背景：互联网公司的服务器时常要面对黑客的攻击，一旦服务器被黑客登录，后果不敢想象，那么如何使用一种简单的方法来做简单的防御呢？

- 处于安全考虑，现在要求屏蔽每分钟ssh尝试登陆linux服务器 超过10次的IP进行屏蔽，请写出解决办法？
  - 答案：编写shell脚本获取对应ip加入黑名单（基于iptables并非firewall）

```
#!/bin/bash
DATE=$(date +"%a %b %e %H:%M") #星期月天时分  %e单数字时显示7，而%d显示07
ABNORMAL_IP=$(lastb |grep "$DATE" |awk '{a[$3]++}END{for(i in
a)if(a[i]>10)print i}')
for IP in $ABNORMAL_IP; do
    if [ $(iptables -vnL |grep -c "$IP") -eq 0 ]; then
        iptables -I INPUT -s $IP -j DROP
    fi
done
```