前言

写这篇有几个原因。第一是工作室的peer有好几个都问过我：安卓手机怎么root啊？怎么解锁那个bl啊？以这次对战诺基亚工程机为契机正好也写一下比较旧的手机怎么root。第二是网络上绝大多数有关Kali Nethunter的刷写教程都是过时的，而其实Kali官网支持的nethunter内核机型本身是在不断更新的，所以也算是给其它有兴趣玩玩Nethunter的同伴铺路，少踩点雷。~~第三是为了水笔记和水数码论坛的经验（这真的可以说吗）~~

准备工作

1.一台支持Kali Nethunter官方镜像的手机，该教程的第一版使用诺基亚3.1工程机版本，型号TA-1070。~~其实本来是想用一加初代来做的，一加的BL锁很好解，同时骁龙801的性能也比430好不少，可惜它被关在学校的驿站里了。。。开学会更新的~~

*如何查看我的手机是否支持Nethunter官方镜像？：https://www.kali.org/get-kali/#kali-mobile

这里需要注意，Nethunter Lite可以被认为是一个运行在Android Runtime上的linux虚拟机（有点类似于Docker），Nethunter Lite由于系统未root是无法使用需要调用安卓系统的攻击方式的，比如HID ATTACKS，蓝牙/Wifi攻击。

*如果我的手机不支持Nethunter镜像怎么办？：可以自己编译。Kali官方开源了编译工具，经过自己的测试该编译工具实际使用起来非常简单（跟着python脚本一步一步来就行）但是编译出来的内核一般会有很多bug要自己排查。教程：https://droidkali.github.io/2021/09/12/build-nethunter-kernel.html

2.一条接触良好的USB线 （对于比较旧的手机可以准备一条9008工程线，便于手机开机引导崩溃时快速恢复）

3.一套螺丝刀，拆机片（当手机卡开机logo无限重启时可拆卸后盖和主板盖板断开电池排线）

流程

解锁Bootloader

诺基亚3.1解锁需要购买解锁码和提权资格。详细流程：https://hikaricalyx.com/2018/05/28/how-to-unlock-qualcomm-based-nokia-android-devices/

一加手机解锁：（待更新）

小米手机解锁：

1.官网下载小米解锁工具：MiFlash_Unlock

2.进入软件，登录小米账号，系统会自动检测帐号是否有解锁手机的资格

3.手机进入Fastboot模式并连接电脑，点击解锁/新买的手机可能有360H或168H解锁限制，需要等待时间清零后方可解锁。

*手机进入Fastboot有两种方式，第一为关机后长按音量下键和电源键知道出现Fastboot类似字样（不同手机可能按键组合不同）；第二为手机打开开发者模式后允许USB调试，连接电脑后使用谷歌官方Platform_tools或第三方开发者的安卓工具箱进入fastboot模式（代码为Adb reboot fastboot）

ADB代码查询：https://quickref.cn/docs/adb.html

刷入合适的系统版本固件

低于安卓9

将链接内提供的安卓9固件直接拷贝入手机根目录，不要改名，在拨号盘内输入* # * # 784 # * # *进入诺基亚升级程序即可自动升级。

高于安卓9

这时需要使用OST LA工具。该工具为售后专用的诺基亚手机系统烧录工具，已破除帐号服务器验证。

进入工具后选定nb0格式的文件，并将手机关机后/Fastboot连接电脑，工具识别后会自行进入Download Mode进行刷写。刷写过程中不可以断开数据线连接。

OST LA教程：https://tieba.baidu.com/p/5349044803

刷入Kali相关固件

这里所有的命令推荐手搓，因为安卓9采用AB分区（非动态），如果将boot刷入当前不活跃的分区会导致开机引导崩溃。

1.手机进入fastboot模式，首先刷入twrp。（请将twrp文件放在桌面）

请务必注意目前手机系统所在的分区，在AB分区的手机中更新系统会切换活跃分区。

查看活跃分区指令：**fastboot getvar current-slot**

修改活跃分区（一般修改到a插槽，如果已经是a可以不管）:**fastboot --set-active=a**

```
C:\Users\XeV1sKyl3R`\Desktop>fastboot --set-active=other reboot
Setting current slot to 'a'                        OKAY [  0.010s]
Rebooting                                          OKAY [  0.158s]
Finished. Total time: 0.171s
```

图片中的代码也是可行的。

切换到A分区之后刷入twrp，指令：**fastboot flash boot_a twrp.img**

（文件名取决于实际文件名）

若无自动重启，则输入**fastboot reboot**。当手机振动时同时按住音量上和电源键，出现android logo时松开电源键，出现twrp logo时松开音量上键。

为了防止重启掉twrp，可以adb push twrp.img在twrp内部重新刷入一次固化。

2.解锁data分区

这个时候data分区是被锁定的，所以twrp无法挂载。先在twrp中清除data分区，然后adb push解密包进行data分区解密：

adb push DisableForceEncryption_Treble.zip /sdcard/

twrp install zip /sdcard/DisableForceEncryption_Treble.zip（也可以直接点击安装）

安装完成后重启到系统，走完系统设置，打开USB调试后重新启动到recovery（twrp）

3.安装剩余组件

原作者专门写了两个sh文件用来刷入firmware和开机动画，其实push之后直接点击安装也可以。

指令：

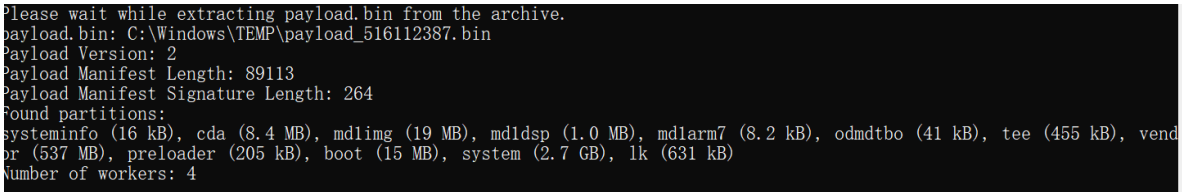
adb push <DOWNLOADED_FILES_PATH>/* /sdcard/

```
adb shell
cd /sdcard/
sh bootanimation.sh
sh firmware.sh
reboot
/////
twrp install zip /sdcard/nethunter-2020.3-es2-pie-kalifs-minimal.zip
twrp install zip /sdcard/Magisk-v24.3.zip
//////这两步也可以直接点击安装
```

注意事项

手机boot崩溃怎么办

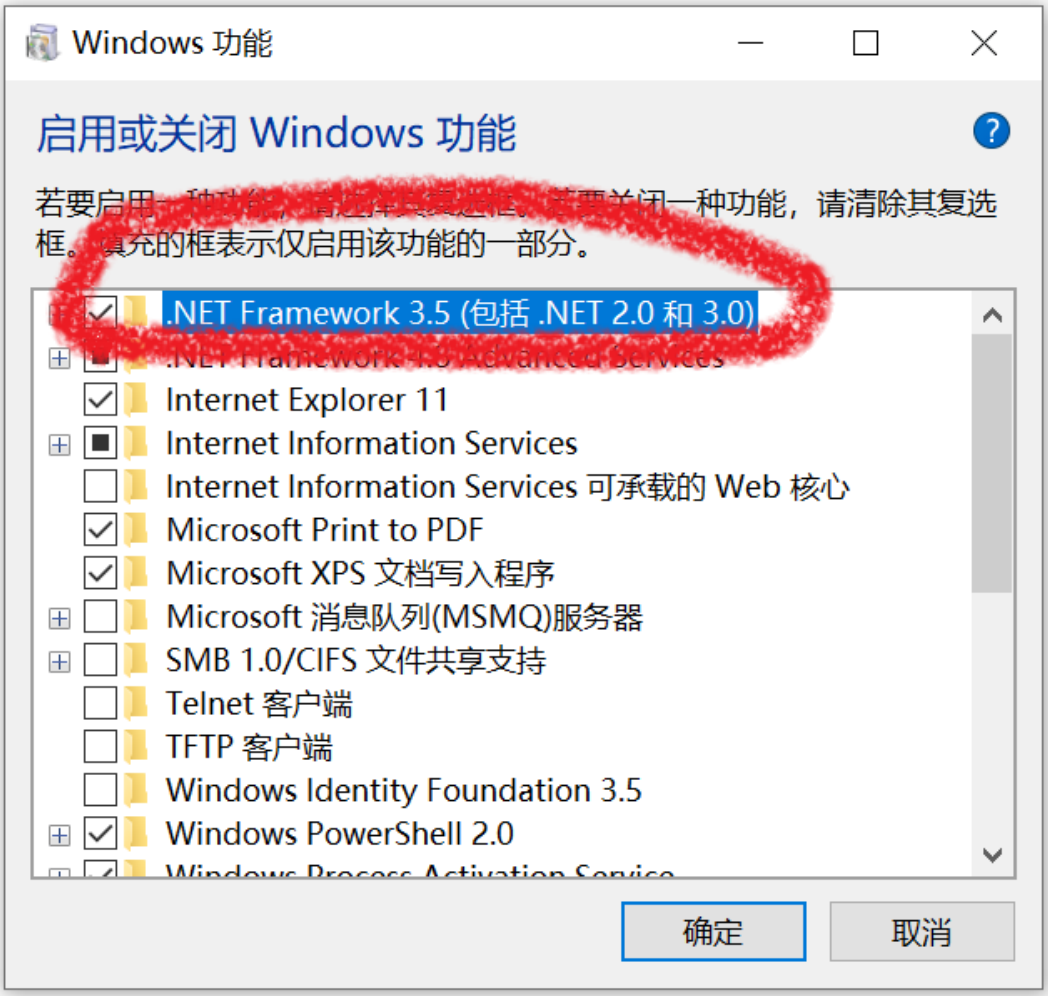
百度搜索Payload dumper.下载好之后将手机所对应的系统包拖拽进入Payload dumper之后解包boot.img;fastboot flash boot_a/b boot.img刷入后即可开机。



OST LA无法启动怎么办

这是由于OST LA软件年代较为久远，需要.NET FRAMEWORK 3.5运行环境（现在基本为.NET FRAMEWORK 4.0)微软自己的Cleanup Tool必须先清理高版本framework才能下载低版本，故不采用。解决方法如下：

控制面板>>程序>>启用或关闭Windows功能



勾选后确定，给予管理员权限，windows会自行完成安装。

补充：Oneplus 2安装Kali Nethunter

解除BL锁；刷入lineageOS16.0底包；通过TWRP刷入Nethunter完整包，结束。