



Kali Nethunter (without root) by F12-Lab

▼ Installation

1st Search for **Termux** on the internet, don't select the first one but the one that says **F-Droid**. Download **F-Droid**, search for **Termux** (Terminal emulator with packages) in it, and install it (it will say it's a virus but ignore that).

2nd Open **Termux**, run "pkg update" (accept everything).

3rd Enable **Termux's** access to the phone's storage with "termux-setup-storage", accept.

4th Install wget with "pkg install wget".

5th Install the package containing nethunter "wget -O install-nethunter-termux <https://offs.ec/2MceZWr>".

6th Do "ls" and you'll see install-nethunter-termux in white, so give it permissions with "chmod +x install-nethunter-termux". Do "ls" again and now it will appear in green.

7th Start the installation by typing "./install-nethunter-termux".

8th A window will open, select 1 (most complete option) (This process takes quite a while, especially rootfs).

9th When it has finished executing, it's recommended to choose no, this will free up space consumed by the rootfs.

9.1 If when executing nethunter it says it hasn't been found, then we've encountered a bug in this installation repository. For this, we should execute ["./install-nethunter-termux"](#) again, and choose the same option as before (If we chose 1, we choose 1 again). Then we'll see the following comment, where we'll say NO.

```
#####
##      a8P      db      88      88      ##
##      .88'      d88b      88      88      ##
##      88'      d8''8b      88      88      ##
##      d88      d8''8b      88      88      ##
##      8888'88.      d8YaaaaY8b      88      88      ##
##      88P' Y8b      d8''''''''8b      88      88      ##
##      88      '88.      d8'      '8b      88      88      ##
##      88      Y8b d8'      '8b 888888888 88      ##
##
##### NetHunter #####

[*] Checking device architecture ...

[1] NetHunter ARM64 (full)
[2] NetHunter ARM64 (minimal)
[3] NetHunter ARM64 (nano)
Enter the image you want to install: 1

[*] Checking package dependencies...
  proot is OK
  tar is OK
  axel is OK
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Calculating upgrade... Done
0 upgraded, 0 newly installed, 0 to remove and 0 not up
graded.

[?] Existing image file found. Delete and download a new
one? [y/N] N
ESC / - HOME ↑ END PGUP
```

Then, after this, it will start downloading the system, this process will take a while if we chose option 1.

```
[*] Checking device architecture ...

[1] NetHunter ARM64 (full)
[2] NetHunter ARM64 (minimal)
[3] NetHunter ARM64 (nano)
Enter the image you want to install: 1

[*] Checking package dependencies...
  proot is OK
  tar is OK
  axel is OK
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Calculating upgrade... Done
0 upgraded, 0 newly installed, 0 to remove and 0 not upg
raded.

[?] Existing image file found. Delete and download a new
one? [y/N] N
[!] Using existing rootfs archive

[*] Extracting rootfs...
```

9.2 When it's finished, we'll see an error message, like this:

```
[*] Extracting rootfs...

[?] Delete downloaded rootfs file? [y/N] n

[*] Configuring NetHunter for Termux ...
./install-nethunter-termux: line 361: chroot/kali-arm64/
etc/resolv.conf: No such file or directory
~ $
```

What we should do to fix this error is to execute in the root directory where we are "`mkdir chroot`". Then we can do "`ls`" to see that the folders "`chroot`" and "`kali-arm64`" are there. Then after checking this we should do "`cp -r kali-arm64 chroot`" (This process also takes time).

9.3 When it has been copied, we should execute "`./install-nethunter-termux`" again and say NO to everything it asks us, then we'll have it installed.

10th Now you can see the various options to start your kali. When we start **Termux** we'll have to type "`nh`" or "`nh -r`" to access kali.

```
[=] Kali NetHunter for Termux installed successfully

[+] To start Kali NetHunter, type:
[+] nethunter                # To start NetHunter CLI
[+] nethunter kex passwd     # To set the KeX password
[+] nethunter kex &         # To start NetHunter GUI
[+] nethunter kex stop      # To stop NetHunter GUI
[+] nethunter -r            # To run NetHunter as root
[+] nh                      # Shortcut for nethunter
```

11th One of the problems is that DNS servers are not configured by default, so we'll have to escalate to superuser with "`sudo su`" (the default password is kali) (sometimes it hangs so we'll do "`CTRL + C`" (if it appears as localhost# type "`bash`"))).

12th Now as root, type "`nano /etc/resolv.conf`".

13th In this file change the nameserver to 8.8.8.8, which are Google's servers. To exit nano: "`CTRL + O`" and "`CTRL + X`".

14th "`Apt update`".

▼ GUI Installation

1st In the **Termux** terminal type "`nethunter kex passwd`".

2nd Enter the password you want to use for your **KEX**, say no after entering the password.

3rd In the **Termux** terminal type "nethunter kex &", this is to activate the GUI. Next you'll see some port numbers, copy the **RFB Port**.

4th Now go to **F-Droid** and install **NetHunter KeX**.

5th Inside **NetHunter KeX** you'll see a section that says VNC Connection Settings, next to localhost there's a space where we'll put the **RFB Port** numbers, leave the one below blank (optional), and in the last one enter the password created in step **2nd**.

▼ Starting from scratch

1st Go to **Termux** and type "nh" or "nh -r (to be root)".

2nd Inside the kali terminal type "kex" (if you start with "nh" or "nh -r", they have different **RFB Ports**).

3rd Go to **NetHunter KeX** and enter.

▼ Troubleshooting (Phantom Process Killer)

If we're with our kali open for a while and it closes, it's because of: **DISABLE PHANTOM PROCESS KILLER In Android 12 & 13**

▼ What exactly are **phantom process killers**?

It's a background process limiter that kills the app processes using excessive CPU or system resources. Let's say the parent app started spawning a child processes of more than 32, if they are found to be using an excessive CPU, the phantom process killer kicks in and kills the entire app Hierarchy. This happens without the consent of the user and the app gets killed automatically and creating a problem for the end-user experience.

The **phantom process killers** are going to be killing our **Termux** over and over, so it's necessary to remove them from our phone.

- Windows (From linux it's tricky, I couldn't find info):

1st To start we need Adb & Fastboot Commands on our windows → **Hello!**

2nd Connect the phone to the PC. Remember to activate debugging from the administrator settings (to activate these settings, tap 7 times on the android version).

3rd Open the terminal and type "adb devices" if a number appears, we can do it.

4th Commands:

```
adb shell "/system/bin/device_config set_sync_disabled_for_tests  
persistent"
```

```
adb shell "/system/bin/device_config put activity_manager  
max_phantom_processes 2147483647"
```

```
adb shell settings put global settings_enable_monitor_phantom_procs false
```

5th More commands to disable **phantom process killers**:

```
adb shell "/system/bin/dumpsys activity settings | grep  
max_phantom_processes"
```

```
adb shell "/system/bin/device_config get activity_manager  
max_phantom_processes"
```

6th The result returned from these commands should be "2147483647".

▼ Troubleshooting (Firefox tab crashes)

FIREFOX TAB CRASH ON KALI LINUX

1st Go to **Firefox**.

2nd In the search bar type "about:config" and accept.

3rd Search for "sandbox".

4th In this section, in media.cubeb.sandbox change it to false.

5th In the same section, in security.sandbox.content.level change the 4 to 0.

6th Close firefox and open it again.

▼ Troubleshooting (Sound doesn't work)

1st In the **Termux** terminal, type "pkg update".

2nd Install PulseAudio, "pkg install pulseaudio".

3rd "nano \$PREFIX/etc/pulse/default.pa".

4th Inside, find "#load-module module-native-protocol-tcp" and remove the # to uncomment it, then add "auth-ip-acl=127.0.0.1 auth-anonymous=1" after it.

It should look like: "load-module module-native-protocol-tcp auth-ip-acl=127.0.0.1 auth-anonymous=1".

5th "nano \$PREFIX/etc/pulse/daemon.conf".

6th Inside, find "; exit-idle-time = 20" change the 20 to -1. Save and exit.

7th Where we are, do "nano sound".

8th Write inside: "pulseaudio --start --load="module-native-protocol-tcp auth-ip-acl=127.0.0.1 auth-anonymous=1" --exit-idle-time=-1" save and exit.

9th For the sound file do "chmod +x sound".

10th Create a new session in **Termux**.

11th In one, start nethunter with "nh".

12th In the other type "./sound".

13th Go back to the first one and type "export PULSE_SERVER=127.0.0.1".

14th Start the GUI with the command "kex" inside the kali terminal.

15th Search for Volume Control and activate the sound.