**如何发现自己正在受到消耗网络资源的DoS攻击（可参考课本p75）**

1、服务器主机上有大量等待的TCP连接；

2、检查网站后台服务器发现大量无用的数据包；

3、一段时期中IP请求异常且源地址虚假；

4、网络流量出现异常变化突然暴涨；

5、当发现Ping超时或丢包严重时，注意连接错误。假如遇到无法访问网站这种情况，并看到类似于“无法访问站点”之类的错误，且无法访问其他Internet服务，则可能是DoS攻击带来的影响。

6、查看自己的邮箱里是否突然收到大量的垃圾邮件。

具体地，可使用netstat命令：

netstat -n -p | grep SYN\_REC | sort -u

列出所有连接过的IP地址。

netstat -ntu | awk '{print $5}' | cut -d: -f1 | sort | uniq -c | sort -n

使用netstat命令计算每个主机连接到本机的连接数。

netstat -na

该命令将显示所有活动的网络连接。

netstat -n -p | grep SYN\_REC | awk '{print $5}' | awk -F: '{print $1}'

列出所有发送SYN\_REC连接节点的IP地址。

netstat -an | grep :80 | sort

显示所有80端口的网络连接并排序。这里的80端口是http端口，所以可以用来监控web服务。如果看到同一个IP有大量连接的话就可以判定单点流量攻击了。

netstat -ntu | grep ESTAB | awk '{print $5}' | cut -d: -f1 | sort | uniq -c | sort -nr

检查 ESTABLISHED 连接并且列出每个IP地址的连接数量。

netstat -plan|grep :80|awk {'print $5'}|cut -d: -f 1|sort|uniq -c|sort -nk 1

列出所有连接到本机80端口的IP地址和其连接数。80端口一般是用来处理HTTP网页请求。

netstat -anp |grep 'tcp|udp' | awk '{print $5}' | cut -d: -f1 | sort | uniq -c | sort -n

列出所有连接到本机的UDP或者TCP连接的IP数量。

**netstat -n -p|grep SYN\_REC | wc -l**

**这个命令可以查找出当前服务器有多少个活动的 SYNC\_REC 连接。正常来说这个值很小，最好小于5。 当有Dos攻击或者邮件炸弹的时候，这个值相当的高。**尽管如此，这个值和系统有很大关系，有的服务器值就很高，也是正常现象。

如何通过netstat命令缓解DDOS攻击呢？一旦获得攻击服务器的IP地址就可以使用以下命令拒绝此IP的所有连接。

iptables -A INPUT 1 -s $IPADRESS -j DROP/REJECT

注意，你需要将 $IPADRESS 替换成需要拒绝连接的IP地址。执行完以上命令后，使用以下命令结束所有的httpd连接以清理系统。

killall -KILL httpd

然后执行以下命令重启httpd服务。

service httpd start           #RedHat 系统

/etc/init/d/apache2 restart   #Debian 系统

当然通过netstat命令只能缓解部分DDoS攻击，而且还很有可能造成大量误封正常访客。所以墨者安全还是建议最好通过专业的网络安全公司部署DDoS高防IP，对恶意攻击流量进行清洗，隐藏服务器源IP，确保源站稳定运行。

**对付分布式拒绝服务攻击的方法有哪些？举例说明（参考课本p77）**

**企业网管理员**

网管员做为一个企业内部网的管理者，往往也是安全员、守护神。在他维护的网络中有一些服务器需要向外提供WWW服务，因而不可避免地成为DDoS的攻击目标，他该如何做呢？可以从主机与网络设备两个角度去考虑。

主机上的设置  
几乎所有的主机平台都有抵御DoS的设置，总结一下，基本的有几种：

* 关闭不必要的服务
* 限制同时打开的Syn半连接数目
* 缩短Syn半连接的time out 时间
* 及时更新系统补丁

网络设备上的设置  
企业网的网络设备可以从防火墙与路由器上考虑。这两个设备是到外界的接口设备，在进行防DDoS设置的同时，要注意一下这是以多大的效率牺牲为代价的，对你来说是否值得。

１.防火墙

* 禁止对主机的非开放服务的访问
* 限制同时打开的SYN最大连接数
* 限制特定IP地址的访问
* 启用防火墙的防DDoS的属性
* 严格限制对外开放的服务器的向外访问

第五项主要是防止自己的服务器被当做工具去害人。

２.路由器  
以Cisco路由器为例

* Cisco Express Forwarding（CEF）
* 使用 unicast reverse-path
* 访问控制列表（ACL）过滤
* 设置SYN数据包流量速率
* 升级版本过低的ISO
* 为路由器建立log server

其中使用CEF和Unicast设置时要特别注意，使用不当会造成路由器工作效率严重下降，升级IOS也应谨慎。路由器是网络的核心设备，与大家分享一下进行设置修改时的小经验，就是先不保存。Cisco路由器有两份配置startup config和running config，修改的时候改变的是running config，可以让这个配置先跑一段时间（三五天的就随意啦），觉得可行后再保存配置到startup config；而如果不满意想恢复原来的配置，用copy start run就行了。

**假如你的主机正在面临DNS欺骗攻击，你打算采取什么解决策略和方案？**

**DNS欺骗检测和防范思路**

**3.1 检测思路**

      发生DNS欺骗时，Client最少会接收到两个以上的应答数据报文，报文中都含有相同的ID序列号，一个是合法的，另一个是伪装的。据此特点，有以下两种检测办法：

      (1)被动监听检测。即监听、检测所有DNS的请求和应答报文。通常DNS Server对一个请求查询仅仅发送一个应答数据报文(即使一个域名和多个IP有映射关系，此时多个关系在一个报文中回答)。因此在限定的时间段内一个请求如果会收到两个或以上的响应数据报文，则被怀疑遭受了DNS欺骗。

      (2)主动试探检测。即主动发送验证包去检查是否有DNS欺骗存在。通常发送验证数据包接收不到应答，然而黑客为了在合法应答包抵达客户机之前就将欺骗信息发送给客户，所以不会对DNS Server的IP合法性校验，继续实施欺骗。若收到应答包，则说明受到了欺骗攻击。

**3.2 防范思路**

      在侦测到网络中可能有DNS欺骗攻击后，防范措施有：①在客户端直接使用IP Address访问重要的站点，从而避免DNS欺骗; ②对DNS Server和Client的数据流进行加密，Server端可以使用SSH加密协议，Client端使用PGP软件实施数据加密。

      对于常见的ID序列号欺骗攻击，采用专业软件在网络中进行监听检查，在较短时间内，客户端如果接收到两个以上的应答数据包，则说明可能存在DNS欺骗攻击，将后到的合法包发送到DNS Server并对DNS数据进行修改，这样下次查询申请时就会得到正确结果。

**四、DNS防护方案**

**4.1 进行IP地址和MAC地址的绑定**

      (1)预防ARP欺骗攻击。因为DNS攻击的欺骗行为要以ARP欺骗作为开端，所以如果能有效防范或避免ARP欺骗，也就使得DNS ID欺骗攻击无从下手。例如可以通过将Gateway Router 的Ip Address和MAC Address静态绑定在一起，就可以防范ARP攻击欺骗。

      (2)DNS信息绑定。DNS欺骗攻击是利用变更或者伪装成DNS Server的IP Address，因此也可以使用MAC Address和IP Address静态绑定来防御DNS欺骗的发生。由于每个Network Card的MAC Address具有唯一性质，所以可以把DNS Server的MAC Address与其IP Address绑定，然后此绑定信息存储在客户机网卡的Eprom中。当客户机每次向DNS Server发出查询申请后，就会检测DNS Server响应的应答数据包中的MAC Address是否与Eprom存储器中的MAC Address相同，要是不同，则很有可能该网络中的DNS Server受到DNS欺骗攻击。这种方法有一定的不足，因为如果局域网内部的客户主机也保存了DNS Server的MAC Address，仍然可以利用MAC Address进行伪装欺骗攻击。

**4.2 使用Digital Password进行辨别**

      在不同子网的文件数据传输中，为预防窃取或篡改信息事件的发生，可以使用任务数字签名(TSIG)技术即在主从Domain Name Server中使用相同的Password和数学模型算法，在数据通信过程中进行辨别和确认。因为有Password进行校验的机制，从而使主从Server的身份地位极难伪装，加强了Domain Name信息传递的安全性。

      安全性和可靠性更好的Domain Name Service是使用域名系统的安全协议(Domain Name System Security, DNSSEC))，用Digital Signature的方式对搜索中的信息源进行分辨，对DATA的完整性实施校验，DNSSEC的规范可参考RFC2605。因为在设立Domain时就会产生Password，同时要求上层的Domain Name也必须进行相关的Domain Password Signature，显然这种方法很复杂，所以InterNIC域名管理截至目前尚未使用。然而就技术层次上讲，DNSSEC应该是现今最完善的Domain Name设立和解析的办法，对防范Domain Name欺骗攻击等安全事件是非常有效的。

**4.3 优化DNS SERVER的相关项目设置**

      对于DNS Server的优化可以使得DNS的安全性达到较高的标准，常见的工作有以下几种：①对不同的子网使用物理上分开的Domain Name Server,从而获得DNS功能的冗余;②将外部和内部Domain Name Server从物理上分离开并使用Forwarders转发器。外部Domain Name Server可以进行任何客户机的申请查询，但Forwarders则不能，Forwarders被设置成只能接待内部客户机的申请查询;③采用技术措施限制DNS动态更新;④将区域传送(zone transfer)限制在授权设备上;⑤利用事务签名对区域传送和区域更新进行数字签名;⑥隐藏服务器上的Bind版本;⑦删除运行在DNS服务器上的不必要服务，如FTP、telnet和Http;⑧在网络外围和DNS服务器上使用防火墙,将访问限制在那些DNS功能需要的端口上。

**4.4 直接使用IP地址访问**

      对个别信息安全等级要求十分严格的WEB站点尽量不要使用DNS进行解析。由于DNS欺骗攻击中不少是针对窃取客户的私密数据而来的，而多数用户访问的站点并不涉及这些隐私信息，因此当访问具有严格保密信息的站点时，可以直接使用IP地址而无需通过DNS解析，这样所有的DNS欺骗攻击可能造成的危害就可以避免了。除此，应该做好DNS Server的安全配置项目和升级DNS软件，合理限定DNS Server进行响应的IP地址区间，关闭DNS Server的递归查询项目等。

**4.5 对DNS数据包进行监测**

      在DNS欺骗攻击中，Client会接收到至少两个DNS的数据响应包，一个是真实的数据包，另一个是攻击数据包。欺骗攻击数据包为了抢在真实应答包之前回复给Client，它的信息数据结构与真实的数据包相比十分简单，只有应答域，而不包括授权域和附加域。因此，可以通过监测DNS响应包，遵循相应的原则和模型算法对这两种响应包进行分辨，从而避免虚假数据包的攻击。

**TCP/IP的安全性隐患？改进措施？**

**1、链路层上的攻击**

在TCP/IP网络中，链路层这一层次的复杂程度是最高的。其中最常见的攻击方式通常是网络嗅探组成的TCP/IP协议的以太网。

以太网卡有两种主要的工作方式，一种是一般工作方式，另一种是较特殊的混杂方式。这一情况下，很可能由于被攻击的原因而造成信息丢失情况，且攻击者可以通过数据分析来获取账户、密码等多方面的关键数据信息。

**2、网络层上的攻击**

如果ARP识别链接错误，这样的话ARP直接应用可疑信息，那么可疑信息就会很容易进入目标主机当中。ARP协议没有状态，不管有没有收到请求，主机会将任何受到的ARP相应自动缓存。

如果信息中带有病毒，采用ARP欺骗就会导致网络信息安全泄露。因此，在ARP识别环节，应加大保护，建立更多的识别关卡，不能只简单通过IP名进行识别，还需充分参考IP相关性质等。

**3、传输层上的攻击**

在传输层还存在网络安全问题。如在网络安全领域中，IP欺骗就是隐藏自己的有效手段，主要是通过将自身IP地址进行伪造，并向目标主机发送恶意的请求，攻击主机，而主机却因为IP地址被隐藏而无法准确确认攻击源。或者通过获取目标主机信任而趁机窃取相关的机密信息。

**4、应用层上的攻击**

对于因特网而言，IP地址与域名均是一一对应的，这两者之间的转换工作，被称为域名解析。而DNS就是域名解析的服务器。DNS欺骗指的是攻击方冒充域名服务器的行为，使用DNS欺骗能将错误DNS信息提供给目标主机。所以说，通过DNS欺骗可误导用户进入非法服务器，让用户相信诈骗IP。