网络安全 – 拒绝服务攻击

曹越

国家网络安全学院

武汉大学

yue.cao@whu.edu.cn

上周回顾 - 1

攻击分类

- **破坏型攻击**
- **利用型攻击**
- **信息收集型攻击**
- **ICMP Flood, SYN Flood**

扫描技术

- **地址扫描**
- **端口扫描**
- **反响映射**
- **慢速扫描**
- **漏洞扫描**

攻击步骤及技巧

上周回顾 - 2

端口扫描

- **基本的TCP connect()扫描**
- **TCP SYN扫描 (半开连接扫描)**
- **TCP FIN扫描 (秘密扫描)**
- **TCP FTP Proxy扫描**
- **分片扫描**

共享/交换以太网上的监听特点及方法

口令攻击

- **字典攻击**
- **强行攻击**
- **组合攻击**

拒绝服务攻击概述

拒绝服务攻击分类

电子邮件轰炸

分布式拒绝服务攻击

反弹技术

拒绝服务攻击概述

拒绝服务攻击分类

电子邮件轰炸

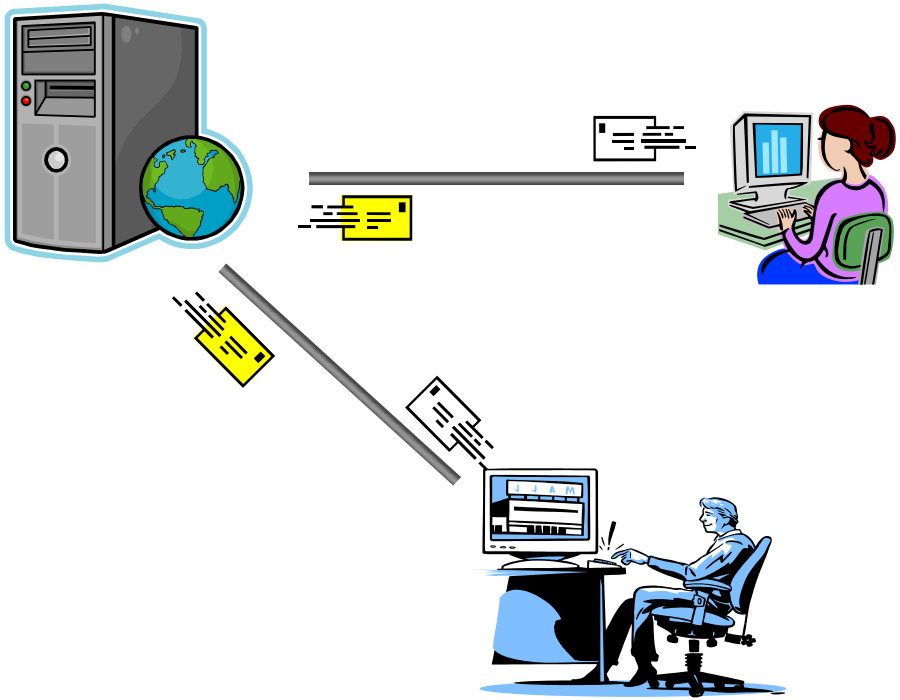
分布式拒绝服务攻击

反弹技术

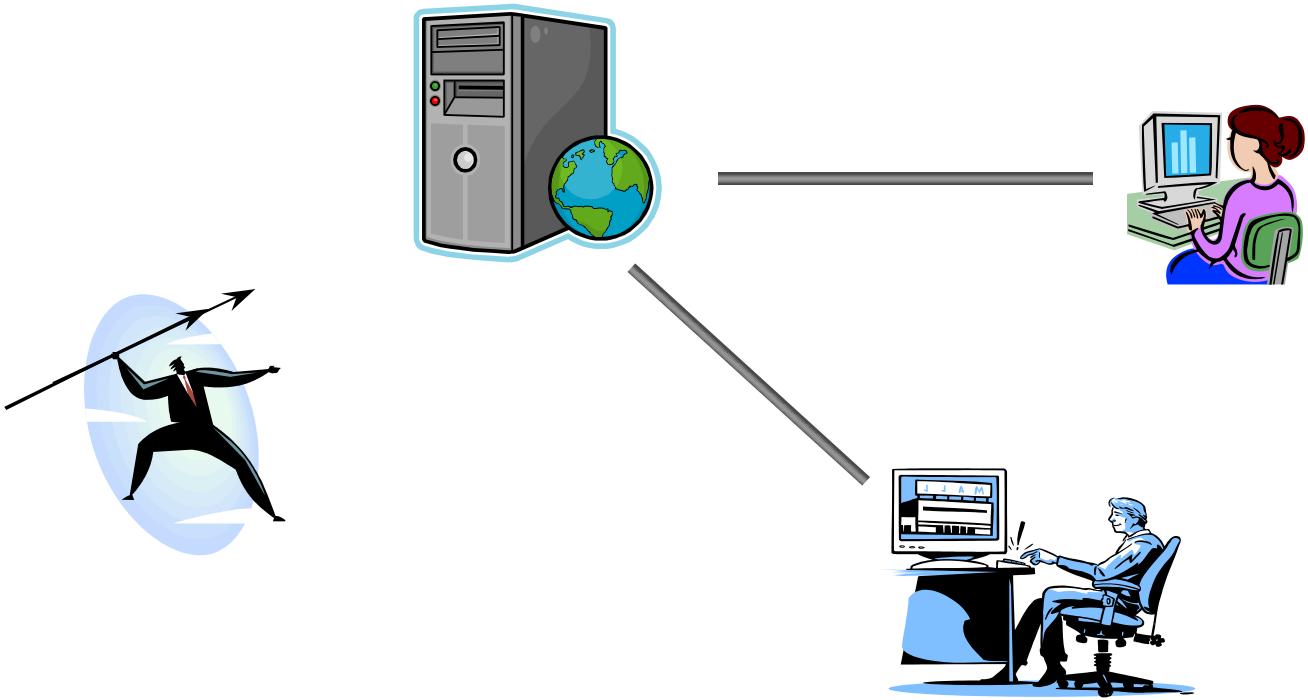
拒绝服务攻击概述 – 章节分解

1. 什么是拒绝服务攻击
2. 拒绝服务攻击定义
3. DOS相关事件
4. 拒绝服务攻击思路

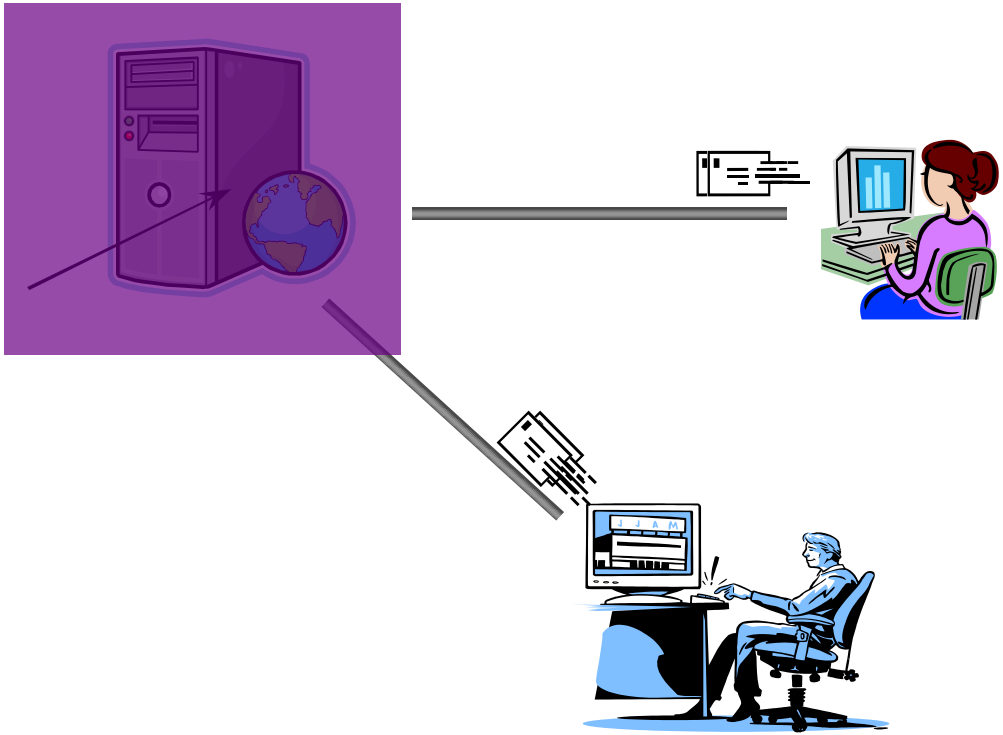
什么是拒绝服务攻击 - 1



什么是拒绝服务攻击 - 2



什么是拒绝服务攻击 - 3



拒绝服务攻击定义

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**
- **不胜负荷以至于瘫痪**
- **而无法向合法用户提供正常服务**

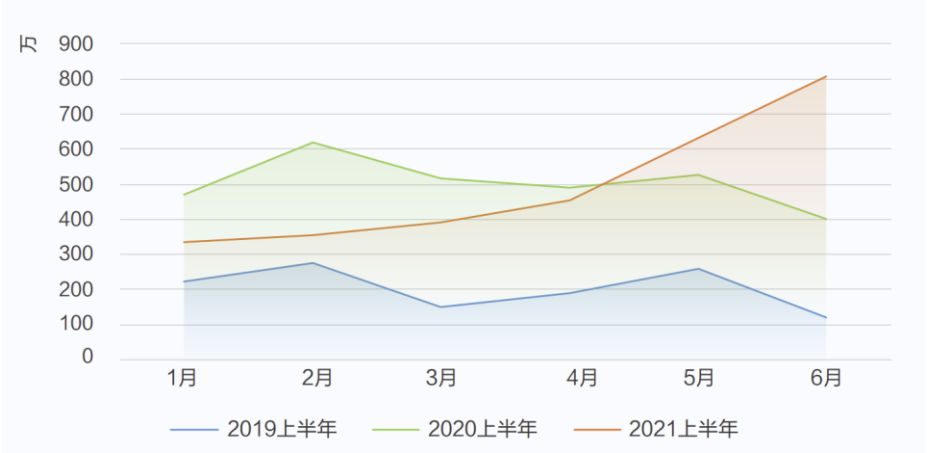
DOS相关事件 - 1

2011 年每天发生的分布式拒绝服务攻击（DDoS）事件中平均约有 7%的事件涉及到基础电信运营企业的域名系统或服务。

2011 年 7 月 15 日，域名注册服务机构三五互联DNS 服务器遭受DDoS攻击，导致其负责解析的大运会官网域名在部分地区无法解析。8月，新疆某运营商DNS服务器也连续两次遭到拒绝服务攻击，造成局部用户无法正常使用互联网。

2016年，McAfee发现首例利用安全防护不严的物联网发起的重大攻击事件。Dyn攻击是一种分布式拒绝服务（DDoS）攻击，利用物联网设备作为僵尸程序来攻击主要的DNS服务提供商。

DOS相关事件 - 2



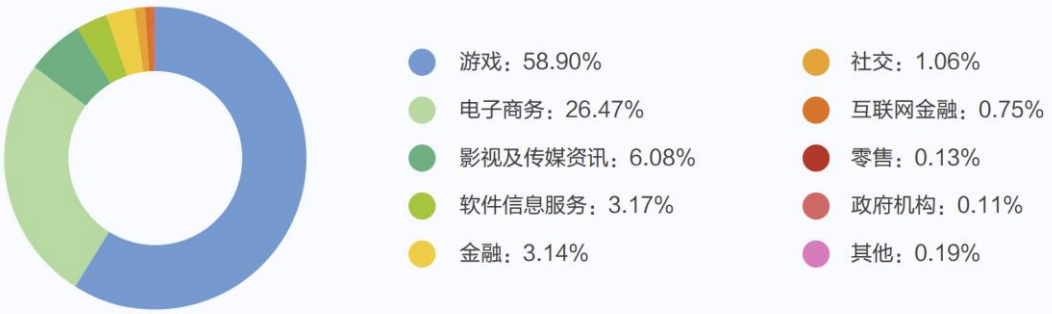


图2-3 2021上半年DDoS攻击行业分布

拒绝服务攻击思路

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

DoS攻击的实现方式

- 资源消耗、服务中止、物理破坏等

拒绝服务攻击概述

拒绝服务攻击分类

电子邮件轰炸

分布式拒绝服务攻击

反弹技术

拒绝服务攻击分类 – 章节分解

1. 拒绝服务攻击分析
2. 攻击实例-消耗网络资源
3. 攻击实例-消耗存储资源
4. 攻击实例-消耗CPU和内存资源
5. 抵御要点

拒绝服务攻击分析

针对物理破坏

- **利用管理上的脆弱性，需要加强管理措施**

对配置文件的修改和破坏

- **利用系统安装时的脆弱性，需要定期检查配置信息**

资源消耗破坏

- **设计之初没有考虑到资源会被长期占用**

服务中断攻击

- **编译阶段脆弱性引起的系统死循环**

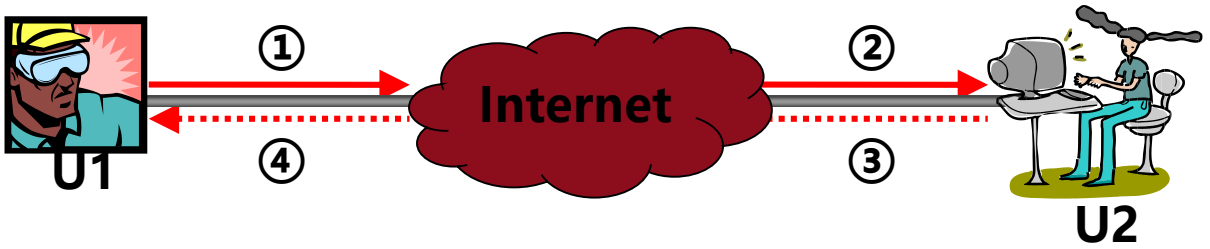
攻击实例 – 消耗网络资源 1

消耗网络资源 

——Smurf 攻击

ICMP示范

包类型：ICMP request
目标地址： U2
源地址：U1



U2在线

包类型：ICMP reply
目标地址： U1
源地址： U2

攻击实例 - 消耗网络资源 2

消耗网络资源 

——Smurf 攻击

攻击示范

Hacker

包类型：ICMP request
目标地址：广播
源地址：Victim

①

Internet

②

③

④

③

④

③

⑤

⑥

Victim

包类型：ICMP reply
目标地址： Victim
源地址： xxxx

攻击实例 – 消耗网络资源 3

消耗网络资源 

——Smurf 攻击(应对)

阻断虚假源地址

Internet

求助ISP, 阻断某IP网段

阻断WAN广播包

攻击实例 – ACK Flood 1

ACK Flood攻击是指攻击者通过僵尸网络向目标服务器发送大量的ACK报文

报文带有超大载荷引起链路拥塞，或者是极高速率的变源变端口的请求导致转发的设备异常从而引起网络瘫痪，或者是消耗服务器处理性能，从而使被攻击服务器拒绝正常服务。

攻击实例 – ACK Flood 2

主机在接收到一个带有ACK标志位的数据包的时候，需要检查该数据包所表示的连接四元组是否存在。

- 如果检查数据包状态合法，然后再向应用层传递该数据包。
- 如果检查数据包不合法，例如该数据包所指向的目的端口在本机并未开放，则回应RST包，告诉对方此端口不存在。

当发包速率很大的时候，主机操作系统将耗费大量的精力接收报文、判断状态，同时要主动回应RST报文，正常的数据包就可能无法得到及时的处理。

其他消耗网络资源攻击

TCP SYN攻击

- 优化系统配置（反馈时间）
- 优化路由配置（丢弃外网IP）
- 完善基础设施（追踪源IP）

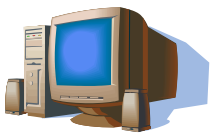
ACK Flood攻击

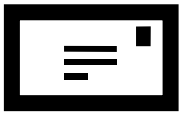
- 检查中发现该数据包不合法，例如该数据包所指向的目的本机端口并未开放，则主机操作系统协议栈会回应RST包告诉对方此端口不存在。
- 查表和回应
- 僵尸主机多的话怎么办?

攻击实例 – 消耗存储资源 1

——TearDrop攻击

文件传输示范





攻击实例 – 消耗存储资源 2

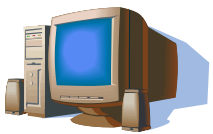
——TearDrop攻击

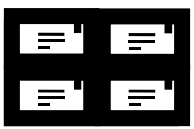
文件传输示范

攻击实例 – 消耗存储资源 3

——TearDrop攻击

文件传输示范





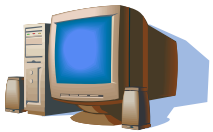
0→19　20→39

40→59　60→79

攻击实例 – 消耗存储资源 4

——TearDrop攻击

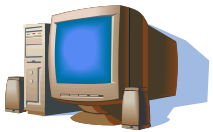
文件传输示范

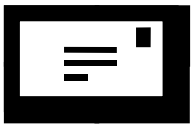


攻击实例 – 消耗存储资源 4

——TearDrop攻击

文件传输示范





0→39

20→39

0→19

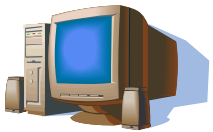
40→59

60→79

攻击实例 – 消耗存储资源 5

——TearDrop攻击

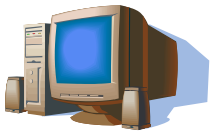
攻击示范



攻击实例 – 消耗存储资源 6

——TearDrop攻击

攻击示范



fp->len = end - offset;

end=39
offset=19
fp->len=20

end=18
offset=19
fp->len=-

0→19

0→

10→18

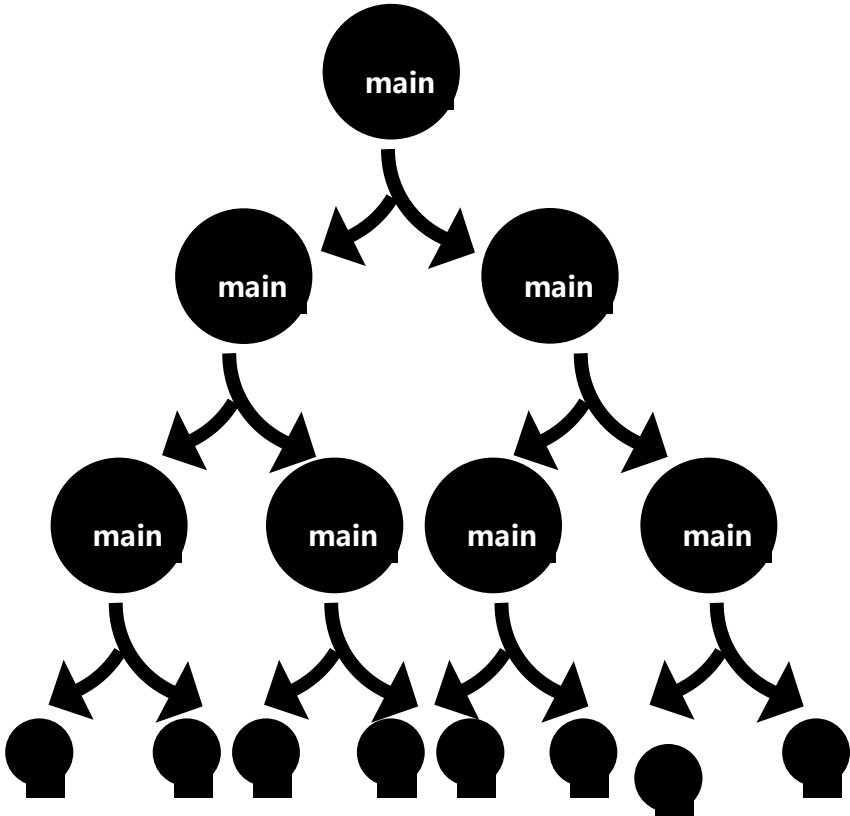
0→19

40→59

60→79

攻击实例 - 消耗CPU和内存资源

```
main()
{
        fork();
        main(
);
}
```



抵御要点

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**

拒绝服务攻击概述

拒绝服务攻击分类

电子邮件轰炸

分布式拒绝服务攻击

反弹技术

拒绝服务攻击分类 – 章节分解

1. 电子邮件轰炸 – 介绍
2. 电子邮件轰炸 – 危害
3. 电子邮件轰炸 – 应对
4. 电子邮件轰炸 – 工具

电子邮件轰炸 – 介绍

最早的一种拒绝服务攻击

- 需要占用存储空间保存邮件
- 需要占用系统资源处理邮件
- 需要占用网络资源发送邮件
- 需要占用过多系统日志空间

电子邮件轰炸 – 危害

消耗大量存储空间

溢出文件系统

加剧网络负担

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 – 应对

短时间内收到大量无用电子邮件

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

电子邮件轰炸 – 工具

常用攻击工具

- upyours4、KaBoom3、HakTek、Avalanche

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

拒绝服务攻击概述

拒绝服务攻击分类

电子邮件轰炸

分布式拒绝服务攻击

反弹技术

分布式拒绝服务攻击 – 章节分解

1. DDoS介绍
2. DDoS特点
3. DDoS攻击过程
4. DDoS攻击现象
5. DDoS攻击应对
6. DDoS攻击常用方式

DDoS介绍 1

1999年8月以来，出现了一种新的网络攻击方法，这就是分布式拒绝攻击（DDoS）

之后这种攻击方法开始大行其道，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

DDoS介绍 2

传统拒绝服务攻击的缺点

- **受网络资源的限制（攻击者本身带宽）**
- **隐蔽性差（从流量异常角度可判断大致位置）**
- **单点位置攻击**

分布式拒绝服务攻击

- **DDoS - Distributed DoS**
- **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**
- **多点位置协同攻击**

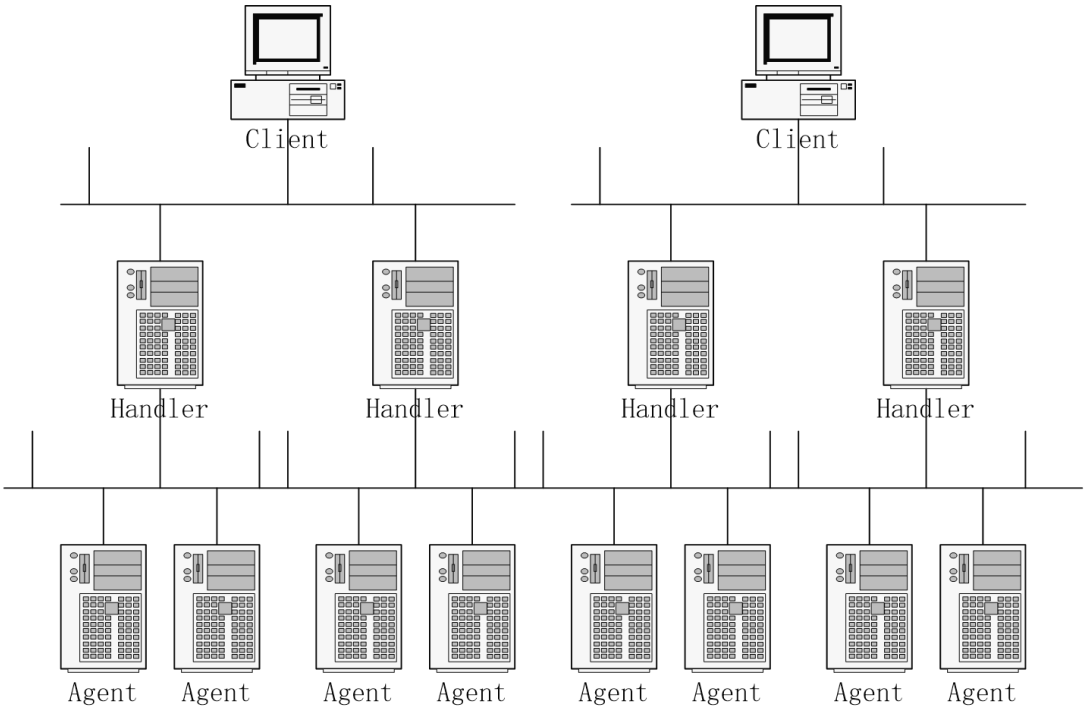
DDoS特点 - 1

由于集中了成百上千台机器同时进行攻击，其攻击力是十分巨大的。即使像Yahoo，Sina等应用了可以将负荷分摊到每个服务器的集群服务器技术，也难以抵挡这种攻击。

多层攻击网络结构使被攻击主机很难发现攻击者

而且大部分装有**主控进程**和**守护进程**的机器的合法用户并不知道自己是整个拒绝服务攻击网络中的一部分，即使被攻击主机监测到也无济于事。

DDoS特点 - 2


Client
Client
Handler
Handler
Handler
Handler
Agent
Agent
Agent
Agent
Agent
Agent
Agent
Agent

DDoS攻击过程 - 1

攻击过程主要有两个步骤：

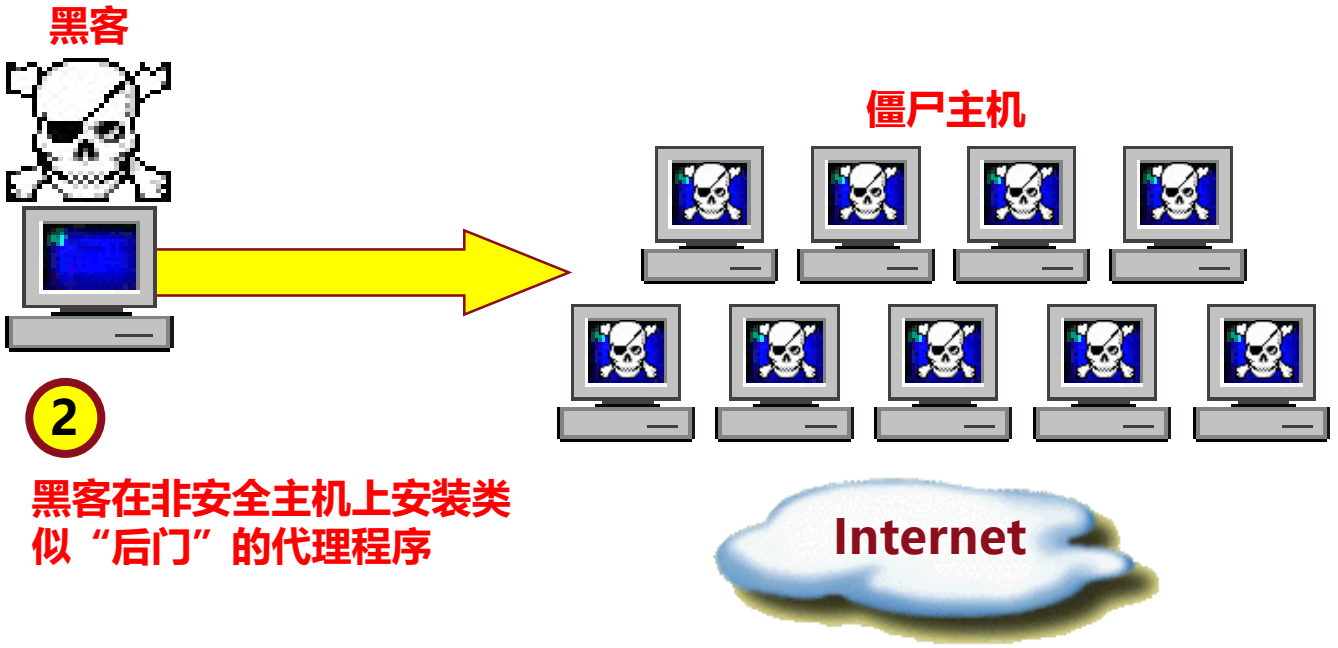
- 攻占代理主机和向目标发起攻击

具体说来可分为以下几个步骤：

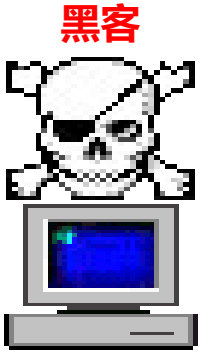
1. 探测扫描大量主机以寻找可入侵主机；
2. 入侵有安全漏洞的主机并获取控制权；
3. 在被入侵主机中安装攻击所用的主控进程或守护进程；
4. 向安装有客户进程的主控端主机发出命令，由它们来控制代理主机上的守护进程进行协同入侵。

DDoS攻击过程 - 2

DDoS攻击过程 - 3



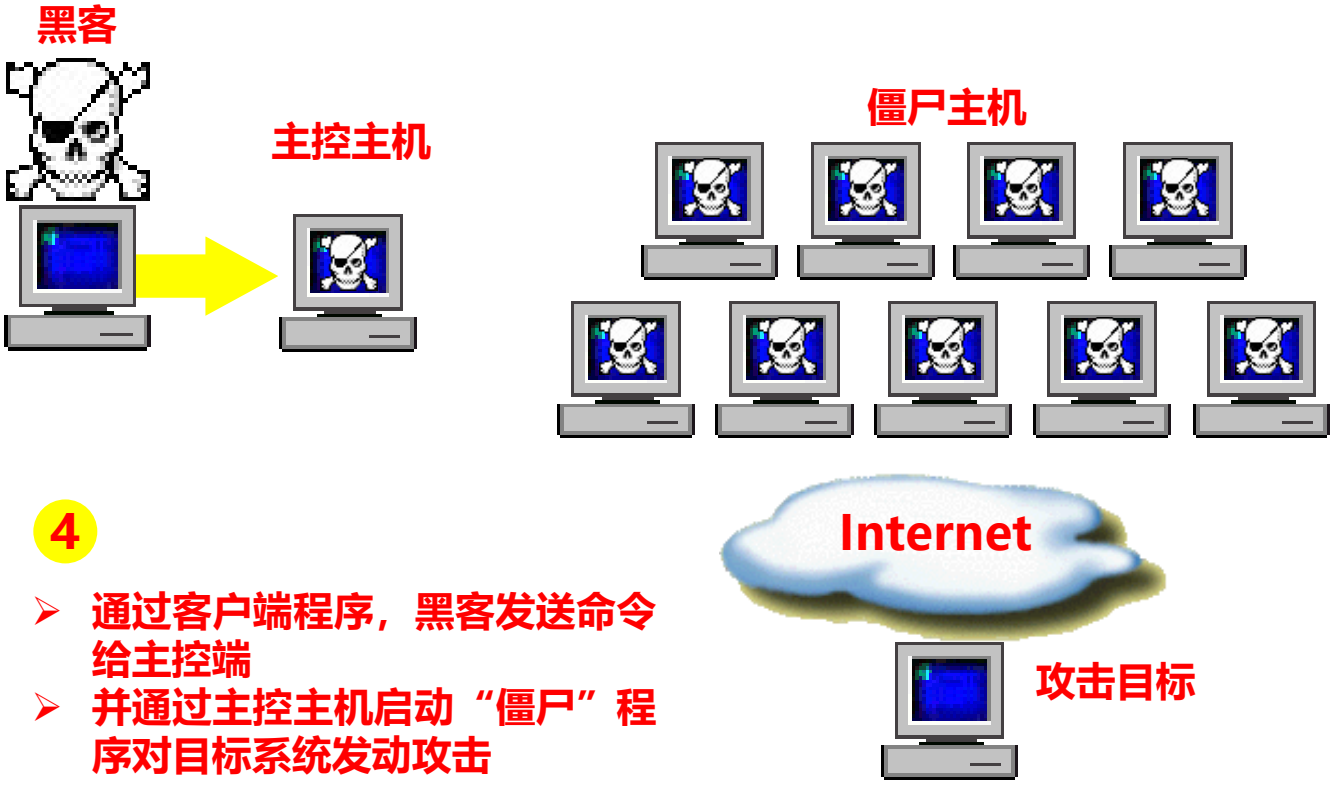
DDoS攻击过程 - 4



3

黑客选择主控主机，用来向“僵尸”发送命令

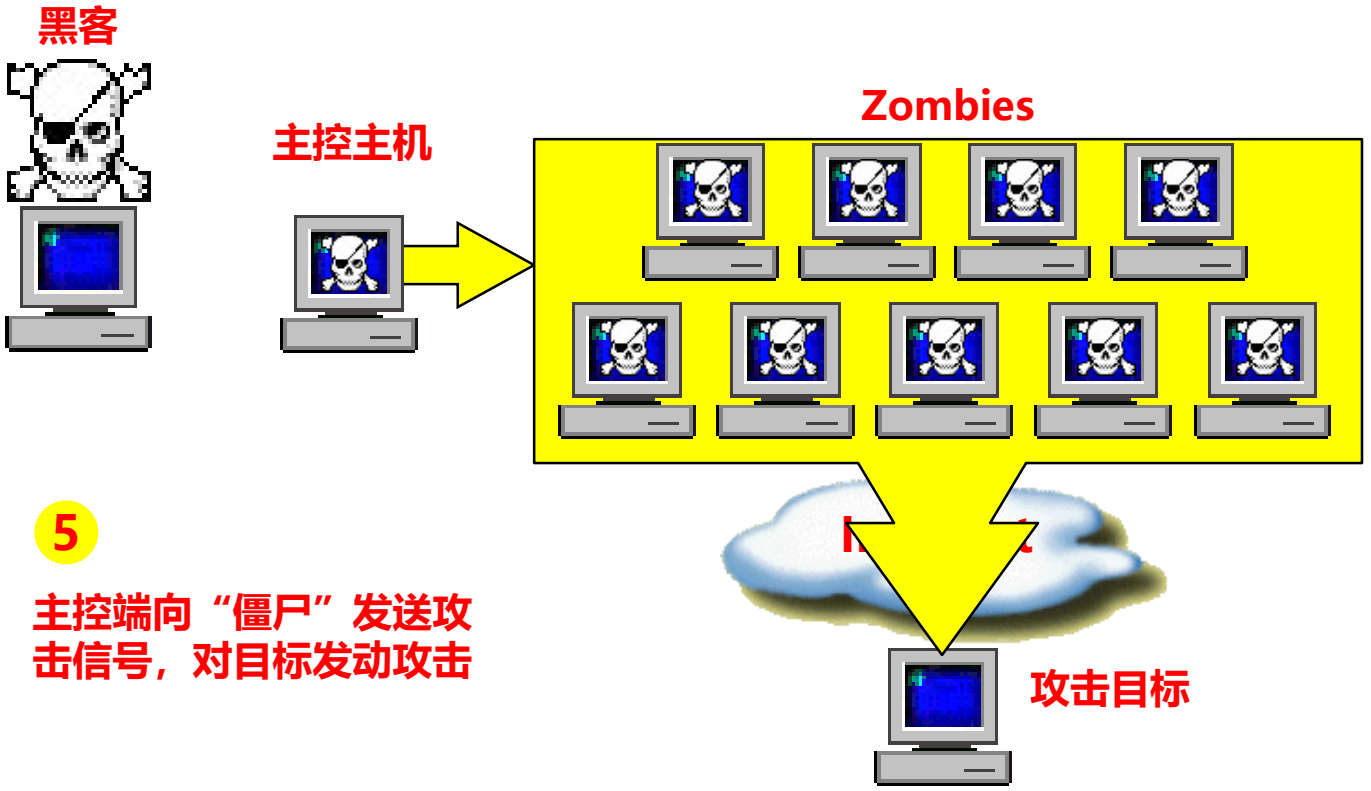
DDoS攻击过程 - 5



4

- 通过客户端程序，黑客发送命令给主控端
- 并通过主控主机启动“僵尸”程序对目标系统发动攻击

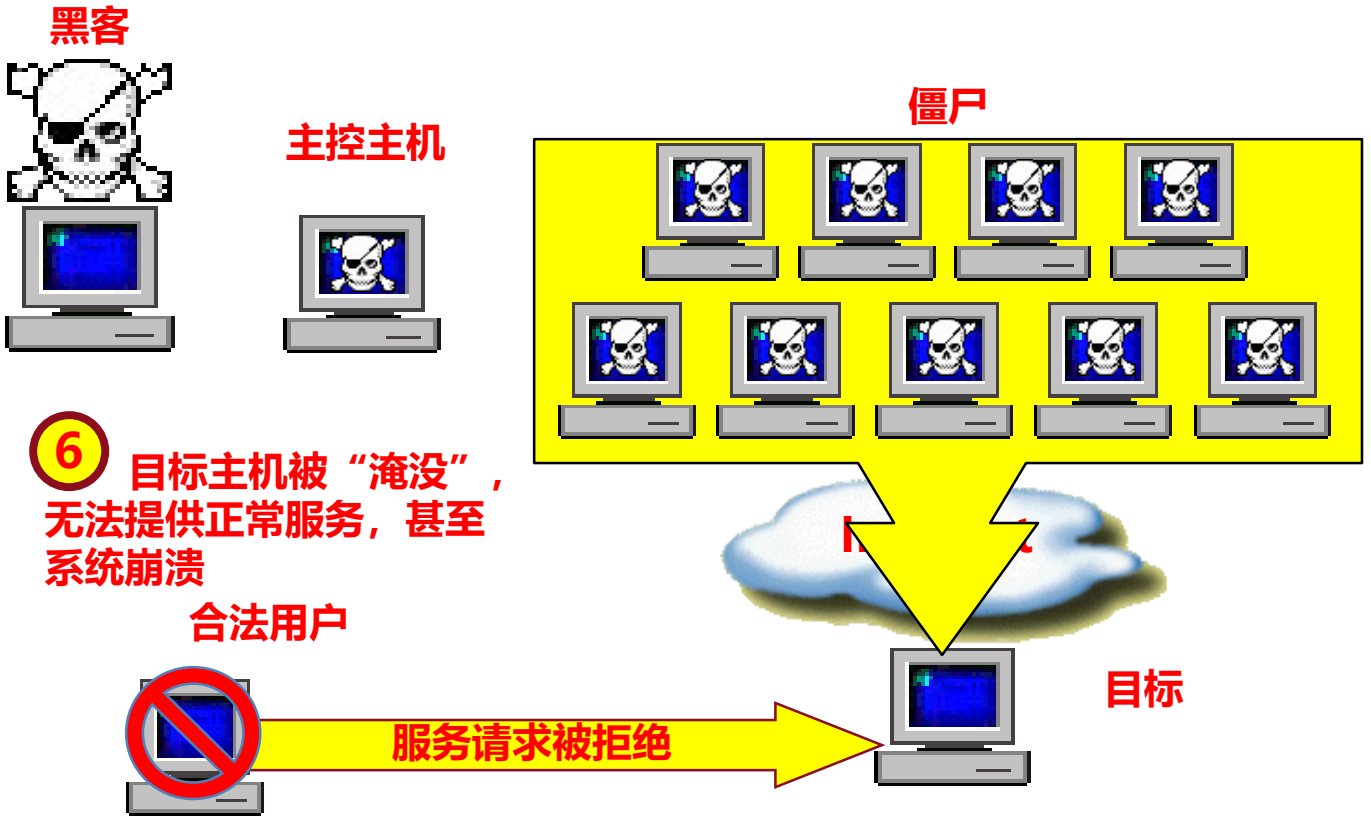
DDoS攻击过程 - 6



5

主控端向“僵尸”发送攻击信号，对目标发动攻击

DDoS攻击过程 - 7



DDoS攻击现象

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
- 到达数据指向端口随意
- 大量源地址为假的无用的数据包（源地址为假）
- 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

DDoS攻击应对

在数据流中搜寻特征字符串

- **尽管攻击包加入伪装，通过字符串特征提取，确定攻击者位置**

利用攻击数据包的某些特征

？

监视本地主机端口的使用

- **对敏感端口监视，如果处于监听状态**

对通信数据量进行统计

DDoS攻击常用方式 - 1

Trinoo（Tribe Flood Network）攻击

- **用UDP包进行攻击的工具软件**
- **与针对某特定端口的一般UDP flood攻击相比，Trinoo攻击随机指向目标端的各个UDP端口，产生大量ICMP不可到达报文，严重增加目标主机负担并占用带宽，使对目标主机的正常访问无法进行**

TFN攻击

- **用ICMP给主控端或分布端下命令，其来源可以做假**
- **发动SYN flood 、UDP flood 、ICMP flood及Smurf(利用多台服务器发出海量数据包，实施DoS攻击)等攻击**

DDoS攻击常用方式 - 2

TFN2K攻击

- **TFN2K是TFN的增强版，它增加了许多诸如加密新功能**

Stacheldraht攻击

- **结合了Trinoo和TFN的特点**
- **SHAFT是一种独立发展起来的DDoS攻击方法，独特之处在于：**
  - **首先，在攻击过程中，受控主机之间可以交换对分布端的控制和端口，这使得入侵检测工具难以奏效**
  - **其次，SHAFT采用了“ticket”机制进行攻击，使其攻击命令有一定秘密性**
  - **第三，SHAFT采用了独特的包统计方法使其攻击得以顺利完成**

拒绝服务攻击概述

拒绝服务攻击分类

电子邮件轰炸

分布式拒绝服务攻击

反弹技术

反弹技术 – 章节分解

1. 反弹技术介绍
2. 反弹技术原理
3. 反弹技术与DDoS区别

反弹技术介绍 1

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文的主机

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

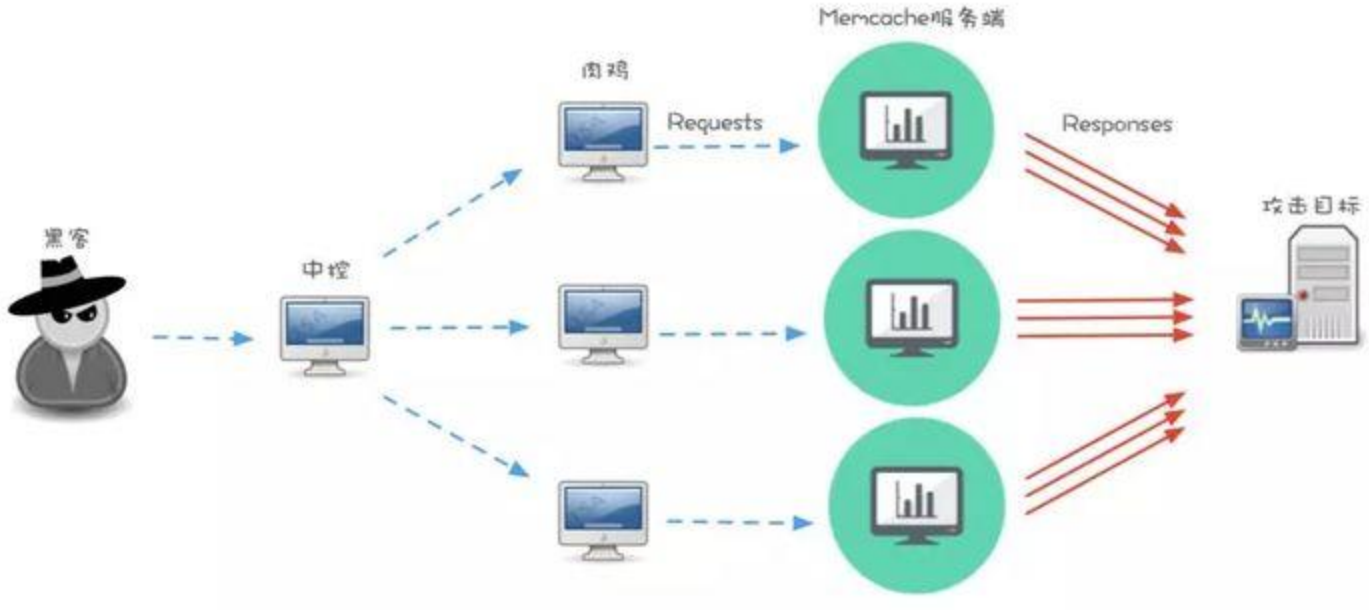
反弹技术介绍 2

然后攻击者们集中事先搞定的从服务器群，向已锁定的反弹服务器群发送大量的欺骗请求数据包（来源地址为受害服务器或目标服务器）。

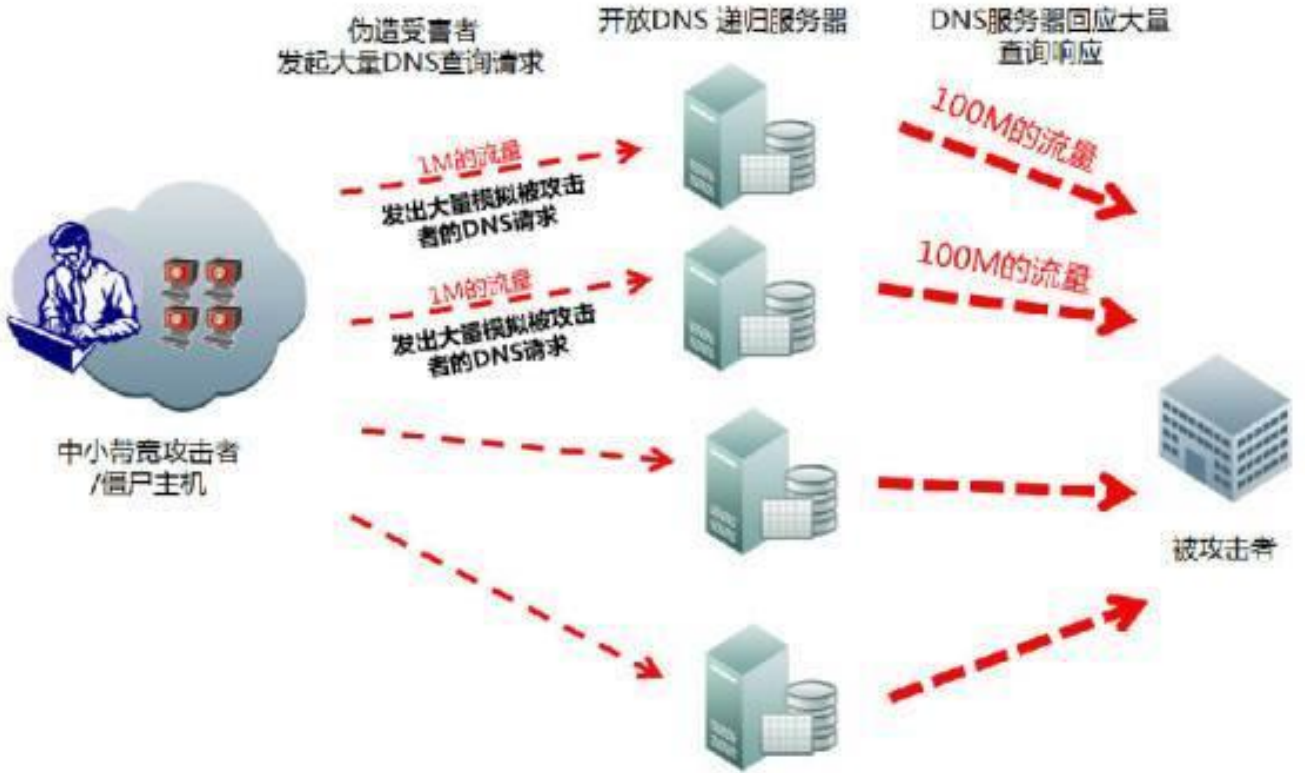
反弹服务器将向受害服务器发送回应数据报。

到达受害服务器的洪水数据报不是几百个，几千个的来源，而是上百万个来源，来源如此分散的洪水流量将堵塞任何其他的企图对受害服务器的连接。

反弹技术介绍 2



反弹技术介绍 2


伪造受害者
发起大量DNS查询请求
开放DNS 递归服务器
DNS服务器回应大量
查询响应
1M的流量
发出大量模拟被攻击
者的DNS请求
100M的流量
1M的流量
发出大量模拟被攻击
者的DNS请求
100M的流量
中小带宽攻击者
/僵尸主机
被攻击者

反弹技术原理

反弹服务器攻击过程和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DDoS区别

- 结构多了第四层——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（反弹端流量弱）
- 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

课后习题

1. 如何对抗TearDrop攻击?

2. 如何发现自己正在受到消耗网络资源的DoS攻击?

3. 对付分布式拒绝服务攻击的方法有哪些？举例说明

谢谢!