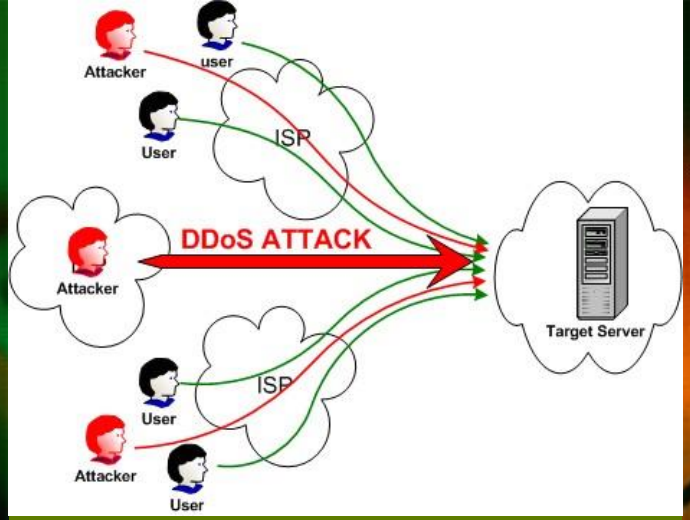


Network Security

第0x09讲 拒绝服务攻击与防御

Contents

001 拒绝服务攻击的概念

010 典型DoS攻击

011 典型DDoS攻击

100 DoS、DDoS攻击的防御

拒绝服务攻击的概念

- **拒绝服务（Denial of Service，DoS）**:一种破坏性攻击，通常利用传输协议弱点、系统漏洞、服务漏洞对目标系统发起大规模进攻，用超出目标处理能力的海量数据包消耗可用**系统资源**、**带宽资源**等，或造成**程序缓冲区溢出**错误，致使其无法处理合法用户的请求，无法提供正常服务，最终致使网络服务瘫痪，甚至系统死机

- 让攻击目标瘫痪的一种“损人不利己”的攻击手段

拒绝服务攻击的概念

- 最著名的DoS之一——**Morris蠕虫**:
  - 1988.11: 众多连在因特网上的计算机在数小时内无法正常工作，遭受攻击的包括 5 个计算机中心和12个地区结点，连接着政府、大学、研究所和拥有政府合同的25万台计算机。直接经济损失达9600万美元
- 许多知名网站如Yahoo、eBay、CNN、百度、新浪等都曾遭受DoS攻击
- 典型案例：百度遭受大规模**SYN Flooding**攻击(2006年)

百度称遭大规模黑客攻击 12日搜索罢工近半小时

“12日下午我们接到网友信息感到特别突然，因为以前从来没有遇到过这样的大规模的攻击。”昨天，百度首席技术官刘建国在电话中告诉记者。百度称遭遇了公司历史上最大规模的不明身份的黑客攻击，并已经向公安机关报案。

据记者了解，9月12日17点30分，有北京、重庆等地的网友反映百度无法正常使用，出现“请求超时”(Request timed out)的信息。这次攻击造成了百度搜索服务在全国各地出现了近30分钟的故障。随后，百度技术部门的员工们快速反应，将问题解决并恢复百度服务。9月12日晚上11时37分，百度空间发表了针对不明攻击事件的声明。“今天下午，百度遭受有史以来最大规模的不明身份黑客攻击，导致百度搜索服务在全国各地出现了近30分钟的故障。”

百度首席技术官刘建国对记者说，“黑客使用的攻击手段是同步泛滥(syn flooding)，这是一种分布式服务拒绝(DDOS)方法。就是通过大量的虚假IP地址，建立不完整连接，使服务超载，从而不能提供正常的服务。”

经过百度技术工程师与不明身份的黑客斗争，百度的搜索服务已经在12日傍晚恢复正常。

拒绝服务攻击案例

百度被黑事件 编辑

2010年1月12日上午7点钟开始，中国最大中文搜索引擎“百度”遭到黑客攻击，长时间无法正常访问。主要表现为跳转到一雅虎出错页面、伊朗网军图片，出现“天外符号”等，范围涉及四川、福建、江苏、吉林、浙江、北京、广东等国内绝大部分省市。

中文名	百度被黑事件	范　围	四川，福建，江苏等地
时　间	2010年1月12日	持续时长	5个小时
表现形式	长时间无法正常访问	事件制造者	不明身份的黑客

目录

1 事件简介
2 影响分析
3 相关案例
4 百度声明
5 后续进展

事件简介 编辑

这次攻击百度的黑客疑似来自境外，利用了DNS记录篡改的方式。这是自百度建立以来，所遭遇的持续时间最长、影响最严重的黑客攻击，网民访问百度时，会被定向到一个位于荷兰的IP地址，百度旗下所有子域名均无法正常访问。[1]

拒绝服务攻击的类型

- 按照攻击行为可分为：
  - **网络带宽攻击**：极大的通信量使可用的**网络资源**被消耗殆尽，最终导致合法用户请求无法通过

  - **连通性攻击**：大量的连接请求冲击计算机，使得所有可用的**系统资源**被消耗殆尽，最终计算机无法处理合法用户请求

拒绝服务攻击的类型

- **滥用合理的服务请求**
  - 过度请求系统的正常服务，占用过多服务资源，致使系统超载。如执行耗时操作（数据库查询，读写文件）、消耗开放连接数等
- **利用传输协议缺陷**
  - 构造畸形的数据包并发送，导致目标主机无法处理，出现错误或崩溃
- **利用服务程序的漏洞**
  - 针对服务程序的特定漏洞，发送一些有针对性的特殊格式的数据，导致服务处理错误而拒绝服务

银行来了百万存款 不过全是一元零钞(图)

典型拒绝服务攻击技术

1. Ping of Death
2. 泪滴（Teardrop）
3. 泛洪类（Flood）
   - UDP泛洪
   - SYN泛洪
   - ACK泛洪
   - Connection泛洪
   - HTTP Get 泛洪
4. Land攻击
5. Smurf攻击
6. Fraggle攻击
7. 畸形消息攻击
8. Slashdot effect
9. WinNuke攻击

Ping of Death（死亡之Ping）：

- ICMP报文长度固定（64KB），很多操作系统只开辟64KB的缓存区用于存放ICMP数据包
- 如果ICMP数据包的实际尺寸超过64KB，就产生**缓存溢出**，导致TCP/IP协议堆栈崩溃，造成主机重启或死机

- “**ping –l**”：指定发送数据包的尺寸：

  Ping -l 65540 192.168.1.140

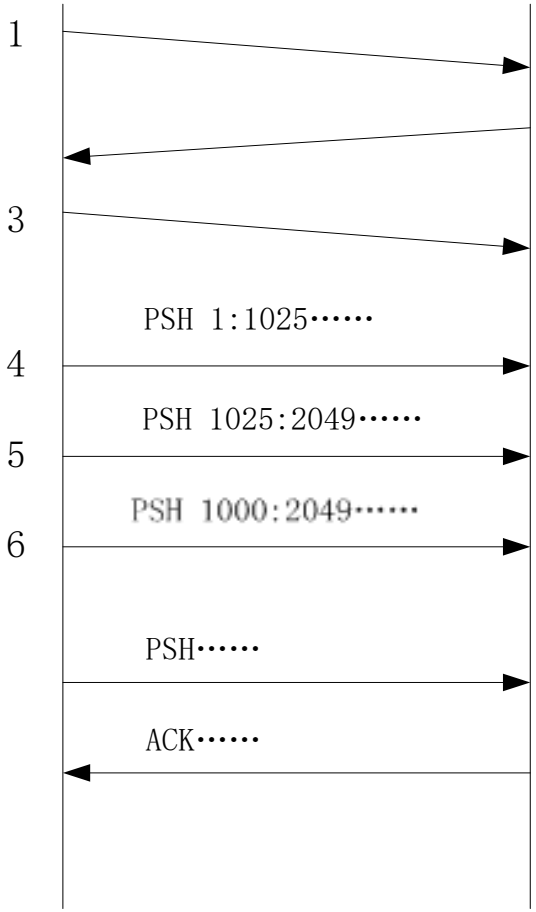
- 现在的操作系统已修补了这一漏洞：

```
C:\>ping -l 65540 192.168.42.131
选项 -l 的值有错误，有效范围从 0 到 65500。
```

典型拒绝服务攻击技术

- **泪滴（分片攻击，Teardrop）**：利用TCP/IP协议缺陷，首个实现攻击的程序名为Teardrop
  - 如果传输的数据无法在一个报文中传输完成，就会被分片，传送到目标主机后再到**堆栈**中进行重组，该过程称为“**分片**”
  - 为能进行数据重组，TCP首部包含——分片识别号、偏移量、数据长度、标志位，目标主机据此将各分片重组还原

典型拒绝服务攻击技术



PSH 1:1025……

PSH 1000:2049……

PSH 2049:3073……

试图重组时
主机崩溃

信息到达目的主机后在堆栈中重组，由于畸形分片的存在，会导致重组出错，错误并不仅仅是影响到重组数据，由于协议重组算法会导致内存错误，引起协议栈的崩溃

UDP泛洪（UDP Flood）：

- 利用主机自动回复的服务（如使用UDP协议的chargen和echo）进行攻击
  - **echo**：回显接收到的数据包
  - **chargen**：收到数据包时随机反馈一些字符，用作测试
- 提供WWW和Mail等的服务设备通常使用Unix服务器，默认打开一些UDP服务,如echo等

- **一方的输出成为另一方的输入**，两台主机间会形成大量的UDP数据包。当多个系统之间互相产生UDP数据包时，最终将导致整个网络瘫痪

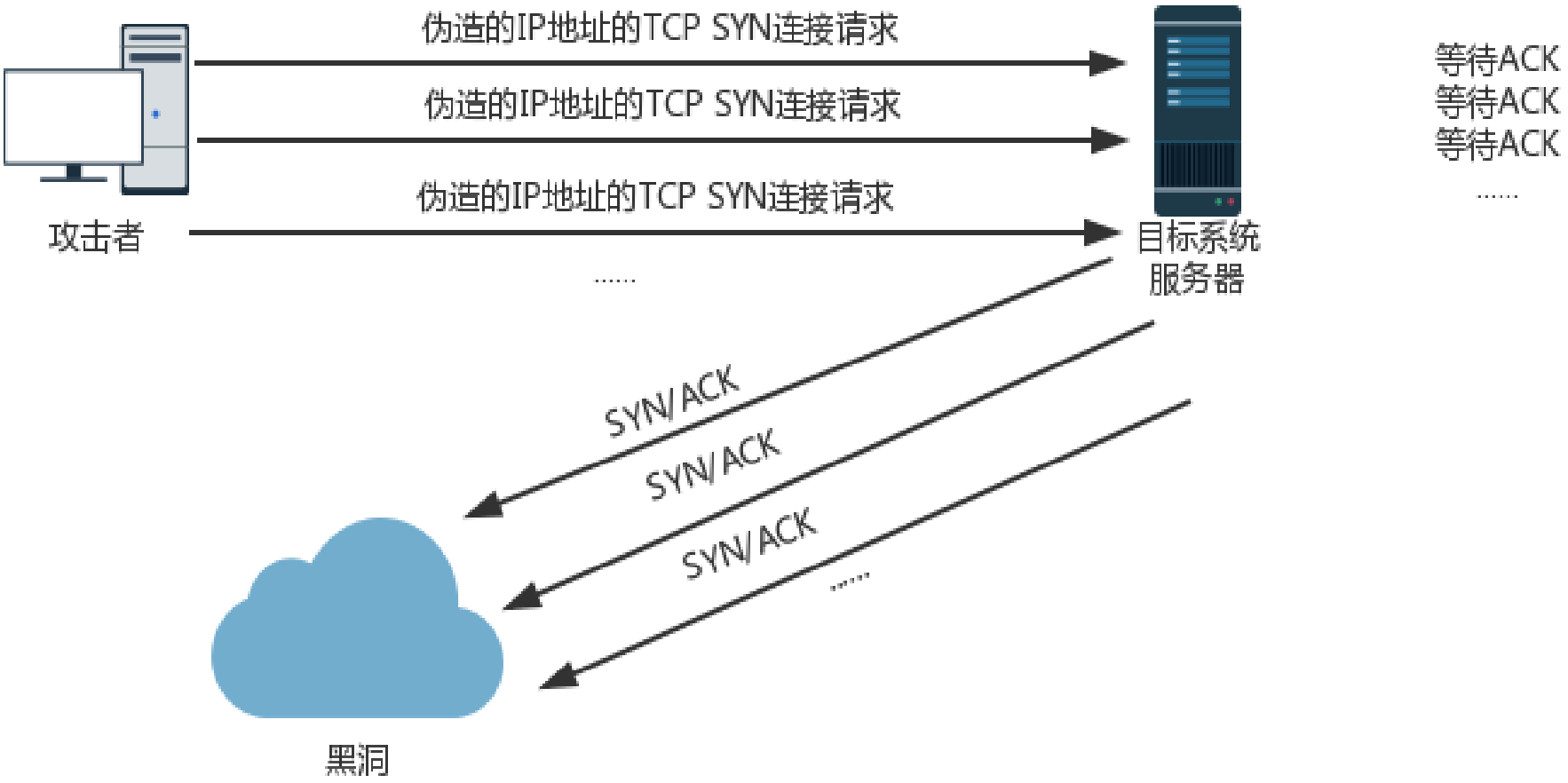
典型拒绝服务攻击技术

SYN泛洪（SYN Flood）：

- **最流行的DoS攻击方式之一**，利用TCP协议缺陷，发送大量伪造的TCP连接请求，使被攻击方资源耗尽(CPU满负荷或内存不足)
- 利用**TCP的三次握手**：客户端向服务器发送SYN后突然死机或掉线，服务器在发出SYN/ACK报文后无法收到客户端的ACK报文，一般会**重试3-5次**，并等待一段时间（可能几分钟）后丢弃该连接。这段时间称为**SYN Timeout**

- 攻击者大量伪造IP地址，服务器将为维护一个非常大的半连接而消耗非常多的资源

典型拒绝服务攻击技术



你在这里等着我回来，等到.....

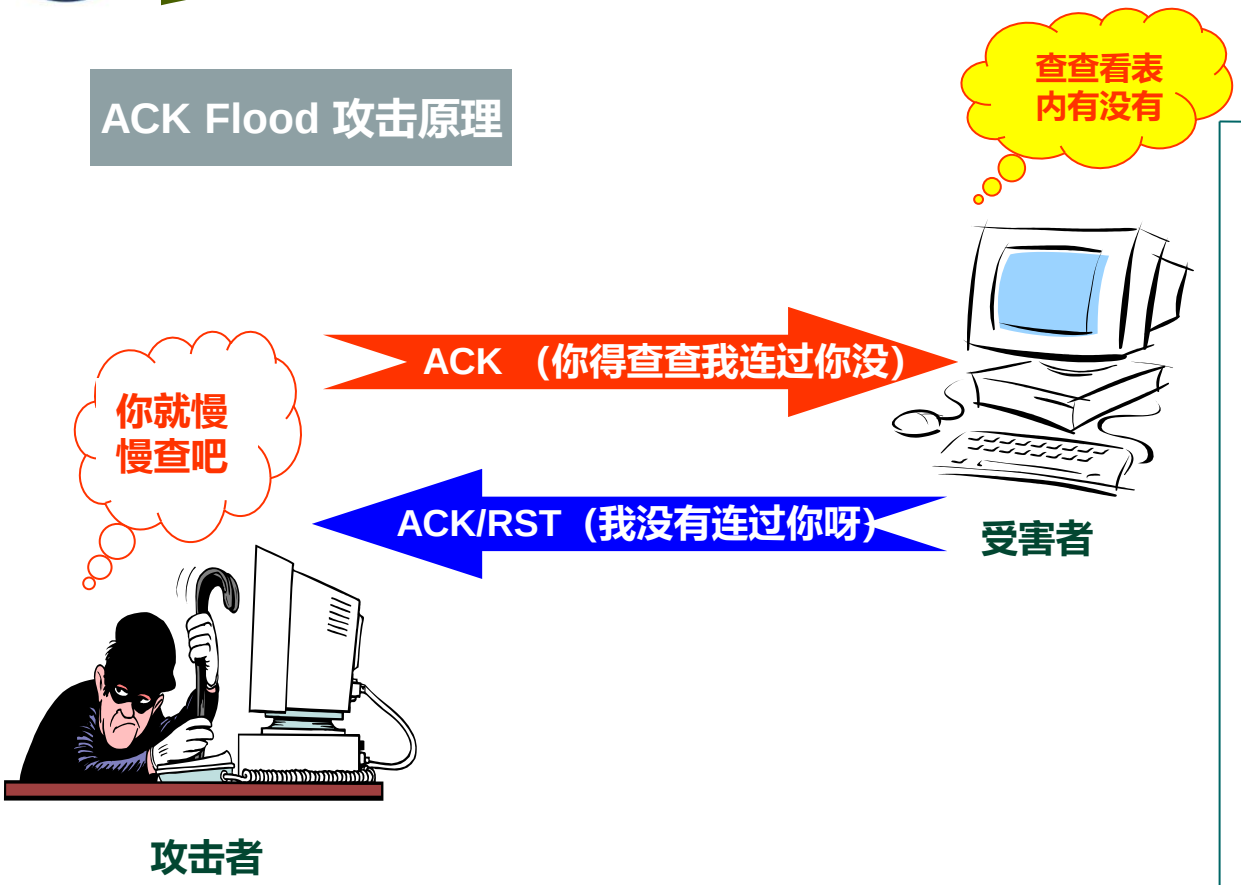
- **SYN泛洪较难防御，以下是几种解决方法：**
  - **缩短SYN Timeout时间**
  - **设置SYN Cookie**：给每个请求连接的IP分配一个Cookie，如果短时间内连续收到某个IP的重复SYN报文，就认定是攻击，丢弃以后来自该IP地址的包
  - **负反馈策略**：一旦SYN半连接的数量超过系统中TCP活动半连接最大连接数的设置，系统将认为受到攻击并作出反应：减短SYN Timeout时间、减少SYN-ACK的重试次数、自动对缓冲区中的报文进行延时等措施
  - **退让策略**
  - **分布式DNS负载均衡**
  - **防火墙**

典型拒绝服务攻击技术

- **退让策略：**
  - SYN Flood攻击的缺陷： 一旦攻击开始，将不会再进行域名解析
  - 服务器受到攻击后**迅速更换IP地址**，那么攻击者攻击的将是一个空的IP地址，而防御方只要将DNS解析更改到新的IP地址就能在很短的时间内恢复用户通过
  - 为迷惑攻击者，甚至可以放置一台“牺牲”服务器让攻击者满足于攻击的“效果” （**蜜罐**）
- **分布式DNS负载均衡**
  - 将用户的请求分配到不同IP的服务器主机上
- **防火墙**
  - 识别SYN Flood攻击所采用的攻击方法，并将攻击包阻挡在外

典型拒绝服务攻击技术

ACK Flood 攻击原理

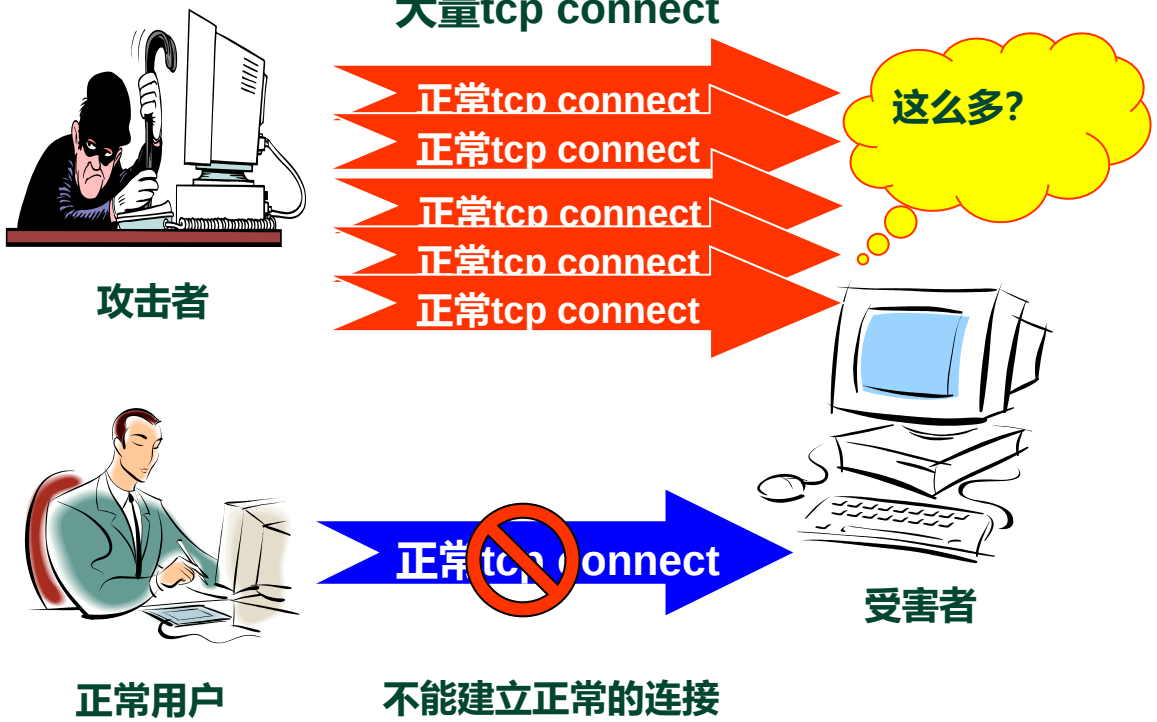


攻击表象

- 大量ACK冲击服务器
- 受害者资源消耗
  - 查表
  - 回应ACK/RST
- **ACK Flood流量要较大才会对服务器造成影响**

典型拒绝服务攻击技术

TCP Connection Flood 攻击原理



攻击表象

- 利用真实 IP 地址（代理服务器、广告页面）在服务器上建立大量连接
- 服务器上残余连接(WAIT状态)过多，效率降低，甚至资源耗尽，无法响应
- 蠕虫传播过程中会出现大量源IP地址相同的包，对于TCP 蠕虫则表现为大范围扫描行为
- 消耗骨干设备的资源，如防火墙的连接数

典型拒绝服务攻击技术

HTTP Get Flood 攻击原理

攻击者

正常HTTP Get请求

正常HTTP Get Flood

正常HTTP Get Flood

正常HTTP Get Flood

正常HTTP Get Flood

正常HTTP Get Flood

正常HTTP Get Flood

受害者(Web Server)

正常HTTP Get Flood

不能建立正常的连接

正常用户

占用

占用

占用

DB连接池

DB连接池用完啦！！

受害者(DB Server)

is.cumt.edu.cn

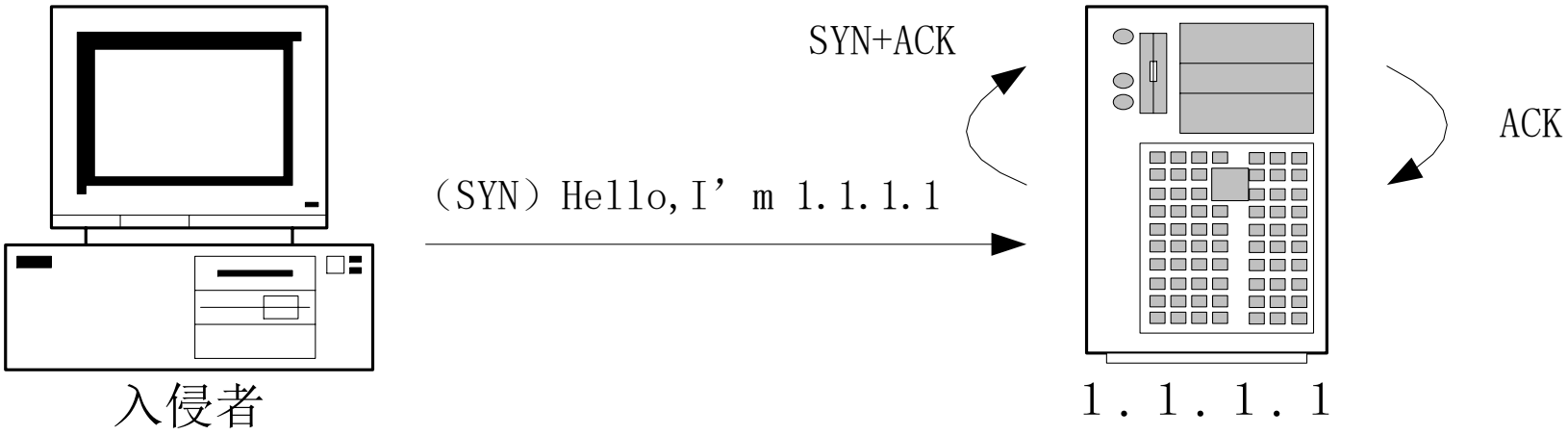
攻击表象

- 利用代理服务器向受害者发起大量HTTP Get请求
- 主要请求动态页面，涉及到数据库访问操作
- 数据库负载以及数据库连接池负载极高，无法响应正常请求

TCP Land攻击:

- 著名黑客组织rootshell发现，利用TCP三次握手的缺陷
- **原理:** 向目标发送大量的**源地址和目标地址相同**的包，造成目标主机解析时占用大量的系统资源，从而使网络功能完全瘫痪
- 目标主机收到这样的连接请求会向自己发送SYN/ACK数据包，导致目标主机向自己发回ACK数据包并创建一个连接
- 大量这样的数据包将使目标主机建立很多无效的连接，大量占用系统资源

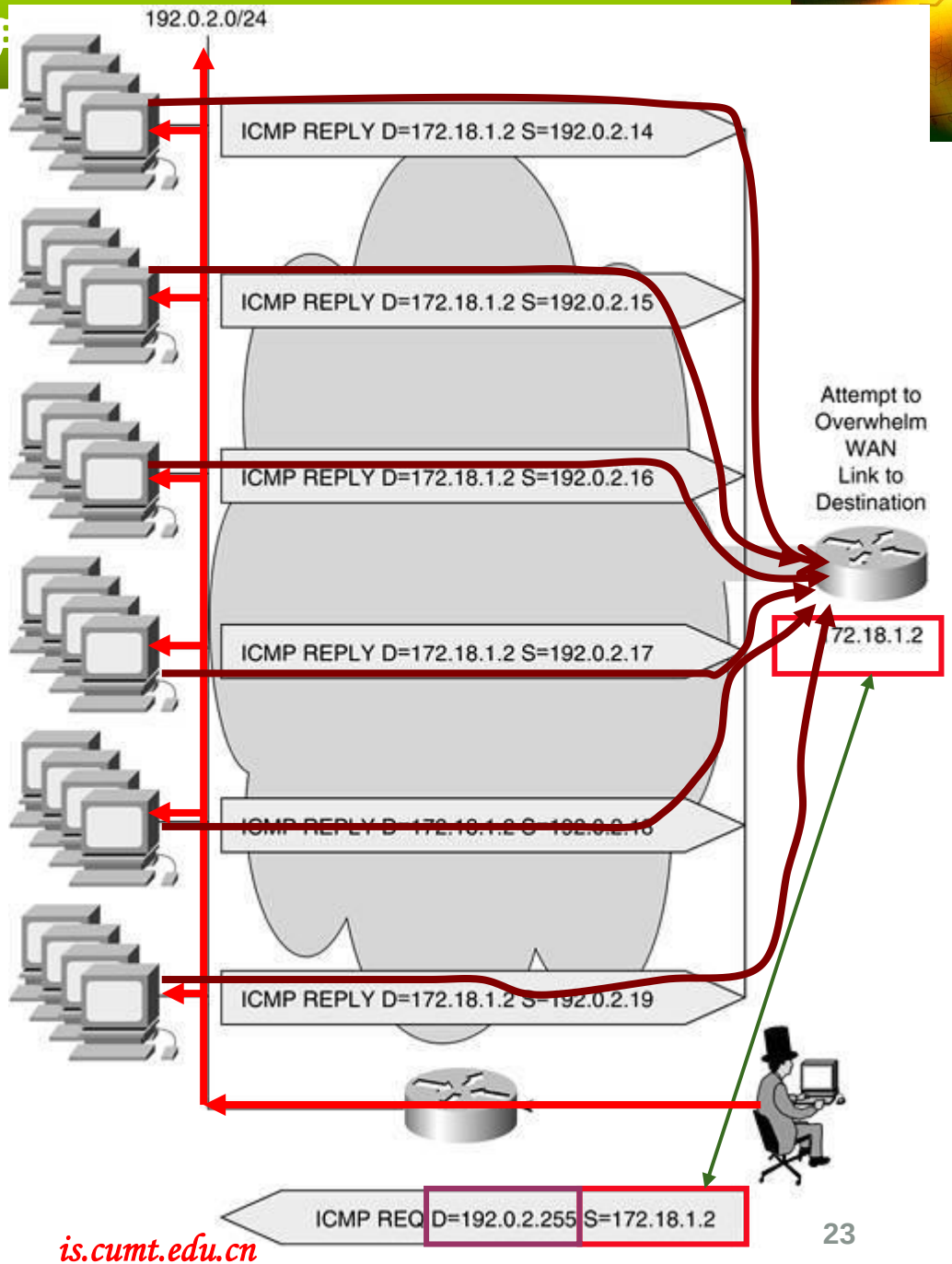
典型拒绝服务攻击技术



- **检测方法：**判断网络数据包的源/目标地址是否相同
- **反攻击方法：**适当配置防火墙或路由器的过滤规则（**入口过滤**）可以防止攻击，并对攻击进行审计

典型拒绝

- **Smurf攻击**:
  - 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，于是大量的ICMP echo回应包被发送给被攻击主机，使其因网络阻塞而无法提供服务
  - 不仅影响目标主机，还能影响目标主机的整个网络系统



Fraggle攻击：

- 原理与Smurf一样，采用向广播地址发送数据包，利用广播的特性将攻击放大以使目标主机拒绝服务
- 不同：Fraggle使用的是UDP应答消息而非ICMP

畸形消息攻击:

- 有**针对性**的攻击方式，利用目标主机或特定服务的安全漏洞进行攻击
- 操作系统上的许多服务在处理信息之前没有进行适当的错误校验，所以一旦收到畸形信息就有可能会崩溃
- 在没有安装相应补丁的**IIS 5**上，递交如下的URL会导致IIS 5停止服务:

  http://testIP/...[25kb of '.']...ida

  递交如下的HTTP请求会导致IIS系统崩溃，需重启才能恢复:

  "***GET /.....[3k]..... .htr HTTP/1.0***"

Slashdot effect:

- 来自Slashdot.org，曾十分知名且浏览人数十分庞大的IT、电子、娱乐网站，也是blog网站的开宗始祖之一
- 在Slashdot.org的文章中放入的链接，有可能一瞬间被点入成千上万次，造成被链接的网站承受不住突然增加的连接请求，出现响应变慢、崩溃、拒绝服务
- 瞬间产生大量进入某网站的动作称作Slashdotting，使web服务器或其他类型的服务器由于大量的网络传输而过载

WinNuke攻击（带外传输攻击）：

- **特征是攻击目标端口**，通常是139、138、137、113、53
- TCP中使用带外数据（Out of Band，OOB）来传送一些比较特殊（如紧急）的数据。在紧急模式下，发送的TCP数据包包含URG标志和16位URG指针
  - URG指针指向包内数据段的某个字节数据，表示从第一字节到指针所指字节的数据是紧急数据，不进入接收缓冲就直接交给上层进程
- WinNuke攻击制造这种报文，但其指针字段与数据的实际位置不符，即**存在重合**。WINDOWS操作系统在处理这些数据时，就会崩溃

典型拒绝服务攻击技术

- 攻击者将特殊TCP带外数据报文发送给已建立连接的主机的NetBIOS端口139，导致主机崩溃后，会显示下面的信息：

An exception OE has occurred at 0028:[address] in VxD MSTCP(01)+ 000041AE. This was called from 0028:[address] in VxD NDIS(01)+ 00008660.It may be possible to continue normally.

Press any key to attempt to continue.

Press CTRL+ALT+DEL to restart your computer.

You will lose any unsaved information in all applications.

Press any key to continue

典型拒绝服务攻击技术

- WinNuke攻击的特征、检测方法和反攻击方法：
  - **特征：**目标端口通常是139、138、137、113、53，而且URG位设为“1”
  - **检测方法：**判断目标端口是否为139、138、137等，并判断URG位是否为“1”
  - **反攻击方法：**适当配置防火墙或过滤路由器可以防止这种攻击手段（丢弃该数据包），并对攻击进行审计（记录事件发生的时间，源主机和目标主机的MAC地址和IP地址）

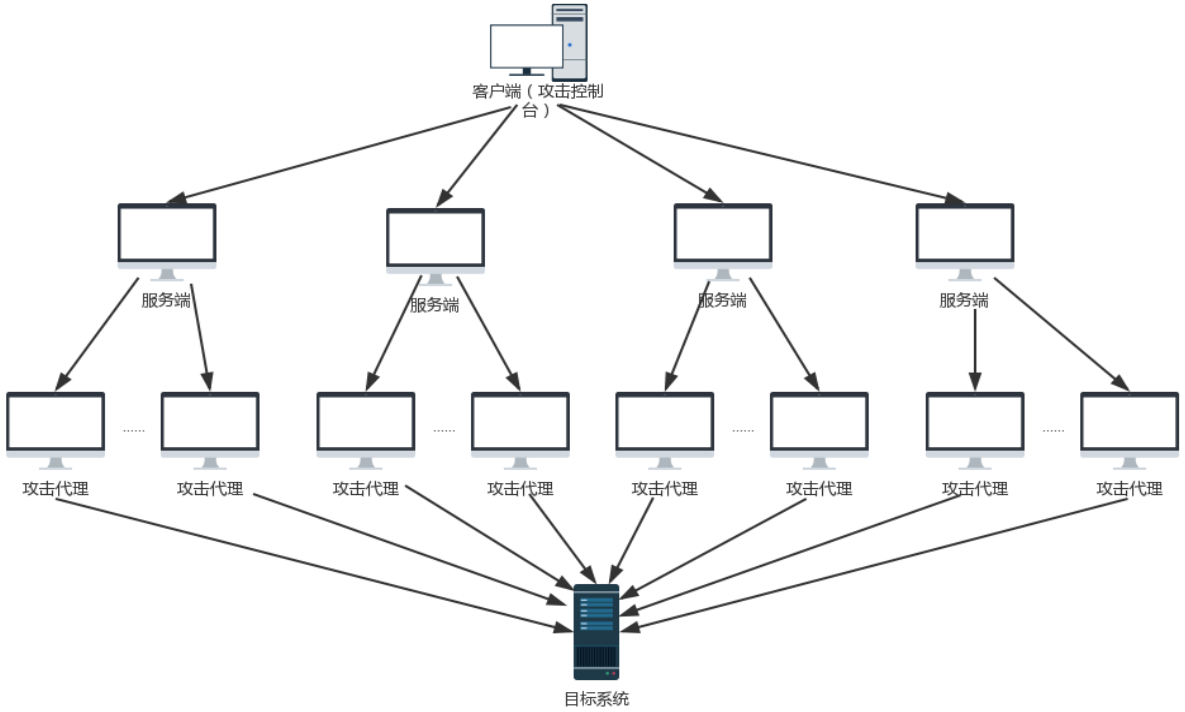
典型分布式拒绝服务攻击技术

- **分布式拒绝服务DDoS (Distributed DoS)：**通过控制分布在网络各处的数百甚至数万台傀儡主机（肉机），发动它们同时向攻击目标进行DoS攻击
- 1999年8月出现的一种新的网络攻击方法
- 现在DDoS开始大行其道，成为黑客攻击的主流手段
- **Yahoo、eBay、CNN**等众多知站点相继被身份不明的黑客在短短几天内连续破坏，系统瘫痪达几个小时甚至几十个小时之久

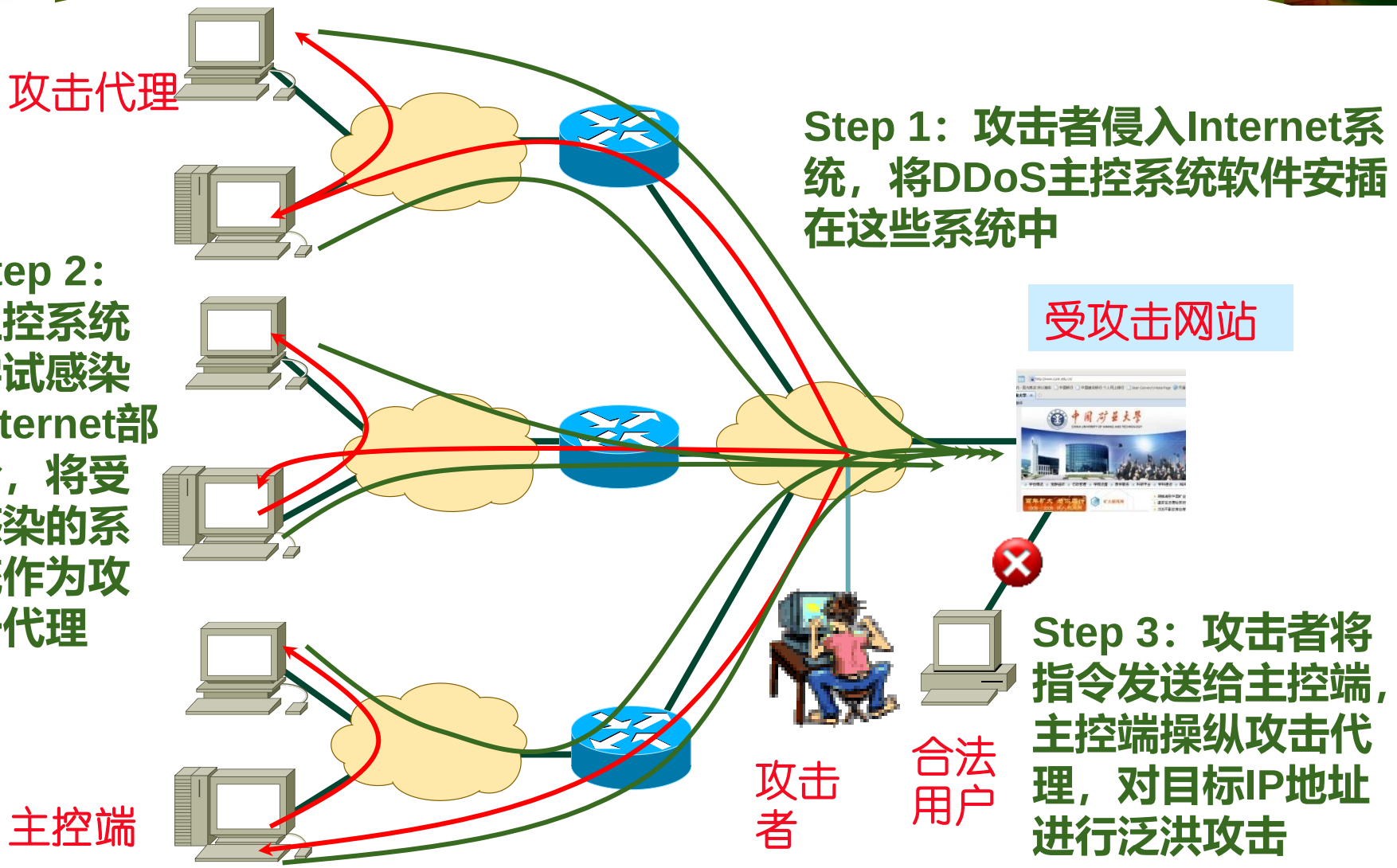
- 被DDoS攻击时的现象：
  - 被攻击主机上有大量等待的TCP连接
  - 网络中充斥着大量的无用数据包，源地址为假
  - 制造高流量无用数据，造成网络拥塞，使受害主机无法正常和外界通讯
  - 利用受害主机提供的服务或传输协议的缺陷，反复高速发出特定的服务请求，使受害主机无法及时处理正常请求
  - 严重时会造成系统死机
  - DDoS攻击期间，用户发出正常的页面请求，请求会完全失败，或者页面下载速度极其缓慢，看起来就是站点无法使用

典型分布式拒绝服务攻击技术

- DDoS软件一般分为客户端、服务端与守护程序，这些程序可以协调分散在各处的机器共同完成对一台主机的攻击
  - 客户端（攻击控制台）：发起攻击的主机
  - 服务端（主控端）：接受客户端发来的控制命令
  - 守护程序（攻击代理）：接收服务端的指令，直接（如SYN Flooding）或间接（如反射式DDoS）与攻击目标进行通信



典型分布式拒绝服务攻击技术



分布式拒绝服务攻击

- 入侵者通过客户端软件向服务端软件发出攻击指令，服务端在接收到攻击指令后，控制攻击代理向目标主机发动攻击。
- 采用三层结构的做法是确保入侵者的安全，一旦客户端发出指令后，客户端就能断开连接，由服务端指挥攻击代理攻击。客户端连接和发送指令的时间很短，隐蔽性极强。
- 入侵者先控制多台无关主机，在上面安装攻击代理与服务端程序。
- 当需要攻击时，入侵者从客户端连接到安装了服务端软件的主机上，发出攻击指令，服务端软件指挥攻击代理同时向目标主机发动拒绝服务攻击。
- 目前流行的分布式拒绝服务攻击软件一般没有专用的客户端软件，使用telnet进行连接和传送控制命令。

分布式拒绝服务攻击

- 通常情况下，服务端与守护进程间并不是一一对应的关系，而是多对多的关系。也就是说，一个安装了攻击代理的主机可以被多个服务端所控制，一个服务端软件也同时控制多个攻击代理。

分布式拒绝服务攻击

与传统的拒绝服务攻击相比，分布式拒绝服务攻击因其显著的特点而备受攻击者青睐

特点：

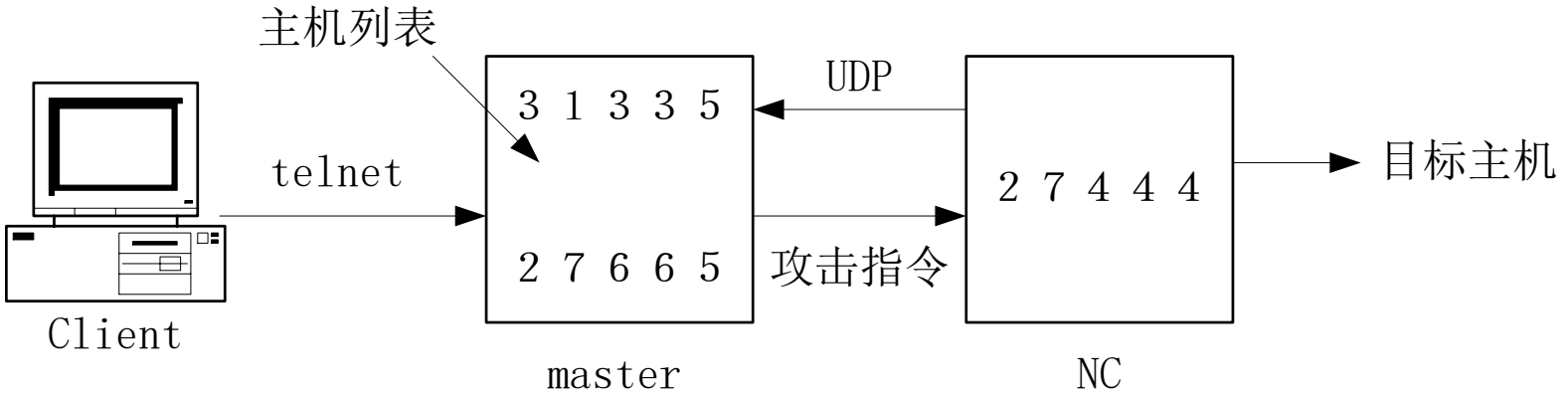
- 分布性：分布式拒绝服务攻击的攻击主体呈现显著的分布性特点，通过分布在不同地点协同发起攻击。
- 隐蔽性：分布式拒绝服务攻击通过傀儡主机发起攻击，对于真正发起攻击的攻击者而言具有很好的隐蔽性，导致追踪攻击者更为困难。
- 攻击威力大：DDoS攻击的危害性非常巨大，除了会造成攻击目标服务能力下降外，还会占用大量网络带宽，造成网络拥塞，威胁到这个网络的安全运行。

典型分布式拒绝服务攻击技术

- **DDoS的工具**:
  - Trinoo
  - TFN2K
  - Stacheldraht
  - Trinity
  - Shaft
  - MStream

Trinoo—介绍

- Trinoo是一个典型的分布式拒绝服务攻击软件，基于UDPflood，它向被攻击目标主机随机端口发送全零的4字节UDP包，被攻击主机的网络性能在处理这些超出其处理能力垃圾数据包的过程中不断下降，直至不能提供正常服务甚至崩溃。
- 由两部分组成，服务端和攻击代理（守护进程），而没有专门的客户端软件，客户端软件可以使用诸如如Telnet代替。如图：



Trinoo—工作原理

- Trinoo的守护进程NC在编译时就将安装有服务程序的主机IP地址包含在内，这样，守护进程NC一旦运行起来，就会自动检测本机的IP地址，并将本机的IP地址发送到预先知道的服务器的31335端口（服务器开启31335UDP端口接收守护进程）。
- 同时，守护进程也在本机打开一个27444的UDP端口等待服务器端过来的命令。
- Trinoo的服务器端在收到守护进程发回来的IP地址后，就明白已有一个守护进程准备完毕，可以发送指控命令了。
- 主服务器会一直记录并维护一个已激活守护程序的主机清单。

Trinoo—设计特色

- Trinooo的所有连接都需要口令，连接的口令是编译时就指定的，缺省情况下，服务端连接守护进程的口令是“144adsl”，而客户端连接到服务端的口令是“betaalmostdone”。不过口令在进行验证时是明文进行传送的。
- Trinoo另一个特色：当客户端连接到服务端时，如果还有其他的连接建立，Trinoo会将一个包含连接IP地址的报警信息发送到已连接的主机。这样，入侵者在控制服务端发动攻击时，还能掌握系统上的用户动向，确保Trinoo客户端的安全。

Trinoo--基本特性及建议的抵御策略

- 在master程序（服务端）与代理程序（守护程序）的所有通讯中，Trinoo都使用UDP协议。所有从master程序到代理程序的通讯都包含字符串"l44"，并且被引导到代理的UDP 端口27444。入侵检测软件检查到UDP 端口27444的连接，如果有包含字符串l44的信息包被发送过去，那么接受这个信息包的计算机可能就是DDoS代理。
- Trinoo master程序的监听端口是27655，攻击者一般借助telnet通过TCP连接到master程序所在计算机。入侵检测软件能够搜索到使用TCP 并连接到端口27655上的数据流。
- Master和代理之间的通讯受到口令的保护，但是口令不是以加密格式发送的，因此它可以被“嗅探”到并被检测出来。

典型分布式拒绝服务攻击技术

- TFN2K:
  - TFN(Tribe Flood Network)：德国著名黑客Mixter编写的DDoS攻击工具
  - 由**服务端程序**和**守护程序**组成，能实施ICMP flood、SYN flood、UDP flood和Smurf等多种拒绝服务攻击
  - 在Solaris、Linux、Windows NT/2000上都能运行
  - 服务端控制守护进程发动攻击时，可以定制通信使用的协议，可使用TCP、UDP、ICMP协议中的任何一种
  - 服务端向守护进程发送控制指令，守护进程不进行回复。所以**TFN2K的隐蔽性更强**，服务端可以对命令报文的源地址进行伪造

典型分布式拒绝服务攻击技术

- TFN2K所有命令都经过**CAST-256算法**（RFC2612）加密。加密关键字在编译时定义，并作为TFN2K客户端程序的口令；且所有加密数据在发送前都被编码（Base64）。TFN2K守护程序接收并解密数据

- **守护进程能通过修改进程名**来欺骗管理员，掩饰自己的真正身份

- 总之，TFN2K采用单向通信、随机使用通信协议、通信数据加密等多种技术保护自身，使实时检测TFN2K更加困难

- **Stacheldraht**：
  - 能发动ICMP Flood、SYN Flood、UDP Flood和Smurf等多种攻击
  - **主要特色：**使用rcp (remote copy，远程复制)技术对代理程序进行更新
  - 基于C/S模式——Master程序与潜在的成千个代理程序进行通讯
  - 攻击者与master程序之间的通讯是加密（Blowfish）的

典型分布式拒绝服务攻击技术

- 上述各种工具均能实施ICMP flood、SYN flood、UDP flood和Smurf等多种拒绝服务攻击
- 从发展过程看，其功能类似，但是**隐蔽性越来越强**，使得检测和追踪变得越来越困难。

拒绝服务攻击的防御

- **防御的困难之处——**不容易定位攻击者
  - Internet上绝大多数网络都不限制源地址，即伪造源地址非常容易
  - 很难溯源找到攻击控制端的位置
  - 各种反射式攻击，无法定位源攻击者

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

拒绝服务攻击的防御

- **DoS的防御方法**：
  - 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
  - 只允许必要的通信
  - 封锁敌意IP地址

有效完善的设计

- 如果某公司有一个运行关键任务的Web站点，但其与路由器之间只有一条单一的连接链路，服务器运行在单一的计算机上，这样的设计是不完善的。
- 这种情况下，攻击者对路由器或服务器进行DoS攻击，会迫使运行关键任务的服务器被迫离线。
- 理想情况下：公司不仅要有多条线路与Internet连接，最好有不同地理区域的连接。
- 公司的服务器位置越分散，IP地址越分散，黑客攻击时寻找与定位的难度就越大。

带宽限制

- 当DoS攻击发生时，针对单个协议的攻击会损耗公司的带宽，以致拒绝合法用户的服务。例如，如果攻击者向端口25发送洪水般的数据，攻击者会消耗掉所有带宽，所有试图连接端口80的用户被拒绝服务。
- 一种防范方法是限制基于协议的带宽。例如，端口25只能使用25%的带宽，端口80只能使用50%的带宽。

及时给系统安装补丁

- 当新的DoS 攻击出现并攻击计算机时，厂商一般会很快确定问题并发布补丁。如果一个公司关注最新的补丁，同时及时安装，这样被DoS攻击的机会就会减少。

运行尽可能少的服务

- 运行尽可能少的服务可以减少被攻击成功的机会。
- 如果一台计算机开了20个端口，这就使得攻击者可以在大的范围内尝试对每个端口进行不同的攻击。相反，如果系统只开了两个端口，这就限制了攻击者的攻击类型。
- 另外，当运行的服务和开放的端口都很少时，管理员可以容易的设置安全措施，因为要监听和担心的事情都很少了。

只允许必要的通信

- 这一防御机制与上一个标准“运行尽可能少的服务”很相似，不过它侧重于周边环境，主要是防火墙和路由器。关键是不仅要对系统实施最少权限原则，对网络也要实施最少权限原则。确保防火墙只允许必要的通信出入网络。
- 许多公司只过滤进入通信，而对向外的通信不采取任何措施，这两种通信都应该过滤。

封锁敌意IP地址

- 当一个公司知道自己受到攻击时，应该马上确定发起攻击的IP地址，并在其外部路由器上封锁此IP地址。但即使在外部路由器上封锁了这些IP地址，路由器仍然会因为数据量太多而拥塞，导致合法用户被拒绝对其他系统或网络的访问。
- 因此，一旦公司受到攻击应立刻通知其上游网络服务提供商封锁敌意数据包。因为ISP拥有较大的带宽和多点的访问，如果他们封锁了敌意通信，仍然可以保持合法用户的通信，也可以恢复遭受攻击公司的连接。

分布式拒绝服务攻击的防御

分布式拒绝服务攻击的监测：

- 监测DDoS时**常犯的错误**是只搜索那些DDoS工具的**缺省特征字符串、缺省端口、缺省口令**等
- **还应着重观察分析DDoS的普遍特征：异常的网络通信流量**

- **常见的异常现象：**
  1. 大量的DNS PTR(DNS的反向解析)查询请求
  2. 超出网络正常工作时的极限通讯流量
  3. 特大型的ICMP和UDP数据包
  4. 不属于正常连接通讯的TCP和UDP数据包
  5. 数据段内容只包含文字和数字字符（例如，没有空格、标点和控制字符）

分布式拒绝服务攻击的防御

- **异常现象1：**大量的DNS PTR查询请求
  - 进行DDoS攻击前总要解析目标的主机名，域名服务器能够记录这些请求。由于每台攻击服务器在进行一个攻击前会发出PTR反向查询请求，即域名服务器会接收到大量的反向解析目标IP主机名的PTR查询请求
- **异常现象2：**超出网络正常工作时的极限通讯流量
  - DDoS攻击时，会出现明显超出该网络正常工作时的极限通讯流量。现在能够分别对不同的源地址计算出对应的极限值。当明显超出此极限值时就表明存在DDoS攻击。
  - 可以在主干路由器端建立ACL访问控制规则以监测和过滤这些通讯。

- **异常现象3：**特大型的ICMP和UDP数据包
  - 正常的UDP会话一般都使用小的UDP包，通常有效数据内容不超过10字节。正常的ICMP消息也不会超过64到128字节
  - 明显大得多的数据包很有可能就是控制信息通讯用的，主要含有加密后的目标地址和一些命令选项。一旦捕获到（没有经过伪造的）控制信息通讯，DDoS服务器的位置就无所遁形了，因为控制信息通讯数据包的目标地址是没有伪造的

分布式拒绝服务攻击的防御

- **异常现象4：**不属于正常连接通讯的TCP/UDP数据包
  - 隐蔽的DDoS工具随机使用多种通讯协议通过无连接通道发送数据。优秀的防火墙和路由规则能够发现这些数据包。另外，连接到高于1024而且不属于常用网络服务的目标端口的数据包也非常值得怀疑

- **异常现象5：**数据段内容只包含文字和数字字符
  - 数据经过BASE64编码后只含有base64字符集字符的特征。TFN2K发送的控制信息数据包就是这种类型的数据包。TFN2K（及其变种）的特征模式是在数据段中有一串A字符（AAA……），这是经过调整数据段大小和加密算法后的结果。如果没有使用BASE64编码，对于使用了加密算法数据包，这个连续的字符就是“\0”

分布式拒绝服务攻击的防御

- **分布式拒绝服务攻击的防御——降低**系统受到拒绝服务攻击的危害:
  - **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**
  - **与ISP服务商合作**
  - **使用扫描工具**

分布式拒绝服务攻击的防御

- **优化网络和路由结构:**
- 提供的服务不仅要有多条与Internet的连接，而且最好有不同地理区域的连接。服务器IP地址越分散，攻击者定位目标的难度就越大，当问题发生时，所有通信可以被重新路由，可以大大降低其影响
- **保护网络及主机系统安全:**
- 本质上，如果攻击者无法获得网络的访问权，无法攻克一台主机，他就无法在系统上安装DDoS服务器。
- 要使一个系统成为服务器，首先要以某种手段攻克它，如果周边环境不会被突破，系统能够保持安全，就不会被用于攻击其他系统。
- 要注意保护主机系统的安全，避免其被攻击者用作傀儡主机，充当DDoS的间接受害者。

分布式拒绝服务攻击的防御

- 安装入侵检测系统
- 与ISP服务商合作（*）
- DDoS非常重要的特点是**洪水般的网络流量**，单凭自己管理网络无法对付这些攻击。当受到攻击时与ISP协商，确定发起攻击的IP地址，请求ISP实施正确的路由访问控制策略，封锁来自敌意IP地址的数据包，减轻网络负担，保护带宽和内部网络

使用扫描工具：

- 许多公司网络安全措施滞后，它们的网络可能已经被攻克并用作DDoS服务器，因此要扫描这些网络查找DDoS服务器并尽可能的把它们从系统中关闭删除

- 一些专业工具或大多数商业的漏洞扫描程序都能检测到系统是否被用作DDoS服务器
  - **Find_DDoS:** TFN2K,Trinoo,Stacheldraht
  - **SARA**(安全审计调查助理)
  - **DDoSPing v2.0**：Wintrinoo，Trinoo，Stacheldraht，TFN
  - **RID**：TFN, TFN2K,Trinoo,Stacheldraht

Summary

- DoS攻击原理：
  - **Ping of Death**
  - **泪滴（Teardrop）**
  - **UDP泛洪**
  - **SYN泛洪**
  - Land攻击
  - **Smurf攻击**
  - Fraggle攻击
  - 畸形消息攻击
  - Slashdot effect
  - WinNuke攻击
- **DDoS攻击原理**
- DoS/DDoS的防御