：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

反弹技术与传统DDoS区别

- 多了第四层——被锁定的反弹服务器层
- 反弹服务器的数量可以远比驻有守护进程的代理服务器多
- 使攻击时的洪水流量变弱，最终才在目标机汇合为大量的洪水
- 目标机更难追查到攻击来源
  - 目标机接收到的攻击数据报的源IP是真实的，反弹服务器追查到的数据报源IP是假的。