**1.如何将本地80端口的请求转发到8080端口，当前主机IP为192.168.16.1，其中本地网卡eth0**

**答案：**

**iptables -t nat -A PREROUTING  -d 192.168.16.1 -p tcp --dport 80 -j DNAT  --to 192.168.16.1:8080**

**2.什么是NAT，常见分为哪几种，DNAT与SNAT有什么不同，应用实例有哪些?**

**答案：**

**NAT也叫做网络地址转换，起初是用来解决ipv4地址资源的日益衰竭。NAT分为源地址转换SNAT，目标地址转换DNAT，与网络地址伪装MASQUERADE。SNAT是指在数据包从网卡发送出去的时候，把数据包中的源地址部分替换为指定的IP，这样，接收方就认为数据包的来源是被替换的那个IP的主机。**

**MASQUERADE是用发送数据的网卡上的IP来替换源IP，因此，对于那些IP不固定的场合，比如拨号网络或者通过dhcp分配IP的情况下，就得用MASQUERADE。**

**DNAT，就是指数据包从网卡发送出去的时候，修改数据包中的目的IP，表现为如果你想访问A，可是因为网关做了DNAT，把所有访问A的数据包的目的IP全部修改为B，那么，你实际上访问的是B。因为，路由是按照目的地址来选择的，因此，DNAT是在PREROUTING链上来进行的，而SNAT是在数据包发送出去的时候才进行，因此是在POSTROUTING链上进行的。**

**下面我给出两个应用实例：**

**1） 内网机器访问外网** **http://ask.apelearn.com/question/3624**

**2） 外网访问内网的ftp http://ask.apelearn.com/question/1003**

**3.包过滤防火墙与代理应用防火墙有什么区别，能列举几种相应的产品吗？**

**答案：**

**包过滤防火墙工作在网络协议ip层，它只对ip包的源地址、目标地址及相应端口进行处理，因此速度比较快，能够处理的并发连接比较多，缺点是对应用层的攻击无能为力。如：iptables，windows等软件类防火墙。代理服务器防火墙将收到的IP包还原成高层协议的通讯数据，比如http连接信息，因此能够对基于高层协议的攻击进行拦截。缺点是处理速度比较慢，能够处理的并发数比较少。如：一些审计类的防火墙，用户行为控制系统等。**

**4.Iptables是否支持time时间控制用户行为，如有请写出具体操作步骤。**

**答案：**

**支持，规则为**

**iptables -A INPUT -p tcp** **—dport 445 -m time --weekdays Mon，Tus，Wed，Thu，Fri --timestart 08:00:00** **—timestop 18:00:00 -j ACCEPT  指定工作日的8点到18点期间，才能访问445端口。**

**5.说出你知道的几种linux/unix发行版本**

**答案：**

**Redhat、CentOS、Fedora、SuSE、Slackware、Gentoo、Debian、Ubuntu、FreeBSD、Solaris、HPUX、AIX**

**6.列出linux常见打包工具并写相应解压缩参数（至少三种）**

**答案：**

**tar -zcvf test.tar.gz test  解压：tar -zxvf test.tar.gz**

**zip -r test.zip test    解压：unzip test.zip**

**gzip test  解压: gzip -d test.gz**

**7.计划每星期天早8点服务器定时重启，如何实现？**

**答案：**

**写入crontab**

**0 8 \* \* 7  init 6**

**8.列出作为完整邮件系统的软件，至少二类。**

**答案：**

**iredmail    Postfix+Cyrus-SASL+dovecot**

**9.当用户在浏览器当中输入一个网站，说说计算机对dns解析经过那些流程？注：本机跟本地dns还没有缓存。**

**答案：  
a.用户输入网址到浏览器；  
b.浏览器发出DNS请求信息；  
c.计算机首先查询本机HOST文件，看是否存在，存在直接返回结果，不存在，继续下一步；  
d.计算机按照本地DNS的顺序，向合法dns服务器查询IP结果；  
e.合法dns返回dns结果给本地dns，本地dns并缓存本结果，直到TTL过期，才再次查询此结果；  
f.返回IP结果给浏览器；  
g.浏览器根据IP信息，获取页面；**

**10.我们都知道，dns即采用了tcp协议，又采用了udp协议，什么时候采用tcp协议？什么时候采用udp协议？为什么要这么设计？**

**答案：**

**DNS主备服务器之间传输数据时使用tcp，而客户端与DNS服务器之间数据传输时用的是udp。tcp和udp最大的区别在于tcp需要三次握手来验证数据包的完整性和准确性，udp不需要验证，速度比tcp要快。DNS主备数据传输需要保证数据准确性，有必要使用tcp通信，而客户端请求服务端，更需要快，所以用udp。**