# SSH Keys

Het is veiliger om een lang en sterk wachtwoord te nemen, dit maakt je account namelijk veel veiliger. Een groot nadeel hiervan is echter wel dat je dit sterke wachtwoord iedere keer opnieuw moet invoeren als je een `sudo` command uit wil voeren. Het is dan ook vrij verleidelijk om de vraag naar het wachtwoord uit te schakelen. Dit kan maar levert alsnog een veiligheidsrisico op. Dit is het moment om over te stappen op SSH keys.

Dit werkt op ieder apparaat dat draait op Debian. Dus ook Raspbian.

# Wachtwoord prompt uitschakelen

Laten we beginnen met het uitschakelen van de prompt voor het wachtwoord als je sudo gebruikt.

1. Voer het commando `sudo visudo` uit.
2. Voeg een nieuwe lijn toe met de volgende inhoud, verander <user> naar je gebruikersnaam.
    1. `<user> ALL=(ALL) NOPASSWD: ALL`
3. Sla het bestand op.
4. Voer `sudo -k` uit om de cache te legen.
5. Test het uit met `sudo ls`.

Helemaal top! De prompt is uitgeschakeld!

# SSH key aanmaken

Dan gaan we nu beginnen met het aanmaken en het vereisen van een SSH key.

> Let op dat je dit niet doet als root-user, dan kan je namelijk niet inloggen met de key!

1. Open een SSH-client (bijvoorbeeld Termius) of open de Terminal.
2. Voer het commando `ssh-keygen` uit om een SSH key te genereren.
3. Druk op enter als je gevraagd wordt waar op te slaan. De standaard locatie is `/home/<user>/.ssh`.
4. Voer eventueel een passphrase in, dit is niet verplicht. Laat de prompt leeg om dit niet in te stellen.
5. Neem de gegenereerde key in gebruik met `ssh-copy-id <user>@<ip-adres>`. Vul bij *<user>* je gebruikersnaam in en bij *<ip-adres>* het adres van het apparaat.
6. Importeer het `/home/<user>/.ssh/id_rsa` bestand in je SSH-client.

Probeer in te loggen zonder wachtwoord. Als dit lukt dan kan je door. Als dit niet gaat verwijder je de .ssh-map en probeer je het opnieuw.

Op dit moment is je key actief maar inloggen met een wachtwoord is nog steeds toegestaan. Dit moeten we uitzetten. Volg de volgende stappen om dit te doen.

1. Bewerk het SSH-config bestand met `sudo nano /etc/ssh/sshd_config`.
2. Ergens rond lijn 58 vind je P*asswordAuthentication*, uncomment deze. Pas *yes* aan naar *no*. Het moet er als volgt uit zien `PasswordAuthentication no`.
3. Herstart de ssh-service met `sudo systemctl restart ssh`.

Nu is het inloggen met een wachtwoord uitgeschakeld en kan je enkel nog maar inloggen met een geldige SSH key. Probeer het uit in een nieuw tabblad voordat je je huidige sluit. Op deze manier weet je zeker dat je jezelf niet buitensluit. Kopiëer de inhoud van het id_rsa-bestand naar je computer en sla deze ergens op waar je hem makkelijk kan vinden en geef het een goede naam. Bij voorkeur sla je de inhoud op in een wachtwoordmanager zodat je er altijd bij kan en niemand deze zomaar kan kapen.

Het is handig om voor de zekerheid een programma als VNC Server geïnstalleerd te hebben zodat je altijd nog op het apparaat zelf in de CLI kan komen om wijzigingen ongedaan te maken of eventueel een nieuwe SSH key te genereren als je er niet meer in komt.

---

Revision #5
Created 1 January 2021 23:07:56 by Nicky Hendriks
Updated 5 January 2021 14:54:30 by Nicky Hendriks