Notificatie bij login via Telegram

Inleiding

Je kan via een bot en een handig script een bericht laten verzenden naar je telegram account als er iemand inlogt op je Linux Server. Zowel voor logins via SSH als via de console.

Ik heb gebruik gemaakt van 2 tutorials en ze iets aangepast omdat ze beiden initieel voor alleen SSH waren danwel dat ze ook notificaties gaven als er een crontaak startte.

Telegram configuratie

Bot aanmaken

Chat ID opvragen

SSH configuratie

Om dit mogelijk te maken onder SSH het volgende.

/etc/profile.d/ssh-telegram.sh

```
# save it as /etc/profile.d/ssh-telegram.sh
# use jq to parse JSON from ipinfo.io
# apt-get install jq
USERID="==xxxxxxx=="
KEY="==API Token=="
TIMEOUT="10"
URL="https://api.telegram.org/bot$KEY/sendMessage"
DATE_EXEC="$(date "+%d %b %Y %H:%M")"
TMPFILE='/tmp/ipinfo-$DATE_EXEC.txt'
if [ -n "$SSH_CLIENT" ]; then
        IP=$(echo $SSH_CLIENT | awk '{print $1}')
        PORT=$(echo $SSH_CLIENT | awk '{print $3}')
        HOSTNAME=$(hostname -f)
        IPADDR=$(hostname -I | awk '{print $1}')
        curl http://ipinfo.io/$IP -s -o $TMPFILE
        CITY=$(cat $TMPFILE | jq '.city' | sed 's/"//g')
        REGION=$(cat $TMPFILE | jq '.region' | sed 's/"//g')
        COUNTRY=$(cat $TMPFILE | jq '.country' | sed 's/"//g')
        ORG=$(cat $TMPFILE | jq '.org' | sed 's/"//g')
        TEXT="Login Alert!!
Datum: $DATE_EXEC:
Gebruiker: ${USER} logde in op $HOSTNAME ($IPADDR)
vanaf: $IP
geoip: $ORG - $CITY, $REGION, $COUNTRY"
        curl -s --max-time $TIMEOUT -d "chat_id=$USERID&disable_web_page_preview=1&text=$TEXT" $URL > /dev/null
        rm $TMPFILE
fi
```

PAM.d configuratie

/usr/local/bin/tgbot.sh

```
#!/bin/bash
# place this following line at the bottom of /etc/pam.d/login
# session optional pam_exec.so type=open_session seteuid /usr/local/bin/tgbot.sh
# This file itself in /usr/local/bin/
KEY="==Api Token=="
URL="https://api.telegram.org/bot$KEY/sendMessage"
TARGET="==xxxxxx==" # Telegram ID of the conversation with the bot, get it from /getUpdates API

TEXT="User *$PAM_USER* logged in on *$HOSTNAME* at $(date '+%Y-%m-%d %H:%M:%S %Z')
Remote host: $PAM_RHOST
Remote user: $PAM_RUSER
Service: $PAM_SERVICE
TTY: $PAM_TTY"

PAYLOAD="chat_id=$TARGET&text=$TEXT&parse_mode=Markdown&disable_web_page_preview=true"

# Run in background so the script could return immediately without blocking PAM
curl -s --max-time 10 --retry 5 --retry-delay 2 --retry-max-time 10 -d "$PAYLOAD" $URL > /dev/null 2>&1 &
```