#!/bin/bash

PATH=/bin:/sbin:/usr/bin:/usr/sbin:/usr/local/bin:/usr/local/sbin:~/bin

export PATH

droppids(){

port\_dropbear=`ps aux|grep 'dropbear'|awk NR==1|awk '{print $17;}'`

log=/var/log/auth.log

loginsukses='Password auth succeeded'

pids=`ps ax|grep 'dropbear'|grep " $port\_dropbear"|awk -F " " '{print $1}'`

for pid in $pids; do

pidlogs=`grep $pid $log |grep "$loginsukses" |awk -F" " '{print $3}'`

i=0

for pidend in $pidlogs; do

let i=i+1

done

if [ $pidend ];then

login=`grep $pid $log |grep "$pidend" |grep "$loginsukses"`

PID=$pid

user=`print\_center -ama $login |awk -F" " '{print $10}' | sed -r "s/'/ /g"`

waktu=`print\_center -ama $login |awk -F" " '{print $2"-"$1,$3}'`

while [ ${#waktu} -lt 13 ]; do

waktu=$waktu" "

done

while [ ${#user} -lt 16 ]; do

user=$user" "

done

while [ ${#PID} -lt 8 ]; do

PID=$PID" "

done

print\_center -ama "$user $PID $waktu"

fi

done

}

sshmonitor(){

h=1

unlimit=$(cat /root/udp/unlimit)

for i in `print\_center -ama "$user\_type"`; do

user="$i"

s2ssh="$(cat /etc/passwd|grep -w "$i"|awk -F ':' '{print $5}'|cut -d ',' -f1)"

if [[ "$(cat /etc/passwd| grep -w $user| wc -l)" = "1" ]]; then

sqd="$(ps -u $user | grep sshd | wc -l)"

else

sqd=00

fi

[[ "$sqd" = "" ]] && sqd=0

if [[ -e /etc/openvpn/openvpn-status.log ]]; then

ovp="$(cat /etc/openvpn/openvpn-status.log | grep -E ,"$user", | wc -l)"

else

ovp=0

fi

if netstat -nltp|grep 'dropbear'> /dev/null;then

drop="$(droppids | grep -w "$user" | wc -l)"

else

drop=0

fi

cnx=$(($sqd + $drop))

conex=$(($cnx + $ovp))

if [[ "$conex" -gt "$s2ssh" ]]; then

pkill -u $user

droplim=`droppids|grep -w "$user"|awk '{print $2}'`

kill -9 $droplim &>/dev/null

usermod -L $user

print\_center -ama "$user $(printf '%(%H:%M:%S)T') $conex/$s2ssh" >> /root/udp/limit.log

[[ $unlimit -le 0 ]] && continue || at now +${unlimit} minutes <<< "usermod -U $user" &>/dev/null

fi

done

touch /root/udp/limit

timer=$(cat /root/udp/limit)

[[ -z ${timer} ]] && timer="3"

at now +${timer} minutes <<< "/root/udp/limiter.sh" &>/dev/null

[[ -z $(cat "/var/spool/cron/crontabs/root"|grep "limiter.sh") ]] && print\_center -ama "@reboot root /root/udp/limiter.sh" >> /var/spool/cron/crontabs/root

}

expired(){

while read line; do

userDate=$(chage -l "$line"|sed -n '4p'|awk -F ': ' '{print $2}')

if [[ $(date '+%s') -gt $(date '+%s' -d "$userDate") ]]; then

if [[ $(passwd --status $line|cut -d ' ' -f2) = "P" ]]; then

usermod -L $line

print\_center -ama "$line $(printf '%(%H:%M:%S)T') expired" >> /root/udp/limit.log

fi

fi

done <<< $(print\_center -ama "$user\_type")

}

all\_user=$(cat /etc/passwd|grep 'home'|grep 'false'|grep -v 'syslog'|grep -v '::/')

case $1 in

-s|--ssh)user\_type=$(print\_center -ama "$all\_user"|grep -v 'hwid\|token'|awk -F ':' '{print $1}') && expired;;

-h|--hwid)user\_type=$(print\_center -ama "$all\_user"|grep -w 'hwid'|awk -F ':' '{print $1}') && expired;;

-t|--token)user\_type=$(print\_center -ama "$all\_user"|grep -w 'token'|awk -F ':' '{print $1}') && expired;;

\*)user\_type=$(print\_center -ama "$all\_user"|grep -v 'hwid\|token'|awk -F ':' '{print $1}') && sshmonitor;;

esac