Linux: als je buitengesloten bent door je eigen beveiliging

Handleiding van Helpmij.nl

Auteur: femke98

April 2012

Wanneer je jezelf hebt buitengesloten met een root wachtwoord wat niet klopt en geen gebruik kan maken van de herstel modus, is dat een lastige situatie. Velen gaan meteen aan het herinstalleren, maar zelfs wanneer je jezelf in zoverre buiten hebt gesloten is het nog mogelijk om je fout te herstellen, dit kan op twee manieren. Het zijn beide geen super gemakkelijke manieren dus let wel goed op dat je geen fouten maakt. De tweede manier kan helemaal grafisch maar **LET WEL HEEL GOED OP DAT JE NIETS VERKEERD DOET.**

1) Via een live-cd met chroot

* Start op vanaf een live-cd

* Open een terminal

Kopieer de volgende regels één voor één naar de terminal. (in de meeste terminals kan je plakken met de: [ctrl]+[shift]+V toetsencombinatie)

sudo su - fdisk -l

Probeer nu te bepalen welke partitie jouw installatie bevat, let op het type en de grootte. Als Gparted aanwezig is op je live-cd dan kan je die ook gebruiken om je partitie te bepalen, sommigen vinden dat prettiger.

In de volgende commando's dien je /dev/sdXx te vervangen door de partitie waarop jouw installatie staat (bv /dev/sda1 of /dev/sdb3)

mount /dev/sdXx /mnt chroot /mnt /bin/bash

Wanneer bovenstaande commando's je geen error terug hebben gegeven bevind je je nu in de Bash schil van je installatie en kan je de wachtwoorden aanpassen met passwd:

passwd gebruikersnaam

Ben je klaar met aanpassen dat kan je met de volgende commando's de installatie verlaten, de partitie afkoppelen en je pc herstarten:
exit umount /mnt reboot

2) Via een live-cd je wachtwoordbestand aanpassen

Nog een manier is door het aanpassen van het opgeslagen wachtwoord van jouw gebruiker in het configuratiebestand /etc/shadow. Dit is bijna zo gemakkelijk als het klinkt, alleen moet je erg goed opletten omdat het wachtwoord niet open en bloot word weergegeven maar geëncrypteerd.

Start op vanaf een live-cd.
* Open je bestandsbladeraar
* Zoek in de zijbalk naar de partitie waarop je bestanden staan en navigeer naar die partitie
* Navigeer naar de /etc map van de partitie (dus /media/uwschijf/etc)
* Open het bestand shadow in een tekstbewerker.
* Kies in het menu van je tekstbewerker voor opslaan als en sla het bestand op als shadow.back-up

* Sluit de backup en heropen het bestand shadow
* Pas het aan aan de hand van het volgende voorbeeld.

pietje:$1$062ub7BL$Inbf3T1hKRdFipCanNWR/1:15228:0:99999:7:::

En voor de duidelijkheid hetzelfde voorbeeld met alle onderdelen in kleur:

(het wachtwoord is het rode gedeelte)
pietje:$1$062ub7BL$Inbf3T1hKRdFipCanNWR/1:15228:0:99999:7:::

/etc/shadow kan soms behoorlijk lang zijn dus gebruik de zoekfunctie om je gebruikersnaam te vinden. In het bestand staat niet alleen je wachtwoord, dat is slechts het gedeelte tussen de eerste en de tweede dubbele punt. In dit voorbeeld heb ik de gebruiker **pietje** gemaakt met het wachtwoord **wachtwoord**.

De hash voor het wachtwoord wachtwoord is:

$1$062ub7BL$Inbf3T1hKRdFipCanNWR/1

(deze kan je later natuurlijk op de vertrouwde manier weer aanpassen)

Ben je klaar met aanpassen dan kan je je computer herstarten en kan je weer gewoon inloggen.

Extra:
Je kan natuurlijk ook meteen je eigen wachtwoord in shadow plakken, je hebt hiervoor wel een live-cd nodig waarop makepasswd geïnstalleerd is. Je maakt de hash alsvolgt in een terminal:

echo "WachtWoordHier" | makepasswd --clearfrom=- --crypt-md5 |awk '{ print $2 }'

Je kan op deze manier alleen geen leestekens gebruiken in je wachtwoord gezien je blijkbaar alleen " mag gebruiken rond je wachtwoord en sommige leestekens dan door Bash geherinterpreteerd worden als commando's of variabelen. Niet helemaal ideaal dus maar goed... goed genoeg voor een tijdelijk wachtwoord.

Jezelf beveiligen tegen deze methodes:
Natuurlijk kan iemand anders ook wat jij kan en is het dus raadzaam jezelf te beschermen tegen de bovenstaande methoden. Je moet hiervoor wel een wachtwoord kunnen onthouden (of je BIOS moet ondersteuning hebben voor hardware sleutels). Alle bovenstaande manieren kunnen tegengehouden worden door het instellen van een boot wachtwoord in je BIOS. Wanneer je dan wilt opstarten van een cd of USB-stick kan dat alleen als je het boot wachtwoord hebt en dat heeft je zusje of de inbreker als het goed is niet. Natuurlijk is ook deze beveiliging niet 100% waterdicht maar het omzeilen ervan vereist een behoorlijke technische kennis van de hardware.

Met dank aan socialdefect, lid van het Ubuntu forum.