

23-02-10 - Root Access op de LG GW620

Wat doe je als eerste als je technicus een nieuwe telefoon in handen krijgt? Dan ga je eerst alles naar je eigen hand zetten met de normale opties en als je daarmee klaar bent, ga je op zoek naar de verborgen mogelijkheden. De LG GW620 draait op Android, het Open Source Operating System van Google. En als iets "open source" is, is het natuurlijk wel heel makkelijk om te kraken.

Wat is Root Access en waarom?

Android is gebouwd op Linux (nog zo'n open source product). Binnen Linux heb je verschillende gebruikers, welke allemaal zo hun eigen permissies hebben. In Microsoft Windows kunnen we een dergelijk systeem ook vinden, namelijk de Administrator en Gebruiker-accounts. In tegenstelling tot Windows, worden de verschillende gebruikerniveaus in Linux wel vaak gebruikt. Uiteraard komt dit doordat Linux door de nerds professionals gebruikt wordt, welke vaak meer nadenken over de risico's (en deze ook vaker lopen). Overigens mag niet onvermeld blijven dat ook Windows zijn best doet om haar klanten op Gebruiker-accounts te laten spelen en alleen in uiterste nood Administrator-rechten gebruikt (UAC).

Het account met de meeste rechten wordt het root-account genoemd in Linux. Deze heb je als normale gebruiker vrijwel nooit nodig. Daarom hebben de ontwikkelaars van Android bedacht, dat het wel veilig is als dat root-account standaard niet te gebruiken is. Au! Dat doet pijn voor de nerds die toch echt alles uit hun telefoon willen halen. Dat is dan ook precies de reden waarom het woord Rooten is uitgevonden.

LG GW620 Rooten

Let op: Dit artikel is geschreven op basis van diverse handleidingen en getest op één LG GW620 (T-Mobile) met Android 1.5. Ik geef geen enkele garantie dat deze methode op iedere LG GW620 werkt en stel mijzelf niet aansprakelijk/verantwoordelijk voor enige vorm van schade. Het volgen van deze stappen is volledig op eigen risico!

Tip: Maak een backup van je contacten, e-mails, foto's en andere data.

Allereerst moet je [Android SDK](#) installeren en vervolgens de [LG drivers](#). Ik heb de Android SDK geïnstalleerd in C:\AndroidSDK. Dit pad zal ik dan ook hanteren tijdens deze tutorial. Uiteraard kun je zelf een ander pad kiezen.

Nu hebben we een speciaal programma nodig, namelijk [Superuser](#). Dit programma

kun je vergelijken met de UAC (User Account Control) in Windows. Wanneer een programma Root Access wil, krijg je netjes een popup en kun je Yes, No of Always kiezen. Download de zipfile en zet de inhoud op een handige plek. Ik heb deze in C:\AndroidSDK\tools\Superuser gezet. In de zip zit een install.bat en install.sh. Ik raad je aan hier van af te blijven!

Nu we de software klaar hebben staan, kunnen we beginnen met de hack (nogmaals: op eigen risico!).

1. Ga op je telefoon naar Instellingen > Applicaties > Ontwikkeling en vink USB-foutopsporing aan.
2. Toets het volgende "telefoonnummer" in op je telefoon (de LG uiteraard):
3845#*620#
3. Er verschijnt nu automatisch een menu. Ga naar "Module Test", "Stability Test" en klik op "Enable Root Permission". Je krijgt geen melding dat het gelukt is, maar je kunt rustig tien keer klikken.
4. Open de command prompt/shell/terminal/DOS/zwart schermje met witte letters. (Voor de Windows-gebruikers zal dit dus zijn: Start > Alle Programma's > Bureau-accessoires > Opdrachtprompt)
5. Navigeer naar de AndroidSDK en dan Tools (cd C:\AndroidSDK\tools).
6. Zorg dat de usb-kabel van de telefoon is aangesloten en geef nu de opdracht "adb shell". Je komt nu in de "shell" van de telefoon als het goed is. Het kan zijn dat je een melding krijgt dat er een service nog niet gestart is en deze nu gestart wordt. Als deze verbinding niet lukt, start de apparaten dan nog eens opnieuw op en probeer het nog een keer van voor af aan.
7. Sluit de shell door "exit" te typen en op enter te drukken.
8. Geef de opdracht "adb remount", zodat alle read/write-permissies goed komen te staan.
9. Voer nu dit uit: adb shell "cat /system/xbin/su > /system/xbin/su.original" (inclusief de aanhalingstekens). Dit maakt een backup van je originele Superuser.
10. Zet nu de nieuwe Superuser erop met: adb push Superuser/bin/su /system/xbin/su (waarbij Superuser/bin/su het pad is naar de su-file op je computer)

11. Zet Superuser ook in de bin-directory van Android: adb push Superuser/bin/su /system/bin/su

12. Stel de rechten in met: adb shell chmod 4755 /system/sbin/su

13. En: adb shell chmod 4755 /system/bin/su

14. Nu rest ons enkel de installatie van de het programma nog: adb install Superuser/bin/Superuser.apk

Start nu een programma dat Root-access nodig heeft (aNetShare of Wireless Tether for Root Users). Je krijgt als het goed is nu netjes een popupje wanneer het programma Root-acties probeert uit te voeren. Met aNetShare had ik zelf wat problemen, doordat deze de actie zelf al geannuleerd had voordat ik op Yes had gedrukt. De oplossing was om op Always te klikken en dan nog een keer te starten.

Laat even een berichtje achter of het gelukt is!