Kali Nethunter (sin root) by F12-Lab

▼ Installation

1º Buscamos en internet ***Termux***, no seleccionamos el primero sino el que ponga ***F-Droid***. Descargamos ***F-Droid***, buscamos en este ***Termux*** (Emulador de terminal con paquetes), y lo instalamos (nos dirá que es un virus pero ignoramos).

2º Abrimos ***Termux***, hacemos "pkg update" (aceptamos todo).

3º Habilitamos el acceso de ***Termux*** al almacenamiento del teléfono, con "termux-setup-storage", aceptamos.

4º Instalamos wget, con "pkg install wget".

5º Instalamos el paquete donde viene nethunter "wget https://gitlab.com/kalilinux/nethunter/build-scripts/kali-nethunter project/raw/master/nethunter-rootless/install-nethunter-termux".

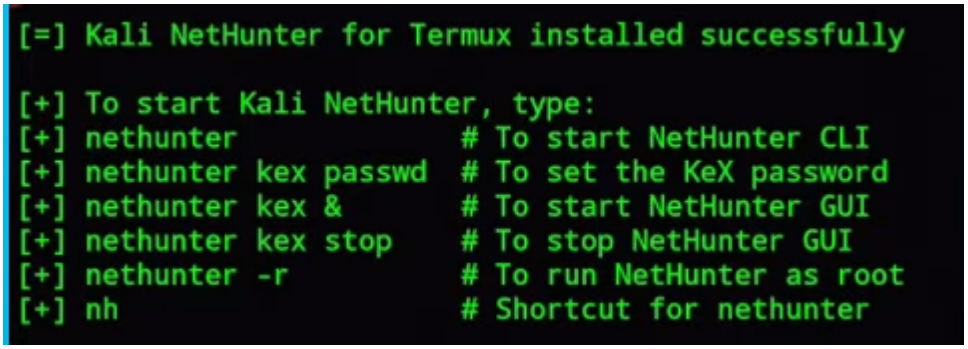
6º Hacemos un "ls" y veremos que nos saldrá install-nethunter-termux en blanco, por lo que le damos permisos con "chmod +x install-nethunter-termux". Volvemos hacer "ls" y ahora nos aparecerá en verde.

7º Hacemos la instalación poniendo "./install-nethunter-termux".

8º Se nos abrirá una ventana, le damos al 1 (opción más completa) (Este proceso tarda bastante, sobre todo rootfs).

9º Cuando se haya ejecutado, es recomendable darle a no, así liberaremos espacio que han consumido los rootfs.

10º Ahora podremos ver las diversas opciones para encender nuestro kali. Cuando iniciemos ***Termux*** tendremos que poner "nh" o "nh -r" para acceder a kali.



11º Uno de los problemas es que los servidores DNS no están configurados por defecto, por lo que tendremos que escalar a superusuario con "sudo su" (la contraseña por defecto es kali) (a veces se queda colgado por lo que haremos "CRTL + C" (si nos sale como localhost# ponemos "bash")).

12º Ahora como root, ponemos "nano /etc/resolv.conf".

13º En este archivo cambiamos el nameserver por 8.8.8.8, que son los servidores de google. Para salir de nano: "CTRL + O" "y" "CTRL + X".

14º "Apt update".

▼ Instalación del GUI

1º En la terminal de ***Termux*** ponemos "nethunter kex passwd".

2º Ponemos la contraseña que queremos usar para nuestro ***KEX***, le decimos que no después de introducir la contraseña.

3º En la terminal de ***Termux*** ponemos "nethunter kex &", esto sirve para activar el GUI. A continuación veremos unos números de puertos, copiamos el RFB Port.

4º Ahora nos vamos a ***F-Droid*** y nos instalamos ***NetHunter KeX***.

5º Dentro de ***NetHunter KeX*** veremos un apartado que pone VNC Connection Settings, al lado de localhost hay un espacio donde pondremos

los números del RFB Port, debajo dejamos en blanco (opcional), y en el último metemos la contraseña creada en el punto 2º.

▼ Iniciar desde cero

1º Nos vamos a ***Termux*** y ponemos "nh" o "nh -r (para ser root)".

2º Dentro de la terminal de kali ponemos "kex" (si inicias con "nh" o "nh -r", tienen RFB Port distintos).

3º Nos vamos a ***NetHunter KeX*** y nos metemos.

▼ Solución de problemas (Phantom Process Killer)

Si estamos un ratillo con nuestro kali abierto y este se cierra es por:
DISABLE PHANTOM PROCESS KILLER In Android 12 & 13

▼ ¿Qué son los ***phantom process killer*** exactamente?

> 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.

Los ***phantom process killer*** son los que van a estar asesinando una y otra vez nuestro ***Termux***, por lo que es necesario quitarlos de nuestro móvil.

- Windows (Desde linux está díficil, no encontré info):

1º Para empezar necesitamos Adb & Fastboot Commands en nuestro windows → **Hola!**

2º Conectamos el móvil al pc. Recordad que hay que activar el debugging desde los ajustes del administrador (para activar estos ajustes, dar 7 veces en la versión de android).

3º Abrimos la terminal y ponemos "adb devices" si nos aparece un número, es que podemos realizarlo.

4º Comandos:

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

5º Más comandos para deshabilitar los ***phantom process killer***:

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

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

6º El resultado devuelto de estos comandos debe ser *"2147483647"*.

▼ Solución de problemas (Firefox tab se crashea)

FIREFOX TAB CRASH ON KALI LINUX

1º Nos metemos a Firefox.

2º En el buscador ponemos "about:config" y aceptamos.

3º Buscamos "sandbox".

4º En este apartado, en media.cubeb.sandbox lo cambiamos a false.

5º En el mismo apartado, en security.sandbox.content.level el 4 lo cambiamos a 0.

6º Cerrar firefox y abrirlo.

▼ Solución de problemas (El sonido no va)

1º En la terminal de ***Termux***, ponemos "pkg update".

2º Instalamos PulseAudio, "pkg install pulseaudio".

3º "nano $PREFIX/etc/pulse/default.pa".

4º Dentro buscamos "#load-module module-native-protocol-tcp" y le quitamos el # para que deje de estar comentado, a continuación de esto ponemos "auth-ip-acl=127.0.0.1 auth-anonymous=1".

Nos quedaría: "load-module module-native-protocol-tcp auth-ip-acl=127.0.0.1 auth-anonymous=1".

5º "nano $PREFIX/etc/pulse/daemon.conf".

6º Dentro buscamos "; exit-idle-time = 20" cambiamos el 20 por un -1. Guardamos y nos salimos.

7º Donde estamos hacemos "nano sound".

8º Escribimos dentro: "pulseaudio --start --load="module-native-protocol-tcp auth-ip-acl=127.0.0.1 auth-anonymous=1" --exit-idle-time=-1" guardamos y salimos.

9º Al archivo sound le hacemos "chmod +x sound".

10º Creamos una nueva sesión en ***Termux***.

11º En una iniciamos nethunter con "nh".

12º En la otra ponemos "./sound".

13º Volvemos a la primera y ponemos "export PULSE_SERVER=127.0.0.1".

14º Iniciamos el GUI con el comando "kex" dentro de la terminal de kali.

15º Buscamos Volume Control y activamos el sonido.