QQ互联 域名备案号

# 支付宝

## 即时到账业务

## App支付

## 手机网站支付

[linux系统](https://www.baidu.com/s?wd=linux%E7%B3%BB%E7%BB%9F&tn=44039180_cpr&fenlei=mv6quAkxTZn0IZRqIHckPjm4nH00T1Ydn1uhmymkm1nYPAm3uWbv0ZwV5Hcvrjm3rH6sPfKWUMw85HfYnjn4nH6sgvPsT6KdThsqpZwYTjCEQLGCpyw9Uz4Bmy-bIi4WUvYETgN-TLwGUv3EnHbzPHfsrjnkPWfYnjnznWTYPs)的服务器被入侵，总结了以下的基本方法，供不大懂linux服务器网理人员参考考学习。  
首先先用iptraf查下，如果没装的运行yum install iptraf装下，看里面是不是UDP包发的很多，如果是，基本都被人装了后门  
1. 检查帐户  
# less /etc/passwd  
# grep :0: /etc/passwd（检查是否产生了新用户，和UID、GID是0的用户）  
# [ls](https://www.baidu.com/s?wd=ls&tn=44039180_cpr&fenlei=mv6quAkxTZn0IZRqIHckPjm4nH00T1Ydn1uhmymkm1nYPAm3uWbv0ZwV5Hcvrjm3rH6sPfKWUMw85HfYnjn4nH6sgvPsT6KdThsqpZwYTjCEQLGCpyw9Uz4Bmy-bIi4WUvYETgN-TLwGUv3EnHbzPHfsrjnkPWfYnjnznWTYPs) [-l](https://www.baidu.com/s?wd=-l&tn=44039180_cpr&fenlei=mv6quAkxTZn0IZRqIHckPjm4nH00T1Ydn1uhmymkm1nYPAm3uWbv0ZwV5Hcvrjm3rH6sPfKWUMw85HfYnjn4nH6sgvPsT6KdThsqpZwYTjCEQLGCpyw9Uz4Bmy-bIi4WUvYETgN-TLwGUv3EnHbzPHfsrjnkPWfYnjnznWTYPs) /etc/passwd（查看文件修改日期）  
# awk -F: ‘$3= =0 {print $1}’ /etc/passwd（查看是否存在特权用户）  
# awk -F: ‘length($2)= =0 {print $1}’ /etc/shadow（查看是否存在空口令帐户）  
   
2. 检查日志  
# last（查看正常情况下登录到本机的所有用户的历史记录）  
注意”entered promiscuous mode”  
注意错误信息  
注 意Remote Procedure Call (rpc) programs with a log entry that includes a large number (> 20) strange characters(-^PM-^PM-^PM-^PM-^PM-^PM-^PM-^PM)  
   
3. 检查进程  
# ps -aux（注意UID是0的）  
# [ls](https://www.baidu.com/s?wd=ls&tn=44039180_cpr&fenlei=mv6quAkxTZn0IZRqIHckPjm4nH00T1Ydn1uhmymkm1nYPAm3uWbv0ZwV5Hcvrjm3rH6sPfKWUMw85HfYnjn4nH6sgvPsT6KdThsqpZwYTjCEQLGCpyw9Uz4Bmy-bIi4WUvYETgN-TLwGUv3EnHbzPHfsrjnkPWfYnjnznWTYPs)of -p pid（察看该进程所打开端口和文件）  
# cat /etc/inetd.conf | grep -v “^#”（检查守护进程）  
检查隐藏进程  
# ps -ef|awk ‘{print }’|sort -n|uniq >1  
# [ls](https://www.baidu.com/s?wd=ls&tn=44039180_cpr&fenlei=mv6quAkxTZn0IZRqIHckPjm4nH00T1Ydn1uhmymkm1nYPAm3uWbv0ZwV5Hcvrjm3rH6sPfKWUMw85HfYnjn4nH6sgvPsT6KdThsqpZwYTjCEQLGCpyw9Uz4Bmy-bIi4WUvYETgN-TLwGUv3EnHbzPHfsrjnkPWfYnjnznWTYPs) /porc |sort -n|uniq >2  
# diff 1 2  
   
4. 检查文件  
# find / -uid 0 –perm -4000 –print  
# find / -size +10000k –print  
# find / -name “…” –print  
# find / -name “.. ” –print  
# find / -name “. ” –print  
# find / -name ” ” –print  
注意SUID文件，可疑大于10M和空格文件  
# find / -name core -exec ls [-l](https://www.baidu.com/s?wd=-l&tn=44039180_cpr&fenlei=mv6quAkxTZn0IZRqIHckPjm4nH00T1Ydn1uhmymkm1nYPAm3uWbv0ZwV5Hcvrjm3rH6sPfKWUMw85HfYnjn4nH6sgvPsT6KdThsqpZwYTjCEQLGCpyw9Uz4Bmy-bIi4WUvYETgN-TLwGUv3EnHbzPHfsrjnkPWfYnjnznWTYPs) {} ;（检查系统中的core文件）  
检查系统文件完整性  
# rpm –qf /bin/ls  
# rpm -qf /bin/login  
# [md5sum](https://www.baidu.com/s?wd=md5sum&tn=44039180_cpr&fenlei=mv6quAkxTZn0IZRqIHckPjm4nH00T1Ydn1uhmymkm1nYPAm3uWbv0ZwV5Hcvrjm3rH6sPfKWUMw85HfYnjn4nH6sgvPsT6KdThsqpZwYTjCEQLGCpyw9Uz4Bmy-bIi4WUvYETgN-TLwGUv3EnHbzPHfsrjnkPWfYnjnznWTYPs) –b 文件名  
# [md5sum](https://www.baidu.com/s?wd=md5sum&tn=44039180_cpr&fenlei=mv6quAkxTZn0IZRqIHckPjm4nH00T1Ydn1uhmymkm1nYPAm3uWbv0ZwV5Hcvrjm3rH6sPfKWUMw85HfYnjn4nH6sgvPsT6KdThsqpZwYTjCEQLGCpyw9Uz4Bmy-bIi4WUvYETgN-TLwGUv3EnHbzPHfsrjnkPWfYnjnznWTYPs) –t 文件名  
   
5. 检查RPM  
# rpm –Va  
输出格式：  
S – File size differs  
M – Mode differs (permissions)  
5 – MD5 sum differs  
D – Device number mismatch  
L – readLink path mismatch  
U – user ownership differs  
G – group ownership differs  
T – modification time differs  
注意相关的 /sbin, /bin, /usr/sbin, and /usr/bin  
   
6. 检查网络  
# ip link | grep PROMISC（正常网卡不该在promisc模式，可能存在sniffer）  
# lsof –i  
# netstat –nap（察看不正常打开的TCP/UDP端口)  
# arp –a  
   
7. 检查计划任务  
注意root和UID是0的schedule  
# crontab –u root –l  
# cat /etc/crontab  
# ls /etc/cron.\*  
   
8. 检查后门  
# cat /etc/crontab  
# ls /var/spool/cron/  
# cat /etc/rc.d/rc.local  
# ls /etc/rc.d  
# ls /etc/rc3.d  
# find / -type f -perm 4000  
   
9. 检查内核模块  
# lsmod  
   
10. 检查系统服务  
# chkconfig  
# rpcinfo -p（查看RPC服务）  
   
11. 检查rootkit  
# rkhunter -c  
# chkrootkit -q

# http错误日志

/var/log/http