

1 Installation von Kali Linux auf Linux-Deploy

Die Installation von Kali Linux Distribution auf Linux-Deploy folgt die folgenden Anweisungen:

Geroottetes Android-Tablet für diese Installation erforderlich

Das Gerät muss gerootet sein. "Root" unter Android ist ganz wichtig. Im Grunde bezeichnet "root" ein Nutzer, der volle Zugriffs- und Schreibrechte auf das System hat.

Es gibt viele Vorteile, wenn ein Gerät gerootet ist. Beispiele:

- Funktionen nachrüsten (z.B. Multi-User auf Handys)
- CPU/GPU-Anpassungen (z.B. für mehr Leistung)

Die administrativen Rechte durch SuperSU

Die administrativen Rechte unter Android werden durch *SuperSU* geregelt, das heißt, jede andere App, die Root-Rechte fordert, muss durch die genannte App manuell freigegeben werden.

benötigte Apps

Die drei folgenden Apps sind vor der Installation von Kali Linux zu installieren.

Die Virtuelle Maschine Busy Box Busybox ist eine Software, die viele der Standard-Unix-Befehle, wie die GNU Core Utilities implementiert. Da jede ausführbare Binärdatei für GNU / Linux mehrere Kilobyte zusätzliche Informationen enthält, die Idee von kombinieren mehr als zweihundert Programme in eine ausführbare Datei ist gut. BusyBox ist eine freie Software.

Linux Deploy Diese Anwendung ist Open-Source-Software für die schnelle und einfache Installation des Betriebssystems (OS) GNU / Linux auf Ihrem Android-Gerät. Die Anwendung erstellt ein Disk-Image auf einer Flash-Karte, montiert es und installiert eine OS-Verteilung. Anwendungen des neuen Systems werden in einer chroot-Umgebung ausgeführt und arbeiten mit der Android-Plattform zusammen.

Android VNC Viewer VNC Viewer ist das ursprüngliche Open Source (GPL) Remote-Desktop-Programm für Android-Geräte. Es ist kostenlos. VNC Viewer ermöglicht den Fernzugriff auf Linux.

Installation und Konfiguration

Die folgende Abbildung 1 zeigt die Schritte zu folgen.

In dieser Abbildung ist genau geschrieben in 8 Schritte, was wir tun sollen. Vom Übernahme der Nutzungsrechten bis die Verbindung mit VNC Viewer.

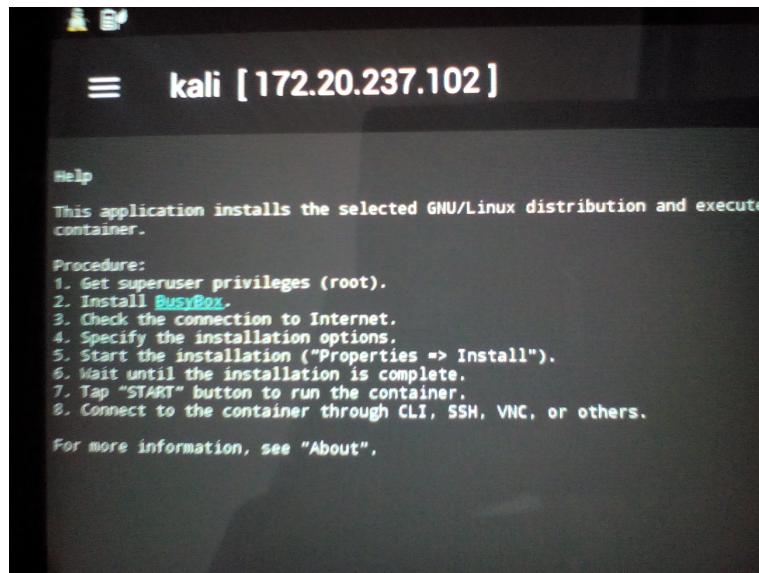


Abbildung 1: Schritte für die Installation von Kali Linux auf Linux Deploy

Wir müssen die Parameter von Kali Linux überprüfen, diese Parameter sind in den Abbildungen 2a, und 2b veranschaulicht.

In der Abbildung 2a sind die Parameter wie folgt konfiguriert:

- die Architektur: armhf (relativ einfache Architektur als andere Prozessorfamilien und geringer Stromverbrauch bei hoher Leistungsfähigkeit)
- Distribution Suite: Kali-Rolling (Sie ist zuverlässig, und die Pakete werden immer wieder aktualisiert)
- Quellpfad: <http://http.kali.org/kali/> (Adresse vom fernen Repository)
- Installation Pfad: \\$\{EXTERNAL_STORAGE\}\linux.img (Die Stelle, wo das Abbild erstellt wird)
- Image Größe(MB): Automatische Berechnung
- Dateisystem: Auto \\ - Benutzername: Kali (diese Parameter kann angepasst werden. Wir haben Kali ausgewählt)
- Benutzerpassword: kali0123 (diese Parameter kann auch angepasst werden. Wir haben Kali0123 ausgewählt)

- Privileged Users: Root
- DNS Server: Automatische Erkennung

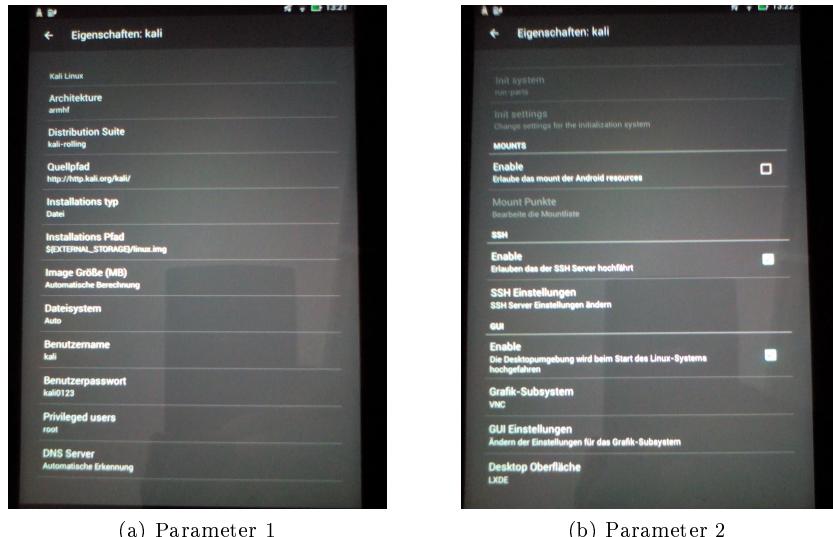


Abbildung 2: Zu überprüfende Eigenschaften von Kali Linux

In der Abbildung 2b sind die Parameter wie folgt konfiguriert:

- SSH Enable (Erlaube das Mount der Android Resources)
- GUI Enable (Die Desktopumgebung wird beim Start des Linux-Systems hochgefahren)

Ganz wichtig für die Installation von Kali Linux, eine gute Internet Verbindung.

Alle benötigten Pakete werden aus unseren Repositories heruntergeladen, das heißt wir benötigen eine schnelle Internetverbindung, um diese Installationsmethode zu verwenden.

Wir müssen auch mindestens 2GB frei auf der internen oder externen Speicher lassen.

Wir klicken dann auf *Install* (Properties → Install)

Sobald die Einstellungen fertig sind, klicken wir auf *Install*.

Diese Aktion wird einen Kali Linux-Bootstrap direkt aus den Repositories starten. Diese Vorgang nimmt ungefähr 30 Minuten Zeit in Anspruch. Wir laden eine Basisinstallation von Kali Linux auf Minimum herunter.

Wir klicken dann auf *Configure*

Die Abbildung 3 zeigt wie das aussieht.

Im Anschluss klicken wir auf *Start*. Sobald die automatische Konfiguration abgeschlossen ist, können wir Linux Deploy automatisch installieren und laden das Kali Linux Chroot-Image. Dazu gehört auch der Start von Diensten wie

SSH und VNC für leichteren Fernzugriff. All dies geschieht automatisch, indem man den Start-Button drückt.

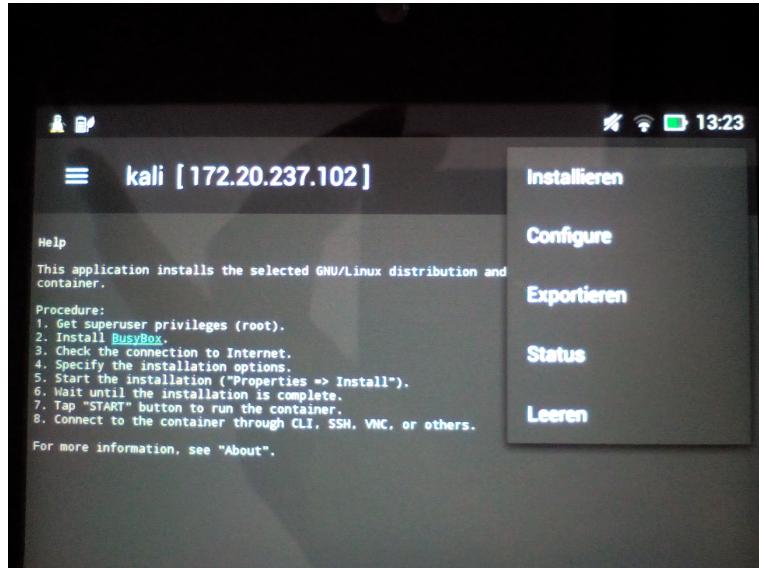
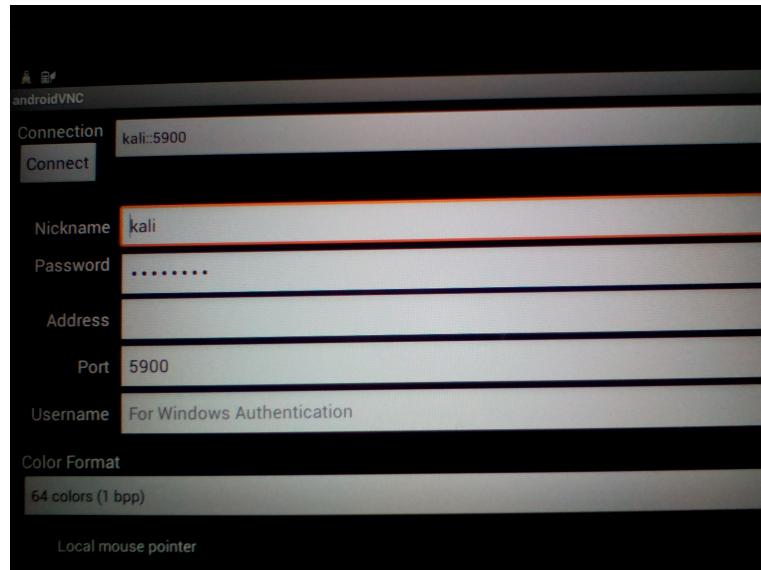


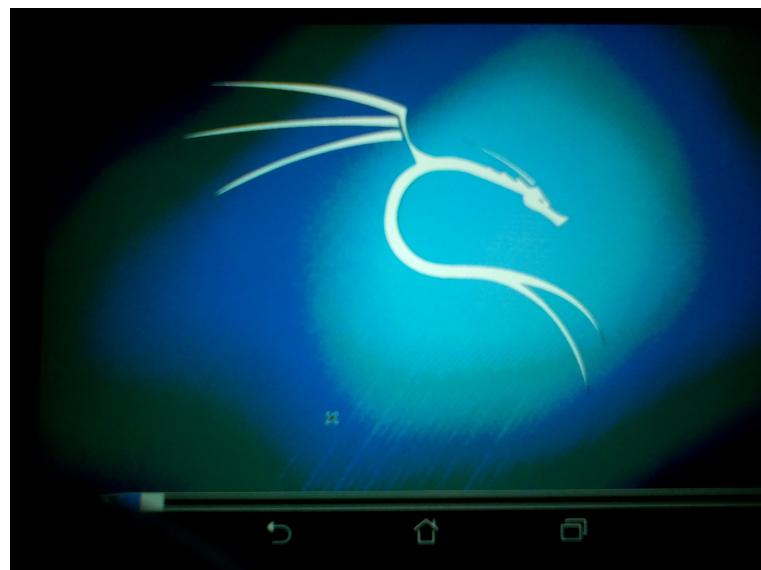
Abbildung 3: Konfigurationsparameter der Linux Deploy Parameter

Meldung mit Android VNC Viewer

Wir melden uns an Android VNC Viewer mit normalen User Parameter, was in der Abbildung 4a zu sehen ist. Anschließend erscheint die GUI von VNC Viewer in der Abbildung 4b.



(a) Anmeldung an Android VNC Viewer



(b) GUI von VNC Viewer

Abbildung 4: Anmeldung und Startbildschirm des VNC Viewer

Literatur Installing and und Running Kali Linux with Linux Deploy. [?]

2 Installation Nethunter

Das Kali Linux Nethunter Projekt ist das erste Open Source Android Penetrationstests Plattform für Nexus-Geräte. NetHunter unterstützt Wireless 802.11 Frame-Injektion sowie BadUSB MITM Angriffe, etc. Die folgende Schritte sind zu folgen, um die Installation von Nethunter zu führen.

Backup

Das Datensicherung ist ganz wichtig. Es passiert immer wieder, dass durch Hardwaredefekte, Systemfehler oder Benutzerfehler die Daten nicht wiederhergestellt werden können.

Wir machen ein Backup vor der Installation, um die Daten zu speichern. Diese Aktion haben wir mit Nexus Root Toolkit angelegt. Das Bild 5dient der Darstellung des Install-Button.

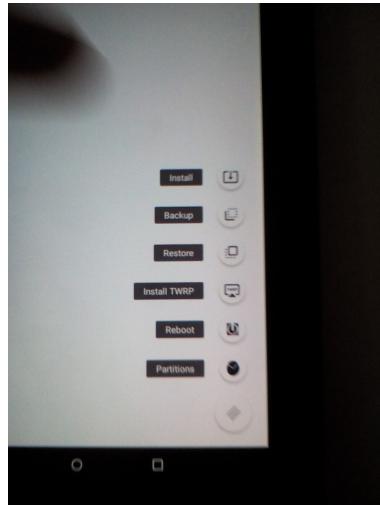


Abbildung 5: Installation

Geroottetes Android-Tablet für diese Installation erforderlich

Das Gerät muss gerootet sein. Die Apps für Nethunter benötigen Super User/Administratorische Rechte.

Sobald der Nutzer Admin-Rechte besitzt, kann er unter Android im Prinzip das komplette System verändern. Dazu gehören unter anderem UI Customization genauso wie das Ändern von Systemeinstellungen. Per Root ist es zum Beispiel möglich, einen systemweiten Equalizer zu installieren, die maximale Lautstärke zu erhöhen und selbst die gesamte Menüführung anzupassen. Per Root-Zugriff lassen sich auch vorinstallierte Apps entfernen, die von vielen Herstellern mitgeliefert werden.

Der Bootloader

Der Bootloader (bootstrap loader) muss entsperrt sein.

Er ist eine Software, der ein oder mehrere Betriebssysteme (Multi-Boot) zu laufen ermöglicht. Das heißt er erlaubt mehrere Systeme zu unterschiedlichen Zeiten auf der gleichen Maschine.

Der Bootloader lädt weitere Teile des Betriebssystems und stellt sicher, dass alles richtig und vollständig ist.

Die administrativen Rechte durch SuperSU

Die administrativen Rechte unter Android werden durch *SuperSU* geregelt.

BusyBox

Die Virtuelle Maschine ist eine Software, die viele der Standard-Unix-Befehle, wie die GNU Core Utilities implementiert. Sie ist automatisch installiert.

Die richtige Version von Kali Nethunter herunterladen

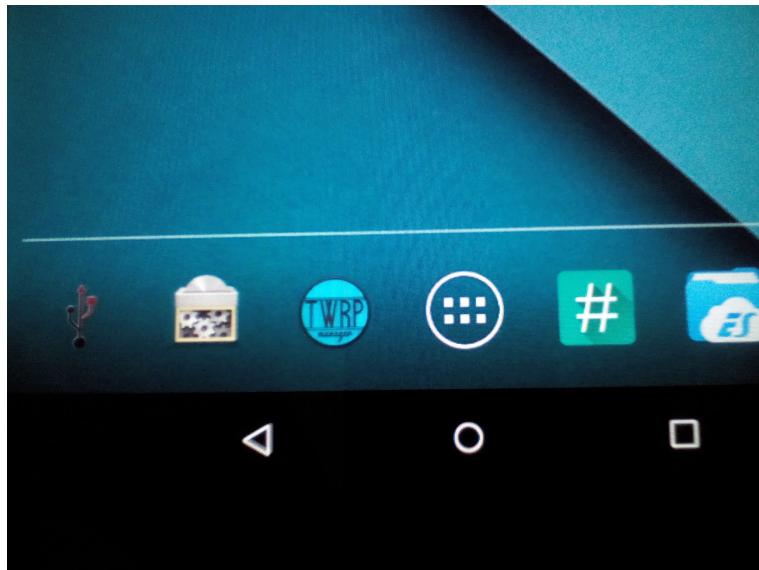
Laden die richtige Version von Nethunter für Nexus 7 Android 5.1.1 herunter. Diese Version heißt *Lollipop* und ist verfügbar unter:

- <http://null-byte.wonderhowto.com/how-to/flash-kali-nethunter-oneplus-and-nexus-devices-most-as-secondary-rom-0162389/>

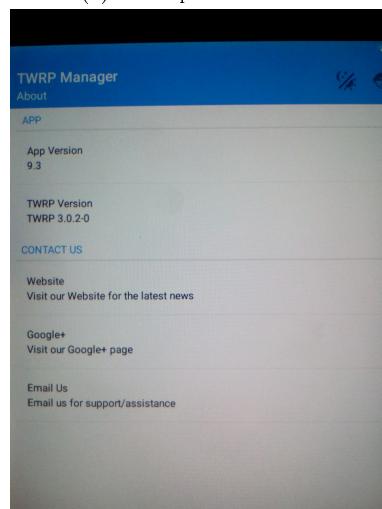
TWRP custom Recovery Installen

Mit Team Win Recovery Project (TWRP) können wir Custom-ROMs installieren und ein komplettes Backup unseres Android-Tablet erstellen. Schauen die Abbildung 6a und 6b an, wie TWRP aussieht, sein Version und Kontakt.

Mit TWRP wählen wir die NetHunter-ZIP-Datei für die Installation aus. Anschließend flaschen wir das Gerät, mit dem Button “Flash Now”. Die Abbildung 7 zeigt das.



(a) Startoption TWRP



(b) Version und Kontakt Anzeige
TWRP

Abbildung 6: TWRP Parameter

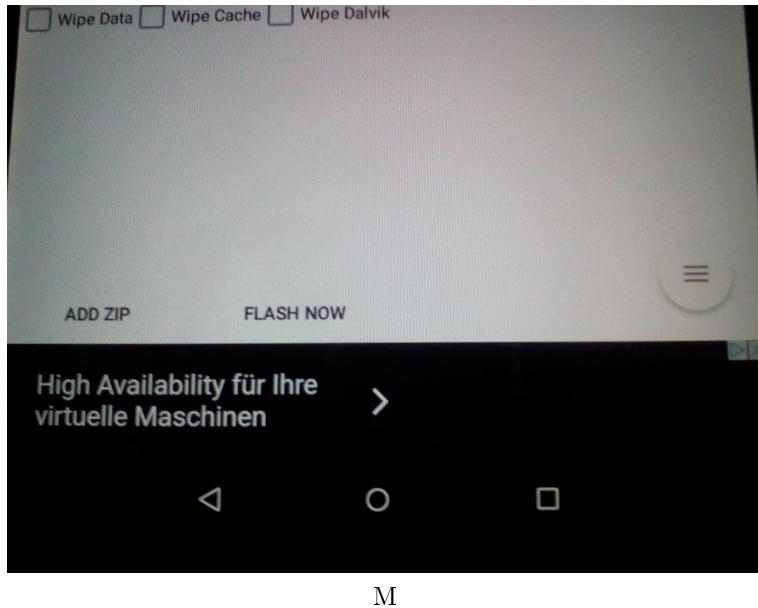


Abbildung 7: Add Zip unf Flash

Danach wird eine “Security Warning” ausgegeben. (Hinweis bezüglich Haf-tung, etc.) Anschauen 8a

Nun wählen wir die Flash-Methode aus. Schauen die Abbildung 8b

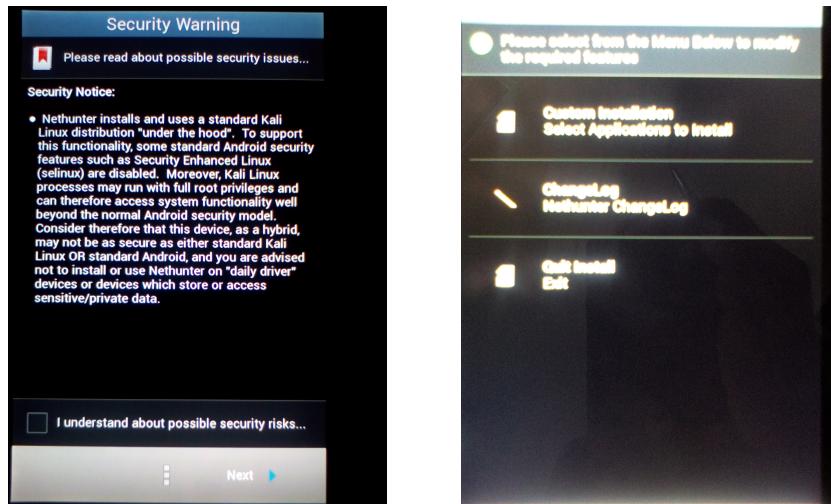
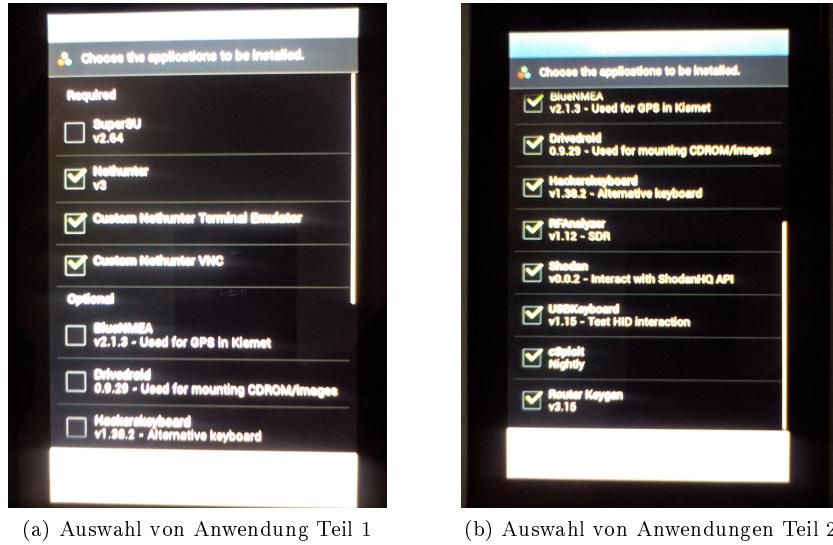


Abbildung 8: Hinweise und Optionen bei der NetHunter Installation



(a) Auswahl von Anwendung Teil 1

(b) Auswahl von Anwendungen Teil 2

Abbildung 9: Anzeigen der möglichen, zu installierenden Anwendungen

Dann wir wählen die App zu installieren. Diese Apps können zusätzlich zu Nethunter installiert werden. Aber für das Projekt wir brauchen die nicht.
Diese Anwendungen sind in der Abbildung 9 zu sehen.

- Nethunter
- Custom Nethunter Terminal Emulator
- Custom Nethunter VNC (Der VNC-Dienst wird auf dem Localhost-Interface oder external auch zuhören)
- BlueNMEA (Sie ist eine Android-Anwendung, die Standortdaten über Bluetooth (RFCOMM) oder TCP im NMEA-Format sendet.)
- drivedroid (Dieses Tool ermöglicht uns emulierte NetHunter zu haben (a bootable ISO or USB))
- Hackerskeyboard
- RF-Analyser (Diese App hilft für die Visualisierung von dem Frequenzspektrum)
- USB-Keyboard (Das Tool kann sich als Tastatur über HID-Stil-Attacken Z.B masquen)
- Router Keygen (frei WPA / WEP-Schlüssel-Generator für mehrere Router auf der ganzen Welt.)

Endlich die Installation starten. Die Abbildung 10 zeigt das.

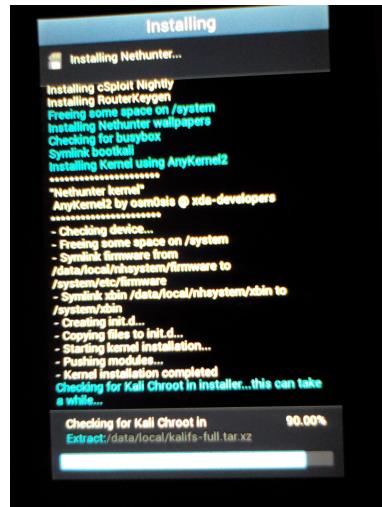


Abbildung 10: Darstellung der Installation von NetHunter

Literatur: Installing and und Running Kali Nethunter. [?]