Wie kommt Nethunter auf ein Nexus 5!?

WORK IN PROGRESS

Vorbereitungen

Entwickler-Optionen

Als erstes müssen die „Developer options“ aktiviert werden:

Settings → „About phone“ → 7 x auf „Build number“ tippen

USB debugging

Als nächstes muss „USB debugging“ aktiviert werden:

Settings → „Developer options“ → Schalter rechts neben „USB debugging“ aktivieren

Bootloader entsperren

Android Debug Bridge (adb) herunterladen und entpacken.

In dem Verzeichnis eine Shell (z. B. bash unter GNU/Linux, zsh unter macOS oder PS unter Windows) öffnen.

Das Gerät durch eine etwas längere Betätigung der Power-Taste und anschließendem Fingertipp auf „Power off“ ausschalten.

Das Gerät mit der Tastenkombination „Volume up“ + „Volume down“ + Power einschalten.

Das Nexus 5 per USB-Kabel mit dem Rechner (in meinem Fall ein MacBook Pro) verbinden.

In der geöffneten Shell folgende Befehle ausführen…

Wird das Gerät erkannt (?):

```
mbp% ./fastboot devices
02e6510b21304672    fastboot
```

Den bootloader entsperren:

```
mbp% ./fastboot oem unlock
                                                    OKAY [ 30.441s]

Finished. Total time: 30.442s
```

Nexus 5 neu starten:

```
mbp% ./fastboot reboot
Rebooting                                          OKAY [  0.001s]
Finished. Total time: 0.001s
```

Da das entsperren ein Zurücksetzen des Gerätes mit sich bringt, muss jetzt etwas länger gewartet werden (ca. 10 Min.).

Wiederherstellungs-Partition austauschen

TWRP für das Nexus 5 herunterladen:

```
mbp% curl https://eu.dl.twrp.me/hammerhead/twrp-3.3.1-0-hammerhead.img -o
recovery.img
```

Überprüfen, dass die Datei während des Downloads keinen Schaden genommen hat:

```
mbp% openssl dgst -sha256 recovery.img
SHA256(recovery.img)=
4cc886f19eb42b37f3a7541fb07c5e3cf18124047fbc524253794ebb07bad23a
```

Wird das Gerät erkannt (?):

```
mbp% ./fastboot devices
02e6510b21304672    fastboot
```

TWRP in die Wiederherstellungs-Partition schreiben:

```
mbp% ./fastboot flash recovery recovery.img
Sending 'recovery' (13290 KB)                      OKAY [  0.629s]
Writing 'recovery'                                 OKAY [  1.060s]
Finished. Total time: 1.891s
```

Bootloader des Nexus 5 neu starten:

3x „Volume up“ („restart bootloader“) → mit Power bestätigen

In die neue Wiederherstellungs-Partition starten:

2x „Volume up“ („Recovery Mode“) → mit Power bestätigen

"rooten"

```
mbp% curl
https://github.com/topjohnwu/Magisk/releases/download/v19.3/Magisk-v19.3.zip
```

```
mbp% ./adb devices
List of devices attached
```

```
02e6510b21304672    recovery
```

```
mbp% ./adb push Magisk-v19.3.zip /sdcard/
Magisk-v19.3.zip: 1 file pushed. 4.6 MB/s (5348187 bytes in 1.104s)
```

boot into recovery

install magisk

reboot (TWRP App darf, muss aber nicht installiert werden)

Browser öffnen

https://magiskmanager.com/#How_to_Download_Magisk_Manager_Latest_Version_734_For_Android_2019_Method_1

„Magisk Manager“-App downloaden

Installation aus nicht vertrauenswürdigen Quellen ermöglichen

Im Datei-Manager die „Magisk Manager“-App anklicken

„Magisk Manager“-App starten und prüfen, ob alles ordnungsgemäß installiert ist

Die Vorbereitungen nochmal durchführen

```
mbp% curl
https://images.offensive-security.com/nethunter/nethunter-hammerhead-marshmallow-kalifs-full-2019.3.zip -o nethunter.zip
```

```
mbp% openssl dgst -sha256 nethunter.zip
SHA256(nethunter.zip)=
b1f9e8aee546011da76aa12b7590467a7983ce2efc723be9955fb9ca85dcf339
```

```
mbp% ./adb devices
List of devices attached
02e6510b21304672    device
```

```
mbp% ./adb push nethunter.zip /sdcard/
nethunter.zip: 1 file pushed. 5.8 MB/s (1444372465 bytes in 235.697s)
```

boot into recovery

install nethunter

reboot

fertig!

From:
https://wiki.neumannsland.de/ - **Patricks DokuWiki**

Permanent link:
https://wiki.neumannsland.de/hacking:nexus5

Last update: **2019/09/28 13:44**