/ADMIN CORNER

DE ACHTERPOORT NAAR JOUW PC

Als je dacht dat jouw Linux-installatie erg veilig is, dan moeten we je teleurstellen. Wist je dat de meeste distributies toelaten om een root shell te openen zónder enig wachtwoord in te geven? Tien seconden navigeren door de bootloader volstaat al om volledige toegang te krijgen tot jouw PC! **Filip Vervloesem**

Het laatste decennium hebben de meeste distro's een enorme vooruitgang geboekt op het vlak van gebruiksvriendelijkheid. Linux installeren, is makkelijker dan ooit en de hardware-ondersteuning is prima in orde. Ook de kans dat je op de commandline terugvalt, bijvoorbeeld omdat je systeem niet correct boot, is kleiner dan ooit. Toch loopt soms iets onverwacht mis. Ook in dat geval willen de distro's je zo goed mogelijk op weg helpen. In Ubuntu en Linux Mint is er bijvoorbeeld een "recovery mode" aanwezig in het Grub bootmenu. Op een dualbootsysteem krijg je het bootmenu te zien bij elke boot: zo kies je of je Linux of Windows (of een andere Linux-distro) wilt booten. Heb je slechts één Linux-distro geïnstalleerd op jouw systeem? Dan verbergt Grub het menu om sneller te booten, want er valt toch niets te kiezen. Wil je alsnog het menu openen, druk dan op de Shift-toets vlak na het booten van je computer. Voor alle zekerheid houd je die toets ingedrukt, zo mis je het juiste moment niet.

RECOVERY MENU

In dit voorbeeld gaan we uit van Linux Mint 18.3. De eerste entry is diegene die Grub standaard opstart: bij ons is dat "Linux Mint 18.3 Cinnamon 64-bit". Daaronder zie je een tweede entry, genaamd "Geavanceerde opties voor Linux Mint 18.3 Cinnamon 64-bit". Selecteer die met de pijltjestoets en druk op Enter om het submenu te openen. Onderaan staat nu een entry die eindigt met "(recovery)". Selecteer die entry en druk nogmaals op Enter om het herstelmenu te openen. Grub start nu een minimale subset van het systeem op, zonder grafische omgeving. Een tiental seconden later kom je in een ander menu terecht met acht verschillende opties. Navigeer naar de voorlaatste, genaamd "root" om een root shell te openen. En ja hoor, je hoeft daarvoor het root-wachtwoord niet in te geven! De root-gebruiker heeft uiteraard toegang tot het volledige bestandssysteem van jouw Linux-installatie. Maar laat jij jouw PC even onbeheerd achter, dan duurt het dus letterlijk maar 30 seconden tot iemand in je bestanden kan spieken! Had je dat gedacht toen je van Windows naar Linux was overgestapt?

OOK ZONDER RECOVERY

Niet alle distributies bieden een gebruiksvriendelijk recovery menu aan, zoals Ubuntu en Linux Mint. In die twee distributies kan je het menu overigens ook uitschakelen, als je dat je een veiliger gevoel geeft. Dat veilige gevoel is helaas onterecht. Het is dan nog steeds mogelijk om een root shell te openen vanuit Grub! Selecteer gewoon de standaard boot entry en druk op de e-toets in plaats van Enter. Je krijgt nu een twintigtal regels te zien met allerlei opties om jouw distro te booten. Gebruik de pijltjestoetsen om te navigeren naar de regel die begint met "linux". Aan het einde van die regel voeg je het woord "single" toe, om in zogenaamde "single user mode" te booten. Met Control-x of F10 boot je jouw aangepaste entry van het bootmenu. Je komt nu wederom terecht in een root shell zónder enig wachtwoord in te geven. Erg moeilijk was dat niet!

BOOTEN IN BASH

In sommige distributies moet je wél het root-wachtwoord invoeren om een shell te openen en dan werken bovenstaande trucs niet. Toch is het ook in die distro's een fluitje van een cent om binnen te komen. In plaats van "single" voeg je de optie "init=/bin/bash" toe aan de boot entry. Linux slaat dan het grootste deel van het normale bootproces over en start rechtstreeks een bash-shell… als root! Even het root-wachtwoord wijzigen vanuit die shell? Geen probleem: mount het root-filesystem read/write en kies een nieuw wachtwoord:

```
$ mount -o remount,rw /
$ passwd
```

Omdat je het normale bootproces omzeild hebt, kan je de computer nu niet meer correct afsluiten. Zodra je de shell sluit, krijg je een kernel panic en moet je het systeem resetten. Zorg er dus zeker voor dat het gewijzigde wachtwoord netjes is weggeschreven naar het root-filesystem:

```
$ sync
$ mount -o remount,ro /
$ exit
```

BEVEILIGEN

Word je al zenuwachtig bij het lezen van bovenstaande trucs? Weet dan dat je Grub kan beveiligen met een wachtwoord: zo kan niemand nog morrelen aan de boot entries. Anderzijds is dat slechts een vertragende maatregel: je hoeft maar een live-cd te booten en je harde schijf te mounten om aan de data te kunnen. Dat kan je dan weer verhinderen met een wachtwoord op je BIOS en door enkel booten vanaf de harde schijf toe te laten. En dat omzeil je weer door je PC te openen en je harde schijf eruit te halen. Zo zie je maar: encryptie is de enige methode die afdoende is om je data te beveiligen tegen mensen die fysieke toegang hebben tot jouw computer.