Kali Nethunter

Brayden Houston

```
$ whoami
Name: Brayden
Interests: homelab, automation, devops
Shameless Plugs: DC608, Wisconsin CRT, ISP Ward
Additional Info: Thoughts are my own and not my employeers
$
```

Quick Reminder From Safety Dwight

What is Kali Nethunter?

Its Kali but on your phone

Why Nethunter?

- Turn you phone into a sick cyberdeck(phone?)

- Plug in usb devices for more options

- Phones are everywhere and who would expect a phone to be a security risk-it looks nothing like a Raspberry Pi or Flipper Zero 🐬

What can we do?

- Bad USB
- Wigle/Kismet Wifi Collection
- BT Attacks
- Wifi Scans, Deauth
- CAN Arsenal
- Way more

What do we need to get started?

- One or more supported tablet, phone, or watch (Sorry iOS 🥲)

- A few minutes or maybe an afternoon

- Decide which edition you want to try

Editions

Edition	Usage
NetHunter Lite	The full NetHunter package for rooted phones without a custom kernel.
NetHunter	The full NetHunter package with custom kernel for supported devices

Feature	NetHunter Lite	NetHunter
App Store	Yes	Yes
Kali cli	Yes	Yes
All Kali packages	Yes	Yes
KeX	Yes	Yes
Metasploit w/o DB	Yes	Yes
Metasploit with DB	Yes	Yes
NetHunter App	Yes	Yes
Requires TWRP	Yes	Yes
Requires Root	Yes	Yes

Couple Differences

Feature	NetHunter Lite	NetHunter
WiFi Injection	No	Yes
HID attacks	No	Yes
BT Arsenal	No	Yes
CAN Arsenal	No	Yes

Full and Lite versions probably aren't daily driver phone material

Install Nethunter

https://www.kali.org/get-kali/#kali-mobile

Phone Options

Nethunter "Pro"

- Pinephone and PinePhonePro

- Some Android Phones

Nethunter
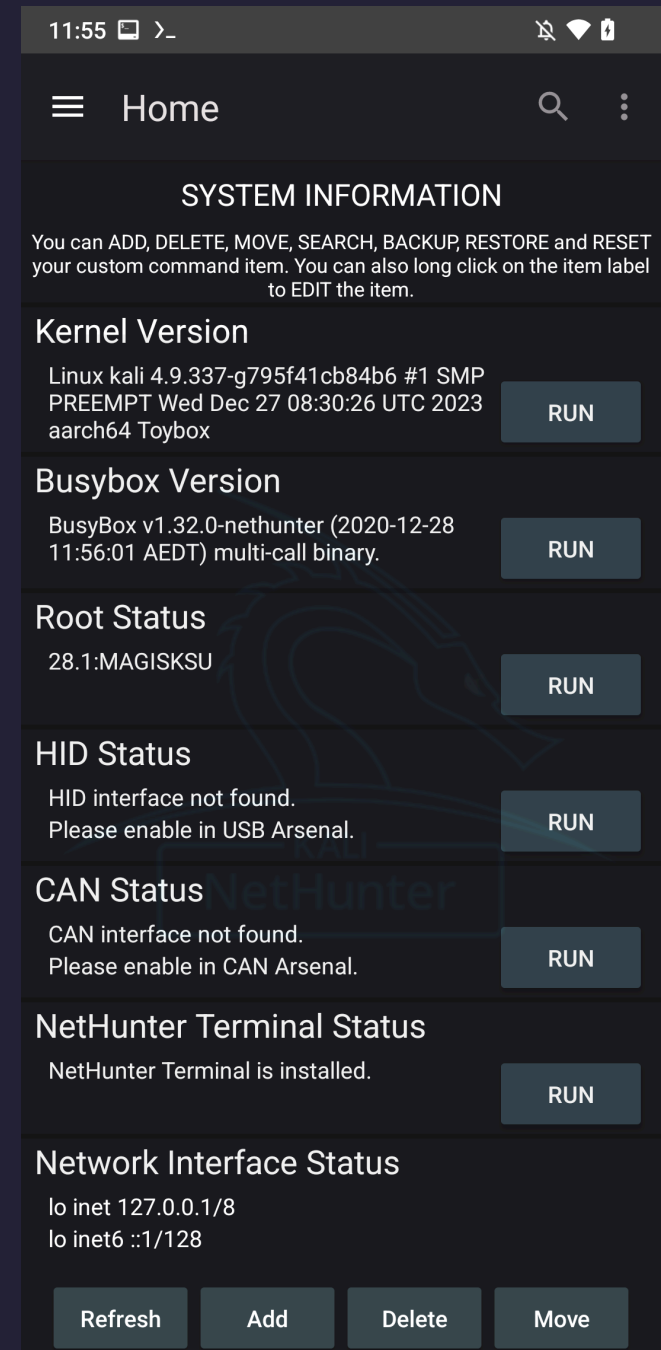
- Most Android Phones

I tried them both

Android Impressions

Still rocking a OnePlus6 as my Nethunter device

One of the "Pro" compatible devices

Having root access lets us do fun things like re-purposing the alert slider

Still use Android apps. Sideload Gapps if you need them

PinePhone Impressions

Kinda like having a Raspberry Pi in your pocket-for better or worse.

The functionality is all there but the Posh Mobile interface isn't my favorite

The beta/developer hardware probably isn't doing the vision for the experience justice

Shout outs to the Pine64 IRC/Discord!

If you run Posh, switch off the default keyboard and thank me later

```
sudo apt install squeekboard
sudo apt remove phosh-osk-stub
sudo init 6
```

Is Rootless An Option?

Yes

NetHunter Rootless	The core of NetHunter for unrooted, unmodified devices

Feature	NetHunter Rootless
App Store	Yes
Kali cli	Yes
All Kali packages	Yes
KeX	Yes
Metasploit w/o DB	Yes

One more thing

New Android Terminal

- Currently Pixel only

- A full Debian VM

- Still some (Android) system and hardware restrictions

- Still under development by Google

- Currently a 16gb max file system

- Yes it runs Doom

Q & A

Slides

If you want to see the devices hands on come to the ISP Village.

Reach out and show me what you do with Nethunter!

I'll push the slides here after the talk:
https://github.com/braydenhouston/CC-KaliNethunter

Helpful Resources

https://forums.kali.org/

Pine64 - Discord and IRC channels

@davidbombale

https://justhack.in/connect-to-kali-nethunter-vnc-server-from-local-network