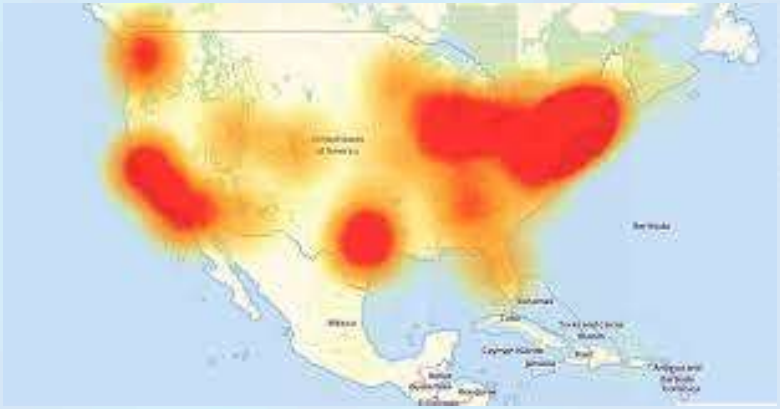
网 络 安 全

——拒绝服务攻击与防御

杭州师范大学信息科学与技术学院

刘雪娇　邮箱：liuxuejiao0406@163.com

DDoS攻击事件



- 2016年10月21日，提供动态DNS服务的Dyn DNS遭到大规模DDoS攻击，此次攻击导致许多使用DynDNS服务的网站遭遇访问问题，其中包括GitHub、Twitter、Airbnb、Reddit等，美国大半个互联网下线。
- 2020年8月9日，白俄罗斯国家安全委员会与内务部网站所在设备遭到DDoS攻击，直接影响其总统选举。
- 2020年8月27日，新西兰证券交易所（NZX）再次发生崩溃，交易所股价和指数报价无法获取，该交易所多次遭受分布式拒绝服务(DDoS)攻击，被迫短时中断交易，其网站和市场公告平台也受到影响。

第九章 拒绝服务攻击

拒绝服务攻击概述

- 拒绝服务（Deny of Service,DoS）

  网络信息系统由于某种原因不能为授权用户提供正常服务。

- 拒绝服务攻击

  - 造成DoS的攻击行为被称为DoS攻击，是指阻止或者拒绝合法使用者存取网络服务器的一种破坏性攻击方式。
  - 拒绝服务的攻击降低了资源的可用性，这些资源可以是处理器、磁盘空间、CPU使用的时间、打印机、调制解调器，甚至是系统管理员的时间，攻击的结果是减少或失去服务。

DoS攻击类型

- 按照DoS攻击行为可分为**网络带宽攻击**和**连通性攻击**。
- 通过消耗掉主机资源和网络带宽资源使主机或网络无法正常提供服务的攻击手段。

- **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。
- **基于系统缺陷型** 攻击者利用目标系统和通信协议的漏洞实现拒绝服务攻击

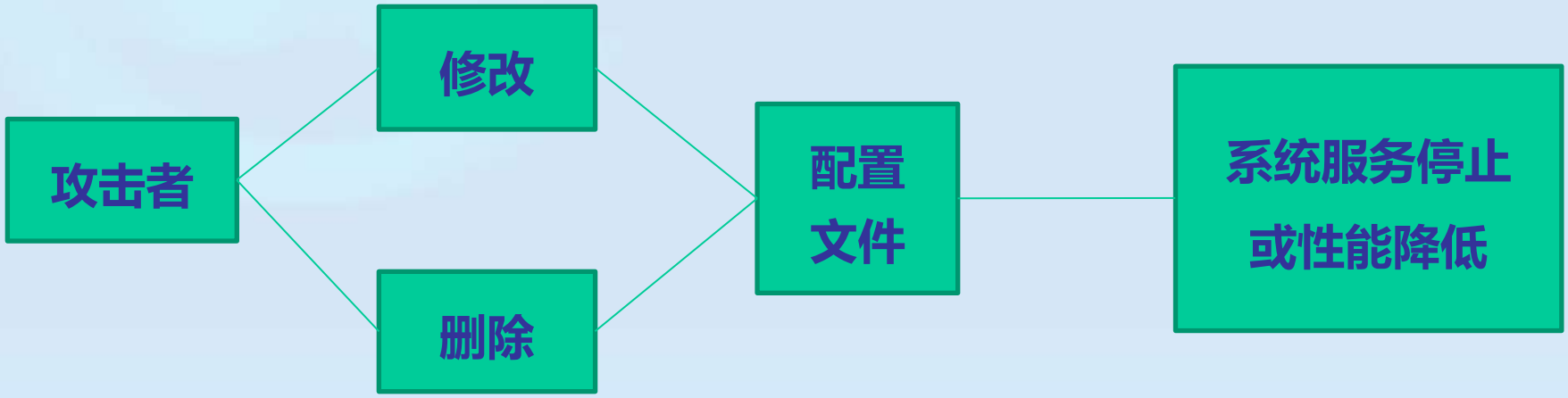
DoS攻击模式

- **消耗有限的物理资源**
  - 网络连接
  - 带宽资源
  - 其他资源，如磁盘空间、进程数

- **物理部件的移除或破坏**
  - 物理设备包括：计算机、路由器、电源、冷却设备、网络配线室等

修改配置信息造成DoS

比如，修改路由器信息，造成不能访问网络；修改NT注册表，也可以关掉某些功能

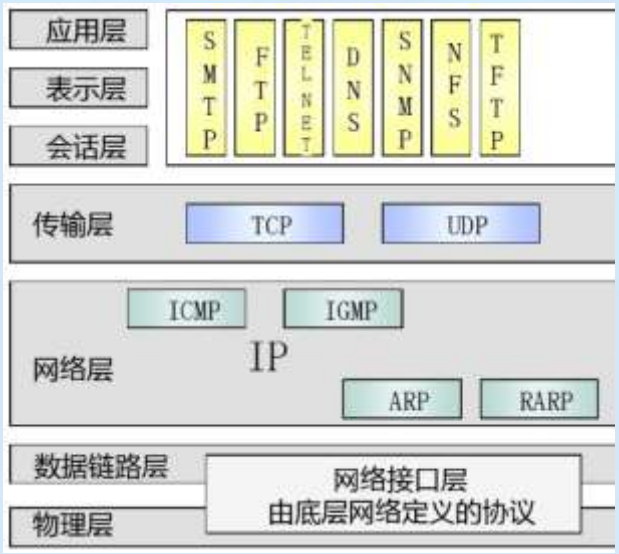


基于系统缺陷型

攻击者利用目标系统和通信协议的漏洞实现拒绝服务攻击。例如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。

拒绝服务攻击分类

- DoS攻击**按TCP/IP协议划分**有：网络层攻击、传输层攻击、应用层攻击。



- **应用层**：HTTP Flood、HTTP慢速攻击、HTTPS Flood、SSL DDoS攻击、SIP Flood
- **传输层**：SYN Flood、SYN-ACK Flood、ACK Flood、FIN/RST Flood、TCP连接耗尽攻击、UDP Flood（包括各种反射攻击）、TCP/UDP分片报文攻击、其余各种与TCP、UDP报文和端口相关的攻击
- **网络层**：IP地址扫描攻击、大部分特殊控制报文攻击、Teardrop攻击、Smurf攻击、IP分片报文攻击、ICMP Flood攻击；

拒绝服务攻击分类

DoS攻击按**攻击方式**划分有：

- **泛洪攻击(Flooding)**：攻击者通过僵尸网络、代理或直接向攻击目标发送大量伪装的请求服务报文，最终耗尽攻击目标资源。发送的大量报文可以是TCP的SYN和ACK报文、UDP报文、ICMP报文、DNS报文、HTTP/HTTPS报文等。
- **畸形报文攻击(Malformation)**：攻击者发送大量有缺陷或特殊控制作用的报文，从而造成主机或服务器在处理这类报文时系统崩溃。畸形报文攻击例如Smurf、Land、Fraggle、Teardrop、WinNuke攻击等。特殊控制报文攻击包括超大ICMP报文、ICMP重定向报文、ICMP不可达报文和各种带选项的IP报文攻击。
- **扫描探测类攻击(Scan&Probe)**：是一种潜在的攻击行为，并不具备直接的破坏行为，通常是攻击者发动真正攻击前的网络探测行为，例如IP地址扫描和端口扫描等。

如何实现

- 通过构造有针对性的、最为消耗服务器端资源的业务请求，让服务器“劳累过度”而停止服务。
- 例如计算的缓存空间
- 访问IO通道数量
- 读写数据库操作
- 磁盘读写操作
- ……

典型的拒绝服务攻击

- 死亡之Ping（Ping of Death）
- 泪滴（Teardrop）
- 泛洪类（ Flooding）
  - UDP泛洪
  - SYN泛洪
  - ACK泛洪
  - Connection泛洪
  - HTTP Get 泛洪
- 利用ICMP协议攻击
- Land攻击
- Smurf攻击
- Fraggle攻击
- 畸形消息攻击
- Slashdot effect
- WinNuke攻击

DoS工具

每一种攻击被揭示出来的时候，都会有一些试验性的代码，例如teardrop.c、synflood.c等，DoS攻击往往比较简单，代码也比较短小。通常，要涉及到IP欺骗

■一些现有的工具

- **Targa：**把几种DoS集中在一起
- **Trinoo：**分布式DoS工具
- **TFN2K：**Targa的增强，可实施DDoS攻击
- **stacheldraht**

泪滴（TearDrop）

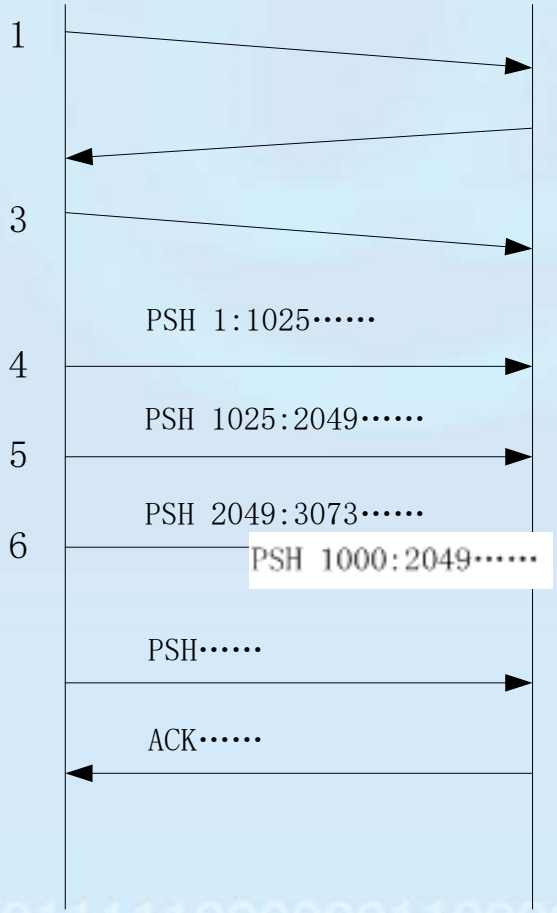
- **泪滴（分片攻击，Teardrop）：利用TCP/IP协议缺陷，首个实现攻击的程序名为Teardrop**
  - ✓ 如果传输的数据无法在一个报文中传输完成，就会被分片，传送到目标主机后再到堆栈中进行重组，该过程称为“分片”
  - ✓ 为能进行数据重组，TCP首部包含——分片识别号、偏移量、数据长度、标志位，目标主机据此将各分片重组还原。

- **概览：IP数据包在网络传递时，数据包可以分成更小的片段。攻击者可以通过发送两段(或者更多)数据包来实现TearDrop攻击。第一个包的偏移量为0，长度为N，第二个包的偏移量小于N。为了合并这些数据段，TCP/IP堆栈会分配超乎寻常的巨大资源，从而造成系统资源的缺乏甚至机器的重新启动。**

泪滴（TearDrop）

- **原理：**向被攻击者发送多个分片的IP包，某些操作系统收到含有重叠偏移的伪造分片数据包时将会出现系统崩溃、重启等现象。
- **受影响的系统：**Linux/Windows NT/95，97年发现
- **攻击特征：**攻击非常简单，发送一些IP分片异常的数据包
- **检测方法：**对接收到的分片数据包进行分析，计算数据包的片偏移量（Offset）是否有误。
- **防御方法：**添加系统补丁程序，丢弃收到的病态分片数据包并对这种攻击进行审计。尽可能采用最新的操作系统，或在防火墙上设置分段重组。

泪滴（TearDrop）



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

ICMP协议漏洞

- **死Ping攻击：**ICMP数据包的尺寸超过64KB上限时，主机就会出现内存分配错误，导致TCP/IP堆栈崩溃，致使主机死机。
- **ICMP Ping淹没攻击：**大量的Ping信息广播淹没目标系统，使得它不能够对合法的通信作出响应。
- **ICMP nuke攻击：**也称为核弹攻击，是指发送目标操作系统无法处理的信息数据包，从而导致该系统瘫痪。
- **通过ICMP进行攻击信息收集**

ICMP协议漏洞

- **ICMP重定向攻击：**

重定向：若路由器收到一个数据报，并发现该数据报存在一个比自己更好的下一跳路由，就会向主机发送重定向报文，让其更新转发表。

由于缺乏合法性检查，黑客通过发送ICMP重定向信息给被攻击的主机，让该主机按照黑客的要求来修改路由表，使得该主机在发送数据包时，都会被黑客获取，进一步实现中间人攻击或者DOS攻击。。

- **ICMP数据包放大：**

攻击者向安全薄弱网络所广播的地址发送伪造的ICMP响应数据包，网络上的所有系统都会向受害计算机系统发送ICMP响应的答复信息，占用了目标系统的可用带宽并导致合法通信的服务拒绝。如Smurf攻击。

Ping of Death

- **原理：**直接利用Ping包，即ICMP Echo包，有些系统在收到大量比最大包还要长的数据包，会挂起或者死机
- **攻击：**直接利用Ping工具，发送超大的Ping数据包，该攻击数据包大于65535个字节。由于部分操作系统接收到长度大于65535字节的数据包时，就会造成**内存溢出**、系统崩溃、重启、内核失败等后果。
- **受影响的系统：**许多操作系统受影响
- **防止措施：**使用新的补丁程序，当收到大于65535个字节的数据包时，丢弃该数据包，并进行系统审计。

“**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。
```

应对ICMP攻击

Ping淹没攻击攻击的**防范方法：**

- 在**路由器**上对ICMP数据包进行**带宽限制**，将ICMP占用的带宽控制在一定的范围内，这样即使有ICMP攻击，它所占用的带宽也是非常有限的，对整个网络的影响非常少
- 在**主机**上设置ICMP数据包的**处理规则**，最好是设定拒绝所有的ICMP数据包。

设置ICMP数据包处理规则的方法：

- 在操作系统上设置包过滤
- 在主机上安装防火墙

Smurf攻击

➢**原理：**

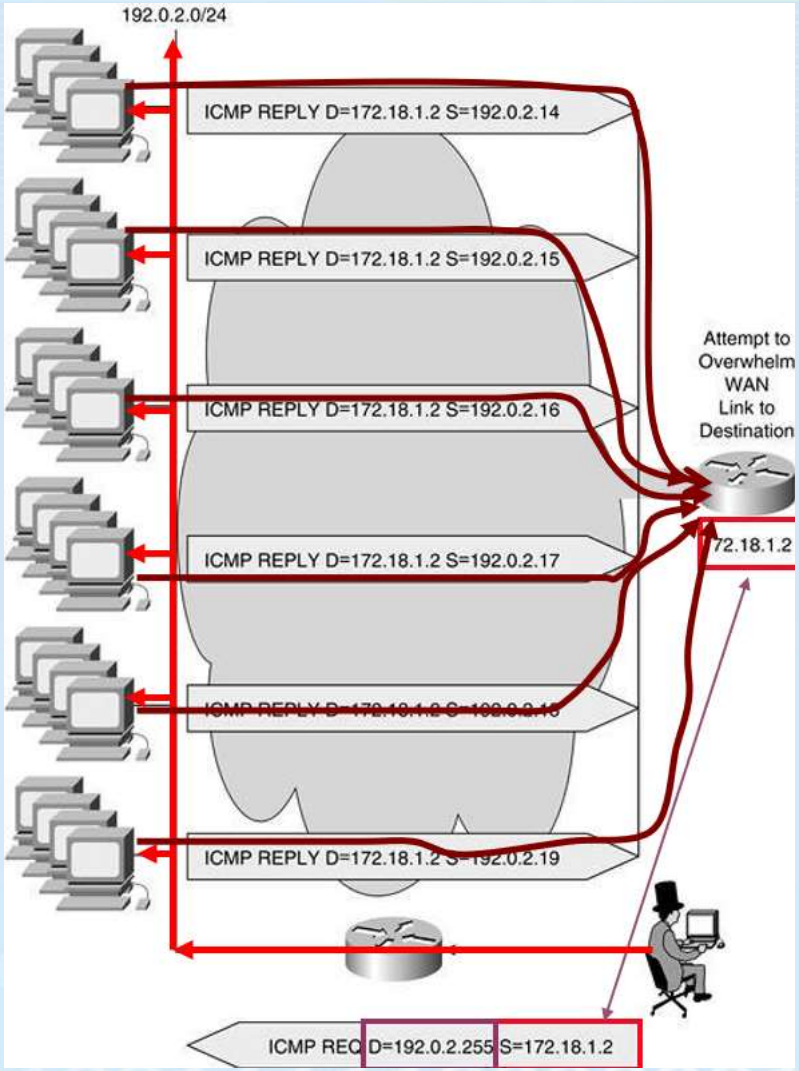
利用**IP欺骗**和**ICMP回应包**引起目标主机网络阻塞

构造数据包时，令**源地址=>被攻击主机地址**，**目的地址=>广播地址**

=> 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

➢这种攻击方式比Ping of death扩散的流量高出1～2个数量级。

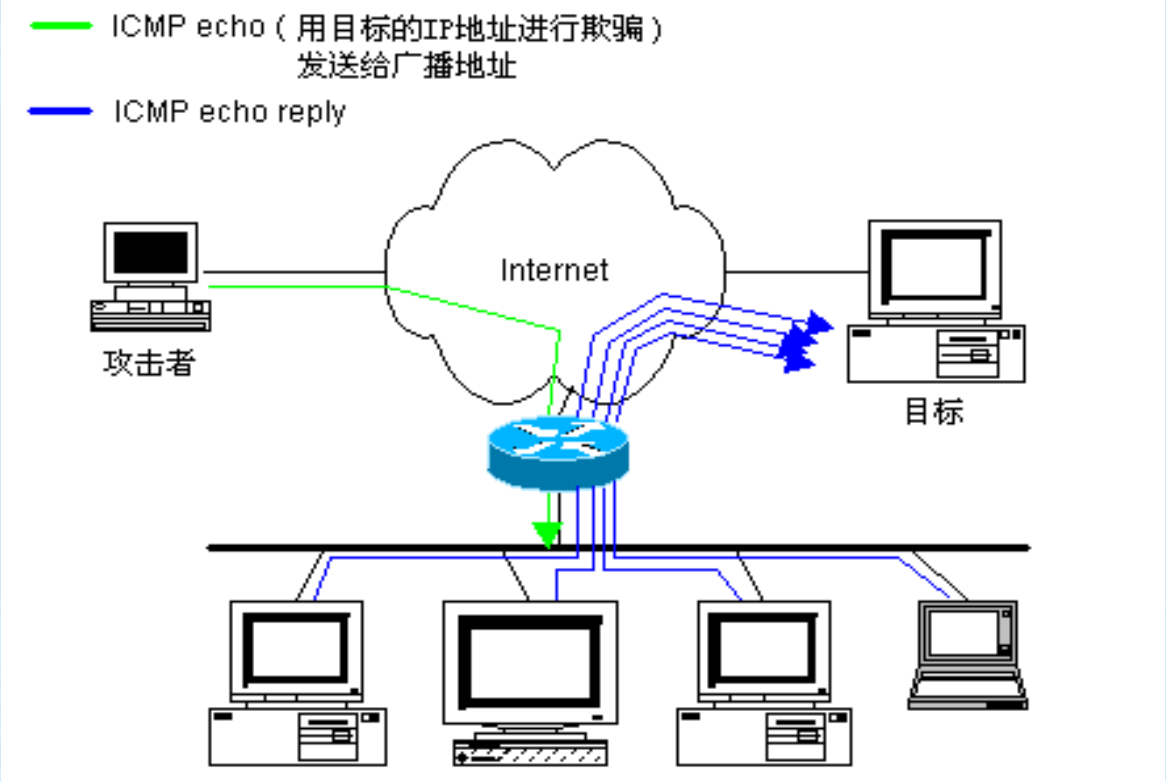
➢更复杂的Smurf攻击将源地址改为第三方的地址，导致第三方崩溃。



➢技术细节

两个主要的特点：使用**伪造的数据包**、使用**广播地址**

不仅**被伪造地址的机器**受害，**目标网**络本身也是受害者，它们要发送大量的应答数据包



Smurf攻击

- 攻击特征

涉及到三方：攻击者，中间目标网络，受害者

以较小的网络带宽资源，通过放大作用，吃掉较大带宽的受害者系统

- Smurf放大器

Smurf放大器网络：不仅允许ICMP Echo请求发给网络的广播地址，

并且允许ICMP Echo-Reply发送回去

这样的公司越多，对Internet的危害就越大

- 实施Smurf攻击

需要长期的准备，首先找到足够多的中间网络

集中向这些中间网络发出ICMP Echo包

Smurf攻击

- **Fraggle攻击（Smurf攻击变种）：**
  - ✓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

典型拒绝服务攻击技术

- **畸形消息攻击：**
  - ✓**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**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***"

典型拒绝服务攻击技术

- **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

典型拒绝服务攻击技术

- **WinNuke攻击（带外传输攻击）：**
  - ✓ 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

- **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）

Land 攻击

- **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
  - ✓ 大量此类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
  - ✓ **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

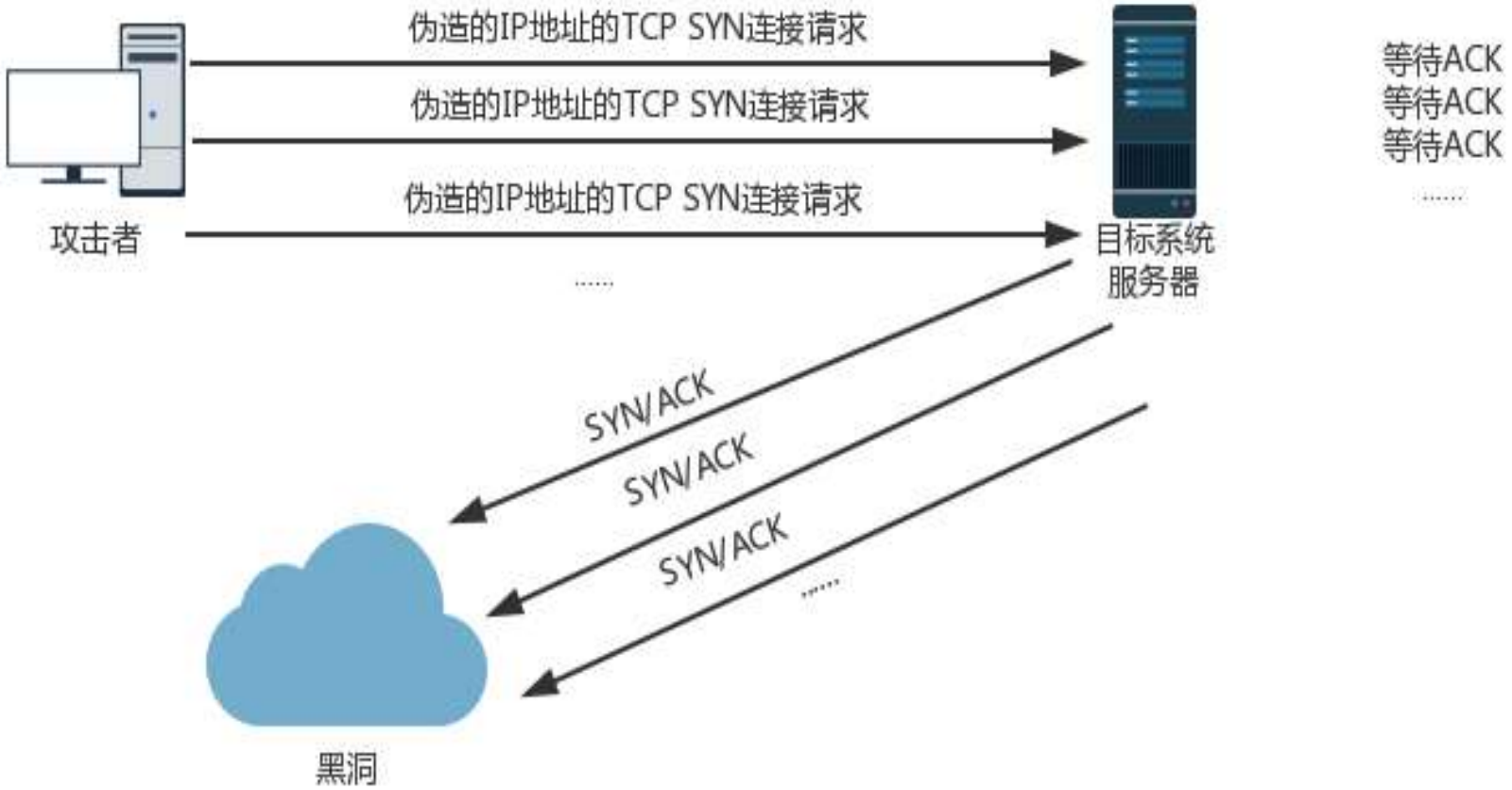
SYN泛洪攻击

- **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

SYN泛洪攻击

➢攻击过程

利用**TCP连接三次握手**过程，打开大量的**半开TCP连接**，使得目标机器不能进一步接受TCP连接。



SYN泛洪攻击

- **受影响的系统：大多数操作系统**
- **攻击细节**

(1)连接请求是正常的，但是，源IP地址往往是伪造的，并且是一台不可达的机器的IP地址，否则被伪造地址的机器会重置这些半开连接；

(2)一般，半开连接超时之后，会自动被清除，所以，攻击者的系统发出SYN包的速度要比目标机器清除半开连接的速度要快；

(3)任何连接到Internet上并提供基于TCP的网络服务，都有可能成为攻击的目标；

(4)这样的攻击很难跟踪，因为源地址往往不可信，而且不在线。

- **攻击特征**

目标主机的网络上出现大量的SYN包，而没有相应的应答包

SYN包的源地址可能是伪造的，甚至无规律可循

SYN泛洪攻击

➢防范措施

SYN泛洪较难防御，以下是几种缓解方法：

- ✓**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**

SYN泛洪攻击

- **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

SYN泛洪攻击

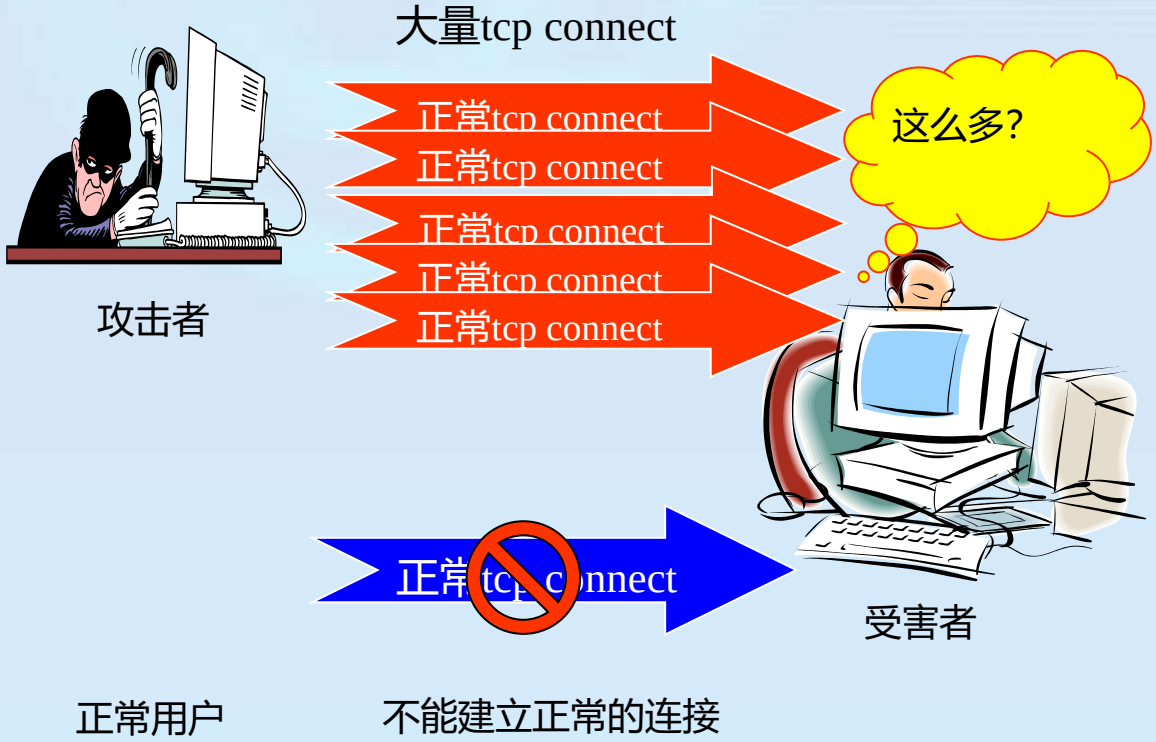
ACK Flood 攻击原理

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

SYN泛洪攻击

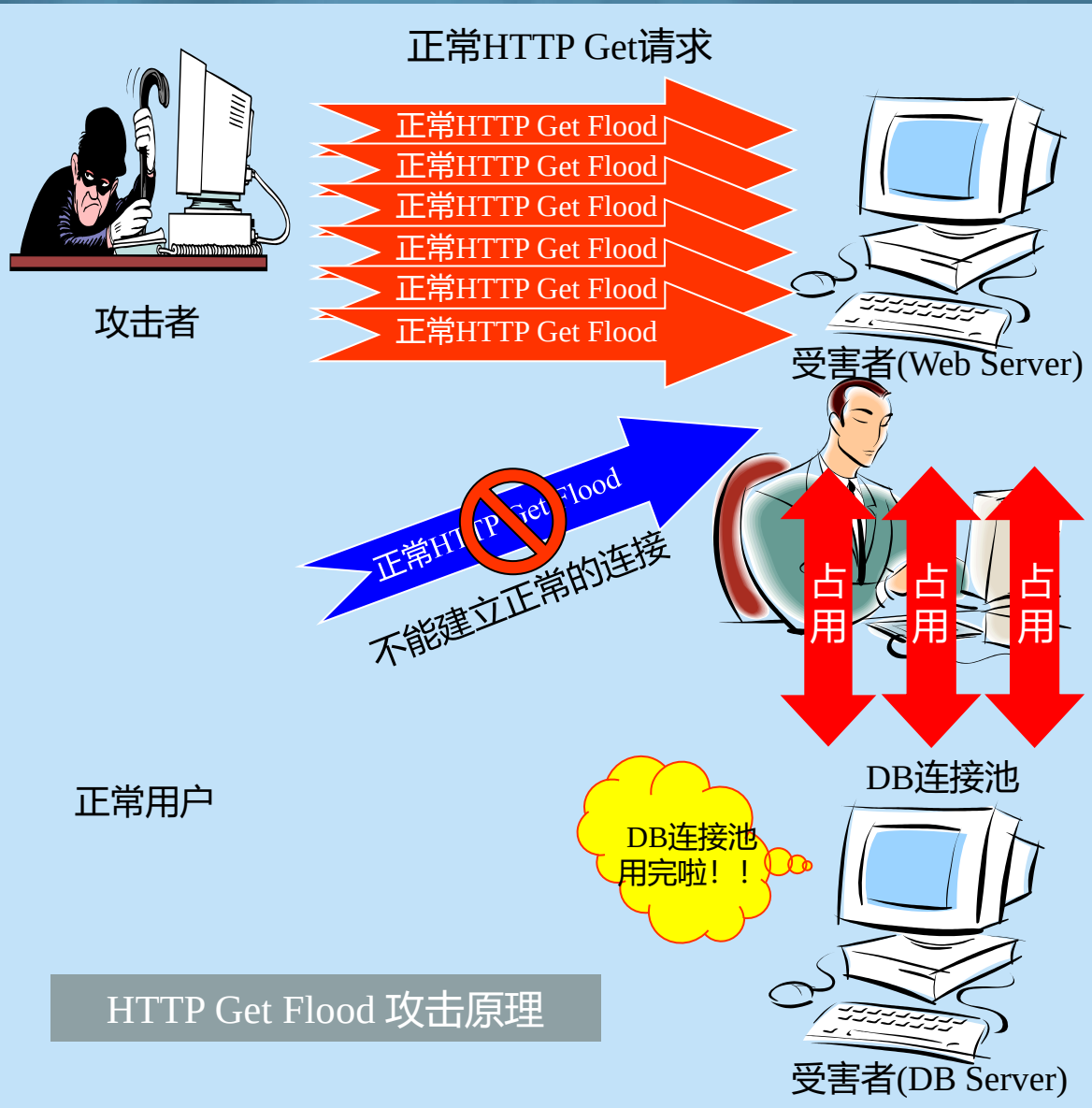
Connection Flood 攻击原理



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

SYN泛洪攻击



HTTP Get Flood 攻击原理

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

分布式拒绝服务攻击

概述：

一种基于DoS的特殊形式的拒绝服务攻击，是一种分布的，协作的大规模攻击方式，主要瞄准比较大的站点，例如商业公司、搜索引擎和政府部门的站点。

原理：

DDoS攻击手段是在传统的DoS攻击基础之上产生的一类攻击方式，DDoS就是利用更多的网络上的傀儡机来发起进攻，以比从前更大的规模来进攻受害者。

分布式拒绝服务攻击

- **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

分布式拒绝服务攻击（DDoS）

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）：**

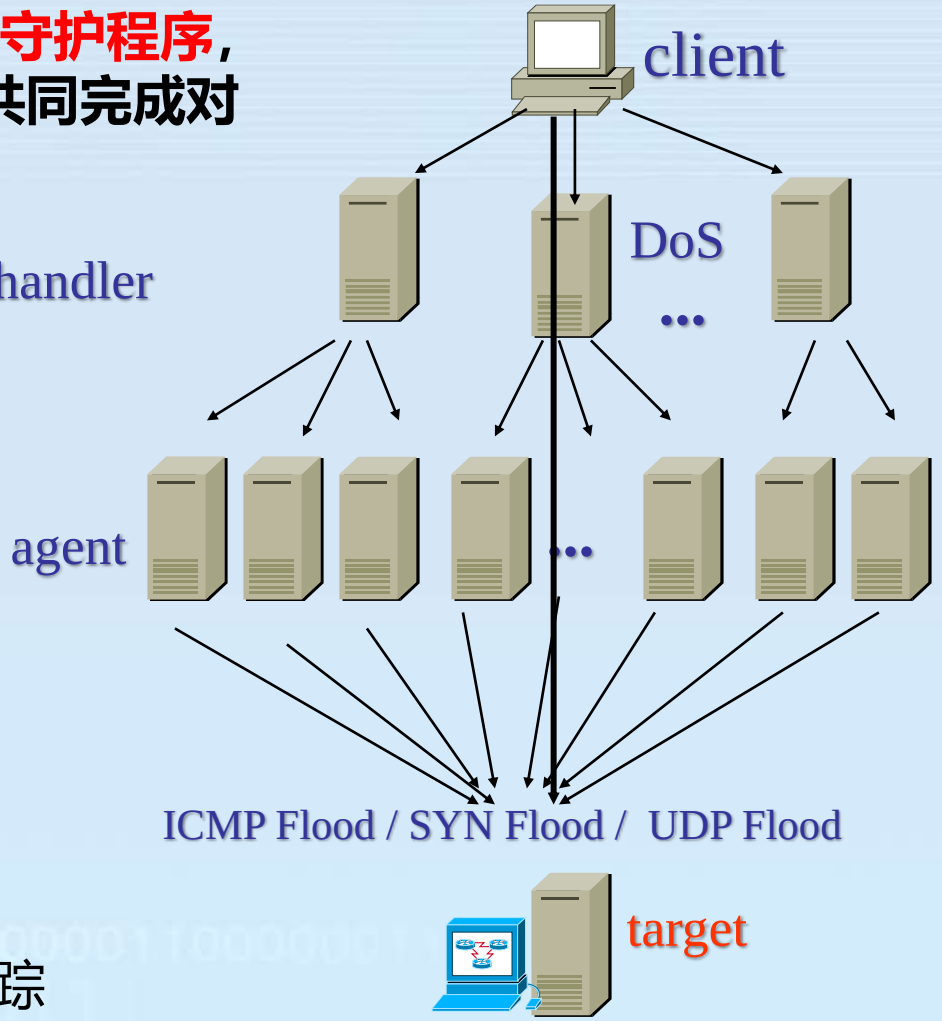
发起攻击的主机

- **（攻击）服务端：**

接受客户端发来的控制命令

- **守护程序（攻击器、攻击代理）：**

直接（如SYN Flooding）或间接（如反射式DDoS）与攻击目标进行通信



- 以破坏系统或网络的可用性为目标
- 难以防范
- 伪造源地址，流量加密，因此难以跟踪

分布式拒绝服务攻击（DDoS）

➢**步骤：**

攻击过程主要有两个步骤：攻占代理主机和向目标发起攻击。

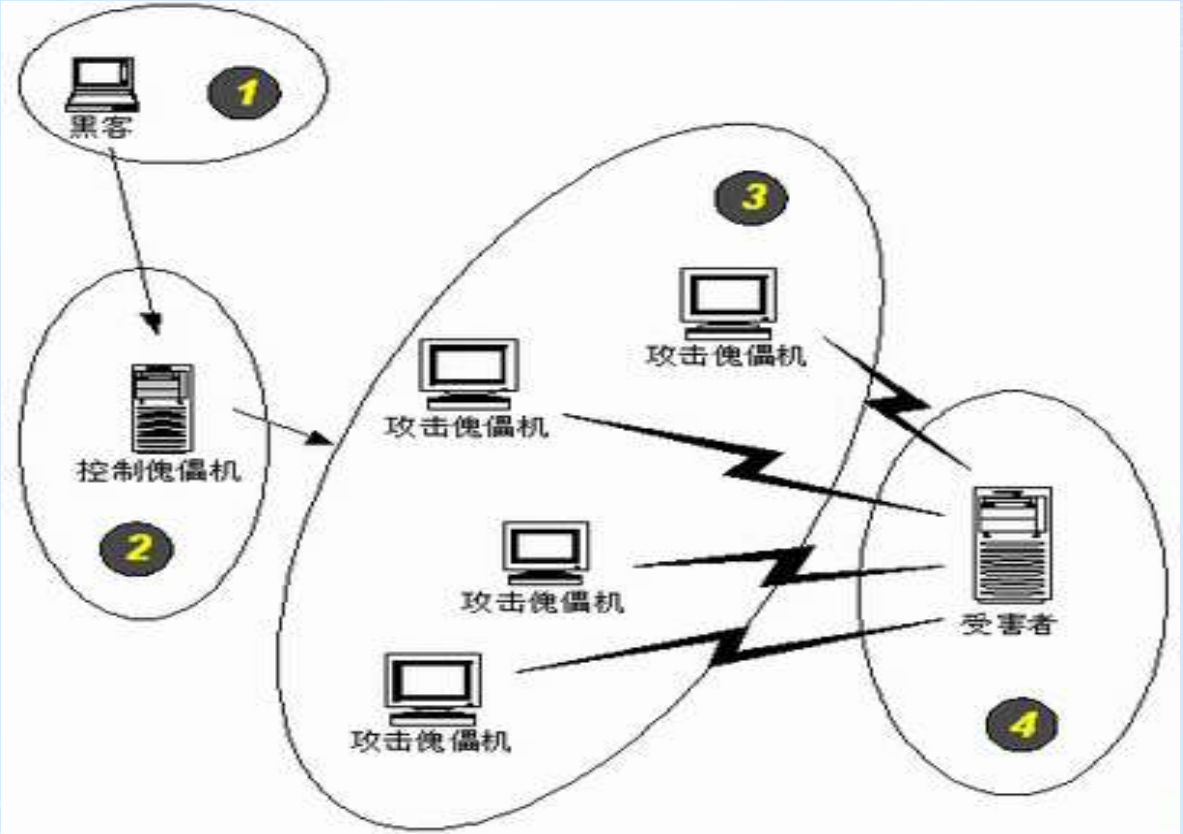
具体步骤：

探测扫描大量主机以寻找可入侵主机目标

入侵有安全漏洞的主机并获得控制权

在每台入侵主机中安装攻击程序

利用已入侵主机继续进行扫描和入侵



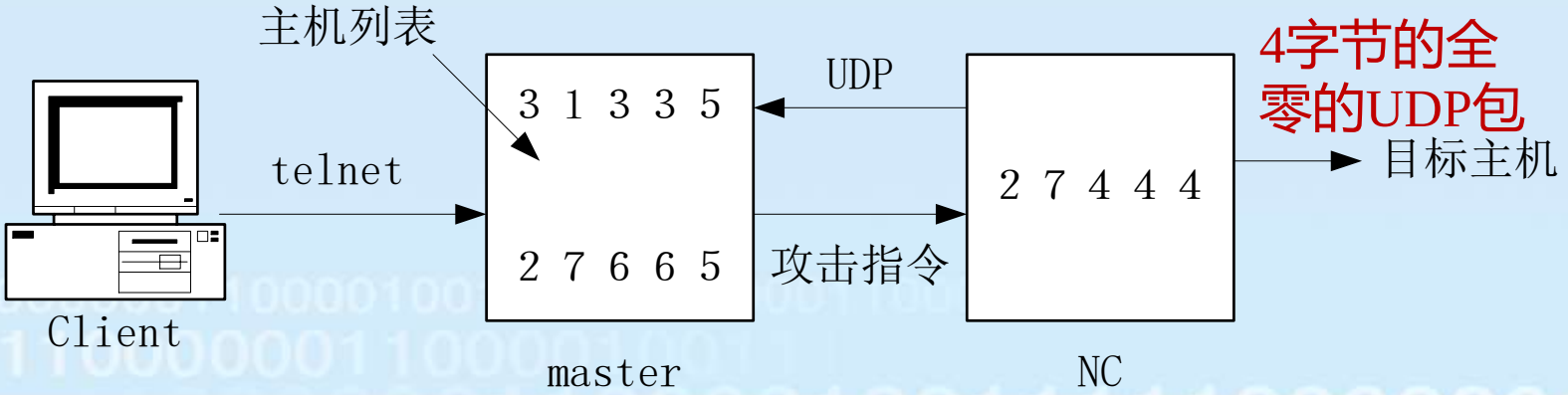
图一　分布式拒绝服务攻击体系结构

分布式拒绝服务攻击（DDoS）

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

- 所有连接都需要口令（编译时指定），缺省情况，服务端master连接守护进程NC的口令是“144adsl”，客户端Client连接master的口令是“betaalmostdone”，且口令明文传送
- 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的工作过程



分布式拒绝服务攻击（DDoS）

- **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

分布式拒绝服务攻击（DDoS）

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Base64编码。TFN2K守护程序接收并解密数据。

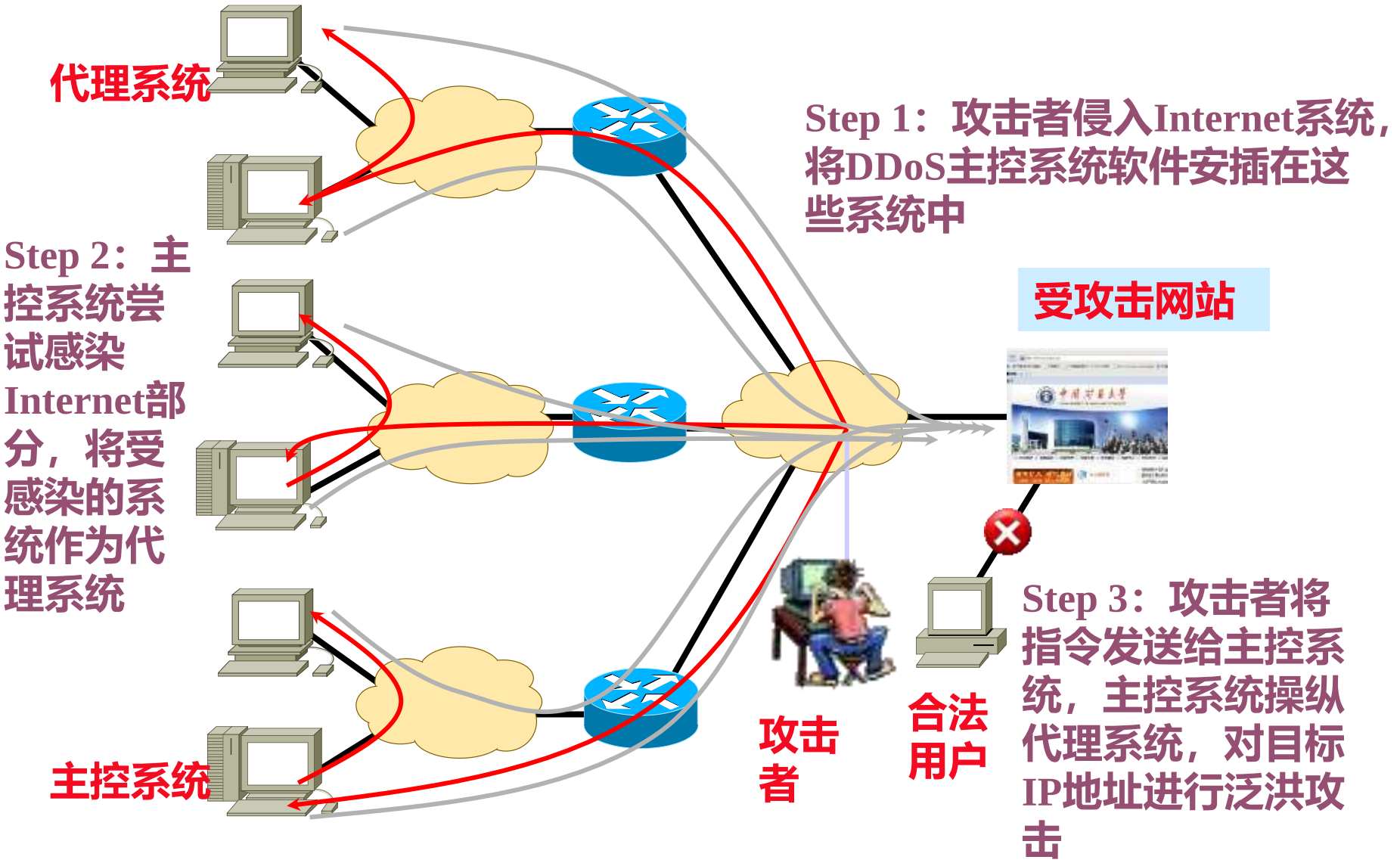
守护进程能通过修改进程名来欺骗管理员，掩饰真正身份

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

分布式拒绝服务攻击（DDoS）

- **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

分布式拒绝服务攻击（DDoS）



分布式拒绝服务攻击（DDoS）

- **特点：**

（1）严重时会造成系统死机

（2）被攻击主机上有大量等待的TCP连接

（3）网络中充斥着大量的无用的源地址为假的数据包，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

（4）利用受害主机提供的服务或传输协议上的缺陷，反复高速的发出特定的服务请求，使受害主机无法及时处理所有正常请求

DDoS攻击的分类和特点

1

带宽消耗型

攻击者利用发包机或攻击工具等手段构造大流量攻击，通过消耗带宽资源和路由过载影响网络连接。常见攻击类型有SYN flood、UDP flood和ACK flood。

2

资源消耗型

通过控制僵尸主机对目标业务和应用发起请求，模拟正常客户端行为，消耗主机资源使服务器运行缓慢或过载。常见攻击类型有HITP GET Flood和DNS Flood。

3

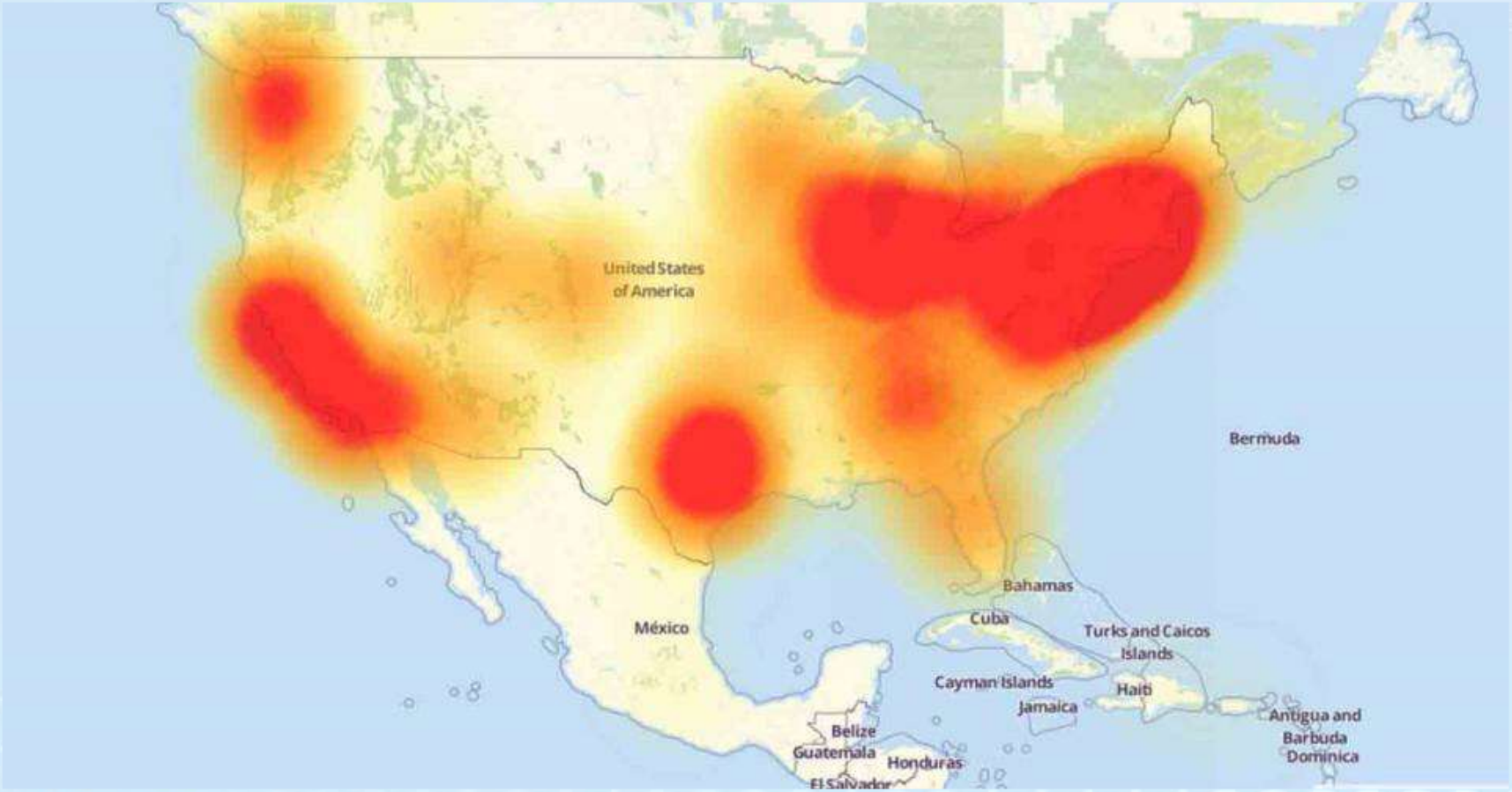
应用利用型

结合目标业务的特征发起大量请求，利用受害主机的业务逻辑缺陷造成服务器性能骤年，无法响应所有访问请求。例如在网络购物车中添加过多的产品造成异常。

带宽消耗型攻击成本低，占DDoS攻击数是的70%以上;资源消耗型攻击操作技术难度大，是攻防双方之间的绝对较量。

Mirai僵尸网络（DDoS→PDoS）

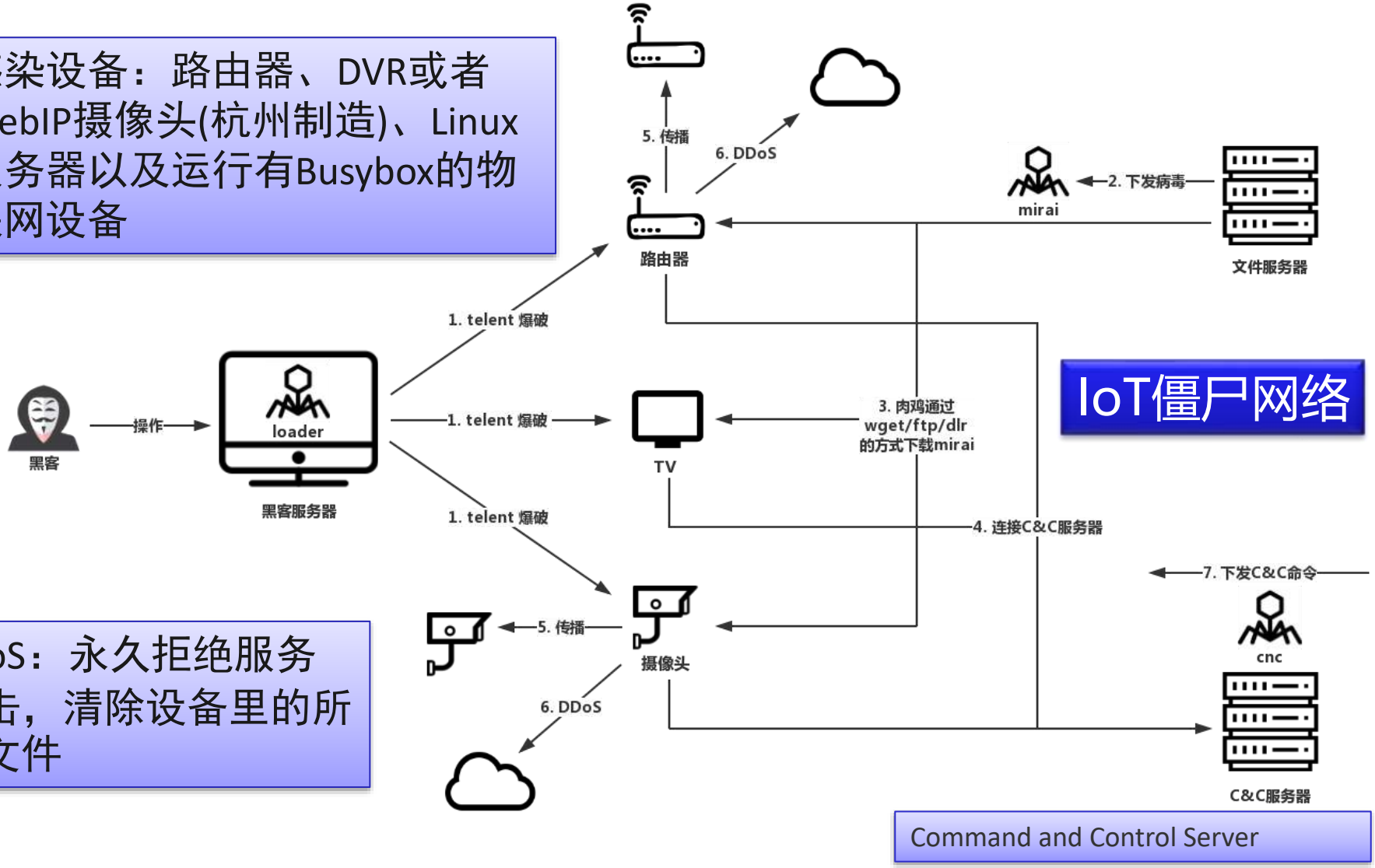
2016.10.21：美国东海岸发生世界上瘫痪面积最大（大半个美国），时间最长（6个多小时）的DDoS攻击



Mirai僵尸网络（DDoS→PDoS）

杭州师范大学
Hangzhou Normal University

感染设备：路由器、DVR或者WebIP摄像头(杭州制造)、Linux服务器以及运行有Busybox的物联网设备



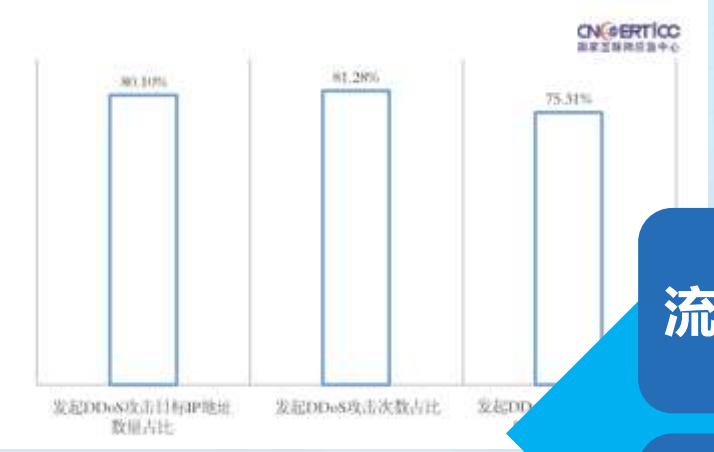
PDoS：永久拒绝服务攻击，清除设备里的所有文件

Mirai僵尸网络（DDoS→PDoS）

- **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

DDoS攻击的发展趋势

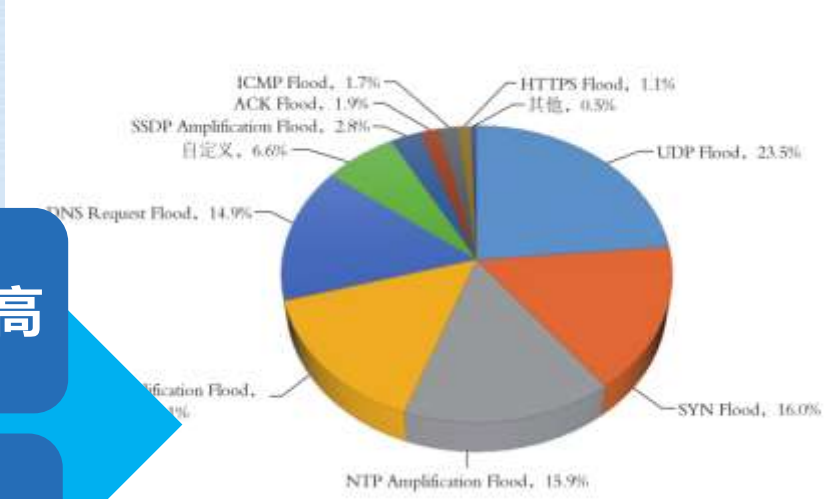


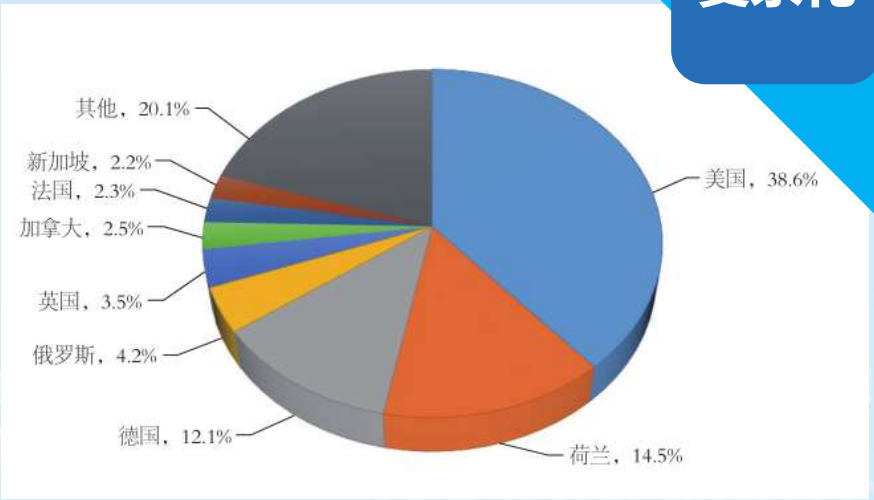
流量大

频次高

复杂化

产业化





分布反射式拒绝服务（DrDoS）

概述：

分布反射式拒绝服务攻击是DDoS攻击的变形，它与DDoS的不同之处就是DrDoS不需要在攻击之前占领大量的“肉鸡”

原理：

黑客利用特殊的发包工具，把伪造了源地址的SYN连接请求包发送到那些被欺骗的计算机上，根据TCP三次握手的规则，这些计算机会向源IP发出SYN+ACK或RST包来响应这个请求。同Smurf攻击一样，黑客所发送的请求包的源IP地址是被攻击主机的地址，这样受欺骗的主机就都会把回应发到被攻击主机处，造成被攻击主机忙于处理这些回应而瘫痪

分布反射式拒绝服务（DrDoS）

■ 特点：

（1）隐蔽性强

伪造IP包源地址是真实的

（2）难度低

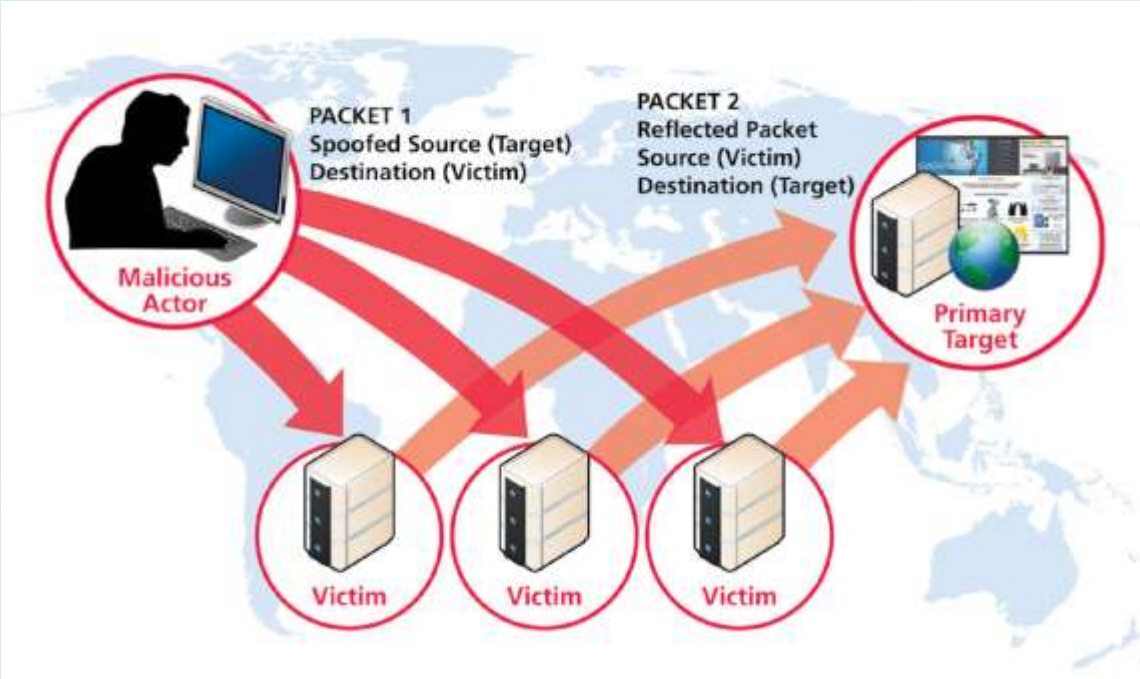
更容易找到反弹服务器

（3）力度大

目标响应会使数据流量大大增加

（4）较难阻止

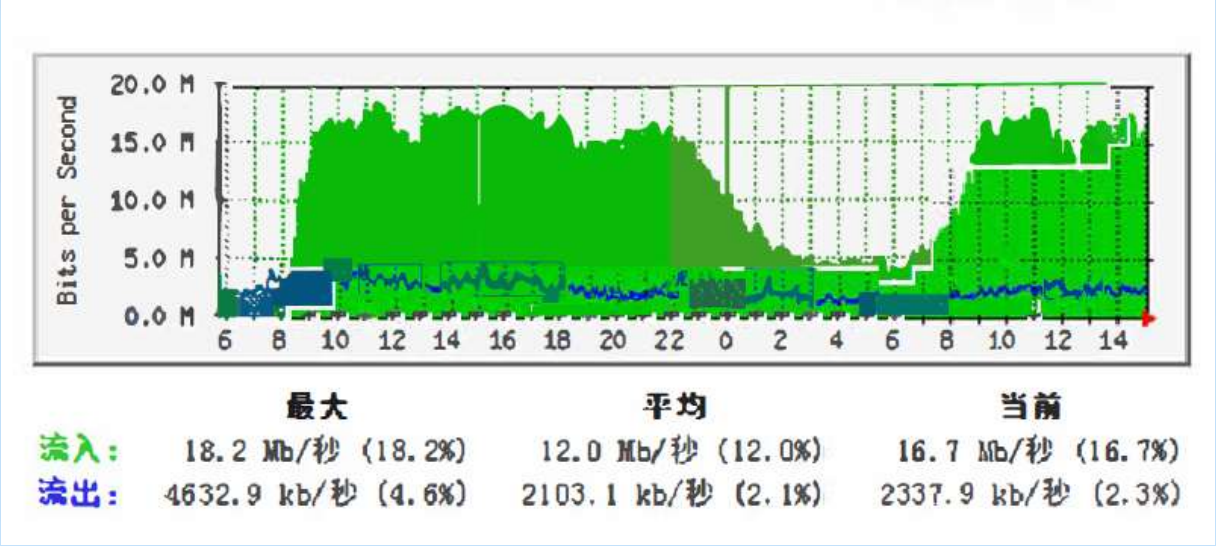
反弹服务是开放的



9.4 拒绝服务攻击的检测与防御

- **拒绝服务攻击的检测：**
- **基于sniffer的流量检测**

1）对称的TCP流
2）报文的相关度
3）流量统计特征
4）IP历史数据



- **连接特征检测**

  任何黑客的攻击都可以视为：一系列动作的组合，在网上表现为一系列数据包的攻击组合。

拒绝服务攻击特征库

- 报文的内容特征
- 到达的流量特征
- 使用的端口

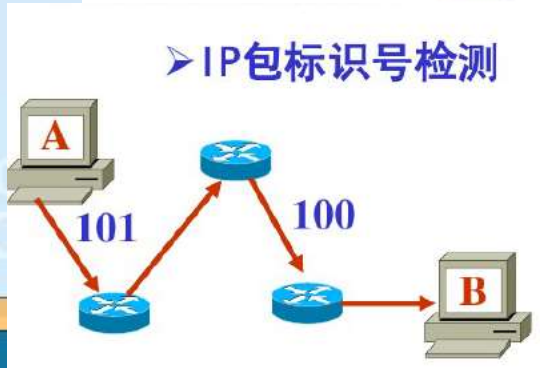
拒绝服务攻击的检测与防御

➢ 伪装数据包的检测

发动拒绝服务攻击的时候， 黑客为了隐藏自己、 摆脱跟踪、 达到以小博大的效果， 经常会伪造数据包。

1）主机服务响应时间检测

2）采用专用的检测工具， 例如经过修改的ngrep可以监听多种类型的拒绝服务攻击 (SYN flood, UDP flood, ICMP flood 和smurf) 等。



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：**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**
  - ✓**运行尽可能少的服务**
  - ✓**只允许必要的通信**
  - ✓**封锁敌意IP地址**

拒绝服务攻击的检测与防御

- **拒绝服务攻击的防御：**
- **1、源端防御。**

所谓源端防御就是阻止源主机，或者攻击主机所在的网络， 对外发送攻击数据包。

- **2、终端防御 。**

所谓终端防御是指在目标主机，或者目标网络上采取防御措施。

- **3、中端防御。**

在攻击数据报发送的途中进行阻塞和过滤。

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，BIND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。存在DDoS攻击当明显超出此极限值时就表明
  - ✓ 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

分布式拒绝服务攻击的防御

- **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:** 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**
  - ✓ **安装入侵检测系统**
  - ✓ **与ISP服务商合作（*）：** DDoS非常重要的特点是**泛洪般的网络流量**，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**

分布式拒绝服务攻击的防御

- **使用扫描工具：**
  - ✓许多公司网络安全措施进行得很慢，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