1. 写一个防火墙配置脚本，只允许远程主机访问本机的 80 端口。

```
iptables -P INPUT ACCEPT
iptables -P OUTPUT ACCEPT
iptables -P FORWARD ACCEPT
iptables -F
iptables -X
iptables -A INPUT -i eth0 -p tcp –dport 80 -j ACCEPT
iptables -P INPUT DROP
```

2. 如何将本地 80 端口的请求转发到 8080 端口，当前主机 IP 为 192.168.2.1

```
/sbin/iptables -t nat -A PREROUTING -p tcp --dport 80 -j DNAT--to 192.168.2.1:8080
/sbin/iptables -t nat -A PREROUTING -p tcp --dport 80 -j REDIRECT --to 8080
```

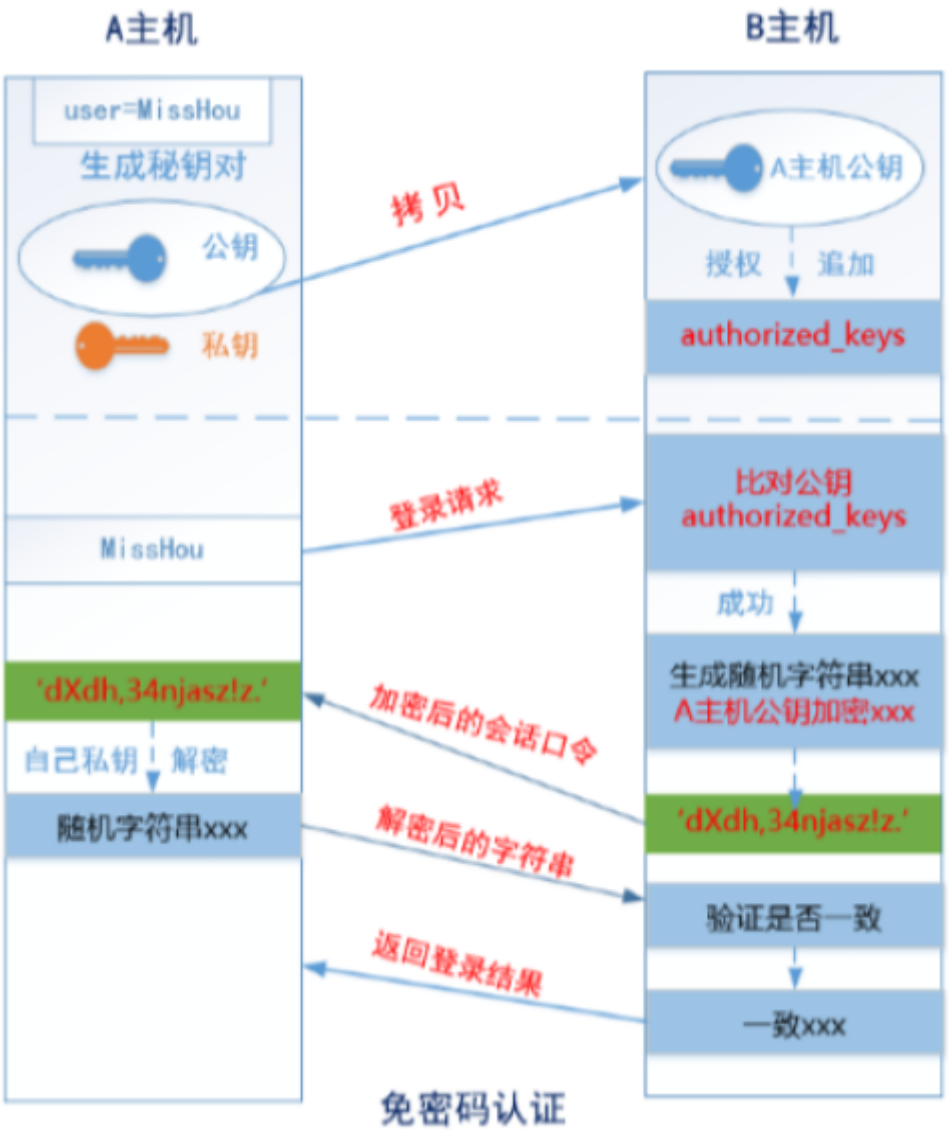
3. 说出 5 个以上常用的服务端口

```
21 ------ ftp
22 ------ ssh
23 ------ telnet
25 ------ snmp
110 ----- ppop3
143 ----- IMAP
873 ----- rsync
80 ------ http
3306 ------ mysql
```

3. FTP 的主动模式和被动模式

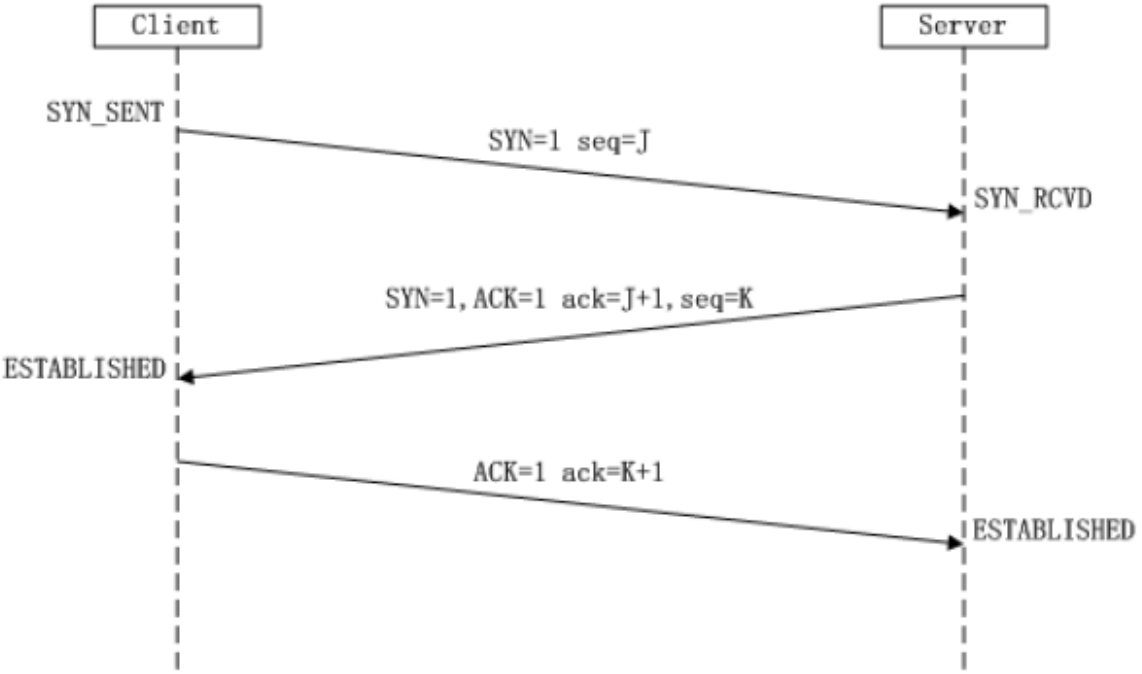
```
FTP 协议有两种工作方式：PORT 方式和 PASV 方式，中文意思为主动式和被动式。

- 主动模式
1. 客户端打开大于 1023 的随机命令端口和大于 1023 的随机数据端口向服务的的 21 号端口发起请求
2. ==服务端== 的 21 号命令端口响应客户端的随机命令端口
3. ==服务端== 的 20 号端口 ==主动== 请求连接客户端的随机数据端口
4. 客户端的随机数据端口进行确认

- 被动模式
1. 客户端打开大于 1023 的随机命令端口和大于 1023 的随机数据端口向服务的的 21 号端口发起请求
2. 服务端的 21 号命令端口响应客户端的随机命令端口
3. ==客户端主动== 连接服务端打开的大于 1023 的随机端口
4. 服务端进行确认
```

4. 请简要说明 ssh 免密登陆过程

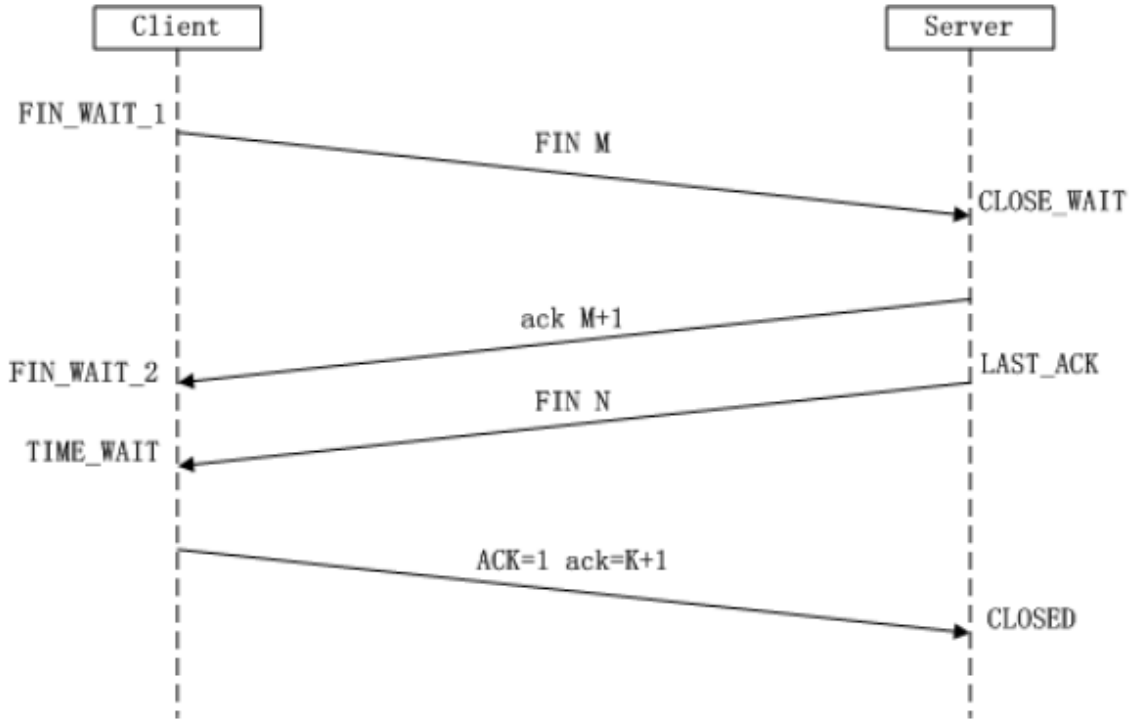


1. 在 server A 上生成公钥私钥。
2. 将公钥拷贝给 server B，要重命名成 authorized_keys
3. Server A 向 Server B 发送一个连接请求。
4. Server B 得到Server A 的信息后，在 authorized_key 中进行比对，如果有相应的 用户名 和 IP，则随机生成一个字符串，并用 Server A 的公钥加密，发送给 Server A。
5. Server A 得到 Server B 发来的消息后，使用私钥进行解密，然后将解密后的字符串发送给 Server B。Server B 进行对比，如果一致，则允许免登录。

5. tcp 的 3 次握手和 4 次挥手的全进程



(1) 第一次握手：Client 将标志位 SYN 置为 1，随机产生一个值 seq=J，并将该数据包发送给 Server，Client 进入 SYN_SENT 状态，等待 Server 确认。
(2) 第二次握手：Server 收到数据包后由标志位 SYN=1 知道 Client 请求建立连接，Server 将标志位 SYN 和 ACK 都置为 1，ack=J+1，随机产生一个值 seq=K，并将该数据包发送给 Client 以确认连接请求，Server 进入 SYN_RCVD 状态。
(3) 第三次握手：Client 收到确认后，检查 ack 是否为 J+1，ACK 是否为 1，如果正确则将标志位 ACK 置为 1，ack=K+1，并将该数据包发送给 Server，Server 检查 ack 是否为 K+1，ACK 是否为 1，如果正确则连接建立成功，Client 和 Server 进入 ESTABLISHED 状态，完成三次握手，随后 Client 与 Server 之间可以开始传输数据了。



（1） 第一次挥手：Client 发送一个 FIN，用来关闭 Client 到 Server 的数据传送，Client 进入 FIN_WAIT_1 状态。
（2） 第二次挥手：Server 收到 FIN 后，发送一个 ACK 给 Client，确认序号为收到序号 +1（与 SYN 相同，一个 FIN 占用一个序号），Server 进入 CLOSE_WAIT 状态。
（3） 第三次挥手：Server 发送一个 FIN，用来关闭 Server 到 Client 的数据传送，Server 进入 LAST_ACK 状态。
（4） 第四次挥手：Client 收到 FIN 后，Client 进入 TIME_WAIT 状态，接着发送一个 ACK 给 Server，确认序号为收到序号 +1，Server 进入 CLOSED 状态，完成四次挥手。

6. 请写出 http 和 https 请求的区别，并写出遇到过的响应状态码

1. https 协议需要到 ca 申请证书，一般免费证书很少，需要交费。
2. http 是超文本传输协议，信息是明文传输，https 则是具有安全性的 ssl 加密传输协议。
3. http 和 https 使用的是完全不同的连接方式，用的端口也不一样，前者是 80，后者是 443。
4. http 的连接很简单，是无状态的；HTTPS 协议是由 SSL+HTTP 协议构建的可进行加密传输、身份认证的网络协议，比 http 协议安全。

状态码常用：
301 永久重定向
403 服务器已经理解请求，但是拒绝执行
404 页面丢失
500 服务器错误

7. 操作系统内存调度方式有哪几种并简单说明

OPT：最佳替换算法（optional replacement），替换下次访问距当前时间最长的页。opt 算法需要知道操作系统将来的事件，显然不可能实现，只作为一种衡量其他算法的标准。

LRU：最近最少使用（Least Recently Used），替换上次使用距离当前最远的页。根据局部性原理：替换最近最不可能访问到的页。性能最接近 OPT，但难以实现。可以维护一个关于访问页的栈或者给每个页添加最后访问的时间标签，但开销都很大。

FIFO：先进先出（**First In First Out**），将页面看做一个循环缓冲区，按循环方式替换。

Clock：时钟替换算法（**Clock**），给每个页帧关联一个使用位。当该页第一次装入内存或者被重新访问到时，将使用位置为 1。每次需要替换时，查找使用位被置为 0 的第一个帧进行替换。

8. 简述 DNS 进行域名解析的过程?

用户要访问 www.baidu.com，会先找本机的 host 文件，再找本地设置的 DNS 服务器
如果也没有的话，就去网络中找根服务器，根服务器反馈结果，说只能提供一级域名服务器 .cn
就去找一级域名服务器，一级域名服务器说只能提供二级域名服务器 .com.cn
就去找二级域名服务器，二级域服务器只能提供三级域名服务器 .baidu.com.cn
就去找三级域名服务器，三级域名服务器正好有这个网站 www.baidu.com，然后发给请求的服务器，保存一份之后，再发给客户端