【shell】deny_hack_ip.sh

簡單阻擋 try 帳號 ip

```
#! /bin/bash
#cat /var/log/secure|awk '/Failed/{print $(NF-3)}'|sort|uniq -c|awk '{print $2"="$1;}' > /root/block.txt
cat /var/log/secure|awk '/Invalid user/{print $(NF-2)}'|sort|uniq -c|awk '{print $2"="$1;}' > /root/block.txt
DEFINE="10"
for i in `cat  /root/block.txt`
do
    IP=`echo | awk '{split("'${i}'", array, "=");print array[1]}'`
    NUM=`echo | awk '{split("'${i}'", array, "=");print array[2]}'`
    if [ $NUM -gt $DEFINE ];then
     grep $IP /etc/hosts.deny > /dev/null
      if [ $? -gt 0 ];then
          echo "sshd:$IP:deny" >> /etc/hosts.deny
      fi
    fi
done
```

修訂版本 #1
★由 treeman 建立於 25 ﷺ 2023 00:31:35
✎由 treeman 更新於 5 ﷺ 2023 10:14:58